

# Fingerprint Authentication System using Hybrid Classifiers

Parvathi R, Sankar M

**Abstract** — Fingerprints are considered as the most widely accepted biometric feature for uniquely identify a person in the field of biometrics. The existing system only contains bayes classifier to improve the retrieval speed and to perform one to many fingerprint matching. When compared to proposed system, the previous work degrades with performance features like accuracy, consistency and retrieval speed. This fingerprint authentication system uses the combination of Henry classification system at enrollment process and Bayes classification system at authentication process. This paper mainly focuses on fingerprint classification and presents an approach to speed up the matching process by classifying the fingerprint pattern into different groups using Henry classification system. By the speed of Bayes classifier, this system does not depend on the huge amount of fingerprint images in database, one can capture large number of training samples per finger. It can improve the performance features like retrieval speed, consistency and accuracy by using the combination of classifiers.

**Index Terms** — Biometrics, fingerprint authentication, Henry classification, Bayes classifier, probabilistic recognition.

## I. INTRODUCTION

The Conventional security systems use either knowledge-based methods like passwords or PIN, or token-based methods such as passport, driving license, ID card [13]. They are prone to fraud because PIN numbers could be forgotten or hacked and the tokens could be lost, duplicated or stolen. To address the need for robust, reliable, and foolproof personal identification, authentication systems will necessarily require a biometric component. Biometric

Systems use a person's physical characteristics (like fingerprints, irises or veins), or behavioral characteristics (like voice, signature or keystroke) to determine their identity or to confirm that they are who they claim to be. Biometric data are highly unique to each individual, easily obtainable non-intrusively, time-invariant (no significant changes over a period of time) [14] and distinguishable by humans without much special training.

Fingerprints are widely accepted biometric feature to uniquely identify person rather than other kinds of feature (face, iris or vein). Fingerprint authentication is becoming more popular in a number of civilian & commercial applications such as bank ATM, Computer login and welfare disbursement. Fingerprint classification refers to the problem

of assigning a given fingerprint into a predefined class (e.g., Henry class) [19] based on its global structure and singular points. A fingerprint identification system authenticates a person's identity by comparing the captured fingerprint with his/her own previously enrolled reference template stored in the database. It conducts a one-to-many comparison to confirm whether or not the claim of identity by the individual is true.

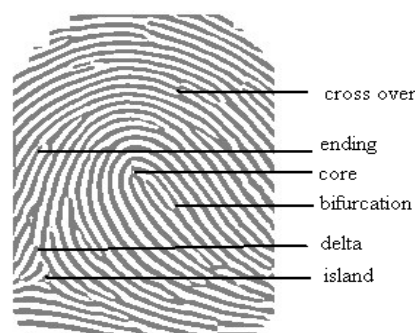


Figure 1: Minutiae- points on a fingerprint

Fingerprint consists of number of lines which flow in different directions is called ridges and the gap between those ridges is known as valleys. A fingerprint pattern can be categorized according to their minutia points such as ridge ending, bifurcation, core, delta, cross over and island that are depicted in Fig.1. A ridge ending is a minutia point where a ridge terminates. A single ridge path is splitted into two paths as a Y- junction.

The core is a center point of the fingerprint pattern. The delta is a singular point from which three ridges deviate. This core and delta locations can be used to match two fingerprints [15].

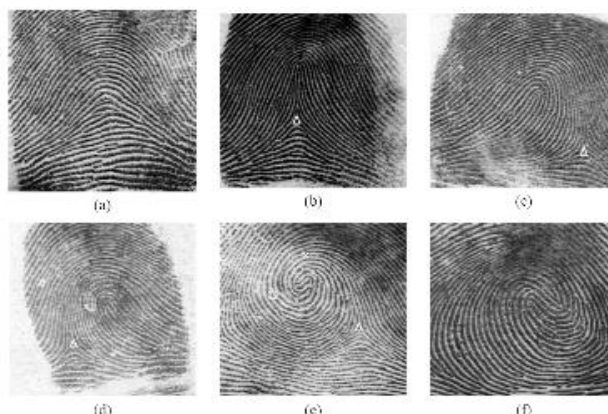


Figure 2: Fingerprints classification involving six categories: (a) arch, (b) tented arch, (c) right loop, (d) left loop, (e) whorl, and (f) twin loop.

