Hybrid Minutiae-based Architecture for Automated Fingerprint Verification System

Ifiok J. Udo
Department of Computer Science
University of Uyo, Uyo, Nigeria

Babajide S. Afolabi
Department of Computer Science and Engineering
Obafemi Awolowo University, Ile-Ife, Nigeria

Bernard I. Akhigbe
Department of Computer Science and Engineering
Obafemi Awolowo University, Ile-Ife, Nigeria

ABSTRACT

Fingerprints are patterns formed on the epidermis of fingertip and they are characterized with minutiae and their overall ridge flow patterns. In this paper, fingerprint minutiae are considered to have both the quantitative and qualitative properties which could help to ensure accurate verification of fingerprint if properly utilized. The hybrid architecture of minutiae-based verification is in effect a model that caters for enhancement in terms of minutiae quantity and quality on fingerprint. While researches have proven that good quality of fingerprint minutiae can guarantee accurate verification of the fingerprint, false acceptance and rejection rates are still being recorded largely because the improvement associated with the quality of minutiae may not be sufficient to address the problems associated with fingerprint during sensing. Nevertheless, an improvement in the number (i.e. quantity) of minutiae extracted from fingerprint could be useful in many instances. Therefore, this paper introduces a dimension whereby necessary and sufficient condition is set for the selection of quantity of minutiae needed for verification. This approach is designed to complement existing minutiae quality enhancement approach aimed at achieving accurate verification in Automated Fingerprint Verification System (AFVS). Hence, hybrid architecture of minutiae-based fingerprint verification is presented based on the data reduction principle of data mining.

General Terms

Biometrics, Security and Privacy

Keywords

Minutiae quantity and quality, fingerprint verification, hybrid architecture, data reduction, AFVS

1. INTRODUCTION

Fingerprints are patterns formed on the epidermis of the fingertip [1]. Among other human features, it is a unique organ which has more discriminators than any other biometric feature currently in use [2]. This implies that fingerprint is richer in authentication credentials than any other biometric features in use, e.g. iris, retinal scans, gaits, etc. Research has revealed that no two human beings share the same fingerprint characteristic features. This could be evident through the study by [3], which posits that the maximum global similarity is present in the monozygotic (i.e. identical) twins, that is, the closest genetic relationship, but there are still micro details available on the fingerprints of identical twins which clearly distinguish one individual from another. The numerous features on fingerprint that can be used for identification are as follows: Minutiae such as singular and common points. These are the ridge endings or bifurcations (i.e. a Y-shaped split of ridge into two components) branches of the fingerprint image. Core and delta on fingerprints image constitute the singular points. A dot is very short ridge that appears like a “dot”. Other features of fingerprint [4] include the overall ridge flow pattern, ridge frequency, location and position of singular points, type, direction and location of minutiae points, ridge counts between pairs of minutiae and location of pores. These fingerprint features are illustrated in Fig. 1. According to [5], the information contained in fingerprint can be categorized into three different levels namely: level 1 (pattern), level 2 (minutiae points) and level 3 (pores and ridge contours). Similarly, different authors have presented various categories of classes of fingerprint which can also allow for the accurate fingerprints classification. According to [6], fingerprints are classified into five classes namely, whorl, right loop, left loop, arch and tented arch.

Fingerprint apart from its uniqueness has other distinct characteristics which can further enhance the effectiveness of biometric technology. The other characteristics of biometric features include permanence (i.e. it does not vary over individuals lifetime), universality (i.e. everyone has it), circumvention (i.e. it is difficult to spoof), acceptability (i.e. it is widely acceptable) and collectability (i.e. it can be quantitatively measured).

Fingerprints are often collected with the help of capturing devices, such as fingerprint scanners, and stored in a database.

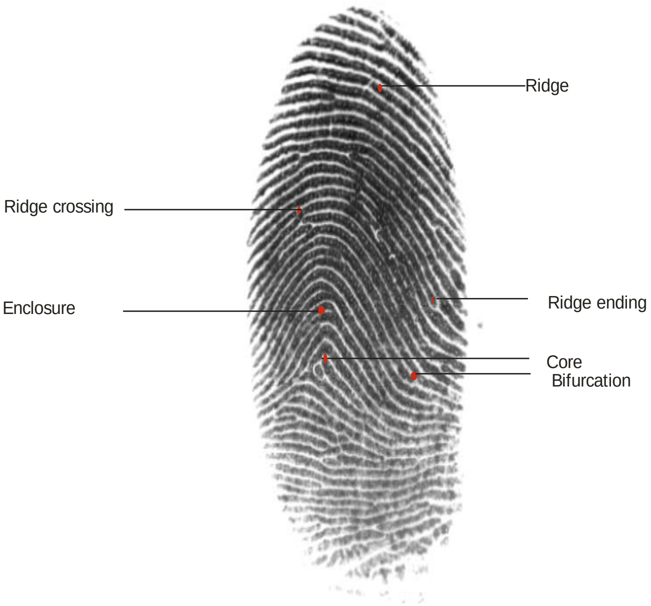

Fig 1: Fingerprint image showing its various features

There is a high level of acceptability of fingerprint technology in software applications. This is as a result of the cost of capturing devices of fingerprint impressions which is becoming cheaper when compared with other biometric capturing devices.

