The Design of Multimodal biometric systems & Mechanism using User's Biometrics Signals

Darshan Charan Nayak
Indira Institute of Management-Pune,
89/2-A, New Pune Mumbai Highway, Tathwade,Pune-411033, India
darshan.nayak@indiraiimp.edu.in

Abstract--In this study the effect of various image-processing techniques such on the detail visibility of core images are investigated. Identification In this research, we proposed robust authentication mechanism using user's biometrics signals for complementing traditional authentication's weak points. Nowadays, authentication system are developed using biometric. Biometrics are a unique, measurable a trait of a human being for verifying his/her identity. The types of biometric used in authentication system are iris, fingerprint, vein pattern, hand geometry etc. A biometric system provides an automated method of identifying a human being based on his/her biometric characteristics. But there are some security problems. Some biometrics can be copied by a malicious user with scanners. All biometrics characteristics extracted from a user are not possible to maintain a steady normal condition. So, we tried to apply user's biometrics signals to authentication system as 3rd authentication factor. A biometrics signal is a pattern recognition that uniquely identifies human being based on his/her physiological traits. A biometrics signals should be impossible to masquerade or manipulate. The proposed method, technique used will give good result and better performance and used robust preprocessing methods are used to reduce the enhancement errors and will improve the quality of images.

Keywords-- Enroll user recognition, Authentication, Biometrics Signal & Biometrics Security

1. INTRODUCTION

Biometric have been used for over a century and are the most widely used form of Fingerprints identification. . Authentication mechanism also prevents forgery and unauthorized access as well as identity check. Authentication is generally performed by three ways such as 'something the user knows', 'something the user has', and 'something the user is'. The first way is to authenticate the user by the information that the user knows like password. The second way is to authenticate the user by tools that the user has like smartcard, Fingerprint identification is commonly employed in Forensic science to support criminal investigations, and in biometric systems such as civilian and commercial identification devices. Despite this widespread use of fingerprints, there has been little statistical work done on the uniqueness of fingerprint minutiae. In particular, the issue of how many minutiae points should be used for matching a fingerprint is unresolved.

An authentication means to authenticate the user him/herself attempting to access the system after identifying user. Authentication is the first step of security requirement for any information communication environment to validate the user.The fingerprint of an individual is unique and remains unchanged over a lifetime. A fingerprint is formed from an impression of the pattern of ridges on a finger. A ridge is defined as a single curved segment, and a valley is the region between two adjacent ridges. The minutiae, which are the local discontinuities in the ridge flow pattern, provide the features that are used for identification. Details such as the type, orientation, and location of minutiae are taken into account when performing minutiae extraction defined a set of features for fingerprint identification, which since then, has been refined to include additional types of fingerprint features. However, most of these features are not commonly used in fingerprint identification systems. Instead the set of minutiae types are restricted into only two types, ridge endings and bifurcations, as other types of minutiae can be expressed in terms of these two feature types. Ridge endings are the points where the ridge curve terminates, and bifurcations are where a ridge splits from a single path to two paths at a Y-junction.

Various authentication systems have been used in internet banking, access control system, credit card, and system security field. But password authentication is vulnerable to password hacking tools such as dictionary attack and brute-force attack. An authentication system using passwords can be replaced and/or intensified by accredited certificate, smartcard and any one of the biometrics. Smartcard also proved to be vulnerable to attack impersonation attack. Nowadays, authentication systems provide double authentication with password and smartcard or biometrics. Especially, biometrics provides a more reliability than other traditional authentication components. Fingerprint images are rarely of perfect quality. They may be degraded and corrupted with elements of noise due to many factors including variations in skin and impression conditions. This degradation can result in a significant number of spurious minutiae being created and genuine minutiae being ignored. A critical step in studying the statistics of fingerprint minutiae is to reliably extract minutiae from fingerprint images. Thus, it is necessary to employ image enhancement techniques prior to minutiae extraction to obtain a more reliable estimate of minutiae locations. The primary aim of this project is to implement a series of techniques for fingerprint image enhancement and minutiae extraction. Experiments using both synthetic test images and real fingerprint images are used to assess the performance of the implemented techniques. These techniques are then used to extract minutiae from a sample set of fingerprint images. By using the extracted minutiae data, preliminary experiments on the statistics of fingerprints can then be conducted. This dissertation is organized into three main topics, with each chapter focusing on a different topic.