Fingerprints can be matched by one of two approaches such as minutia matching and global pattern matching. In

**Manuscript received on July, 2012.**

**Parvathi R.** Assistant Professor, Department of Information Technology, PSNA College of Engineering and Technology, Dindigul, Tamilnadu, India

**Sankar M.** Assistant Professor, Department of Electrical and Electronics Engineering, RVS College of Engineering and Technology, Dindigul, Tamilnadu, India.

minutia matching, each minutia is matched with above mentioned minutia points. In global pattern matching, the global pattern [13] of Fingerprint consists of six patterns: arch, tented arch, right loop, left loop, whorl, and twin loop as mentioned in Fig.2. The ridge flow constitutes a global pattern of the fingerprint. Each pattern can be compared by the flow of ridges at all locations between a pair of fingerprint images.

## II. LITERATURE REVIEW

K.C Leung and C.H. Leung [1] proposed a method to recognize the fingerprint image with the help of bayes classifier. Even though it overcomes the problem of one to one matching and slow retrieval of image, it does not have the Henry classes to improve consistency problem [15] and used only one sample per finger which degrades accuracy of the system. Jinwei Gu [3] proposed a method for fingerprint verification which includes both minutiae and model based orientation field is used. It gives robust discriminatory information other than minutiae points. Fingerprint matching is done by combining the decisions of the matchers based on the orientation field and minutiae.

M. R. Girgisa [8] proposed a method to describe a fingerprint matching based on lines extraction and graph matching principles by adopting a hybrid scheme which consists of a genetic algorithm phase and a local search phase. Experimental results demonstrate the robustness of algorithm. Luping Ji and Zhang Yi [9] proposed a method for estimating orientation field by neuron pulse coupled neural network and block direction by projective distance variance of a ridge. Alessandra Lumini, and Loris Nanni [10] developed a method for minutiae based fingerprint and its approach to the problem as two - class pattern recognition. The obtained feature vector by minutiae matching is classified into genuine or imposter by Support Vector Machine resulting remarkable performance improvement. Mohamed [18] presented fingerprint classification system using Fuzzy Neural Network. The fingerprint features such as singular points, positions and direction of core and delta obtained from a binarised fingerprint image. The method is producing good classification results.

Prabhakar S, Jain. A.K. [15] has developed filter-based representation technique for fingerprint identification. The technique exploits both local and global characteristics in a fingerprint to make identification. The matching stage computes the Euclidian distance between the template finger code and the input finger code. The method gives good matching with high accuracy.

## III. STATISTICAL PATTERN RECOGNITION USING NBC

Generally, Pattern recognition is performed by one of the three approaches like syntatic, statistical and neural networks [12]. The Statistical methods are necessary, because, many different measurement vectors will correspond to noisy or distorted versions of the same basic pattern or template and thus require assignment to the corresponding classes [2].

A Naive Bayes classifier (NBC) is a simple probabilistic statistical classifier [1] based on applying Bayes theorem with strong (naive) independence assumptions [16]. The Bayes Theorem [12] is

basis of the Bayesian approach for pattern recognition which is described as follows:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \quad (3.1)$$

$$\text{Where, } P(B|A) = \frac{P(A \cap B)}{P(A)} \quad (3.2)$$

In general, all random variables will not be mutually independent; the probabilities of an event A may well depend on the previous or simultaneous occurrence of an event B. A is said to be conditioned on B, The need to incorporate this type of dependence into the theory resulted in the definition of the conditional probability  $P(A|B)$ , which is the probability that A will occur given that B already has.