According to [7], a typical life-scan fingerprint contains between thirty (30) to forty (40) minutiae, but empirical study by Federal Bureau of Investigation (FBI) has revealed that two individuals will not have more than eight common minutiae. The challenge of establishing the exact number of minutiae that can adequately establish the identity of an individual is still a subject of research in recent times.

During individual's biometric authentication process [8], matching is used to compare the identity of individual's fingerprint with the stored impression (i.e. template) on the database(s). Matching is referred to the comparison and retrieval of the individual's authentication credentials from its database. According to [9], fingerprint matching is categorized as either verification or identification. Verification which is the focus of this paper entails one-to-one matching. This context implies comparison of a claimant's fingerprint against an enrollee to ascertain the identity of a claimant. In the other hand, identification is a one-to-many matching strategy. This matching strategy is performed where a fingerprint of unknown ownership is matched against the database of known fingerprint template to associate it with an identity.

The major challenges that impede fast and accurate matching of fingerprint in any of the matching strategies used are intra-class variability and inter-class similarity. Inter-class similarity is the semblance between impressions of different fingerprints. It is caused by similarity in global structures and ridge orientation. However, intra-class variability is the deviation between impressions of the same fingerprints. This is caused by sensor noise, partial overlap, non-linear distortion and translation.

Biometric technology unlike conventional identity authentication system that uses identity cards, passwords and security codes, requires more precise identification of individual and measures so that it is difficult to compromise or circumvent the verification system by impostors.

The research communities has addressed various problems linked to biometric authentication in general and fingerprint matching in particular, but false acceptance and rejection rates still persist. These problems may stem from the fact that researchers have placed importance on only the quality of fingerprint image with disregard to its quantity in a minutiae-based verification approach. The quality of minutiae accounts for the brightness, contrast and sharpness of the fingerprint, while quantity takes the numerical measure of the extracted or available minutiae into account.

Data reduction which is used to drive the proposal for the hybrid architecture is an essential element in selecting a minutiae subset representative from fingerprint in the process called instance selection. This technique is aimed at addressing improvement in the number of minutiae that could help to achieve higher accuracy level in fingerprint verification system apart from the quality enhancement strategies. The quantity of minutiae is a measure of the number of minutiae points that is required for accurate fingerprint verification. It is also the true subset representation of minutiae that will be necessary and sufficient for the verification of fingerprint otherwise regarded as the improved quantity of minutiae.

Therefore, this paper seeks to provide hybrid minutiae-based fingerprint verification architecture aimed at addressing improvements on the fingerprint verification system with regards to minutiae qualitative and quantitative enhancements.

1.1 Statement of the Problem

The uniqueness of fingerprint as a biometric feature for verification is challenged by both intra-class variability and inter-class similarity. These problems are attributed to similarity in global structures and ridge orientation among others such as: sensor noise, partial overlap, non-linear distortion and translation. These attendant problems pose a major hindrance to the determination of the actual number of minutiae necessary for verification in AFVS applications, thereby aiding false acceptance and rejection rates. There is therefore the need for a hybrid verification architecture that will capture the improvement in both the quality and quantity of the fingerprint minutiae to ensure accurate verification of fingerprints. Hence, this paper seeks to improve on the minutiae-based fingerprint verification architecture by incorporating the improvement on the quantity of minutiae component into existing enhanced minutiae quality approach of the verification system.

The remaining part of this paper is organized as follows: Section two presents the approaches to fingerprint matching and draws attention to the strength and weaknesses of such architecture and models. Section three presents the proposed hybrid architecture of the minutiae-based fingerprint verification system. However, conclusion and the future work are subsumed in section four.

2. APPROACHES TO FINGERPRINT MATCHING

There is a three-class categorization of fingerprint matching approaches [3], [10] and [11]. These approaches include: minutiae-based matching, ridge feature-based matching and correlation-based matching. Nevertheless, hybrid or multimodal approach [12] is also in vogue. The aforementioned approaches are good but researches have proven minutiae-based verification to be more efficient approach in terms of accuracy. The accuracy indicators being used are false acceptance rate, false rejection rates as well as equal error rates.

