International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Iris and Signature Features Based Multimodal biometric System: A Review

[1]Dr.Swati Sharma
Associate professor
Jodhpur National University
er.swati.sharma15@gmail.com

[2]Gurdeep Singh
Assistant professor
Mullana University
gurdeep16india@gmail.com

[3]Nitin Sondhi
Assistant professor
Mullana University
nitin.sandhi@gmail.com

Abstract: *Biometrics is a measurable distinctive physical characteristic or personal trait that can be used to identify an individual or to verify the claimed identity of an individual. The system reliability increases when multiple traits are being accounted for in the identification process. The limitations of uni- biometric systems can be alleviated by multi-biometric systems. This paper presents the concept of iris and signature biometrics as well as their feature extraction methods.*

Keywords: *Iris Recognition, Features Extraction, Multi-biometrics.*

1. Introduction

Now a days, one of the main threats that IT system and security environment can have, is the possibility of intruders in the system. This is normally solved by user authentication schemes based on passwords, secret codes and identification cards or tokens. Schemes based only on passwords or secret codes can be cracked by intercepting the presentation of such a password or by brute force attacks [1]. On the other hand, an intruder can attack systems based on identification card or token by robbing, copying or simulating them. As it is a well-known, biometric deal with identification of individuals based on their physical and behavioral features. Biometric solutions, such as identification systems using fingerprint, iris, face, and palm print, hand geometry, signature, etc.; have many advantages over the traditional authentication techniques based on what you know or what you possess. Instead of carrying bunk of keys, all those access cards or passwords you carry around with you, your body can be used to uniquely identify you.

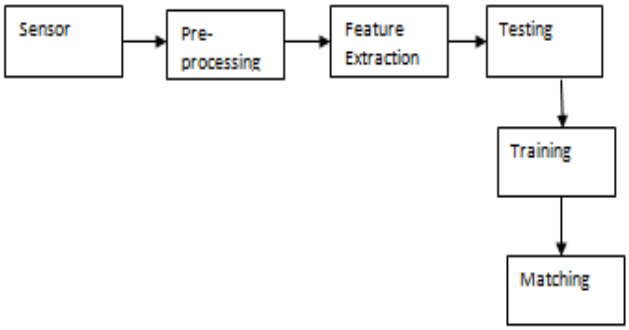

Figure 1: Biometric Processing

Among them, iris and signature recognition is tested as the most accurate manner of personal identification. Therefore nowadays many automatic security systems based on iris and signature recognition have been deployed worldwide for border control, restricted access and so on.

2. Related Work

S.No	Author	Technique
1.	Papli [2]	presents a new oRGB-SIFT descriptor for signature verification, and then integrates it with other color SIFT features to produce the novel Color SIFT Fusion (CSF)
2.	PraloyMisra [3]	Existing signature verification systems have been thoroughly studied and a model is designed to develop an offline signature verification system.
3.	Neeraj Shukla [4]	The handwritten signatures analyzed using SIFT.
4.	Deng et.al [5]	developed a system that uses a closed contour tracing algorithm to represent the edges of each signature with several closed contours
5.	Fang et.al [6]	proposed two methods for the detection of skilled forgeries using template matching
6.	Eric et.al [7]	proposed a modified Kolmogora, complexity measure based on maximum Shannon entropy of wavelet packet reconstruction to quantify the iris information
7.	Jiali et. al [8]	the iris recognition algorithm based on PCA (Principal Component Analysis) is first introduced and then, iris image synthesis method is presented
8.	Hyung et.al [9]	Iris texture is reflected according to the magnitude of iris power spectrum in frequency domain

3. BASIC CONCEPTS

SIGNATURE

Handwritten signature authentication is the process of verifying the identity of a person based on user's handwritten signature [6] Signature has been widely accepted as a means of legal and commercial transactions identity authentication [8]. Signatures have played a historical role in authenticating documents. Being part of everyday life, signature based authentication is remarked as a consistent non-invasive authentication procedure by the majority of the users, therefore, it can help in overcoming some of the privacy difficulties.

Table- Comparison of different signature cryptographic characteristics

Parameters	Handwritten Signature	Biometric Signature	Digital Signature
Confidentiality	No	Yes	Yes
Integrity	No	Yes	Yes
Authentication	Yes	Yes	Yes
Authorization	No	Yes	Yes
Non-Repudiation	yes	yes	Yes

IRIS

Iris recognition is most prominent technique. Iris recognition systems are gaining interest because it is stable over time. Iris scan has been developing an identification/verification system capable of positively identifying and verifying the identity of individuals. The unique patterns of the human iris, used for overcoming previous shortcomings.

4. FEATURE EXTRCATION TECHNIQUES OF IRIS AND SIGNATURE

1. HCT

The Hough transform can be applied to detect the presence of a circular shape in a given image. It is used to detect any shape or to locate the iris in the face. The characteristic equation of a circle of radius r and center (a, b) is given by:

$$(x-a)^2 + (y-b)^2 = r^2$$

This circle can be described by the two following equations:

$$x = a + r \cos(Q)$$
$$y = b + r \sin(Q)$$

2. GENETIC ALGORITHM

As a preparation to start the optimization process, a Genetic Algorithm, requires a group of initial solutions as the first generation. The first generation is usually a group of randomly produced solutions created by a

random number generator. The population, which is the number of individuals in a generation, should be big enough so that there could be a reasonable amount of genetic diversity in the population. Also, it should be small enough for each generation to be computed in a reasonable period of time using the computer resources available. Typically, a population includes individuals between 20 and 100. The fitness function is evaluated to measure how close that the individuals fit the desired result. A fitness function could be either complex or simple depending on the optimization problem addressed. In a case of minimization problem, the most fitted individuals will have the lowest numerical value of the associated fitness function.