The basic idea of Bayes rule is that the outcome of an event (A) can be predicted based on some evidences (x) that can be observed. The Bayes rule has,

- i) **Priori probability:** This is the probability of an event before the evidence is observed.
- ii) **Posterior probability:** This is the probability of an event after the evidence is observed.

Informally, Bayes rule says:

$$\text{Posterior} = \frac{\text{likelihood} \times \text{prior}}{\text{Evidence}} \quad (3.3)$$

$P(A)$  is called the prior probability of A i.e. before having the data or evidence x. The term  $p(x|A)$  is called the likelihood(probability density function)[16] and  $P(A|x)$  is called the posterior probability i.e. after having the evidence. The conditional probability is obtained by:

$$P(A|x) = \frac{p(x|A)P(A)}{p(x)} \quad (3.4)$$

In the general problem where many measurements/features are used to distinguish between many classes, the approach Statistical Pattern Recognition (SPR) using NBC for recognizing the pattern can be summarized [12] as follows:

**Table 1:** Algorithm of NBC for pattern recognition

<ol style="list-style-type: none"> <li>1. Establish a training set <math>\{x^{(j)}, w_i^{(j)}\}</math>, <math>j=1,2,\dots,N_t</math> for each class <math>w_i</math>, where <math>i</math> and <math>j</math> are number of classes and number of training samples respectively.</li> <li>2. Compute a priori information such as probability density function <math>p(x w_i)</math>, <math>P(w_i)</math> and <math>P(w_j)</math>.</li> <li>3. Given a new unclassified measurement <math>y</math>, use Bayes theorem to obtain the measurement conditioned probability                     <math display="block">P(w_i   y) = \frac{p(y w_i)P(w_i)}{p(y)} \quad \text{for each class } w_i .</math> </li> <li>4. Choose <math>w_i</math> such that <math>P(w_i   y) &gt; P(w_j   y)</math> for all <math>i \neq j</math>.</li> </ol>
---

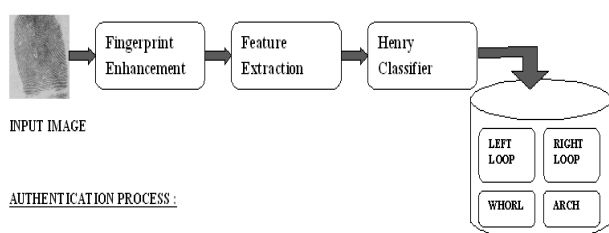
The algorithm describes how the classifier recognizes the pattern. The defined system has number of classes each of which contains huge amount of training samples. The probability for test pattern and each class is calculated to identify which class has higher probability conditioned with input feature probability [12]. A class with higher probability is selected as an expected class which contains pattern related to test pattern. By using training sets, probability density function is calculated for both test pattern and template. These probability density functions are used by

Bayes theorem to find conditioned probability. By comparing those probabilities, the Bayes rule can find whether the new unclassified pattern is matched to template pattern.

#### IV. PROPOSED SYSTEM

Proposed system is focused on fingerprint classification which includes widely accepted Henry classification system [2] at enrollment process and Bayes classifier [16] at authentication process. The system model consists of two phases such as enrollment and authentication phases. In the enrollment phase, user registers their personal information with their fingerprint through fingerprint sensor device [15]. The system directly stores their personal information on database. But the fingerprint images should be stored on database after performing some internal processes like enhancement, feature extraction and classification process using Henry classification scheme [2], as in Fig.3.