In this paper, minutiae-based verification architecture is presented in a hybrid form aimed at further enhancing the accuracy of AFVS.

2.1 Fingerprint Matching Models

The literature reviewed under the existing approaches pointed to the qualitative concordance [3] as an important factor for reducing false acceptance and rejection rates in automated fingerprint matching systems. Therefore, the works of the following authors [13], [2], [1] and [5] have presented matching architecture that enhanced only the quality of fingerprint image. Nevertheless, the quantitative factor which may be of benefit to fingerprint verification in AFVS has not been adequately harnessed by researchers. This paper therefore observes that, existing models that are not inspired by both the improvement on quality and quantity of minutiae is likely to increase false acceptance and rejection decisions of the fingerprint matching systems.

2.1.1 Generalized fingerprint matching architecture

The work of [2] presented fingerprint ideas, influences, trends and a general description of practice as obtained in the biometric feature authentication researches. In this architecture, fingerprint matching is divided into registration and recognition phases. The weakness of this architecture is the consideration of only fingerprint features in terms of qualitative attributes obtained from fingerprint image. The architecture did not consider how much features fingerprint could accurately involved in fingerprint matching. This fingerprint matching architecture is represented in Fig. 2.

2.1.2 2.1.2 Fingerprint identification architecture

The identification architecture is presented by [12] in order to reduce the false acceptance and rejection rates in fingerprint identification. There are several components of the architecture such as: image acquisition, edge detection, thinning, feature extraction and classifier. The overall work is tailored towards obtaining an improvement on the qualitative concordance of fingerprint image which could help in the classification of fingerprint. The function of the edge detection is meant for extracting the available points on the fingerprint image in a way that significantly preserve the important structural properties of the image. However, feature thinning is not meant to specify the quantity of minutiae required for matching but the process of removing the selected foreground pixels from binary images and also shaping the structures (i.e. reduction in thickness) of ridges. This later process is aimed at tidying up the output of edge detectors which could help to also determine the accurate flow pattern of ridges, hence improving the quality of fingerprint image.

2.1.3 Fingerprint hierarchical matcher architecture

[5] in order to reduce false acceptance and rejection rates in fingerprint matching presented hierarchical matcher architecture. The architecture is informed by improving image quality to obtain a high quality fingerprint image. The various components of this architecture such as image processing and fingerprint image enhancement modules are aimed at producing good quality fingerprint image during minutiae extraction process. The work of [5] also used level two (2) and level three (3) fingerprint features, such as pores and ridge contours respectively, in addition to minutiae as input to the matching system. This is meant to further obtain more discriminative features from fingerprint that could add up to more information about the image. The problem with obtaining more input information (such as pores and ridge contours) obtained in addition to minutiae is the storage cost incurred in terms data storage and retrieval. Apart from increasing the financial difficulty in obtaining much memory space by the users, the matching process could be slow and processing time increased, if there is insufficient memory to cater for the requirements of the system. The schematic representation of the hierarchical matcher architecture is shown in Fig. 3.

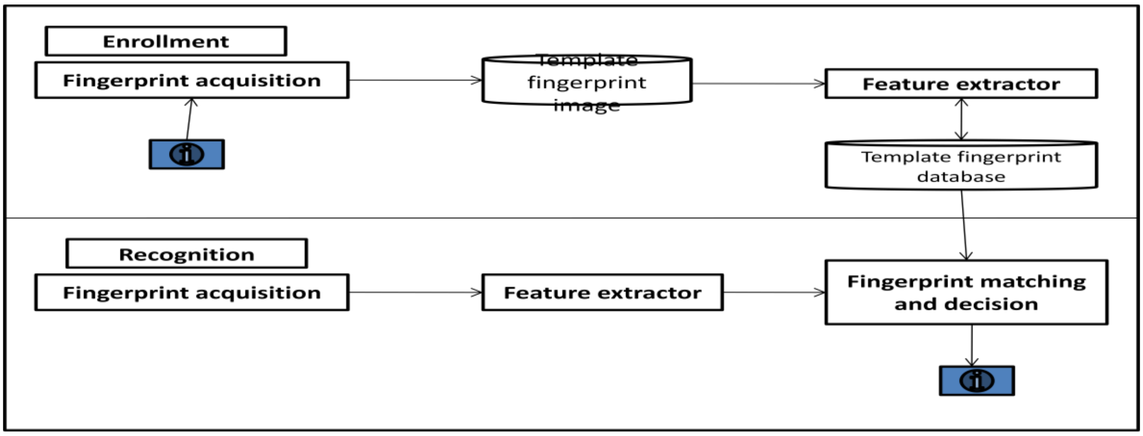

Fig 2: Fingerprint Matching Architecture [2]

3. THE PROPOSED HYBRID MINUTIAE-BASED FINGERPRINT VERIFICATION ARCHITECTURE

The hybrid architecture provides a means of considering an improvement on both the number of minutiae extracted (i.e. quantity of minutiae instances) and quality of minutiae. It is believed that improving the quantity of minutiae instance and also obtaining good quality image can contribute to an improved result of fingerprint verification. More so, improving the quantity of minutiae by means of data reduction approach will reduce demand for more storage needs and speed up processing time of fingerprint verification in AFVS.