Biometrics is widely used at various security fields. For example, fingerprint scanners have already used in smartphone and recognition sensors installed in automobiles. Nevertheless, biometrics has some limitations to be used alone because the fingerprint is often affected by handwork environment, and the voice is affected by flu or throat infection. So, complementary authentication factor is necessary to overcome these weak points. Recently, we are actively researching biometrics signals to apply to security system. Biometrics signals refer a pattern recognition technology that is uniquely the automated identification of human being based on his/her physiological attributes. We added biometrics signal to authentication mechanism for reinforcing reliability. Fingerprints are the oldest and most widely used form of biometric identification. Despite the widespread use of fingerprints, there is little statistical theory on the uniqueness of fingerprint minutiae. A critical step in studying the statistics of fingerprint minutiae is to reliably extract minutiae from the fingerprint images. However, fingerprint images are rarely of perfect quality. They may be degraded and corrupted due to variations in skin and impression conditions. Thus, image Enhancement techniques are employed prior to minutiae extraction to obtain a more reliable estimation of minutiae locations, this dissertation, firstly provide discussion on the methodology and implementation of techniques for fingerprint image enhancement and minutiae extraction. Experiments using a mixture of both synthetic test images and real fingerprint images are then conducted to evaluate the performance of the implemented techniques. In combination with these techniques, preliminary results on the statistics of fingerprint images are then presented and discussed.

The first step of the fingerprint enhancement algorithm is image segmentation. Segmentation is the process of separating the foreground regions in the image from the background regions. The foreground regions correspond to the clear fingerprint area containing the ridges and valleys, which is the area of interest. The background corresponds to the regions outside the borders of the fingerprint area, which do not contain any valid fingerprint information. When minutiae extraction algorithms are applied to the background regions of an image, it results in the extraction of noisy and false minutiae. Thus, segmentation is employed to discard these background regions, which facilitates the reliable extraction of minutiae.

Computational techniques involving contrast enhancement and noise filtering on two-dimensional image arrays are developed based on their local mean and variance. These algorithms are no recursive and do not require the use of any kind of transform. They share the same characteristics in that each pixel is processed independently. Consequently, this approach has an obvious advantage when used in real-time digital image processing applications and where a parallel processor can be used. For both the additive and multiplicative cases, the a priori mean and variance of each pixel is derived from its local mean and variance. Then, the minimum mean-square error estimator in its simplest form is applied to obtain the noise filtering algorithms. For multiplicative noise a statistical optimal linear approximation is made. Experimental results show that such an assumption yields a very effective filtering algorithm. Examples on images containing 256 Ã— 256 pixels are given. Results show that in most cases the techniques developed readily adaptable to real-time image processing.

A method of improving the definition of a video picture by a computer program, which reduces the lowest grey values to black and the highest to white: used for pictures from micro2scopes, surveillance cameras, and scanners.

Image enhancement is the improvement of digital image quality (wanted e.g. for visual inspection or for machine analysis), without knowledge about the source of degradation. If the source of degradation is known, one calls the process image restoration. Both are iconical processes, viz. input and output is images.