##### ENROLLMENT PROCESS:



##### AUTHENTICATION PROCESS:

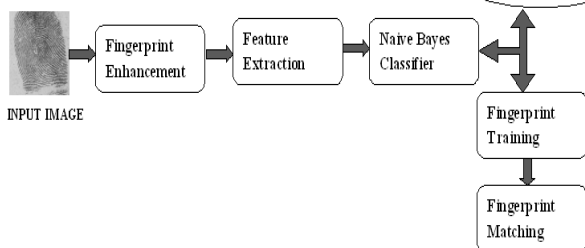


Figure 3: Fingerprint Authentication System (FPAS)

The feature enhancement involves some preprocessing like remove background, reduces noise exist on image, enhance the definition of ridges against valleys and produces the clear thinned minutia [7]. From the enhanced minutia, minutia points (features) are extracted using feature extraction techniques [4]. The extracted features are accepted by Henry classification system to determine which type of pattern such as left-loop, right-loop, arch or whorl [2]. (The detailed function of enhancement, feature extraction and classification are described later).

The second phase of the system model is authentication process in which registered user enters their user name, password along with fingerprint image using sensor. The username and password is verified by the normal procedure of authentication system. But, the fingerprint image can be authenticated by following some basic steps that shown in fig.4. The feature of image is extracted by the same procedure of enhancement and feature extraction process which are done at enrollment process. The extracted feature is fetched by the Naive Bayes (NBC) to classify the image according to prescribed pattern.

The Fingerprint Authentication system (FPAS) uses following five steps to recognize the given fingerprint image (Fig.4).

- A. Fingerprint Enhancement
- B. Feature extraction
- C. Fingerprint Classification
- D. Fingerprint Training
- E. Fingerprint matching

##### A. Fingerprint Enhancement

A fingerprint image may be one of the noisiest of image types. This is due to the fact that finger tips become dirty, cut, scarred, creased, dry, wet, worn, etc. The image enhancement step is designed to reduce this noise and to enhance the clear definition of ridges against valleys. Two image processing operations designed for these purposes are the adaptive matched filter and adaptive thresholding [14].

Even though there may be discontinuities in particular ridges, one can always look at a local area of ridges and determine their flow. This filter is applied to every pixel in the image. Based on the local orientation of the ridges around each pixel, the matched filter is applied to enhance ridges oriented in the same direction as those in the same locality, and decrease anything oriented differently. The incorrect ridges can be eliminated by use of the matched filter [15].

##### B. Feature Extraction

The fingerprint minutiae are found at the feature extraction stage. Operating upon the thinned image, the minutiae are straightforward to detect. Endings are found at termination points of thin lines. Bifurcations are found at the junctions of three lines. There will always be extraneous minutiae found due to a noisy original image or due to artifacts introduced during matched filtering and thinning. These extraneous features are reduced by using empirically determined thresholds [3]. For instance, a bifurcation having a branch that is much shorter than an empirically determined threshold length is eliminated.

Two endings on a very short isolated line are eliminated because this line is likely due to noise. Two endings that are closely opposing are eliminated because these are likely to be on the same ridge that has been broken due to a scar or noise or a dry finger condition that results in discontinuous ridges. Endings at the boundary of the fingerprint are eliminated because they are not true endings but rather the extent of the fingerprint in contact with the capture device. Feature attributes are determined for each valid minutia found [4]. These fingerprint enhancement and feature extraction is performed as the same for both enrollment and authentication process.

##### C. Fingerprint Classification

The extracted feature of fingerprint is accepted by the classifier to maintain separately according to the pattern type such as right loop, left loop, whorl and arch. The system uses the combination of Henry classifier at enrollment stage and Naive Bayes classifier at authentication stage. By using Henry classification system [2], fingerprint images are classified into four classes such as Right Loop, Left Loop, Whorl and arch. During

