A SECURE EMAIL CLIENT APPLICATION USING RETINAL IMAGE MATCHING

ANKITA KANTESH[1], SUPRIYA S. BEHERA[2], JYOTI BHOITE[3], ANAMIKA KUMARI[4]

[1,2,3,4] B.E, University of Pune
E-mail: ankitadgreat0@gmail.com, supriyabehera007@gmail.com, jyoti.bhoite2491@gmail.com, anamika0288@gmail.com

Abstract- As technology advances, more and more systems are introduced which will look after users comfort. Retinal image matching is a technique that can be used in image matching for person identification or patient longitudinal study. Vascular invariant features are extracted from the retinal image and a feature vector is constructed for each of the vessel-segments in the retinal blood vessels. The feature vectors are stored in a database which maintains the vessel-segments actual hierarchical positions. Using these feature vectors, corresponding images are matched. The method identifies the same vessel in the corresponding images for comparing the desired feature or features. The application that we have developed uses advanced image processing algorithms to accurately process retinal images. In this way it is a foolproof technique and authentication can be done without any chance of failure. Thus we can see that new technologies always have more benefits and are more user-friendly.

Keyword- Retinal Image ,Vessel Bifurcation, Branch and Crossover Points, Invariant Feature, Feature Vector.

I. INTRODUCTION

Retina-scan technology makes use of the retina, which is the surface on the back of the eye that processes light entering through the pupil. Retinal Scan technology is based on the blood vessel pattern in the retina of the eye. The principle behind the technology is that the blood vessels at the retina provide a unique pattern, which may be used as a tamper-proof personal identifier. [7] Since infrared energy is absorbed faster by blood vessels in the retina than by surrounding tissue, it is used to illuminate the eye retina. Analysis of the enhanced retinal blood vessel image then takes place to find characteristic patterns. Retina-scan devices are used exclusively for physical access applications and are usually used in environments that require high degrees of security such as high-level government military needs. [8] Retina-scan technology was developed in the 1980's and is well known of all the biometric technologies.

So considering the above points, we have designed an email client application which stores the retinal images of the account holders as the password of their respective accounts in the database. This means that when a particular account holder logs in to his account, he has to provide his retinal image as his accounts password. His retina is scanned and its image is captured. The image is then compared with the images stored in the database. If both the images match, authentication is considered as successful otherwise it is considered as failed.

This will provide a high security to the account holders as well as to their data. Retina-scan technology image acquisition requires specific hardware and software.

The user positions his eye close to the unit's embedded lens, with the eye socket resting on the sight. In order for a retinal image to be acquired, the user must gaze directly into the lens and remain still. A low intensity light source is utilized in order to scan the vascular pattern at the retina. This involves a 360 degree circular scan of the area taking over 400 readings in order to establish the blood vessel pattern. This is then reduced to 192 reference points before being distilled into a digitized 96 byte template and stored in memory for subsequent verification purposes. Normally it takes 3 to 5 acceptable images to ensure enrollment. The more a user is acclimated to the process, the faster the enrollment process works. After image acquisition, software is used to compile unique features of the retinal blood vessels into a template.

Retina-scan technology possesses robust matching capabilities and is usually configured to do one-to-many identification against a database of users.

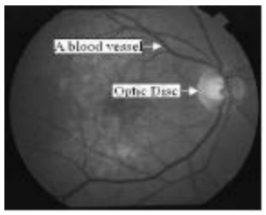
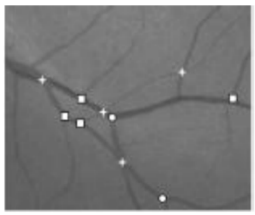


Fig. (a)


Fig. (b)

Retinal image matching methods for person identification in the main, register images after vessel segmentation, or match bifurcation or branch points in the corresponding images [1],[2]. In the first approach, retinal blood vessels are used as the

biometric parameter, with a prior registration stage needed to align the template image and the acquired image. The second approach segments the blood vessels from the image and computes the bifurcation/branch and crossover points (Fig a). Vascular bifurcation/Vascular branch and crossover points are defined as follows. Vascular bifurcation splits a vessel into two vessels. We can define a branch as a new vessel formation where a minor (smaller width) vessel grows or comes out from a major (wider) vessel. A crossover is defined as a region where two vessels (major or minor) cross each other. Overall, bifurcation/branch and crossover point geometry provide higher degree in generating unique pattern for an individual person. At present, retinal vascular bifurcation and branch points are considered as the same parameter for image matching applications.

