ISSN: 2393-8528

IJICSE
Open Access

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 4 Issue 3; May-June-2017; Page No. 85-89

Revised Edge Detection Based Feature Extraction in Biometrics

Gowder Praveena Hiriyan

M.C.A., M.Phil., Assistant Professor, Department of Computer Science

KG College Of Arts and Science, Coimbatore, India

gowderpraveena@kgcas.com

Received 08 April 2017; Accepted 10 May 2017

ABSTRACT

Digital Image Processing, enlightenment for a number of developing technologies indulges in the enhancement and intensification of the approaches in different fields. Edge Detection the key concept incorporated in Feature Extraction adds light in its path. Over the years Biometrics has provided authentication and secrecy. The changing nature of the "life measurement" due to the changes seen in the physiological and behavioral aspects has enforced an event constituting a process of combining a few of the metrics to form a relational concept. Multimodal brought forth Biometrics with new ranks.

An Adaptive Biometric system was also developed. The adaptive nature turns out be a threat. Biometric Feature Extraction when provided with enhanced Edge Detection algorithm omits the deflections caused due to small changes. Thus when combined with Multimodal Biometrics can produces highly positive results. This paper studies in brief the Biometric Technology and its enhancement made possible with the help of a highly threshold able and suppressible Edge Detection algorithm.

Keywords: Edge Detection, Biometrics, Image processing, imaging, Feature Extraction and Feature Matching

INTRODUCTION

Digital image processing, a concept of using computer algorithms to perform image processing is a a subcategory or field of digital signal processing, digital image processing has many advantages over processing. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the build-up of noise and signal distortion during processing [4].

In an image processing, input is given as an image for any form of signals processing is said to be image processing such as a photograph or video frames; the output of image processing may be either an image or a set of properties or parameters related to the image. In present day sciences and innovations, pictures likewise increase substantially more extensive degrees because of the perpetually developing significance of logical representation. The image as treated as a two-dimensional signal in most of the image processing techniques and applying standard signal-processing techniques to it.

In the terminology of machine learning, Type of instance supervised learning, i.e. learning where a training set of correctly identified observations is available [3].

The comparing unsupervised strategy is called as grouping, and includes accumulation information into classes in view of some measure of intrinsic similitude or separation.

Image processing involves the concepts of classification, feature Extraction, and pattern recognition. Feature extraction is a special form of reduction. The relating unsupervised system is called as bunching, and includes gathering information into classes in view of some measure of characteristic likeness or separation. Moving the input data into the set of features is called feature extraction.

On the off chance that the components separated are effectively picked it is normal that the elements set will extricate the important data from the info information so as to play out the coveted procedure utilizing this decreased portrayal rather than the full size info [3].

A feature is defined as an "interesting" part of an image, and features are used as a beginning point for many computer vision algorithms. Since components are utilized as the underlying point and extremely essential for ensuing calculations, the general calculation will frequently just be comparable

Corresponding author: Gowder Praveena Hiriyan |

to its element identifier. Consequently, the desirable property for a feature detector is redundant: whether or not the same feature will be detected in two or more different images of the same scene.

Existing Technology - Biometrics

The "Biometrics" which is usually associated with the use of unique physiological properties to identify an individual. The application which most people associate with biometrics is security. Biometric location has in the end a more extensive importance as PC interface turns out to be more characteristic.
A number of biometric traits have been developed and are used to authenticate the person's identity. The idea is to use the special characteristics of a person to identify him. By using special characteristics we mean the using the features such as face, iris, fingerprint, signature etc.

The strategy of ID in perspective of biometric properties is supported over existing passwords and PIN based strategies for different reasons such as: The person to be identified is required to be physically present at the time-of-identification. Identification based on biometric techniques obviates the need to remember a password or carry a token.

A biometric procedure is basically an example acknowledgment prepare which makes an individual distinguishing proof by deciding the legitimacy of a particular physiological or behavioral trademark controlled by the client. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic"[7].