## Fingerprint Authentication System using Hybrid Classifiers

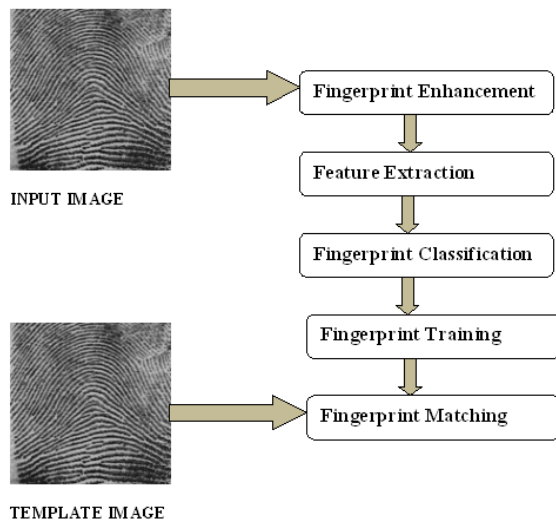


Figure 4: Basic steps involved in Fingerprint Authentication System.

Authentication process, Naive Bayes classifier is involved for training and matching process of fingerprint by using bayes theorem [12].

### a) Henry Classification Process

Normally the fingerprints are classified as Whorl, arch and loop. The Henry classification system [19] classified fingerprint images into five classes (Henry classes) such as Right Loop, Left Loop, Whorl, arch and tented arch. Since the 65% of people having fingerprint with loop domain, the system further divides this loop domain into two parts i.e. left loop (32% apx.) and right loop (33% apx) , whorls are nearly 30%, and perhaps 5% are arches [3]. Therefore, there is no need of assigning separate class for tented arch. The fingerprint image of tented arch should keep under arch classes in the database. So, the system has only four different domains i) Left-Loop ii) Right-Loop iii) Whorl and iv) Arch as shown in figure 3. Correspondingly, the database is divided into four domains to improve the retrieval speed of image during authentication and also improve consistency because of having subset of database [15]. During enrollment process, Henry classification system [2] classifies the human fingerprint image and keeps those fingerprints as template in database according to the prescribed pattern classes.

When the system has four classes rather than five classes, then the system would improve that performance with accuracy and consistency measures [15]. After classification (discussed in [19]) the input template will be stored in appropriate domain. Generally, the database contains the fingerprint templates in an ordinary manner. But, here, the database contains the different set of templates according to classification in the proposed system.

### b) Naive Bayes Classifier (NBC)

During authentication process, NBC accepts the extracted feature as input vector(x) after the enhancement and feature extraction process.

In general, The problem of fingerprint recognition is to associate classes  $w_i$ ,  $i = 1, \dots, N_c$ , where  $i$  is number of

classes(i.e., here,  $i=4$ ). The NBC in this system allows one of distinct approach which has the following steps:

Table 2: Algorithm of FPAS for Fingerprint classification

- ii) Given a input feature vector  $x$  , Establish a training set  $\{x^{(j)}, w_i^{(j)}\}$ ,  $j = 1, 2, \dots, N_t$  for each class  $w_i$ , where  $i$  and  $j$  are number of classes and training samples respectively.
- ii) Compute a priori information such as probabilities for each class  $P(w_i)$  , feature vector  $p(x)$  and probability density function  $p(x|w_i)$  .
- iii) Determine the posterior probability by using,
 
$$P(w_i | x) = \frac{p(x|w_i)P(w_i)}{p(x)}$$
- iv) Repeat for all possible classes and choose that which class  $w_i$  gives the highest probability.
- v) Decide that class  $w_i$  as the expected class in which the given input feature vector  $x$  belongs to that class.

In this classification process, the NBC can find the correct class to which extracted input feature is associated. For instance, assume that input feature vector is whorl domain; NBC can determine the whorl class to which the input pattern searches the template for match. To accomplish this task, NBC follows the algorithm (shown in Table 2, which is expanded from the algorithm prescribed in Table 1) and computes probability for both input pattern and each template associated with classes to identify which class has higher probability. A class with higher probability (higher similarities) is selected as an expected class which contains feature related to input fingerprint image.