Classified bifurcation and branch points can add higher degree in the uniqueness of the retinal vascular pattern. Considering these issues, we propose an automatic retinal image matching method, which has high potential for and biometric security application. The method uses retinal vascular bifurcation, branch and crossover points as features to match the images.

II. CURRENT METHODOLOGY

For disease prediction or clinical trial, the most widely used approach is to take person's retinal image as shown in above (Fig. b) within a time interval and compare these images to observe the change(s) in the vascular features [4],[3]. In various studies [5],[6] people have reported the effect of hypertension treatment on retinal vessel diameter and tortuosity performed on person's retinal images taken before and after medication. These studies considered mainly the manual or semiautomatic methods for image analysis that are very time consuming and expensive. Furthermore, these studies are based on analyzing a single feature which is not enough to observe multiple feature changes. None of these techniques is able to match the vascular features from two images based on vessel-segments hierarchical position, which is very important for automated patient longitudinal study.

III. PROPOSED METHODOLOGY

We have designed an email client application which stores the retinal images of the account holders as the password of their respective accounts in the database. This means that when a particular account holder logs in to his account, he has to provide his retinal image as his accounts password. His retina is scanned and its image is captured. The image is then compared with the images stored in the database. If both the images match, authentication is considered as successful otherwise it is considered as failed. The method that we have proposed for retinal scanning includes construction of a feature set that consists of Length/Width ratio, existing crossover, crossover location and acute angle between the major and minor vessel. This feature vector construction is done through the following methods:

A. Blurring
B. RGB to HSV conversion with Thresholding
C. Histogram Equalization
D. Blob Detection
E. Optic Disc detection
F. Thinning
G. Control Point Detection

The proposed method consists of 2 phases:
A. Registration phase
B. Login phase

In registration phase, the feature set of a person's retinal image is obtained through the above methods and stored in a database. In the login phase, authentication is done. Authentication is done with the help of template matching. When a person comes for authentication, the retinal image of the person is captured and compared with the images that are stored in the feature set of that particular person in the database.

If both the images match, the person is authenticated correctly, otherwise authentication is considered as failed.

IV. IMPLEMENTATION

The implementation of our email client application is done using java. The implementation procedure is described below:

A. Blurring:
In image terms blurring means that each pixel in the source image gets spread over and mixed into surrounding pixels. Blurring is done to reduce the sharpening effect. This makes the detection more accurate. In our application we are using Color Blurring.

Steps for Gray scaled blurring:
Traverse through entire input image array. Read individual pixel color value (24-bit). Split the color value into individual R, G and B 8bit values.
Separate RGB color for each pixel using.
R = col & 0xff;
G = (col >> 8) & 0xff;
B= (col >> 16) & 0xff;

Calculate the RGB average of surrounding pixels and assign this average value to it. Repeat the above step for each pixel. Store the new value at same location in output image.



Fig.(a) Fig.(b)

B. RGB to HSV Conversion & Thresholding:

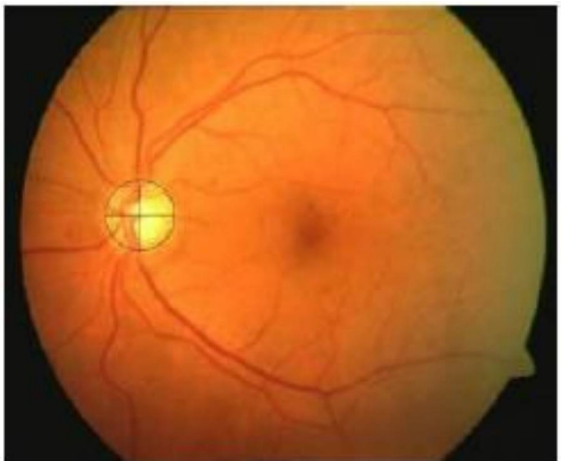
Thresholding is the simplest method of images segmentation. During the thresholding process, individual pixels in an image are marked as "object" pixels if their value is greater than some threshold value (assuming an object to be brighter than the background) and as background pixels otherwise. This convention is known as threshold above. First we convert the image from RGB to HSV. From a grayscale image, thresholding can be used to create binary images. Otsu's method is used to automatically perform histogram shape-based image thresholding, or, the reduction of a graylevel image to a binary image. The algorithm assumes that the image to be thresholded contains two classes of pixels (e.g. foreground and background) then calculates the optimum threshold separating those two classes so that their combined spread(intra-class variance) is minimal. In Otsu's method we exhaustively search for the threshold that minimizes the intra-class variance.