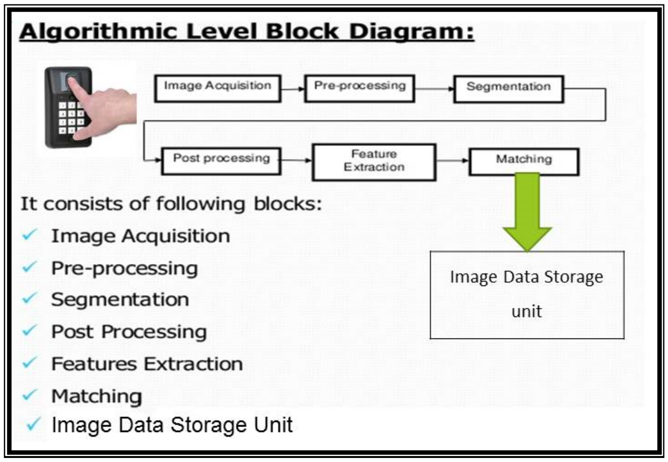
After registration on the microscope the digital images are loaded to image processing software for further processing. The data includes information about pseudo color, pixel dimensions, time scale etc.First image data get adjusted by background subtraction, contrast enhancement etc. Colors might be assigned; sub volumes selected; z-mismatches corrected by pixel-shifts. The software’s offer different options to look at the multidimensional data sets.i.e. slice viewer, gallery view, section view, projections, full 3D volume representations, surface models, time bar, color coded overlays of several channels, transparencies, ...The software offers analytical tools for measurement and quantification: automated counting of features, measurements of areas and volumes, tracing of filaments, measuring of distances, evaluation of co localization, ...

Apart from geometrical transformations some preliminary grey level adjustments may be indicated, to take into account imperfections in the acquisition system. This can be done pixel by pixel, calibrating with the output of an image with constant brightness. Frequently space-invariant grey value transformations are also done for contrast stretching, range compression, etc. The critical distribution is the relative frequency of each grey value, the grey value histogram.

Biometrics	Classification			
Physiological				
	Fingerprint	Face	Iris	Hand
Behavioral				
	Keystroke	Signature	Voice	Handwriting

In imaging science, image processing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it.

Image processing usually refers to digital image processing, but optical and analog image processing also are possible. This article is about general techniques that apply to all of them. The acquisition of images (producing the input image in the first place) is referred to as imaging.



Algorithmic Level Block Diagram:

It consists of following blocks:

- ✓ Image Acquisition
- ✓ Pre-processing
- ✓ Segmentation
- ✓ Post Processing
- ✓ Features Extraction
- ✓ Matching
- ✓ Image Data Storage Unit

Fig.1. The block diagram of the research platform for Image Processing, analysis & understanding

Image Processing (image in → image out)
Image Analysis (image in →measurements out)
Image Understanding (image in → high-level description out)

Biometrics characteristics are a unique, measurable physiological and/or behavioral trait of a human being for automatically recognizing or verifying his/her identity. All human have their own unique biometrics in the overall human body structure. As mentioned above, biometrics classifies physiological and behavioral factors. Typical physiological factors are fingerprint, hand, face, iris, etc. Behavioral factors include keystroke, signature, voice, handwriting, etc.

Fig.2. The Classification of Biometrics block diagram of the research platform

EXPERIMENTAL RESULTS

Biometrics is used to security system because it has inherent properties, universality, measurability, singularity and so on. Biometrics need not be remembered or had like passwords and smartcard. It is not easily lost or forged. And it should be collected in real time. So, biometrics based security system provides a more authentication reliability than traditional systems like passwords, smartcard, etc. Biometrics based security system provides verification of the user's identity by matching the measured biometrics attributes with his own biometric template stored in the database. It is essentially user characteristics recognition system that operates by extracting from physiological characteristics of a user into templates, and compares these templates set with the template set in the database. The collection sensor collects user's biometric characteristics using any sensors such as camera, fingerprint scanner, etc. The feature extractor processes extraction and encoding of specific characteristics from user's biometric characteristics to convert feature templates. In case of fingerprint, it extracts location and direction of the ridges and bifurcations from fingerprint image. And then new feature template is compared with stored templates in a database to determine the degree of similarity or correlation. If new feature template is matched with individual templates stored in a database, it permits access to resources. The biometric based security systems offer several advantages. It could be created specific personalized key for each user because biometrics is unique to each person. It also is needed not change authentication key periodically like password because biometrics characteristics are permanent and not changeable. It couldn't be transferred or spoofed their own biometrics characteristics to other users because biometrics characteristics are only measured in real time when user requests authentication to system. For these advantages, the biometrics is popularly used to security systems such as database security and access control in physical security like building, gate, and office. But, there is no a biometrics based security system adequate to all application because biometrics characteristics have some inherent vulnerabilities. For example, it is impossible that all biometrics characteristics extracted from a user always keep a normal condition. Because it is difficult to extract accurate templates if human eats the food before sleeping. It is still needed to improve accuracy to reduce false rejection rate. So, it is better to use with another authentication factor to improve security performance.