This classification process is described according to the bayes theorem as follows:

Consider the input feature vector  $x$  value is obtained by the feature extraction process. The problem of fingerprint recognition is to associate classes as  $w_i$ ,  $i = 1, \dots, N_c$  , where  $N_c$  is the number of classes The probabilities for each class  $P(w_i)$  and input feature vector  $p(x)$  are calculated by using bayes rule. To find the conditional probability  $P(w_i | x)$ , NBC can determine the mean ( $\mu_i$ ), variance ( $\sigma$ ) and probability density function  $p(x|w_i)$  [12] by using training set at training process. These steps(i-iii) is to be repeated for all possible classes and choose that which gives the highest probability.

The probability density function for feature vector  $p(x|w_i)$  can be calculated only from the training set. These probability density functions have same variance  $\sigma$  with different means  $\mu_1$  and  $\mu_2$  and it can be established by using:

$$p(x|w_i) = \frac{1}{\sqrt{2\pi\sigma}} \exp \left\{ -\frac{1}{2} \left( \frac{x - \mu_i}{\sigma} \right)^2 \right\} \quad (4.1)$$

Where  $i=1, 2, 3, 4$

Once the various densities have been computed, an application of Bayes theorem yields the required  $P(w_i | x)$  via,

$$P(w_i | x) = \frac{p(x|w_i)P(w_i)}{p(x)} \quad (4.2)$$

Where,  $i=4$  and  $p(x)$  is the unconditional density function which can also be computed from the training set.

Assume that there is two classes, then the Bayes theorem [] shows that if  $P(w_1|x) > P(w_2|x)$  implies,

$$\frac{p(x|w_1)P(w_1)}{p(x)} > \frac{p(x|w_2)P(w_2)}{p(x)} \quad (4.3)$$

so using the fact that  $P(w_1) = P(w_2)$  yields,

$$P(w_1|x) > P(w_2|x) \Rightarrow p(x|w_1) > p(x|w_2) \quad (4.4)$$

and this allows a decision rule[12],

Choose  $w_1$  if  $p(x|w_1) > p(x|w_2)$  otherwise choose  $w_2$  which is based only on p.d.f.s calculated from the training set.

NBC is the probabilistic method to classify the fingerprint images by comparing probability of input vector  $P(x)$  with associated class probability  $P(w_i)$ . When a class  $w_i$  has highest probability among four kind of classes conditioned on  $P(x)$ , then the classifier decides that given input vector  $x$  belongs to that class.

#### D. Training

The training process is performed before the NBC classification due to calculate the conditional probability  $P(w_i | x)$  which requires mean ( $\mu_i$ ), variance ( $\sigma$ ) and probability density function  $p(x|w_i)$  [16]. NBC can establish a training set for each class to which the input feature vector searches the template for match. It is assumed throughout that training data is available i.e. a sequence of feature vectors  $x^{(j)}$ , the number of training samples  $j = 1, 2, \dots, N_t$  are known, together with the correct class for each vector  $w_i^{(j)}$ , then NBC establish the training set  $\{x^{(j)}, w_i^{(j)}\}$ ,  $j = 1, 2, \dots, N_t$ . This allows the construction of the conditional probability density function (p.d.f.)  $p(x|w_i)$  which specifies the probability of expected feature vector  $x$  can arise from a class  $w_i$ [12].

#### E. Matching

The Bayes theorem is also used to match [16] whether the given input feature vector is equivalent to template vector by using Table. 3.

**Table 3:** Algorithm of FPAS for Fingerprint Matching

- i) Given a input feature vector  $x$  and template feature vectors  $y_j$ , Establish a training set  $\{x^{(k)}, y_j^{(k)}\}$ ,  $k = 1, 2, \dots, N_f$ , where  $j$  and  $k$  are number of template vectors and features per template vector respectively.
- .ii) Compute a priori information such as probabilities for each template vector  $P(y_j)$ , feature vector  $p(x)$  and probability density function  $p(x|y_j)$ .
- iii) Determine the posterior probability by using,
 
$$P(y_j | x) = \frac{p(x|y_j)P(y_j)}{p(x)}$$
- iv) Repeat for all possible template vector and choose that which template vector  $y_j$  gives the highest probability.
- i) Decide that template vector  $y_j$  as the expected template vector which is matched with the given input feature vector  $x$ .

