International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 10: October 2015, pp 32-33. www.aetsjournal.com ISSN (Online) : 2394-6237

A Survey on Face Detection using an Image through Finger Print Matching in Live

Manoj Prabhakar J, Dr.P Ezhilarasu, Satheesh Kumar D, Sowmya R

***Abstract*—** In this paper, we discuss the various authentication types with an example. In particular, we discuss the eye blink, face detection and fingerprint matching techniques that are used to identify a person in live. Many papers are taken for the survey. Its advantages and disadvantages are discussed.

***Keywords*—** Spooling, Eyeblink, Fingerprint matching, Face recognition.

I. INTRODUCTION

Authentication is the process of confirming the truthiness of an attribute of a single piece of data (a datum) claimed true by an entity [1]. The authentication process starts with identification. It affirms that a person is credible after verification of a person's data correctly. The authentication process takes the input data with the existing data for matching. Then it makes the decision about the person whether he/she is the credible person. This process mainly used to ensure information security. Sometimes external data also consider during this process.

There exist many types in Authentication. Those are

1. Authentication based on SMS.
   Ex. Getting the one-time password for opening email in a two-step authentication process and performing internet banking.
2. Authentication based on Password.
   Ex.Entering into the system using login password.
3. Authentication based on PIN.
   Ex.Internet banking transaction using the PIN number for the debit card.
4. Authentication based on Symmetric key.
   Ex. Both the sender and the receiver sharing a common key for performing encryption and decryption in an encryption environment.
5. Authentication based on Public Key.
   Ex. The sender and receiver utilize two different keys - a public key to perform encryption and a privet key to perform decryption.
6. Authentication based on Biometric.
   Ex. DNA Matching
   The DNA segments are used to identify an individual.
   Ear
   The Ear's shape are used to identify an individual.
   Eyes - Iris Recognition
   The iris was used to identify an individual.
   Eyes - Retina Recognition
   The backside of the eye that has patterns of veins used to recognize an individual.
   Face Recognition
   The Face patterns or facial features used as an authentication or recognition for identifying an individual.
   Fingerprint Recognition
   The surface of the human finger has ridges and minutiae. It can be used to identify an individual.
   Finger Geometry Recognition
   The finger's 3D geometry used to identify an individual.
   Gait
   The individuals walking style or gait used to determine identity

Fingerprint matching technique comes under biometric and in particular it is visual metric. This process used to finalize whether the two sets of fingerprint ridge attribute come from the unique finger. There exist numerous algorithms that do fingerprint matching in plenty different ways. Pattern based algorithms take and compare the basic fingerprint patterns (arch, whorl, and the loop) between a previously stored template and a candidate's fingerprint. It requires that the images, aligned in the same orientation. To implement this, the algorithm finds a point in the central position of the fingerprint image and centers on that. In a pattern-based algorithm, the template has the type, size, and orientation of patterns within the aligned fingerprint image. The candidate's fingerprint image graphically compared with the template to finalize the degree to which they match.

There are three basic patterns of fingerprint ridges. Those are arch in which ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger loop. In this, ridges enter from one side of a finger, then form a curve, and then exit on that same side. Finally, whorl where Ridges form circularly around a central point on the finger. Mostly for fingerprint matching out of five fingers

Manoj Prabhakar J, PG Scholar, Department Of Computer Science And Engineering, Hindusthan College Of Engineering And Technology, Coimbatore, Tamilnadu, India (Email; manojprabhakarj92@gmail.com)

Dr.P Ezhilarasu , Associate Professor, Department Of Computer Science And Engineering, Hindusthan College Of Engineering And Technology, Coimbatore, Tamilnadu, India. (Email: prof.p.ezhilarasu@gmail.com)

Satheesh Kumar D , Assistant Professor, Department Of Computer Science And Engineering, Hindusthan College Of Engineering And Technology, Coimbatore, Tamilnadu, India. (Email: dsatheeshme@gmail.com)

Sowmya R, PG Scholar, Department Of Computer Science And Engineering, Hindusthan College Of Engineering And Technology, Coimbatore, Tamilnadu, India. (Email: sowmyacsebe@gmail.com)

index and thumb fingers are used. When the particular user was accessing it, it shows the details of the particular user already stored in the database. Face recognition may also used.