While there are many biometric systems in the market, the aim of biometric systems, image enhancement is to improve the interpretability or perception of information in images for human viewers, or to provide better input for other automated image processing techniques. The importance of high-fidelity enhancement in low quality fingerprint image cannot be overemphasized. Most of the existing fingerprint enhancement methods are contextual filter-based methods and they often suffer from two short comings: (1) there is block effect on the enhanced images; Authentication system aims to prevent forgery and unauthorized access as well as identity check. The common authentication approach is the use of passwords. But, as password has been used for a long time, it is possible to copy by malicious user. Smartcard appears to resolve security problem of password in a secondary authentication approach. This also proved to be vulnerable to attack impersonation attack [8, 9]. Recently, the biometrics based authentication techniques is popularly used in the security field. But this has risk that hacker can steal biometrics from user and manipulates biometrics templates in the database by hacking.

The problem of biometric sensor interoperability has received limited attention in the literature. Most biometric systems operate under the assumption that the data, images to be compared are obtained using the same sensor are restricted in their ability to match or compare biometric data originating from different sensors. Although progress has been made in the development of common data exchange formats to facilitate the exchange of feature sets between vendors, very little effort has been invested in the actual development of algorithms and techniques to match these feature sets. In the Fingerprint Verification Competition, for example, the evaluation protocol only matched images originating from the same sensor although fingerprint data from different commercial sensors was available. This is an indication of the difficulty in accommodating sensor interoperability in biometric systems discuss this problem and present a case study involving two different fingerprint sensors.

The purpose of various enhancement techniques for finger print images conducted three different types of experiments in order to study the effect of changing sensors on matching performance.

1. Matching images within the MSU DBI database.
2. Matching images within the MSU VERIDICOM database.
3. Matching images from MSU DBI against those from MSU VERIDICOM.

Enrollment:-Users are not required to carry any cards. On enrollment, a user places his or her finger on the scanner, which captures a fingerprint image. The image is sent to client Pc. If the image quality is acceptable, fingerprint minutiae information is extracted, and the image is then discarded. The minutiae information is sent via a secure line to the biometric server, usually located in a secure room. This information is stored in a database on the biometric server. The system may enroll one or up to all ten fingers. Modern one-to-many systems are capable of searching as many as 20,000 templates, even more at times, in real time, within a few seconds.

Identification:-To obtain access to a facility, the user places the appropriate finger on the sensor, and the captured fingerprint is sent to the client. The client extracts the minutiae information (with the fingerprint image subsequently discarded) and sends it to the biometric server. Here, the minutiae information is run in a one-to-many mode against the entire database of stored templates. If there is a match with one of the templates, the user is granted access. Alternatively, the system may go to the next level of authentication, for example: the corresponding photo of the user whose template has been matched is retrieved from the database and displayed to the operator. If the photo matches to the individual, the user is granted access.

3. SIGNIFICANCE OF THE STUDY

In some Canadian jurisdictions, personal information is defined as recorded information about an identifiable individual, other than contact information. Under that broad definition, any biometric information is personal information is considered personally identifiable if an individual may be uniquely identified either from this information only or in combination with any other information. If it is determined that the information is Personal information not just contact information, it will also be considered personal information by other Canadian jurisdictions.