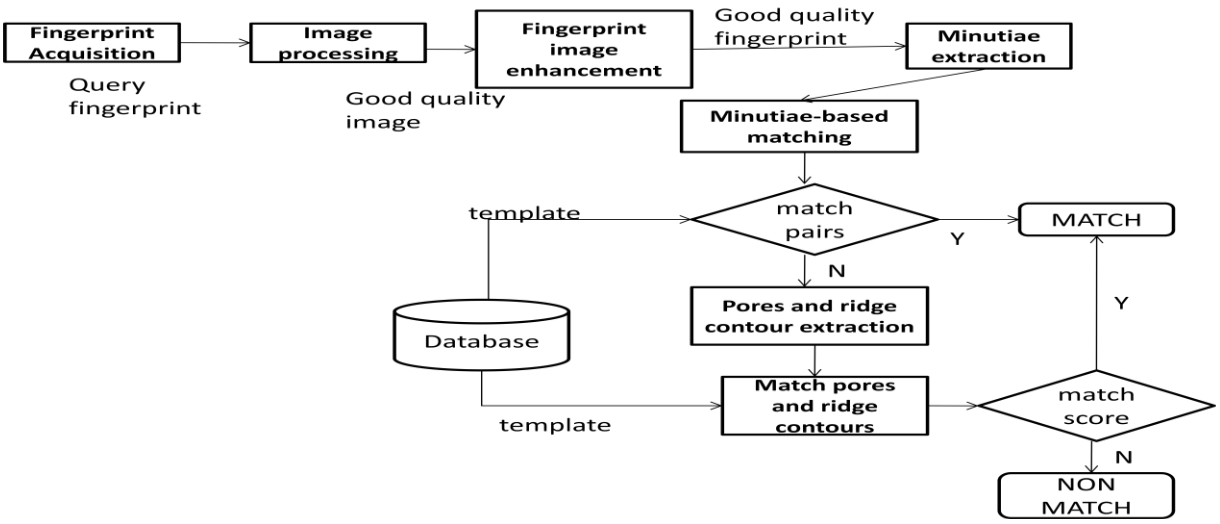

Fig. 3: Fingerprint hierarchical matcher architecture [5]

In this architecture, instance selection is meant to reduce the quantity of redundant minutiae and retain relevant ones. This technique is aimed at representing the true subset of fingerprint minutiae representative that could help to determine the quantity of minutiae necessary for verification in minutiae-based fingerprint verification. The benefits of determination of exact number of minutiae necessary for fingerprint verification span reduction in large search space [14] available whenever a query fingerprint is presented for verification in databases. It could also help in the reduction in computational loads of applications with minimal processing resources e.g. match-on-cards and match-on-chips systems. The hybrid minutiae-based verification architecture is presented in Fig 4.

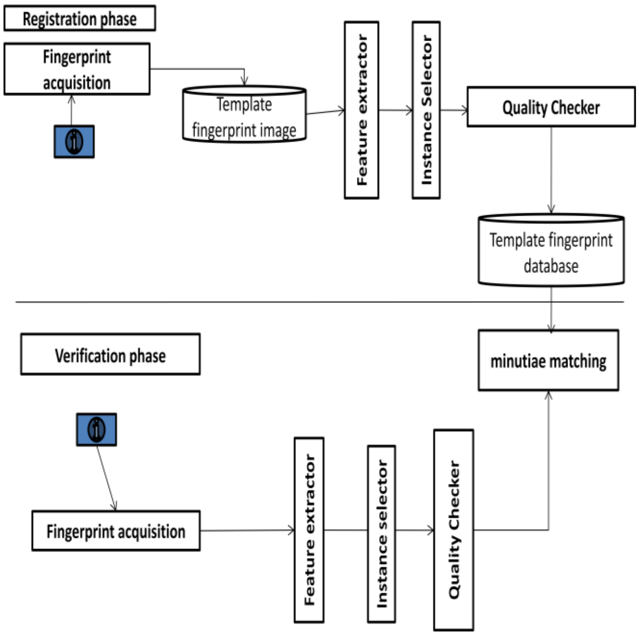

Fig 4: Proposed hybrid minutiae-based fingerprint verification architecture

3.1 Data Reduction and Minutiae Instance Selection

Data reduction is the process of reducing large volumes of data to manageable sizes. It is also an essential element of data preparation in data mining context [15]. This is performed either as feature selection, instance reduction and hybrid approaches. In minutiae reduction, selecting a subset of relevant minutiae could be achieved in the form of feature selection although minutiae in this case are not regarded as features but instances. This approach of reduction is therefore referred to instance selection. Instance selection is achieved with instance selector in Fig. 4.

