An Efficient Approach to Improve Response Time in Multibiometric Patterns Retrieval from Large Database

S.Balgani#, S.Sangeetha*,
#Department of Computer Science and Engineering, V.S.B Engineering College

Abstract
Biometric technologies are automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioural characteristics. In a biometric identification system, the identity corresponding to the input data (probe/investigation) is typically determined by comparing it against the templates of all identities in a database (gallery).Exhaustive/in-depth matching against a large number of identities increases the response time of the system and may also reduce the accuracy of identification. One way to reduce the response time is by designing biometric templates that allow for rapid matching. An alternative approach is to limit the number of identities against which matching is performed based on criteria that are fast to evaluate. In the Existing system the search space is reduced by partitioning the database into several bins. Following such binning, the biometric database will be partitioned such that the templates in each bin are similar and correspond to some natural or statistical class. In case of the traditional 1: N comparisons for identification, the time needed for the system would be to determine the distance between the test template and the N templates in database. Thus the total time needed in such a case could be given as: Q (N). The proposed work focuses on reducing the search space using Gittins index algorithm and also improves the accuracy of identification.

Keywords
Biometrics, feature extraction, image retrieval, indexing, pattern matching

1. Introduction

Biometric recognition, or simply biometrics, is the science of establishing the identity of a person based on physical or behavioural attributes. It is a rapidly evolving field with applications ranging from securely accessing one's computer to gaining entry into a country. While the deployment of large-scale biometric systems in both commercial and government applications has increased the public awareness of this technology [10].Biometrics is playing a major role in all over the world in automated personal identification systems deployed to enhance security. The characteristics of human beings may vary from one person to another. This property is used by the Biometric technology to distinctly identify each person. Biometric system is essentially a pattern recognition system which recognizes a user by determining the authenticity of a specific physiological or behavioural characteristic possessed by the user. Several important issues must be considered in designing a practical biometric system [1].First a user must be enrolled in the system so that his biometric template can be captured. This template is securely stored in a central database or a smart card issued to the user. The template is retrieved when an individual needs to be identified. Depending on the context, a biometric system can operate either in verification (authentication) or an identification mode. In biometry, there are two types of biometric methods. One is called behavioural biometrics. It is used for verification purposes. Verification is determining if a person is who they say they are. This method looks at patterns of how certain activities are performed by an individual. Physical biometrics is the other type used for identification or verification purposes. Identification refers to determining who a person is. This method is commonly used in criminal investigations [1]. In the recent years, a number of recognition and authentication systems based on biometric measurements have been proposed. Algorithms and sensors have been developed to acquire and process many different biometric traits. Moreover, the biometric technology is being used in novel ways, with potential commercial and practical implications to our daily activities [9].

2. RELATED WORK

The retrieval of a small number of candidate identities from a database based on the probe data is known as database filtering. Filtering can be accomplished by using classification or indexing schemes. In a classification scheme, identities in the database are partitioned into several classes. Only the identities belonging to the same class as that of the probe image are retrieved during the search process for further comparison. Clustering is the classification or partitioning of data into subsets or clusters, so that data in each subset share certain properties. Data clustering is a common statistical analysis tool used in different fields like image analysis, pattern recognition and machine learning.

Manuscript received May 5, 2014
Manuscript revised May 20, 2014

A.Fingerprint Indexing

If the training samples used to design a classifier are labeled by their class membership, the partitioning technique is called supervised clustering. However if a collection of unlabeled samples have to be partitioned, the partitioning technique is called unsupervised clustering [2].
K-means algorithm is an unsupervised clustering algorithm to cluster objects into K partitions based on their attributes [2]. The goal is to determine the K-means of data generated from Gaussian distributions-means algorithm tries to minimize the total intra class variance or the squared error function E,where there are K clusters C_i, i=1,2……..k and μ_i is the centroid of all the points X j in cluster G.

B.Face Indexing

Indexing methods for face databases usually focus on a specific recognition algorithm. The approach of Lin et al proposes an efficient indexing structure for searching a human face in a large database [3].

The approach is based on the classical eigenface method and uses the coefficients of projection to rank the database images with respect to each eigenface .The probe is ranked in the same way and a local search is performed foe each eigenface to find the database image that is closest to the probe.Takacs propose a face similarity measure derived as a variant of the Hausdorff distance by introducing the notion of a neighborhood function (N) and associated penalties (P)[4].Torralbaet al implement machine learning techniques to convert the Gist descriptor (a real valued vector that describes orientation energies at different scales and orientations within an image) to a compact binary code, with a few hundred bits per image[5].