Types of Biometrics

Biometrics is the science and innovation of measuring and examining natural information. In data innovation, biometrics insinuates developments that measure and separate human body qualities for example, DNA, fingerprints, eye retinas and irises, voice designs, facial examples and hand estimations, for validation purposes.

Biometric identifiers are the unmistakable, quantifiable attributes used to name and portray people. Biometric identifiers are consistently requested as physiological versus behavioral qualities. Physiological qualities are identified with the state of the body. Delineations join, however are not limited to one of a kind stamp, palm veins, stand up to affirmation, DNA, palm print, hand geometry, iris acknowledgment, and retina as shown in the Figure1 and Figure2. Behavioral attributes are identified with the example of conduct of a man, including yet not constrained to writing musicality, step, and voice. A couple of examiners have generated the term behavior metrics to delineate the last class of biometrics.

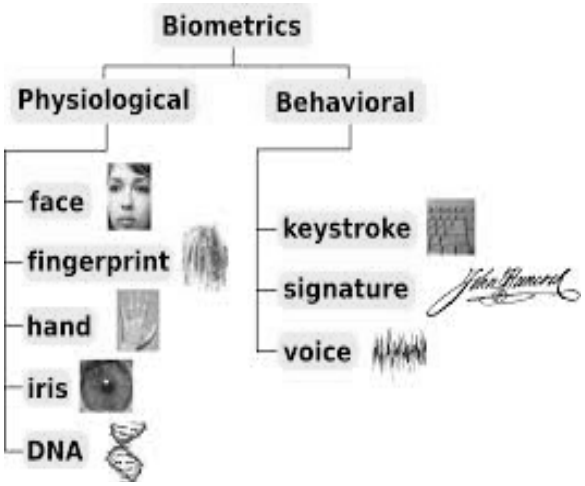

Figure1. Biometrics Classification

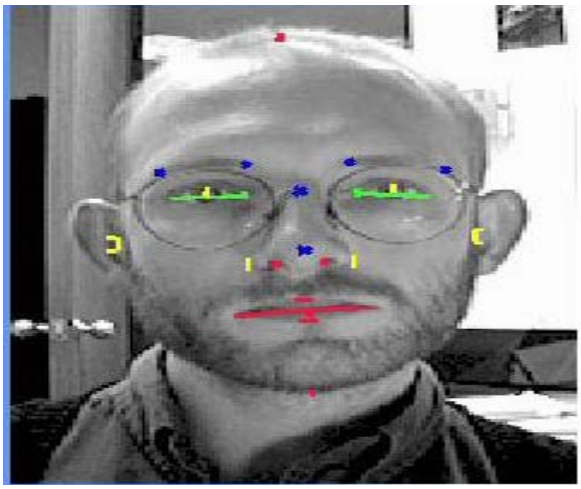

Figure 2:

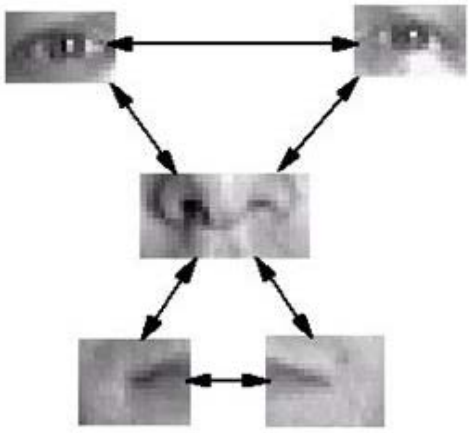

Figure 3: Facial Recognition

Figure 4: Fingerprint Recognition

Figure 5: Types of Biometrics

A biometric system can be either an 'identification' system or a 'verification' (authentication) system, or both combined.

Identification - One too many: Biometrics can be used to determine a person's identity even without his knowledge or consent

Verification - One to One: Biometrics can also be used to verify a person's identity.