3.1.1 Approaches to Instance selection

In data mining, data reduction poses many advantages to subsequent phases of data preprocessing and helps to present data in the format that would enhance further machining. Data reduction is subdivided into two types namely: feature selection or dimensionality reduction and reduction in size. However, there are several methods of feature selection which are currently used in data mining. According to [16], methods of feature selection may be divided into three broad categories namely:

Wrapper method: This method requires evaluation of each potentially useful subset of features by a classifier. It treats computational intelligence algorithms as black boxes with some parameters to be determined on the basis of test runs. The method is also equivalent to assigning binary weights to input during feature subset selection.

Method that is based on specific properties of computational intelligence methods.

Filtering: This method is based on evaluation of individual features in respect to the task performed, or filtering features that potentially carry useful information independently from the final computational intelligence method used.

In this paper, data reduction on minutiae is performed based on mutual information which is an information theoretic approach. This process is called instance selection. Instance selection is meant to characterize both the relevance and redundancy of minutiae. Relevant instances will provide information about the same class of minutiae by themselves or in a subset with others, whereas redundant minutiae instances will provide the same information about the class which another subset has already provided. Mutual information in fingerprint minutiae is defined mathematically as follows:

Let the fingerprint contains minutiae in form of common point (q) and singular points (s); mutual information between q and s are presented in equation 1 and 2, respectively, thus:

$$\mathrm{I(q,s)} = \sum_{j=1}^{Z}\sum_{k=1}^{Z} \mathrm{p}(\mathrm{r_k(q)} \wedge \mathrm{r_j(s)}) \,.\, \log_2 \frac{\mathrm{p}(\mathrm{r_k(q)} \wedge \mathrm{r_j(s)})}{\mathrm{p}(\mathrm{r_k(q)}).\,\mathrm{p}(\mathrm{r_j(s)})} \qquad 1$$

Where $\mathrm{I(q,s)}$ represents mutual information between two minutiae instances q and s. Also, $\mathrm{r_1(q), r_2(q), \ldots, r_Z(q)}$ is a partition of the range q into equal regions.

$$\mathrm{I(S,q)} = \sum_{i=1}^{M}\sum_{j=1}^{Z} \mathrm{p}(\mathrm{S_i} \wedge \mathrm{r_j(q)}) \,.\, \log_2 \frac{\mathrm{p}(\mathrm{S_i} \wedge \mathrm{r_j(q)})}{\mathrm{p(S_i)}.\,\mathrm{p}(\mathrm{r_j(q)})} \qquad 2$$

Where $\mathrm{I(S,q)}$ is the mutual information between the set of singular point, S, and quantity of minutiae instances (i.e. common points), q, obtained from fingerprint and $\mathrm{p}\left(\mathrm{r_j(q)}\right) = \mathrm{p(p \in r_j(q))}$ is the probability of finding common points with quantity q in the region of $\mathrm{r_j(q)}$.

However, the algorithm for finding the true subset representative of minutiae instances could be formulated with mutual information criteria specified in equation 1 and 2. In this paper, the criterion is modified to consider minutiae without paying attention to its various types.

3.2 Components of Hybrid Minutiae-based AFVS

The verification system is divided into two main parts namely: the registration and verification phases.

3.2.1Registration phase

In all biometric systems, registration of individual biometric identities is a commonplace. It is an essential step to the accurate verification of identity on the system. Registration phase deals with image acquisition and storage for further processing to aid in accurate verification and fast retrieval of individual’s fingerprint identity. The various components proposed for this phase in the hybrid architecture include: image acquisition, storage for template fingerprint image, feature extractor, instance selector, quality checker and template fingerprint image database. Similarly, the verification phase considers all the steps as it is in the registration phase except template fingerprint image database.

3.2.2 Verification phase

The verification phase compares fingerprint minutiae from the stored template with the query fingerprint image. The components needed for effective verification is discussed as follows:

Image acquisition

Image acquisition entails the collection of image for the system either for the purpose of registration and/ or verification. The process of registration of image and its corresponding identity precedes verification and not vice versa. Fingerprint sensing is the technique that is used for image acquisition. It can either be an offline or live-scan sensing obtained from various kinds of sensors.