There are two main groups of fingerprint algorithms: minutiae-based and non-minutiae, or pattern-based. The vast majority of systems use minutiae-based algorithms. However, this does not preclude the use of some non-minutiae information as an auxiliary means to improve system performance. In one-to-many matching applications, it is very likely that optional and/or extended data will be used, given the challenges of such an identification system. However, this research work will here make a conservative assumption that only the basic minutiae information is collected in a particular application. In other words, the fingerprint template stored contains at least the number of minutiae per finger, the minutiae positions x, positions y, and directions. This information is not a “meaningless number” but a biological characteristic of an individual’s finger and is, therefore, highly sensitive personal information. Unlike many other forms of personal information, this biometric information cannot be changed, cancelled, or revoked.

4. OBJECTIVES

Fingerprint image quality assessment is crucial for many fingerprint applications. It affects the performance and interoperability of fingerprint identification, authentication, and built on based crypto systems.

Finger-scan technology is the most widely deployed biometric technology, with a number of different vendors offering a wide range of solutions. Among the most remarkable strengths of fingerprint recognition, In this research work can mention the following:

- Its maturity, providing a high level of recognition accuracy.
- The growing market of low-cost small-size acquisition devices, allowing its use in a broad range of applications, e.g., electronic commerce, physical access, PC logon, etc.
- The use of easy-to-use, ergonomic devices, not requiring complex user-system interaction. On the other hand, a number of weaknesses may influence the effectiveness of fingerprint recognition in certain cases:
- Its association with forensic or criminal applications.
- Factors such as finger injuries or manual working can result in certain users being unable to use a fingerprint-based recognition system, either temporarily or permanently.
- Small-area sensors embedded in portable devices may result in less information available from a fingerprint and / or little overlap between different acquisitions.

After go through literature of fingerprint enhancement techniques this research came to think about objectives like:

1. To collect database from various level.
2. To study and compare existing enhancement techniques.
3. To know best suitable tech for fingerprint enhancement.
4. On the basis of performance evolution, this research set better tech for enhancement of fingerprint.

5. Motivating Factors Associated With Fingerprint Analysis:

In this research work investigated the emotional and motivational factors involved in fingerprint analysis in day-to-day routine case work and in significant and harrowing criminal investigations. Thematic analysis was performed on interviews with HR or Admin experienced fingerprint examiners from a variety of law enforcement agencies. The data revealed factors relating to job satisfaction and the use of skill. Individual satisfaction related to catching criminals was observed; this was most notable in solving high profile, serious, or long-running cases. There were positive emotional effects associated with matching fingerprints and apparent fear of making errors. Finally, in this research work found evidence for a need of cognitive closure in fingerprint examiner decision-making.

6. Conclusive Review Results and Future Work:-

In this paper, we designed 3-layered authentication mechanism using user's biometrics signals for complementing traditional authentication's weak points. Nowadays, authentication system are developed using biometric information. But there is also some security problem. Some biometrics is possible to copy by a malicious user with scanners. It is also impossible that all biometrics characteristics extracted from a user always keep a normal condition.

Cyber We proposed to apply biometrics signals to 3rd layered defense for improving authentication reliability. Biometrics signal is a natural, unique feature and an important physiological characteristic in the human body. It is difficult to copy or imitate because it can collect from only inside of human body in real time. The key of the 3-layered authentication mechanism is to request authentication factor to user based on biometrics signals.