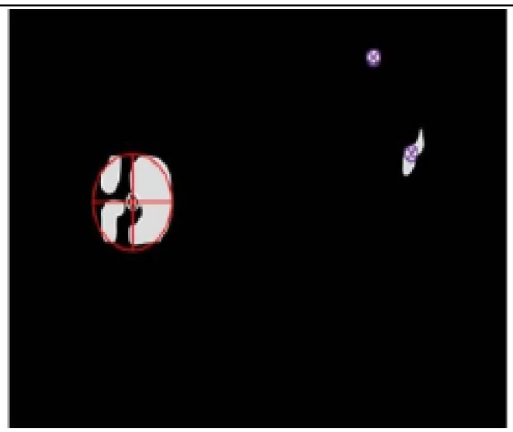


Fig. (a) Fig. (b) Fig.(c)

C. Blob Detection:

In Blob detection, we search for an area where maximum no. of pixels can be found. This maximum number of pixels is assumed to be having the optic cup part of disc and it is considered to be the primary region of interest.





D. Optic Disc Detection:

The optic disc is usually the brightest component on the fundus, and therefore a cluster of high intensity pixels will identify the optic location. We call this cluster of high intensity pixels as a blob.

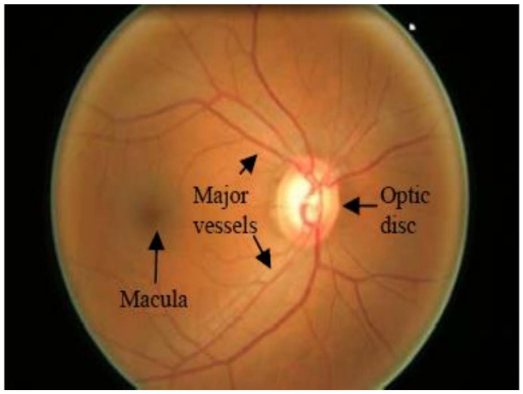


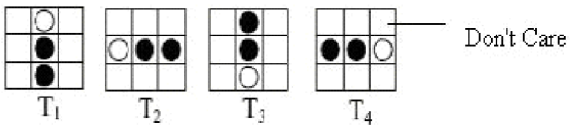
Fig. (a)

E. Thinning:

Thinning algorithm is a morphological operation that is used to remove selected foreground pixels from binary images. To explain in more simplified way thinning is a technique, which extracts the skeleton of an object as a result. Here the edge pixels having at least one adjacent background point are deleted. It preserves the topology (extent and connectivity) of the original region while throwing away most of the original foreground pixel. The skeleton represents the shape of the object in a relatively small number of pixels. Thinning works for objects consisting of lines (straight or curved). This method does not work for object having shapes that encloses a large area. For thinning we use the Stentiford algorithm, which is explained below.

Stentiford Thinning Algorithm:

It uses a set of four 3 x 3 templates to scan the image. Figure below shows these four templates.



In Stentiford algorithm we perform the following steps:

i. Find a pixel location (i, j) where the pixels in the image match those in template T1. With this template all pixels along the top of the image are removed moving from left to right and from top to bottom.

ii. If the central pixel is not an endpoint, and has connectivity number = 1, then mark this pixel for deletion.

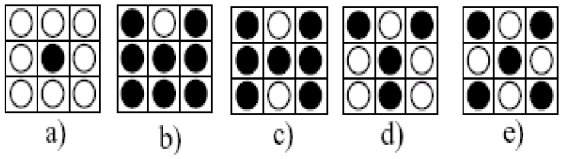
iii. Endpoint pixel: A pixel is considered an endpoint if it is connected to just one other pixel. That is, if a black pixel has only one black neighbor out of the eight possible neighbors.

iv. Connectivity Number: The Connectivity number is a measure of how many objects are connected with a particular pixel.

The following is the equation to calculate Connectivity number.

$$C_n = \sum_{k \in S} N_k - (N_k \cdot N_{k+1} \cdot N_{k+2})$$

Where: Nk is the colour of the eight neighbours of the pixel analyzed. N0 is the center pixel. N1 is the colour value of the pixel to the right of the central pixel and the rest are numbered in counter clockwise order around the center. S = {1, 3, 5, 7}



v. The following are the connectivity numbers for Figure 2.1:
   a) Connectivity number = 0.
   b) Connectivity number = 1.
   c) Connectivity number = 2.
   d) Connectivity number = 3.
   e) Connectivity number = 4.