Template fingerprint database

The acquired image is processed and stored in a form that will be suitable for comparison and retrieval by computer programs. The stored image served as a template in the biometric system. During the process of verification, the captured image is compared with the already stored fingerprint template and the degree of variability is calculated for the system. The system uses the degree of variability result to make either acceptance or rejection or decision.

Instance selector

This is a module that is meant to address the improvement on the quantity of fingerprint minutiae instances. The quantity of minutiae is a measure of the optimal number of minutiae points that is required for accurate fingerprint verification. This implies the true subset representative of minutiae that will be necessary and sufficient for the verification of fingerprint based on the quantity of minutiae. On the contrary, this is not minutiae dimensionality reduction or feature selection such as location coordinates, orientation information, type and texture. It is only meant to address the quantity of minutiae instance selection.

The architecture although it is not dependent on any methodology, it solely describes the general description of practices to be performed in minutiae-based fingerprint verification. However, the criteria to address instance selection on fingerprint minutiae are set based on maximum normalized mutual information that exist between minutiae and reference points taken from the selected rectangular region of interest. The normalized mutual information is aimed at reducing the level of uncertainty of minutiae subset and it is formulated in equation 3.

$$\mathrm{nM(X,Y)} = \frac{\mathrm{H(X) + H(Y)}}{\mathrm{H(X,Y)}} \qquad 3$$

Where $\mathrm{nM(X,Y)}$ is the normalized mutual information between two minutiae X and Y, $\mathrm{H(X)}$ is the entropy of X, $\mathrm{H(Y)}$ is the entropy of Y and $\mathrm{H(X,Y)}$ is the joint entropy of X and Y.

Given both equations 1 and 2, it is assumed that minutiae are generalized and treated equally with no priority attached to any of its different types (such as core, delta, bifurcations, ridge endings etc). Therefore, equation 3 is being formulated to reduce the level of uncertainty between minutiae, hence targeted to improve the accuracy of the verification system.

This is in line with the postulation of [17] Cover and Thomas (1991), which states that mutual information is the reduction in the uncertainty of one random variable due to the knowledge of the other. This will reduce uncertainty of a minutia with respect to others, and it will also give room for selection of appropriate quantity of minutiae for subsequent processing.

Nevertheless, in this paper, the algorithm specified for finding the true subset representative of minutiae instances is based on the criteria specified in equation 3. The resulting quantity of minutiae instances obtained is used in the computation of quality measurement of fingerprints minutiae formulated in the work of [18].

Quality checker

Due to the proposition by biometric researchers that good quality image will simplify the verification process and could also lead to accurate system decision based on acceptance and rejection rates of fingerprint, it is necessary to address verification problem based on the improved quality of minutiae. This module is responsible for assessing the fingerprint image portion(s) of concern (otherwise called region of interest) for quality conformance. In this module, image could be represented in either spatial or frequency domains. The choice of domain depends on the researchers. Frequency domain implies that image are represented in terms of sinusoidal waves to simplify quality enhancements based on the issues such as translation, rotation, distortion of the transformed fingerprint image. Similarly, the spatial domain shows fingerprint representation on dimensional spaces or planes. Fingerprint image may be enhanced if it fails the quality checker test. In the work of [8] and [5], good quality image obtained by image enhancement is used for further verification stages.

However, the enhancement of quality of minutiae performed in this component of the architecture is not enough to address the improvement of quantity of minutiae instances that is needed for the accurate verification, hence the introduction of the feature selector module to address the selection of optimal quantity of minutiae. The quantity of minutiae to be used in verification could be useful in application areas with minimum fingerprint image processing capabilities among other concerns.

The result of the quality checker forms the template minutiae coordinate system that will be subjected to verification process with the near or same similarity score of query image.

Verificator

Verificator module is designed to perform the verification of fingerprints based on the minutiae points stored in the database. The main purpose of verification is to compare the query and template minutiae images so that accurate decision could be taken on the identity of individual laying claims on it. Hence, minutiae verification module is used to perform the comparison and retrieval of distinguishing features in template fingerprint database obtained during feature extraction. The output obtained from this module is used to compute the matching score. Therefore, the acceptance or rejection decisions will be based on a certain pre-determined threshold for the computed matching score. This threshold value is allowed to cater for adjustments or some level of variability resulting from the system on the fingerprint image during processing.