The same algorithm (described in Table 1) is modified for matching process. NBC can determine whether the desired template exist on database by using this algorithm. In classification, desired class is obtained, within that class; NBC can determine which template [12] is matched to the input feature vector. The same procedure is used to find the

template. By finding conditional probability  $P(y_j | x)$ , NBC can obtain the template.

Consider the same input feature vector  $x$  and the template feature vectors  $y_j$  of the associated classes is found by classification procedure. The probabilities for each template vector  $P(y_j)$ , feature vector  $p(x)$  and probability density function  $p(x|y_j)$ , as in (4.1) are calculated to find the conditional probability  $P(y_j|x)$  by using training set  $\{x^{(k)}, y_j^{(k)}\}$ ,  $k = 1, 2, \dots, N_f$ , where  $j$  and  $k$  are number of template vectors and features per template vector respectively. These steps(i-iii) is to be repeated for all possible template vectors and choose that which gives the highest probability.

Once the various densities have been computed, Bayes theorem can determine the posterior probability by using,

$$P(y_j | x) = \frac{p(x|y_j)P(y_j)}{p(x)} \quad (4.5)$$

where,  $j$  is number of template vector.

If  $P(y_n | x)$  is highest probability, then the classifier decides that input feature vector  $x$  is matched with  $n^{\text{th}}$  template feature vector  $y_n$ , where  $1 \leq n \leq j$ .

All features must be present in training samples for the calculation of class statistics and feature projection [16]. It should be pointed out that substituting a mean class feature value to the missing feature on training samples would match and also flatten the shape of the cluster for that class in the feature space. In particular, the variance along the dimension of missing feature would be smaller than expected value when the "real" feature value is available.

The Naive Bayes classifier is designed for use when features are independent of one another within each class. It is used for fast retrieval of image and to match with appropriate image of corresponding classes by establishing training set for each class. This process is to be fast and more efficient especially even when the database stored more than lakhs of templates.

#### V. PERFORMANCE ANALYSIS

The NBC can improve the performance features like retrieval speed, consistency and accuracy. The Bayes classifier can improve the consistency because of maintaining different subset of database according to the prescribed classes. Hence, there is no need to search among all kinds of images exist in single set of database. This will improve the retrieval speed of the image from database [1].

When the Bayes classifier works with number training samples and the associated templates, then it delivers better accuracy than other existing classifier [16]. The identification rate is the percentage of test fingerprints which are correctly classified according to their nominal fingerprint patterns [14]. Since the speed of Bayes classification does not depend on the number of training samples per finger, one can capture many instances of the same finger to make effective training process.

#### VI. CONCLUSION

This paper has proposed two effective classifiers for fingerprint classification which do not require core and delta information and which have been designed to work on high

retrieval speed, consistency and accuracy. The combination of classifiers described here produces significantly better results than any of the other classifiers.

The Performance for this Henry system is comparable to the performance of continuous classifiers and extensions are investigated to adapt the methods for non-Henry and continuous classification.

This fingerprint authentication system can be employed in any real time security applications such as bank ATM, personal computer login, email login( any network services), welfare association and other kind of civilian purposes.

The limitation of the proposed system is that it does not perform particularly well with a single genuine sample per finger. It is probably an excellent choice only when more training samples are available. Bayes classifier increases the little complexity of training the samples to recognize the fingerprint.