The processing seen in any biometrics is as shown in Figure3. During Capture process, raw biometric is captured by a sensing device such as a fingerprint scanner or video camera. The second period of handling is to extricate the distinctive qualities from the crude biometric test and change over into a prepared biometric identifier record Next stage does the procedure of enlistment. The processed sample, a mathematical representation of the biometric is stored / registered in a storage medium for future comparison during an authentication. The original biometric sample cannot be reconstructed from this identifier, thus increasing the security.

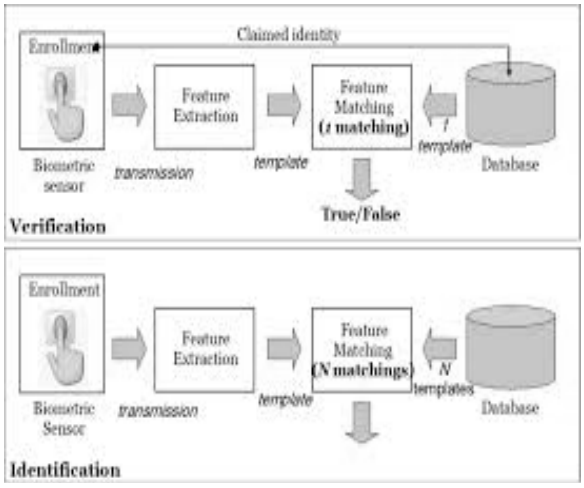

Figure 6: Processes involved in Biometric Verification and Identification.

Biometric data is usually encrypted when it's gathered. Here how the biometric verification works on the backend: To convert the biometric input, a software application is used to identify specific points of data as push comes to points. The match points in the database are processed using an algorithm that translates information into a numeric value. The database value is compared with the biometric input the end users has entered into the scanner and certification is either approved or denied.

Multimodal Biometrics

The disadvantages of soft biometrics are overcome using multimodal Biometrics. At a state Biometrics underwent a threat of soft biometrics is that the tendency of the lively characteristics to change over time and period. The combination of two or more biometric authentications as shown in the Figure4 again lifted the performance.

Figure 7: Biometrics incorporating more than one measure of authentication

Information fusion is divided into three parts, pre-mapping fusion, midst-mapping fusion, and post-

mapping fusion/late fusion. In pre-mapping fusion information can be merged at sensor level or feature level. Sensor-level combination can be for the most part composed in three classifications, single sensor-various occurrences, intra-class numerous sensors, and between class different sensors. Feature-level fusion can be mainly organized in two classes: intra-class and inter-class. Intra-class is again classified into four subcategories as same sensor-same features, same sensor-different features, different sensors-same features, and Different sensors-different features.

Adaptive biometric Systems

In an aim to auto-update the templates or model to the intra-class variation of the operational data Adaptive Biometrics were developed. The advantages of the system include less collection of biometric samples during the enrollment process and reduction in the cost of maintaining a biometric system. In spite of these advantages, the system faced several problems including mis-classification error (false acceptance), and cause adaptation using impostor sample.

Privacy concerns of finding more than what is needed and performing more than the requirement has limited the performance of the system. The threat to the individual is very high. In the process of securing his secrecy there is a possibility of the individual being pushed into the ground of insecurity. Biometrics technology is often not a process that is changeable. Cancelable biometrics is a path in which to fuse security and the substitution highlights into biometrics. At long last Soft Biometrics confinements incorporate physical exercises or followed human attributes, which have been gotten from the way individuals ordinarily recognize their associates. Those attributes have a low discriminating power, thus not capable of identification performance.

Proposed Technology -Edge Detection in Biometrics

Feature Detection and Extraction are performed in order to classify the background and the objects seen in the background which are considered to be features. Feature detection is a low-level image processing operation. That is, it is generally executed as the primary operation on a picture, and checks each pixel to check whether there is an element display at that pixel. In the event that this is a piece of a bigger calculation, then the calculation will regularly just look at the picture in the locale of the components. As an inherent pre-essential to highlight distinguishing proof, the information picture is generally smoothed by a Gaussian portion in a scale-space portrayal and one or a few element pictures are processed, frequently communicated as far as nearby subsidiary operations [5][6].