But we have to solve the problem with the collection sensor for the biometrics signals collection and the absence of the definition method of accurate normal biometrics signal templates. Review of literature on fingerprint image enhancement put forward attention that there are researches available in spatial domain filtering but very few research work found using filter in frequency domain. Also very few work could be found taking ridge frequency enhancement in review literature process. Though ridge orientation and ridge detection, on single pixel found very well in spatial domain filtering. There are few research work reviewed based on fuzzy concept and filter. In our proposed future work ridge detection and ridge frequency enhancement, both is considered, it is reason two distinct filters one for ridge detection and another for ridge frequency are proposed to be designed

Although biometric technologies present a number of benefits, ranging from stronger user authentication, greater convenience for a majority of users, to improved security and operational efficiencies, they also present a number of risks to informational privacy. Any perceived or real threat to privacy could result in a serious loss of public faith and support. Consequently, organizations must carefully assess, prior to deployment, whether their needs can be met using alternative non-biometric means, and whether the privacy risks are outweighed by the necessity of installing a biometric system.

Image quality is related directly to the ultimate performance of automatic fingerprint authentication systems. Good quality fingerprint images need only minor preprocessing and enhancement for accurate feature detection algorithm. This paper reviewed a large number of techniques described in the literature to extract minutiae from fingerprint images. The approaches are distinguished on the basis of several factors like: the kind of input images they handle i.e. whether binary or gray scale, techniques of binarization and segmentation involved, whether thinning is required or not and the amount of effort required in the post processing stage, if exists. But low quality fingerprint images need preprocessing to increase contrast, and reduce different types of noises as noisy pixels also generate a lot of spurious minutiae as they also get enhanced during the preprocessing steps. Further, more emphasis is to be laid on defining the local criteria, in order to establish the validity of a minutia point, which is particularly useful during fingerprint matching and adopting more sophisticated identification models, for instance extending minutiae definition by including trifurcations, islands, bridges, spurs etc. Also, the paper leads to the further study of the statistical theory of fingerprint minutiae. In particular approaches can be investigated to determine the number of degrees of freedom within a fingerprint population which will give a sound understanding of the statistical uniqueness of fingerprint minutiae.

The performance of a fingerprint feature extraction and matching algorithms heavily depends upon the quality of the input fingerprint image. Various enhancement approaches such as Histogram equalization, have shown to improve the fingerprint image quality and recognition performance in different studies. Gabor filters have both frequency-selective and orientation-selective properties. It is observed that Gabor filter method of fingerprint image enhancement is giving better results. Minutiae extraction algorithm can detect all the minutiae, including both true and false minutiae, using the Rutovitz Crossing Number (CN) on the skeleton images after thinning stage. In literature review it is found that there are few Fingerprint Image Enhancement research work, which has been done, is based on ridge direction but if the image enhancement done based on ridge frequency along with ridge direction, image would be very quite clear. Selecting such image features i.e. Frequencies and directions which minimize energy function based on energy minimization principle, a very good enhanced image can be produced. Both the features of the images are required to be enhanced, so two distinct filters in Fourier domain, one for enhancing ridge frequencies and other for ridge directions, have to be designed. Images that occur in practical applications invariably suffer from random degradations that are collectively referred to as noise. If a large enough number of frames are averaged together, then the resulting image should be nearly noise-free, and hence should approximate the original image. In our job we get acceptable testing and experimentations based on Matlab filtering in progress of petroleum core image analysis. Generated Mfiles shows the varying gray scale intensity and its effect on the dynamic structure of the core image.

7. ACKNOWLEDGEMENT

I wish to express my sincere thanks to our – IT &Computer

Science department, for providing me with all the necessary facilities for the research also wish to express mysincere thank you to my guide Dr. Sagar Shyamsundar Jambhorkar's continuous encouragement. I am extremely thankful to him for sharing his experience. I take the opportunity to express gratitude to the entire department

Faculty & staff members for their support. I also thank my department & my director for encouraging me.