EXAMPLE: Schools, colleges, Hospitals, IT Companies uses these sort of techniques

II. Various Authentication Methods

The various authentication methods are as given in the table 1.

Table 1 Analysis of Authentication methods

S.No	Title	Description
1.	Filter Bank-based Fingerprint Matching [2]	To identify frauds in our society and also to save our personal identification this fingerprint based matching is used to preserve our data.
2.	Eyeblink-based anti-spoofing in face recognition from a generic web camera [3]	In this method, Eyeblink technique is carried out to recognize the face whether the given image is fake or not.
3.	Face spoofing detection from single images using micro-texture analysis [4]	In this spoofing attack occurs when a person tries to attack others data. The quality of an image measured here. Also the face prints that contain defects that can be detected
4.	Blinking-based live face detection using conditional random fields [5]	In this method, it needs a web camera for capturing the video clips. Blinking is the only clue used here, Rather than speaking, Face moving doesn't require here.
5.	A TV flow based local scale measure for texture discrimination [6]	In this total variation, flow pixels can change their value with a speed that is inversely proportional to size of region
6.	Face liveness detection under bad illumination conditions [7]	In this technique, it tells about spoofing Face recognition of photos and videos of some other persons
7.	Real-time face detection and motion analysis with application in liveness assessment [8]	In this process, Liveliness method is being detected. It processes each frame at a real time
8.	Scale-space and edge detection using anisotropic diffusion [9]	This method is used mainly for intra-region smoothing rather than inter-region smoothing. Finally, it shows out number of images, parallel hardware implementation are made feasible
9.	Lightness and retinex theory [10]	The color sensation shows a strong correlation with their reflectance, Although amount of visible light reaches its eye dependence
10.	LIBSVM: A library for support vector machines [11]	In this method, it mainly uses that helps the user easily apply SVM(Support Vector Machines) to their applications

III. Conclusion

In this paper, we studied about various authentication techniques that identify a person. The human body has so many parts. Ex. Face, eye, leg, hand, ear, etc. But only a few parts are used to implement authentication process. In this paper, we studied the face detection, eye blink, and fingerprint matching techniques. The results of these techniques are analyzed. The result shows that eye blink techniques give better authentication as compared to fingerprint matching and face detection.

References

[1] https://en.wikipedia.org/wiki/Authentication
[2] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Trans. Image Process.*, vol. 9, no. 5, pp. 846–859, May 2000.
[3] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcamera," in *Proc. IEEE 11th Int. Conf. Comput. Vis. (ICCV)*, Oct. 2007, pp. 1–8.
[4] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–7.
[5] L. Sun, G. Pan, Z. Wu, and S. Lao, "Blinking-based live face detection using conditional random fields," in *Proc. Adv. Biometrics*, Oct. 2007, pp. 252–260.
[6] T. Brox and J. Weickert, "A TV flow based local scale measure for texture discrimination," in *Proc. 8th Eur. Conf. Comput. Vis. (ECCV)*, May 2004, pp. 578–590.
[7] B. Peixoto, C. Michelassi, and A. Rocha, "Face liveness detection under bad illumination conditions," in *Proc. 18th IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2011, pp. 3557–3560.
[8] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-time face detection and motion analysis with application in 'liveness' assessment," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 548–558, Sep. 2007.
[9] P. Perona and J. Malik, "Scale-space and edge detection using anisotropic diffusion," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 12, no. 7, pp. 629–639, Jul. 1990.
[10] E. H. Land and J. J. McCann, "Lightness and retinex theory," *J. Opt. Soc. Amer.*, vol. 61, no. 1, pp. 1–11, 1971.
[11] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, Apr. 2011, Art. ID 27.