ISSN:0975-9646

A Note on Authentication Accuracy with Multiplicity of Biometric Images

Mohammed Aamir Ali T and Varun Kumar M
School of Information Technology and Engineering
VIT University, Vellore, Tamil Nadu, India.

Abstract- This project cum paper we have implemented basically deals with authentication and the various improvements that can be brought about by integrating them with real time scenarios. Our basic aim of it to implement is to develop a secure environment that cannot be breached easily. There are many applications or algorithms that provide authentication at the finest level but we are a step ahead I believe because of the uniqueness of the idea and effort put behind it. Let me give you a brisk knowledge of what we have done with it "by increasing the number of biometric images for authentication, authentication accuracy is expected to be improved". This paper considers simple algorithms for verification and identification with multiple biometric images for each person.

INTRODUCTION

Personal authentication has been an essential issue in many social infrastructure systems. Biometric authentication has attracted attention as a technology to compensate some weaknesses of token- and knowledge-based authentication. With the spread of computers and networks, the scope of applications of personal authentication was extended into a wide area, and the number of persons who use each application system is supposed to become huge. Especially for biometric authentication, accuracy of personal authentication becomes an important factor by the increase of the number of persons. The aim of our research is to find a way to improve accuracy of biometric authentication. One of the straightforward approaches for the improvement is increasing the amount of information for authentication such as the number of biometric images registered in an authentication system (such registered images are called "templates"). This trial to improve authentication accuracy by several biometric images can be a typical application of statistical analyses. However, in order to apply such analyses appropriately into biometric images, some knowledge of biology about the part of human beings or of image processing about the feature extraction will be required after all. We simply focus on the results of comparisons of biometric images. Our approach is on the assumption that the basic authentication with a single template for each person is conducted on the basis of the result of a comparison between the template and an inputted image, and then the effects of the number of templates on accuracy are evaluated as the change from the basic authentication. Then, we consider two simple ideas in order to treat the results of comparisons for multiple templates, that is, a majority vote and the arithmetic mean of the similarities. There exist two possible procedures of biometric authentication, that is, verification and identification. At least for identification, the effects of the number of templates for each person on accuracy are not trivial even for the simple methods to treat multiple results of comparisons. In this project cum paper, we define simple algorithms for verification and identification based on the idea of a majority vote and the mean of similarities. And then, we apply the algorithms to practical palm print images in order to examine the error rates as accuracy of authentication. In order to measure the similarity of two images, we consider the matching of the features extracted by Scale-Invariant Feature Transform (SIFT). There already exist some researches that apply SIFT to authentication with biometric images such as fingerprints and palm prints. Additionally, it is expected to be applicable to general comparison based authentication algorithms with multiple biometric images.

WORKING

This section defines working of our proposed system and how algorithms are devised for image matching which being an essential part our research.

PROFILE VECTORS

The proposed system creates user profile as follows-

Master vector – (User ID, Sound Signature, and Tolerance)
Detailed Vector – (Image, Click Points)
As an example of vectors
Master Vector - (Varun, Dolphine.wav, 10)
Detailed Vector - **Image Click points**

I1	(123,678)
I2	(176,134)
I3	(450,297)
I4	(761,164)

Enter User ID and select one sound frequency which we intend to play at the time of login, then a tolerance value is also selected which will decide if the user is legitimate or an imposter. To create a detailed vector the user has to select a point on the image and get its (x, y) co-ordinates using getClickpoints function and upon which another image is uploaded and similar steps are to followed in order to upload more and more images thus improving and increasing the layers of security for authentication. Thus the profile vector is created.

SYSTEM TOLERANCE

After creation of the login vector, system calculates the Euclidian distance between login vector and profile vectors stored. Euclidian distance between two vectors **p** and **q** is given by-Above distance is calculated for each image if this distance comes out less than a tolerance value D. The value of D is decided according to the application. In our system this value is selected by the user.

CUED CLICK POINTS

Cued Click Points (CCP) is a proposed alternative to Pass Points. In CCP, users click one point on each of c = 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging, as we discuss later. As shown in Figure 1, each click results in showing a next-image, in effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point 4 Cued Click Points dictates the next image. If they dislike the resulting images, they could create a new password involving different click-points to get different images.

We envision that CCP fits into an authentication model where a user has a client device (which displays the images) to access an online server (which authenticates the user). We assume that the images are stored server-side with client communication through SSL/TLS.