The Edge Detection algorithm is being applied in order to extract the variations seen in the Biometric. At the time of enrollment the variations called feature extracted are considered as a template for verification. During verification if the Biometric measure comes across any of the disadvantages as discussed before it is made to go through another process of extracting the irrelevant data. The data such as scars, cuts, dust particles, and wrinkles are considered as features in this process. These features may be extracted from the background and then combined with the enrollment image to produce the verification image. The interesting points of the metrics are to be selected from the Edges with continuity [1][2].

The algorithm for this proposed technique is formulated as shown in the Figure5. This revised feature extracting technique establishes a possibility of the Biometric technology indulging in efficiency and enhanced security.

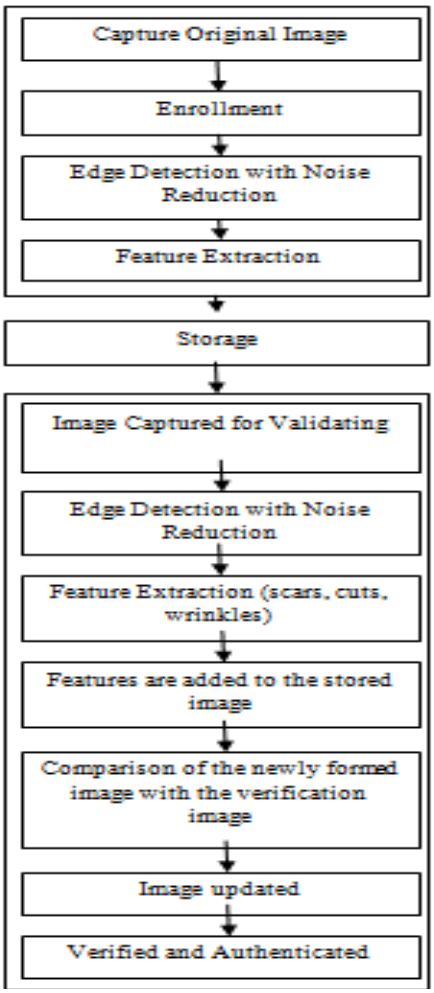

Figure 8: Algorithm of Biometric with Revised feature Extraction

Conclusion

Edge Detection Concept has exclusively become a part of Digital Image processing. The algorithms developed has enhanced and been adapted in a number of techniques. The extraction in the proposed method in this paper is formulated such that during the process of verification it is able to detect and extract the scars, cut, dust particles, wrinkles etc. which are then added to the existing image of enrollment and compared for verification, thus producing an adaptive change. It is possible that the change is accurately detected and is efficient without any issues concerned in the Adaptive Biometric Systems.

Reference

1. Ravi. J, K. B. Raja, and Venugopal. K.R "Fingerprint Recognition Using Minutia Score Matching" International Journal of Engineering Science and Technology Vol.1 (2), 2009, 35-42, ISSN: 0975-5462.
2. Anil K. Jain, Jianjiang Feng, and Karthick Nandakumar, "Fingerprint Matching" IEEE Computer Society 0018-9162.
3. Raman Maini and Dr. Himanshu Aggarwal, "Study and Comparison of Various Image Edge Detection Techniques" International Journal of Image Processing (IJIP), Volume (3) : Issue (1)
4. G.T. Shrivakshan and Dr.C. Chandrasekar "A Comparison of various Edge Detection Techniques used in Image Processing" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 1, September 2012. ISSN (Online): 1694-0814.
5. M. Kalpana, G. Kishorebabu, and K.Sujat, "Extraction of Edge Detection Using Digital Image Processing Techniques" International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue.5 Issn 2250-3005September| 2012 .
6. Sharath Pankanti, Salil Prabhakar, and Anil K. Jain, "On the Individuality of Fingerprints" IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 24, NO. 8, August 2002.
7. Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Salil Prabhakar, Member, IEE, "An Introduction to Biometric Recognition" IEEE Transactions on Circuits And Systems For Video Technology, Vol. 14, no. 1, January 2004.