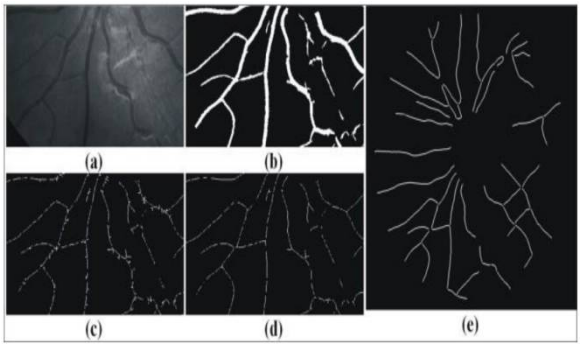
vi. Repeat steps 1 and 2 for all pixel locations matching T1.

vii. Repeat steps 1-3 for the rest of the templates: T2, T3, and T4.

viii. T2 will match pixels on the left side of the object, moving from bottom to top and from left to right. T3 will select pixels along the bottom of the image and move from right to left and from bottom to top. T4 locates pixels on the right side of the object, moving from top to bottom and right to left.

ix. Set to white the pixels marked for deletion.

Figure below shows some examples of the thinning process using the Stentiford Algorithm.



F. Control Point Detection:

After the Thinning process is over, control point detection is done. Vascular invariant features are extracted from the retinal image and a feature vector is constructed for each of the vessel-segments in the retinal blood vessels. These features include: Length to Width ratio(Length/Width), Bifurcation or Branch point, Existing Crossover, Crossover Location, etc.

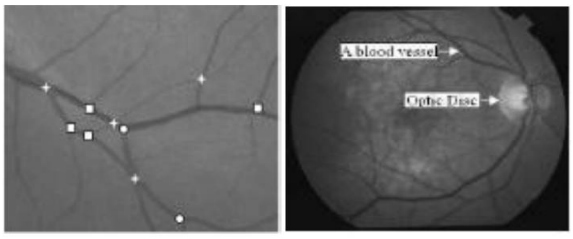


Fig. (a)

G. Template Matching:

Template matching is a technique in digital image processing for finding small parts of an image which match a template image.



Fig. (a) Fig. (b)

CONCLUSION

In this paper we have described a novel approach for securing the email application by using retinal image matching. Initial results suggest that the method is very accurate in matching the retinal images and finding the corresponding blood vessels. At present we are acquiring multiple images for the same person

to enable a large scale study and further validation of the method. Thus we have designed a mailbox in which the password will be the unique retinal image of the account holder, which will validate the user and prove his/her identity once the image is matched. This method has proved to be the most secure method where the user need not worry about the hackers, as the passwords use for various mailboxes, contains characters, numbers, that are very easy to hack. This is not the case with the retinal image matching method of authentication, and the hacker has to think several times before hacking it.

REFERENCES:

[1] Marino, C., Penedo, M. G., Penas, M., Carreira, M. J., and Gonzalez, F. (2006). Personal authentication using digital retinal images. Pattern Analysis Application, 9:21–33.

[2] Harris, A. J. and Yen, D. C. (2002). Biometric authentication: assuring access to information. Information Management and Computer Security, 10(1):12–19.

[3] Abrahams, I.W. and Gregerson, D. S. (1983). Longitudinal study of serum antibody responses to bovine retinal santigenin endogenous granulomatous uveitis. British Journal of Ophthalmology, 67:681–684.

[4] Stanford, M. R., Graham, E., Kasp, E., Sanders, M. D., and Dumonde, D. C. (1988). A longitudinal study of clinical and immunological findings in 52 patients with relapsing retinal vasculitis. British Journal of Ophthalmology, 72:442–447.

[5] Hughes, A. D., Stanton, A. V., Jabbar, A. S., Chapman, N., Martinez-Perez, M. E., and Thom, S. A. (2008). Effect of antihypertensive treatment on retinal microvascular changes in hypertension. Journal of Hypertension, 26:1703–1707.

[6] Taarnhoj, N. C. B. B., Munch, I. C., Sander, B., Kessel, L., Hougaard, J. L., and Kyvik, K. (2008). Straight versus tortuous retinal arteries in relation to blood pressure and genetics. British Journal of Ophthalmology, 92:1055–1060.

[7] Julian Ashbourn. (2002), Biometrics: Advanced Identity Verification, London: Springer-Verlag, p. 55.

[8] Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 106.

★★★