3. EXISTING SYSTEM

The search space can be reduced by partitioning the database into several bins. Following such binning, the biometric database will be partitioned such that the templates in each bin are similar and correspond to some natural or statistical class. In general, a biometric template *Xi* can be represented as a *k* dimensional vector [x1, x2… xk].In case of the traditional 1: N comparisons for identification, the time needed for the system would be to determine the distance between the test template and the N templates in database. Thus the total time needed in such a case could be given as: Q (N) [6] . Using the binning approach, when a test template is to be identified, we have to simply find the C closest bins in which a probable match for the test template could be. To achieve this, we initially have to find the distance of the test template from all the bin centers. Furthermore, obtaining the C closest bin centers could be achieved in a single scan, needing at most C ´ M number of comparisons. Thus the time complexity for determining the C closest bins could be given by Q (C´M). Further, the above analysis was done assuming a uniform distribution for all the bins. Even in the usual case of skewed distribution within the bins, the factor C´ Q(AM) could be replaced by Q(PSYS´ N) , in which case too our analysis of the time requirement would hold true since PSYS´ N < N[14]. It is to be noted that vector representation may not be applicable to temporal biometric templates such as those found in speech and signature. In such situations, Fourier Transform or discrete cosine transform (DCT) may be better used to obtain a vector representation. The FAR of a modality is limited by the recognition algorithm and cannot be reduced indefinitely if we are to accommodate any level of intra-user variance. Thus, a more practical approach to improve the speed and accuracy a biometric identification system is by reducing the number of records against which matching is performed during a query. This requires that the records in the database be classified, partitioned and indexed in some manner. Then the resulting FAR, FRR values and total number of false accepts are reduced [6].

4. PROPOSED SYSTEM

1. Dataset Preprocessing:

In the dataset preprocessing the images of face and finger print are collected and stored in the database .For face images we use dataset from FERET and the FRGC and fro finger print images we use WVU fingerprint database. There are 1195 subjects with frontal face images in the FERET database. We use only 1010 of these subjects because the images of the remaining 185 subjects could not be processed The WVU fingerprint database contains images of 4 different fingers (left index, left thumb, right index, right thumb) from 270 subjects. We treated the individual fingers as independent “subjects,” resulting in a total of 1080 subjects.

2. Generation of Index codes for all the Images:

The index code of an image is the list of its match scores against the reference images. An image is taken and it is matched with the set of reference images already stored in the database. So as compared to the number of reference images the index codes varies the reference images may be viewed as “basis” vectors in the original feature space. If two images ,the input and reference images are similar then their values are expected to be lesser than the

threshold ,where the threshold is set before processing ,if the C values are greater than threshold it is assumed that the two images belongs to different individuals.
During identification, the indexing system first computes the index code S of the probe. Then it outputs all enrolled identities whose index codes are within a certain distance from S. The index codes are generated from both face and Fingerprint Images .

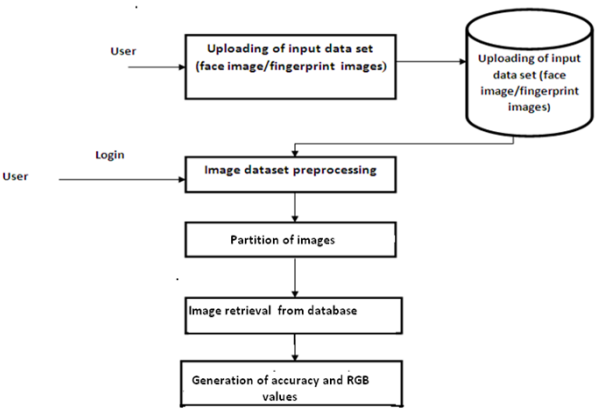

Fig 1 Architecture diagram for proposed system

3. Input Image Clipping Processing:

Clipping refers to any procedure which identifies the portion of a picture which is either inside or outside a region using any clipping algorithm. The region against which an object is to be clipped is; called clipping window. Clipping is a process of capturing or processing an image where the intensity in a certain area falls outside the minimum and maximum intensity which can be represented.

In the input image clipping process, the input image is partitioned into several patches and each patch will search for corresponding matches in database. If any match is found then RGB and colour code value is generated for that image.

4. Selecting the reference Image and retrieving the Image:

Reference images can be selected from the database itself. They can also be synthetically generated images. While the entire database can be viewed as a candidate pool for selecting reference images, practical considerations dictate the use of a small random subset of images for this purpose.