### REFERENCES

- [1] K. C. Leung and C. H. Leung, "Improvement of Fingerprint Retrieval by a Statistical Classifier", IEEE Transactions on Information Forensics And Security, Vol. 6, No. 1, March 2011 ,Pp 59 -69.
- [2] Chander Kant & Rajender Nath , "Reducing Process-Time for Fingerprint Identification System", International Journals of Biometric and Bioinformatics, Vol.3, Issue (1).
- [3] Jinwei Gu, Jie Zhou, and Chunyu Yang, "Fingerprint Recognition by Combining Global Structure and Local Cues", IEEE Transactions on Image Processing, vol. 15, no. 7, pp. 1952 – 1964, 2006.
- [4] Ravi. J, K. B. Raj, Venugopal K. R, "Fingerprint Recognition Using Minutia Score Matching", International Journal of Engineering Science and Technology, Vol.1 (2), 2009, 35-42.
- [5] Mary Lourde R and Dushyant Khosla, "Fingerprint Identification in Biometric Security Systems", International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010 ,1793-8163.
- [6] Monowar Hussain Bhuyan, Sarat Saharia, and Dhruva Kr Bhattacharyya, "An Effective Method for Fingerprint Classification", International Arab Journal of e-Technology, Vol. 1, No. 3, January 2010.
- [7] Heeseung Choi, Kyoungtaek Choi, and Jaihie Kim, "Fingerprint Matching Incorporating Ridge Features with Minutiae", IEEE Transactions on Information Forensics And Security, Vol. 6, No. 2, June 2011.
- [8] M. R. Girgisa, A. A. Sewisyb and R. F. Mansourc, "Employing Generic Algorithms for Precise Fingerprint Matching Based on Line Extraction", Graphics, Vision and Image Procession Journal, vol. 7, pp. 51-59, 2007.
- [9] Luping Ji, Zhang Yi, "Fingerprint Orientation field Estimation using Ridge Protection", The Journal of the Pattern Recognition, vol. 41, pp. 1491-1503, 2008.
- [10] Alessandra Lumini, and Loris Nann, "Advanced Methods for Two-Class Pattern Recognition Problem Formulation for Minutiae-Based Fingerprint Verification", Journal of the Pattern Recognition Letters, vol. 29, pp. 142-148, 2008.
- [11] Sheng Li and Alex C. Kot, "Privacy Protection of Fingerprint Database", IEEE Signal Processing Letters, Vol. 18, No. 2, February 2011
- [12] Keith Worden, Statistical Pattern Recognition, (lecture notes), September 2008.
- [13] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar. Handbook of Fingerprint Recognition. (Springer- Verlag,2003).
- [14] Lawrence O ' Gorman, Veridicom Inc., Chat ha m, NJ, Overview of fingerprint verification technologies, (Elsevier Information Security Technical Report, Vol. 3, No. 1, 1998).
- [15] Salil Prabhakar, Fingerprint Classification and Matching Using a Filterbank, Computer Science & Engineering, doctoral diss., Michigan State University,2001.
- [16] Ludmila I. Kuncheva, *Combining Pattern Classifiers Methods and Algorithms*, Bangor, Gwynedd, United Kingdom, September 2003.

- [17] F.A. Afsar, M. Arif and M. Hussain, Fingerprint Identification and Verification System using Minutiae Matching, National Conference on Emerging Technologies 2004.
- [18] Mohamed. S. M and Nyongesa.H, Automatic Fingerprint Classification System using Fuzzy Neural techniques, IEEE International Conference on Artificial Neural Networks, vol. 1, pp. 358-362, (2002).
- [19] The Henry Fingerprint Classification System, Available: [www.namus.gov](http://www.namus.gov).



**Parvathi R** is pursuing Ph.D (Part time) in Anna University, Chennai. She is working as Assistant Professor in PSNA College of Engineering and Technology, Dindigul, Tamilnadu. She is the member of IAENG. Her interests are biometrics, image processing and network security.



**Sankar M** is working as Assistant Professor in RVS College of Engineering and Technology, Dindigul, Tamilnadu. He is a member of ISTE and IAENG. He is interested in image processing and power electronics.