8. REFERENCES:

The Researcher has gone through Ebesco Database, J-Gate and Proquest Database and found some relevant articles and research papers related to the topic under study. The researcher also went through research report available in online Research and Development Center. A brief literature review is given below:

1. P. Tuyls, B. Škorić, and T. Kevenaar, eds. Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting. Springer-Verlag, London, 2007.
2. R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, Fingerprint Image Reconstruction from Standard Templates. IEEE Transactions On Pattern Analysis And Machine Intelligence, v. 29, No. 9, pp. 1489 - 1503, 2007. http://www.bromba.com/faq/biofaqe.htm
3. W. M. Grossman. Is school fingerprinting out of bounds? The Guardian,March 30,2006.http://www.guardian.co.uk/technology/2006/mar/30/schools.guardianweeklytechnologysection
4. N. Rosenkrans. Meal ID system gets personal. Winona Daily News, April 17, 2008.http://www.winonadailynews.com/articles/2008/04/17/news/00lead
5. D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. Handbook of Fingerprint Recognition. Springer, New York, 2003.
6. R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A.W. Senior. Guide to Biometrics. Springer, 2003.
7. S. Pankanti, S. Prabhakar, and A. Jain, On the individuality of fingerprints. IEEE Transactions on Pattern Analysis And Machine Intelligence, v. 24 , No. 8, pp. 1010-1025, 2002.
8. N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, v. 40, No. 3, pp. 614–634, 2001.
9. Y. Zhu, S. C. Dass, and A. K. Jain, Statistical Models for Assessing the Individuality of Fingerprints. IEEE Transactions on Information

Forensics and Security, v. 2, No. 3 (Part 1), pp. 391-401, Sept. 2007.also http://www.cse.msu.edu/cgi-user/web/tech/reports?Year=2006.

10. SO/IEC 19794-2:2005, Information Technology—Biometric Data Interchange Formats—Part 2: Finger Minutiae Data, 2005.

11. MINEX'04. Performance and Interoperability of the INCITS 378 Fingerprint Template. NISTIR 7296, National Institute of Standards and Technology, March 21, 2006. http://fingerprint.nist.gov/minex04/minex_report.pdf

12. A variety of procedures for change detection based on comparison of multi temporal digital remote sensing data have been developed. An evaluation of results indicates that various procedures of change detection produce different maps of change even in the same environment.

13. Biometric Systems: Technology, Design and Performance Evaluation. by J. Wayman, A. Jain, D. Maltoni, and D. Maio, Eds. Springer, 2004.

14. William K. Pratt, United States. Advanced Research Projects Agency, University of Southern California. Image Processing Institute University of Southern California, University Park, 1973 and the University of Wisconsin - MadisonVolume 453 of USCEE report

15. Gonzalez and Woods 92 Rafael C. Gonzalez and Richard E. Woods, Digital Image Processing, Addison-Wesley Publishing Company, 1992.

16. Gonzalez, R. C., Woods, R. E., and Eddins, S. L. [2009]. Digital Image Processing Using MATLAB, 2nd ed., Gatesmark Publishing, Knoxville, TN.

17. Gonzalez, R. C. and Woods, R. E. [2008]. Digital Image Processing, 3rd ed., Prentice Hall, Upper Saddle River, NJ.

18. S. P. Cheon, J. M. Kang, M. W. Park and J. H. Eom, "The Scheme of 3-Level Authentication Mechanism for Preventing Internal Information Leakage In", The 4th International Conference on Digital Information and Communication Technology and its Application, (2014), pp. 154-157.

19. R. Awasthi and R. A. Ingolikar, "A Study of Biometrics Security System", J. Innovative Research & Development, vol. 2, Issue 4,
(2013), pp. 737-760.

20. H. Lee, J. Jung, T. Kim, M. Park, J. Eom and T. M Chung, "An Application of Data Leakage Prevention System based on Biometrics Signals Recognition Technology In", The 3rd International Conference on Networking and Technology, (2014).

21. N. Dahiya and C. Kant, "Biometrics Security Concerns In", The 2nd International Conference on Advanced Computing & Communication Technologies, IEEE Press, New York, (2012), pp.297-302.