For implementation, CCP initially functions like Pass Points. During pass- word creation, a discretization method is used to determine a click-point's tolerance square and corresponding trellis. For each click-point in a subsequent login attempt, this grid is retrieved and used to determine whether the click-point falls within tolerance of the original point. Fig. 1. CCP passwords can be regarded as a choice-dependent path of images

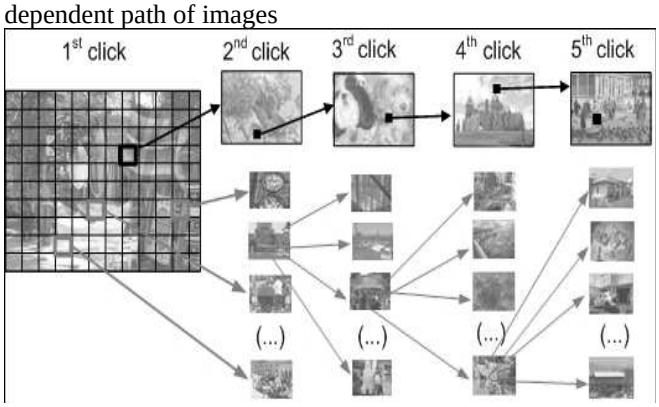
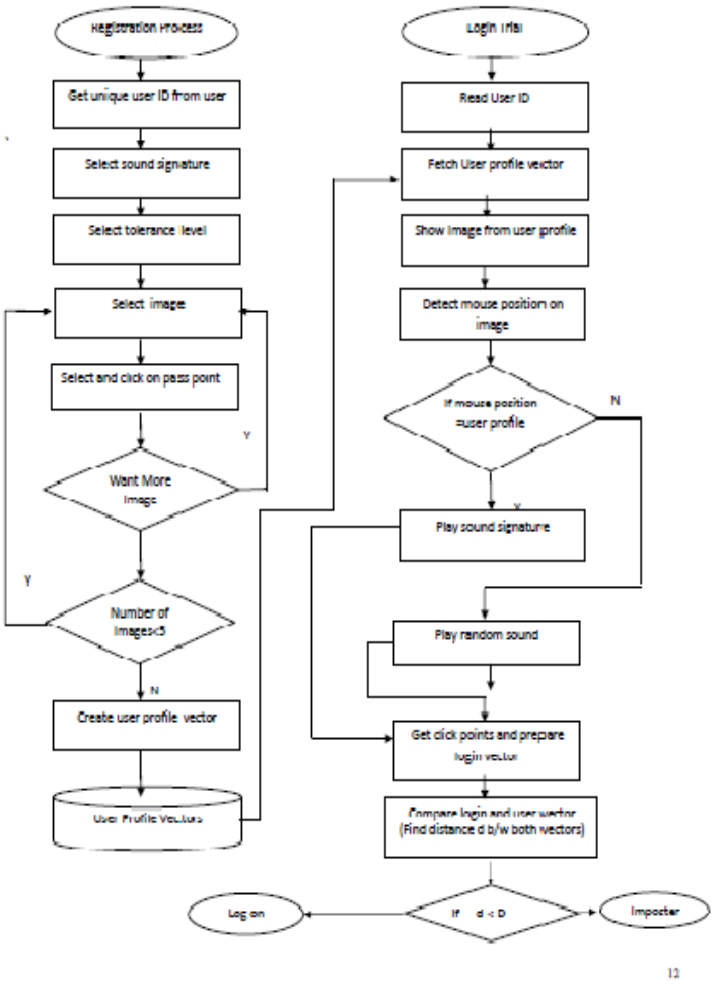


Fig.1.

The following the architecture of our proposed system:



System Architecture

CONCLUSION

We conducted an accuracy analysis of personal authentication with user images. The effects of the number of templates for each person on accuracy of verification and identification were examined by considering simple algorithms based on the ideas of a majority vote and the arithmetic mean of similarities. As the result of the experiments with practical user images, we achieved improvements of the error rates in verification and identification. I would like to conclude saying that this effort put forth by us will overcome issue of shoulder browsing thus improving authentication accuracy to the next level. But this is not the end of it, there will more better alternatives in the near future hopefully.

REFERENCES

[1] OpenCV. http://opencv.willowgarage.com/wiki/.
[2] PolyU Palm print Database. http://www.comp.polyu.edu.hk/˜biometrics/.
[3] I. Awad and K. Baba. “Evaluation of a fingerprint identification algorithm with sift features”. In Proc. 2012 IIAI International Conference on Advanced Applied Informatics,
[4] C. M. Bishop. Pattern Recognition and Machine Learning. Springer, 2006.
[5] J. Chen and Y.-S. Moon. “Using SIFT features in palm print authentication”. In Proc. 19th International Conference on Pattern Recognition, pages 1–4. IEEE, 2008.
[6] S. Egawa, A. I. Awad, and K. Baba. “Evaluation of acceleration algorithm for biometric identification”. In Networked Digital Technologies, Part II, volume 294 of Communications in Computer and Information Science, pages 231–242. Springer, 2012.
[7] G. Iannizzotto and F. L. Rosa. “A SIFT-based fingerprint verification system using cellular neural networks”. In Pattern Recognition Techniques, Technology and Applications, pages 523–536. InTech, 2008.
[8] A. K. Jain, A. A. Ross, and K. Nandakumar. Introduction to Biometrics. Springer, 2011.
[9] D. G. Lowe. “Object recognition from local scale-invariant features”. In Proc. IEEE International Conference on Computer Vision, pages 1150–1157, 1999.
[10] D. G. Lowe. “Distinctive image features from scaleinvariant keypoints”. International Journal of Computer Vision, 60(2):91–110, 2004.