5. RESULTS

Fig 2 Face Input Image

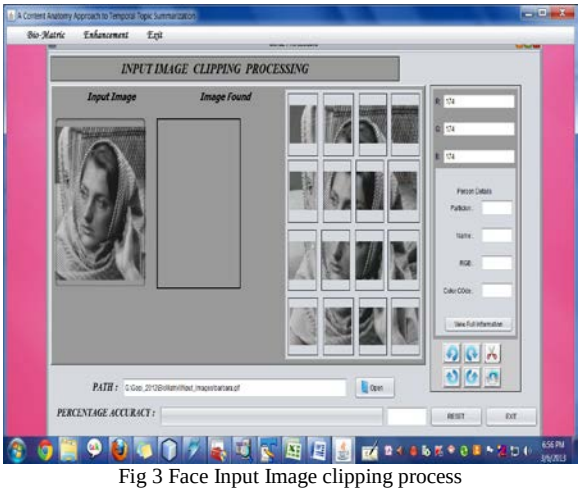

Fig 3 Face Input Image clipping process

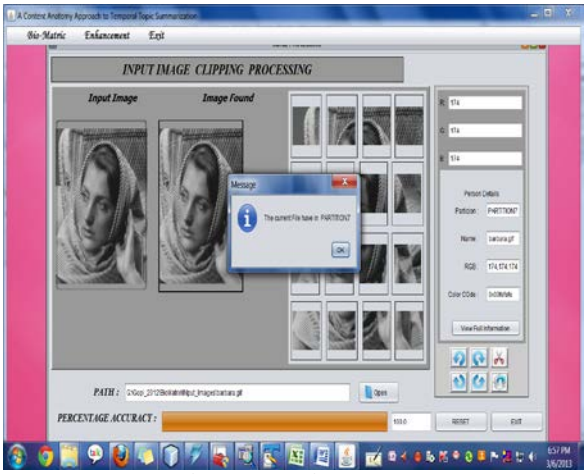

Fig 4 Display of Input Image from partitioned Database

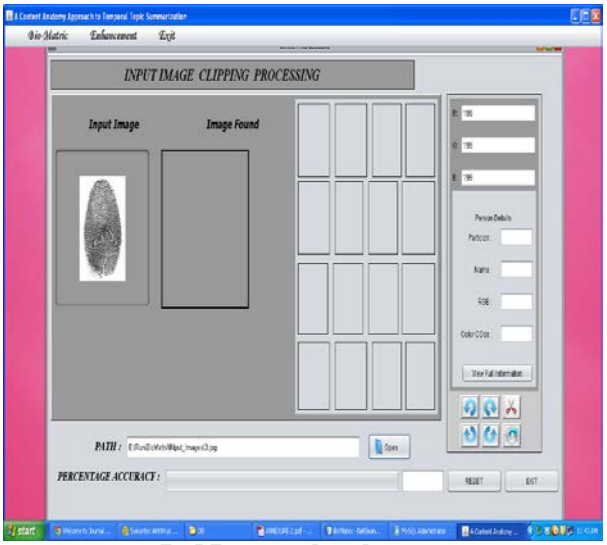

Fig 5 Fingerprint Input Image

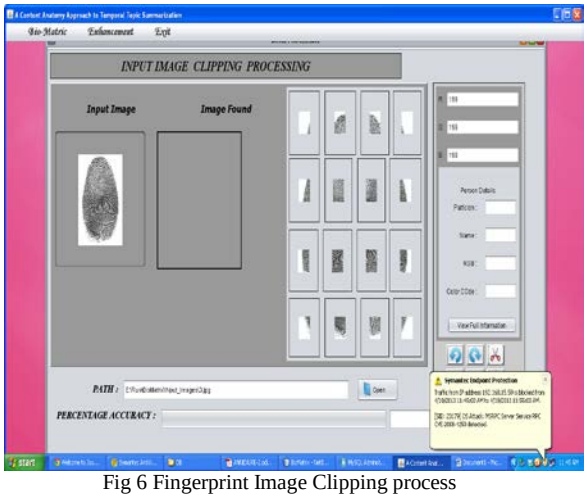

Fig 6 Fingerprint Image Clipping process

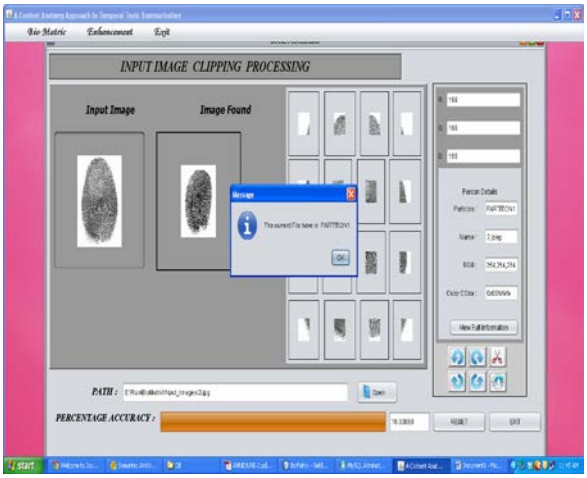

Fig 7 Display of Input Fingerprint Image from partitioned Database

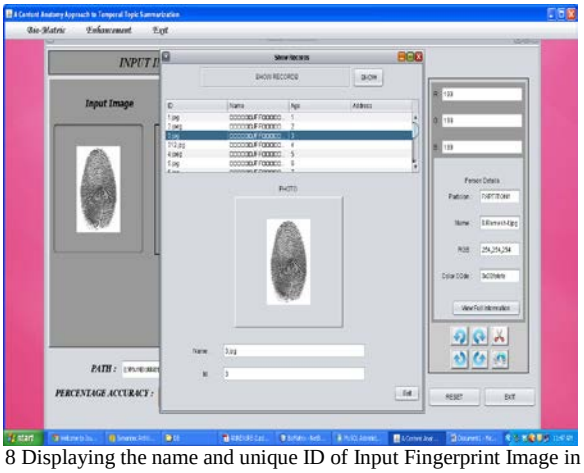

Fig 8 Displaying the name and unique ID of Input Fingerprint Image in Database

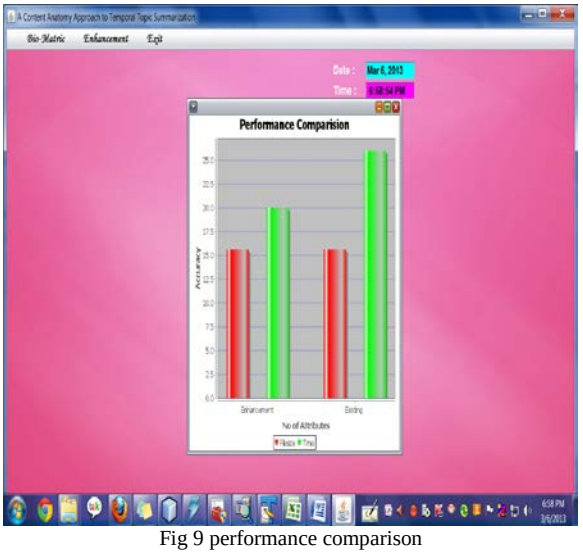

Fig 9 performance comparison

6. APPLICATIONS

Access control

Obtaining access to a secured area or system is mostly a two-step process:

- Identification, the process by which the user professes an identity by providing a username, a pin code or some other form of ID.
- Authentication, the process of verification or testing to make sure that the user is who he claims to be.

Fig 10: Mobile hard disk with fingerprint reader

Biometrics can be used for both steps, identification requiring a one-to-many search in the templates database and authentication a one-to-one comparison of the measured biometric with the template that is associated to the claimed identity.

There exist three types of authentication factors: *something you know* (e.g. password), *something you have* (e.g. token device, badge) and *something you are*. Biometrics fall in the third category, which is by definition the most secure because most companies still struggle to implement good password practices and when token devices or badge readers are used they get lost or are shared among colleagues[8].

A lot of commercial, biometric access control solutions are available, and many more are in development.

- Access control to computer systems (workstations): USB fingerprint readers, voice and face recognition software using standard camera and microphone hardware, etc.
- Door security: doors with biometric locks using iris recognition, fingerprint readers, etc.
- Portable media such as USB sticks and mobile hard drives with integrated biometric access control and mostly encrypting your data using a built-in algorithm.
- Safes with biometric locks.

1) Time and attendance management

The problems with time registration and attendance management are very similar to those encountered with access control. Nowadays most systems identify employees with a pin code or a badge. In practice employees loose their badge or forget their pin code, even worse some employees let collegues who arrive early apply their badge or pincode to the system.

Using biometric time registration or attendance management avoids fooling and also reduces overhead for security personnel when badges are lost or pincodes forgotten. A number of commercial solutions already exists [8].

2) Surveillance

Screening large crowds for fugitive criminals or missing children, or border control in for example airports can be largely automated using biometrics. The cost of such implementations of biometrics is very high and for existing **surveillance** systems the success rates vary.