1. **[Start]** Generate random population of *n* chromosomes (suitable solutions for the problem)
2. **[Fitness]** Evaluate the fitness *f(x)* of each chromosome *x* in the population
3. **[New population]** Create a new population by repeating following steps until the new population is complete
    1. **[Selection]** Select two parent chromosomes from a population according to their fitness (the better fitness, the bigger chance to be selected)
    2. **[Crossover]** With a crossover probability cross over the parents to form a new offspring (children). If no crossover was performed, offspring is an exact copy of parents.
    3. **[Mutation]** With a mutation probability mutate new offspring at each locus (position in chromosome).
    4. **[Accepting]** Place new offspring in a new population
4. **[Replace]** Use new generated population for a further run of algorithm
5. **[Test]** If the end condition is satisfied, **stop**, and return the best solution in current population
6. **[Loop]** Go to step **2.**

3. ICA

Independent component analysis (ICA) is a statistical and computational technique for revealing hidden factors that underlie sets of random variables, measurements, or signals. ICA defines a generative model for the observed multivariate data, which is typically given as a large database of samples. In the model, the data variables are assumed to be linear mixtures of some unknown latent variables, and the mixing system is also unknown. The latent variables are assumed non-gaussian and mutually independent and they are called the independent components of the observed data. These independent components, also called sources or factors, can be found by ICA.

Putting it in mathematical terms, we seek a linear transformation V of the data D such that when P = V*D we now have Cov(P) = I (I being the identity matrix, zeros everywhere and 1s in the Diagonal; Cov being the covariance). It thus means that all the rows of the transformed matrix are uncorrelated (see covariance matrix).

Let consider "centered" matrix Z of matrix D :Cov(D) = Cov(Z) = (Z*Z')/(n-1), (as defined previously z_i,j = d_i,j - mean(d_i))

Then it is easy to show that Cov(P) = I by setting $\mathbf{V} = \mathbf{C}^{-1/2}$, where C = Cov(D) is the correlation matrix of the data, since then we have

$$\begin{aligned} \mathrm{Cov}(P) &= \mathrm{Cov}(V*D) \\ &= \mathrm{Cov}(C^{-1/2}*Z) \\ &= C^{-1/2}*Z*Z'*C^{-1/2} \text{ by definition} \\ &= C^{-1/2}CC^{-1/2} = I. \end{aligned}$$

4. SIFT

Scale-invariant feature transform (or SIFT) is an algorithm in computer vision to detect and describe local features in images. The algorithm was published by David Lowe in 1999.
SIFT key- points of objects are first extracted from a set of reference images and stored in a database. An object is recognized in a new image by individually comparing each feature from the new image to this database and finding candidate matching features based on Euclidean distance of their feature vectors.
SIFT algorithm:

- Scale-space extrema detection
- Keypoint localization
- Interpolation of nearby data for accurate position
- Discarding low-contrast keypoints
- Eliminating edge responses
- Orientation assignment
- Keypoint descriptor

5. CONCLUSION

This paper shows that the integration of different biometric sources, often termed as biometric fusion, is another main design issue. It has a good impact on the performance of the system. The fusion scheme can be classified into sensor level, feature level, score level and decision level. The choice of fusion depends on the type of information from the biometric sources namely, raw

biometric samples, feature sets, match score and decision labels. In this work two behavioral biometric traits, signature and iris are integrated for identification. And has been analyzed that what feature extraction methods can be used.

REFERENCES

[1] Binsu C. Kovoor, M. H. Supriya and K. Poulose Jacob, "A Prototype for a Multimodal Biometric Security System Based on Face and Audio Signatures", International Journal of Computer Science(IJCSc), vol 2, No.1, pp 143-147, Jan-June 2011.

[2] Papli, "New Colour Sift Descriptors", International Journal of Biometrics, Volume 3 Issue 1, December 2011, Pages 56-75

[3] PraloyMisra thesis on "Offline Handwritten signature Verification ", 2013.

[4] Neeraj Shukla, "Invariant Features Comparison in Hidden Markov Model and SIFT for Offline Handwritten Signature Database, International Journal of Computer Applications (0975 – 8887) Volume 2 – No.7, June 2010.

[5] Peter ShaoHua Deng, et al, "Wavelet-based off-line handwritten signature verification", Computer vision and image understanding , Vol.76, Issue 3, pp. 173-190, Dec 1999.

[6] B. Fang, Y.Y. Wang, C.H. Leung, Y.Y. Tang, P.C.K. Kwok, K.W. Tse and Y.K. Wong, "A Smoothness Index Based Approach for Off-line Signature Verification", 2000.

[7] Eric Sung, Xilin Chen, Jie Zhu and Jie Yang, "Towards non-cooperative iris recognition systems", Seventh international Conference on Control, Automation, Robotics And Vision (ICARCV'02), Dec. 2002, Singapore, pp. 990-995.

[8] Jiali Cui, Yunhong Wang, JunZhou Huang, Tieniu Tan and Zhenan Sun, "An Iris Image Synthesis Method Based on PCA and Super-resolution", IEEE CS Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04), 23-26 August 2004, Cambridge, UK, Vol. 4, pp. 471-474.

[9] HyungGu Lee, Seungin Noh, KwanghyukBae, Kang-Ryoung Park and Jaihie Kim, "Invariant biometric code extraction", IEEE Intelligent Signal Processing and Communication Systems (ISPACS 2004), 18-19 November, 2004, Seoul, Korea, pp. 181-184.