3.3 Flowchart of Hybrid Minutiae-based Fingerprint Verification System

The diagram in Fig 5 represents a schematic diagram of the proposed hybrid architecture. Therefore, based on the schematic diagram, specific methodologies will be assigned to respective entities to achieve their purposes. These entities considered in this paper are: orientation field estimation, ridge enhancement/ thinning, minutiae extraction and instance selection. These aforementioned processes constitute the image extraction phase, while minutiae matching and image extraction phase inclusively constitute the verification phase of the entire hybrid minutiae-based fingerprint verification system.

3.3.1 Analysis of flowchart of hybrid minutiae-based fingerprint verification architecture

Input fingerprint image is obtained during the registration and verification processes. The obtained image is converted to a format suitable for feature (i.e. minutiae) extraction to be performed. Orientation field estimation is carried out on the image to determine ridge discontinuities otherwise called minutiae. Minutiae are grouped as singular and common points. This process of minutiae extraction is combined with ridge thinning and enhancement. Enhancement is performed only if the quality of the image as measured by the quality checker would not guarantee the needed accuracy of the verification system. Both the singular and common points are obtained and a minutiae subset representative is presented by performing instance selection on the minutiae. The resulting minutiae could be stored on the template depending on whether it is the registration or verification process. If it is the verification phase, the query fingerprint minutiae subset obtained would not be stored but used for computation of matching score which is used for comparison with that of the stored template of the corresponding claimant’s identity.

Depending on the threshold value set for the verification system, the result is presented as an acceptance or rejection decision. This flowchart is in line with the flowchart presented in the work of [19]), except for the fact that improvement on the minutiae quantity of instance is not addressed alongside with minutiae quality.

4. MERITS OF HYBRIDARCHITECTURE

The advantage of the proposed hybrid verification model over existing ones is the reduction in the size of fingerprint image template while aiming at improving the accuracy of the system. This reduction in the size of the fingerprint image will have a direct effect on the utilization of memory of the computer system. The proposed model will be particularly useful in application areas where systems with minimal processing power is required to achieve accuracy in biometric systems. Examples of such area of applications are match-on-cards and match-on-chips systems. In addition, the application of the proposed model to expensive platforms such as learning management systems could cut the cost of memory requirements that is needed for enrolment purposes. This will in turn address the challenge faced by organizations or institution that will use the system in terms of its expensive nature.

4.1 Conclusion and Future work

Minutiae-based verification has been proven by researches to record higher accuracy than other techniques of fingerprint verification even though errors are still being recorded in terms false acceptance and rejection rates. This makes minutiae-based matching one of the best matching techniques of fingerprint verification. In this paper, hybrid architecture is proposed to further increase the level of accuracy of the minutiae verification of fingerprint. Therefore, the major contribution of this paper is proposing hybrid architecture for minutiae-based fingerprint verification. The architecture is aimed at providing information on how to arrive at the exact number of minutiae that will be necessary and sufficient for fingerprint verification in application areas of use in software applications. In future, the algorithms of the various components of the proposed architecture will be provided and evaluated with existing verification algorithms. The implementation of the proposed architecture will also be presented.

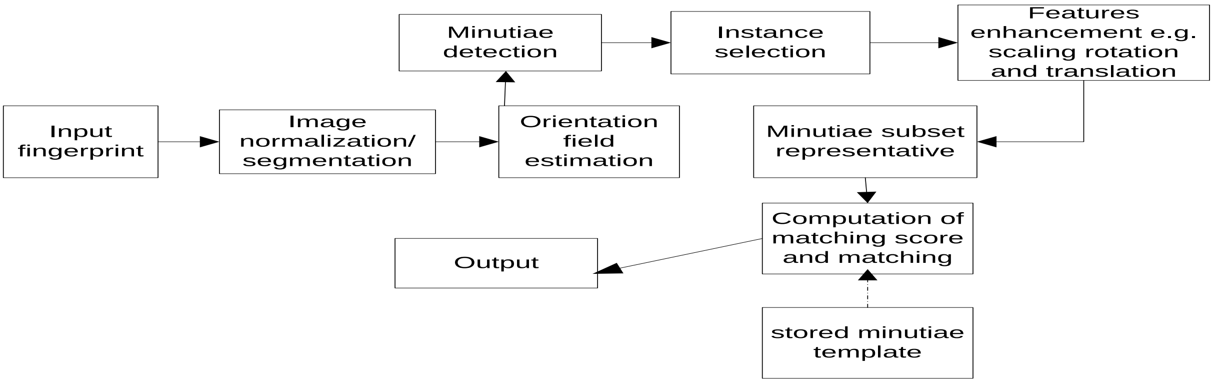
Minutiae detection
Instance selection
Features enhancement e.g. scaling rotation and translation
Input fingerprint
Image normalization/ segmentation
Orientation field estimation
Minutiae subset representative
Computation of matching score and matching
Output
stored minutiae template

Fig 5: Schematic diagram of hybrid minutiae-based fingerprint verification architecture

5. REFERENCES

[1] Singh, S. D and Majhi, S. P (2009). Fingerprint recognition: a study on image enhancement and minutiae extraction. B.Tech. Thesis, Department of Electronics & Communication Engineering National Institute of Technology Rourkela, Rourkela.