Fig 11 Fingerprint reader used for border control by the US department of Homeland Security

US-Visit program

The US department of Homeland Security applies fingerprint recognition for border control. Non-US citizens between 14 and 79 years old, entering the United States have all 10 fingerprints taken by electronic means. This is part of the US-Visit program. Fingerprints of tourists and immigrants are cross-checked with different databases to identify terrorists, criminals and illegal immigrants. In fiscal year 2007 (source: www.cis.org):

- a total of 46,298,869 entries were recorded at air and sea ports;
- 236,857 were identified as possible overstays;
- 11,685 biometric watch-list hits occured at the port of entries, these included individuals with criminal histories for crimes such as murder and drug trafficking as well as immigration violations.

Japan implemented a similar system under the name J-VIS, scanning both index fingers of foreign visitors. Also the United Arab Emmirates implemented a border control system using iris recognition.

This type of immigration and border control system is reason for much controversy. Most debate is actually on how databases, or so-called watch-lists, containing the biometrics of criminals were compiled. Also it is common believe that criminals or terrorists will find a way to pass the biometric controls unhindered.

Face recognition for surveillance

It is said that some casino's are using face recognition to automatically search the crowd for card counters and cheaters, it is unknown whether they are successful with this or not.

Face recognition was trialed in the UK; at the London Borough of Newham 250 surveillance cameras were installed to scan faces within their view. Images were compared against a database of criminals, if a match was found an alert was sent to the police. It is said, however, that not ever one criminal was arrested thanks to the system. We must add to this that the system was installed already in 1998 and that seen the technological difficulties to scan and recognize faces in a crowd it is clear that face recognition was 10 years ago not yet up to that challenge.

A more interesting way to use face recognition for surveillance is with so called facetraps. The difficulty with using surveillance camera footage is that subjects are only seldom looking directly into the camera; the resulting images are therefore difficult to process for face recognition algorithms. A facetrap is a location where a camera can be set up in such a way that the subject, without even realizing it, automatically looks directly into the camera. Examples of such locations are counters, elevators, clocks or television screens at which visitors look [8].

CONCLUSION

We presented the method of partitioning biometric databases for efficient identity retrieval..The biometric matcher that is inherent to the system can be used for generating colour codes. The search space is reduced since 1:1 comparison is made during the search process. The hit rate and penetration rate is also improved. The FAR, FRR, ERR values are also reduced. The proposed method is easy to implement and deploy and can be applied to various biometric databases which significantly improve the response time of large-scale of multimodal databases and also improves the accuracy of identification.

REFERENCES

[1] http://www.creativeworld9.com/2011/03/abstract-on-biometrics.html
[2] A.Ross, K.Nandakumar, and A. Jain, Handbook of Multibiometrics, 1st Ed. New York: Springer, 2006.
[3] K.-H. Lin, K.-M. Lam, X. Xie, and W.-C. Siu, “An efficient human face indexing scheme using eigenfaces,” in *Proc. Int. Conf. Neural Networks And Signal Processing*, Dec. 2003, vol. 2, pp. 920–923.
[4] B. Takács, “Comparing face images using the modified Hausdorff distance,”*Pattern Recognit.*, vol. 31, no. 12, pp. 1873–1881, 1998.
[5] A. Torralba, R. Fergus, and Y. Weiss, “Small codes and large image databases for recognition,” in *Proc. Conf. Computer Vision and Pattern Recognition*, 2008, pp. 1–8.
[6] A. Mhatre, S. Palla, S. Chikkerur, and V. Govindaraju, “Efficient search and retrieval in biometric databases,” *Biometric Technol. Human Identification II*, vol. 5779, no. 1, pp. 265–273, 2005
[7] A. Gyaourova and A. Ross, “A coding scheme for indexing multimodal biometric databases,” in *Proc. IEEE Computer Society Workshop on Biometrics at the Computer Vision and Pattern Recognition (CVPR) Conf.*, Miami, FL, Jun. 2009.
[8] http://www.biometric solutions.com/applications/index.php
[9] http://www.intechopen.com/books/recent-application-in-biometrics
[10] http://books.google.co.in/books/about/Introduction_to_biometrics.html?id=ZPt2xrZFtzkC&redir_esc=y
[11] Wen-Ying Ma,Nanjing Univ,of posts & telecommun,Nanjing,china sheng Li;Yong-Fang Yan;chao Lan;shi-Qiang Gao;Hui Tang;Xiao-Yuan Jing,” Multi-Modal Biometrics Pixel Level Fusion and KPCA-RBF Feature Classification for Single Sample Recognition Problem “,Image and signal processing,2009,CISP’09.
[12] Aglika Gyaourova,Arun Ross “Index codes for Multi-biometric pattern retrieval”,IEEE transactions on information forensics and security,Vol.7,No.2,April 2012.