[2] Bharkad, S and Kokare, M. (2011). Fingerprint Identification- Ideas, Influences and Trends of New Age. Pattern Recognition, Machine Intelligence and Biometrics. Springer, Heidelberg, pp.410-446. doi:10.1117/1.JEI.23.2.023007

[3] Maltoni, D. Maio, D. Jain, A.K. Prabhakar, S. (2003). Handbook of Fingerprint Recognition. Springer, New York. bias.csr.unibo.it/maltoni/handbook/index.pdf

[4] Geng, X. and Smith-Miles, K.(2009). Incremental Learning. Encylopedia of Biometrics, Vol. 1. Springer, USA.

[5] Rawat, A. (2009). A Hierarchical Fingerprint Matching System. Bachelor-master Thesis of Department of Computer Science and Engineering, Indian Institute of Technology, Kanpur. www.security.iitk.ac.in/contents/publications/mtech/AbhishekRawat.pdf

[6] Ratha, N.K., Karu, K., Chen, S. and Jain, A. K. (1996). A real-time matching system for large fingerprint databases. IEEE transactions on pattern analysis and machine intelligence, 18(8):799-813. dl.acm.org/ citation.cfm?id=236268

[7] Gupta, M. (2001). Biometric Technologies Overview. Global Information Assurance Certification Paper. SANS Institute 2001-2002. (Available at: http://www.giac.org/paper/gsec/533/biometric-technologies-overview/101261 on 29th May, 2012).

[8] Jain, A. K., Ross, A and Prabhakar, S. (2004). An Introduction to Biometric Recognition. IEEE Transaction on Circuits and Systems for Video Technology, 14(1):4-20. citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.113.6189

[9] O'Gorman (1998). Overview of fingerprint verification technologies, Elsevier Information Security Technical Report, Vol. 3, No. 1 . http://dx.doi.org/10.1016/S1363-4127(98)80015-0

[10] Parta, A. (2006). Development of efficient methods for face recognition and multimodal biometrics. Master of Science thesis of department of Computer Science and Engineering, Indian Institute of Technology, Madras. www.cs.bris.ac.uk/home/cszap/MS-Thesis-Arpita.pdf

[11] Alonso-Fernandez, A., Bigun, J., Fierrrez, J., Fronthaler, H., Kollreider, K. and Ortega-Garcia, J. (2009). Fingerprint Recognition. Guide to Biometric Reference Systems and Performance Evaluation. Springer-Verlag, London. DOI: 10.1007/978-1-84800-292-0.

[12] Bellakhdhar, F., Ayed, M. B., Loukil, K., Bouchhima, F. and Afid, M. (2013). Multimodal biometric identification system based on face and fingerprint. Proceedings of International Conference on Intelligent Control and Information Processing, vol 3. pp 219-222.

[13] Barua, K., Bhattachrya, S. and Mali, K. (2011). Fingerprint Identification. Global Journal of Computer Science and Technology, 11(6).computerresearch. org/ stpr/index.php/gjcst/article/download/831/737

[14] Ho, C. C. and Eswaran, C. (2013). Consolidation of Fingerprint Databases: Challenges and Solutions in the Malaysian context. International Journal of Computer Information System and Industrial management Applications,5(2013):373-382. DOI:10.1109/HIS.2011.6122148

[15] Li, X. (2002). Data Reduction via Adaptive Sampling. Communication in Information and Systems, 2(1):53-68. www.ims.cuhk.edu.hk/~cis/2002.1/Reduction2.pdf

[16] Duch, W., Biesiada, J., Winiarski, T., Grudzinski, K. and Gradbczewski, K. (2003). Feature Selection based on Mutual Information. Advances in Soft Computing, 19(2003):173-178.

[17] Cover, T. M. and Thomas, J. A. (1991). Elements of Information Theory. John Wiley & Sons Inc.

[18] Xu, H., Veldhius, R. N., Kevenaar, A. M., Akkermanns, A. (2009). A Quality Integrated Spectral Minutiae Fingerprint Recognition System. In 30th Symposium of Information Theory in the Benelux, Netherlands. doc.utwente.nl/72098/

[19] Zhou, J., Zhang,, D., Gu, J. and Wu, N. (2004). Graphical Representation of Fingerprint Images. Kluwer Academic Publishers, USA. dl.acm.org/ citation. cfm?id =985860