International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-2 Issue-2, May 2013

Thermal Recognition in Biometrics Approach

Niketa Vishwanath Patil, S.U.Kadam

Abstract: ***Humans recognize each other according to their various characteristics for ages. We recognize others by their face when we meet them and by their voice as we speak to them. Identity verification (authentication) in computer systems has been traditionally based on something that one has (key, magnetic or chip card) or one knows (PIN, password). Things like keys or cards, however, tend to get stolen or lost and passwords are often forgotten or disclosed. To achieve more reliable verification or identification we should use something that really characterizes the given person. Biometrics offer automated methods of identity verification or identification on the principle of measurable physiological or behavioural characteristics such as a fingerprint or a voice sample. The characteristics are measurable, unique and these characteristics should biometrics not be duplicable. Proper design and implementation of the biometric system can indeed increase the overall security; especially the smartcard based solutions seem to be very promising. Making a secure biometric systems is, however, not as easy as it might appear. The word biometrics is very often used as a synonym for the perfect security***

KEY WORDS: Biometrics, Facial Recognition, Fingerprint Matching, Palm Geometry, Thermal face recognition, Thermal recognition

I. INTRODUCTION

Biometrics is a technology used for measuring and analyzing a person's unique characteristics. There are two types of biometrics: behavioural and physical. Behavioural biometric is generally used for verification. While physical biometric is used for either identification or verification [1]. Biometrics is the science of using digital technology to identify individuals based on the individual's unique physical and biological qualities. Simply, biometrics is the technique of verifying a person's identity from a physical characteristic (i.e., fingerprint, hand print, face, scent, thermal image, or iris pattern), or personal trait (voice pattern, handwriting, or acoustic signature). A biometric system is an automatic device for verifying or recognizing the identity of a person on the basis of a physiological characteristic. It can be seen as a special kind of pattern recognition system. The database containing the expressive representation of the characteristic the biometric system is based on, can be either central or distributed. In the case of a distributed database, each individual has a magnetic or smart card in which his biometric characteristic is recorded. The techniques of user authentication are linked to passwords, user IDs, identification cards and PINs (personal identification numbers).

Revised Manuscript Received on 30 May 2013.
* Correspondence Author
Niketa Vishwanath Patil, Department of Computer Engineering, Padmabhooshan Vasantdada Patil Institute Of Technology, University of Pune, Pune, India.
S.U.Kadam, Department of Computer Engineering, Padmabhooshan Vasantdada Patil Institute Of Technology, University of Pune, Pune, India.

These techniques suffer from several limitations: Passwords and PINs can be guessed, stolen or illicitly acquired by covert observation [2]. The biometrics systems provide a more accurate and reliable user authentication method. Existing user authentication techniques include: 1. something you know, e.g. password or PIN. The issue is that many password are easy to guess, and can also be easily forgotten. 2. Something you have, e.g. key or car. They can be lost, stolen or duplicated. 3. Something you know and have, e.g. card + PIN. Thermo grams require an infrared camera to detect the heat patterns of parts of the body that are unique to every human being (such as the face). Normally they are expensive because of the sensors.

A. TYPES OF BIOMETRICS- There are eight types of Biometrics as [3]:

1. Facial Recognition: A physical biometric trait that analyses facial features shown in Fig 1
2. Facial Thermogram: A specialized face recognition technique that senses heat in the face caused by the flow of blood under the skin shown in Fig. 2
3. Fingerprint Matching: A biometric trait that analyze the minute ridges patterns of finger shown in Fig. 3
4. Palm Geometry: A physical biometric that analyses the palm of the hand. Typically this will involve an analysis of minutiae data shown in Fig 4
5. Iris Recognition: A physical biometric that analyses iris features, found in the coloured ring of tissue that surrounds the pupil shown in Fig 5 6. Retina Recognition: A physical biometric that analyses the layer of blood vessels situated at the back of the eye shown in Fig 6
7. Signature Verification: A behavioural biometric that analyses the way an end user signs. The signing features such as speed, velocity and pressure exerted by a hand holding a pen are as important as the static shape of the finished signature shown in Fig 7
8. Speech Recognition: A part physical, part behavioural biometric that analyses patterns in speech shown in Figure 8.

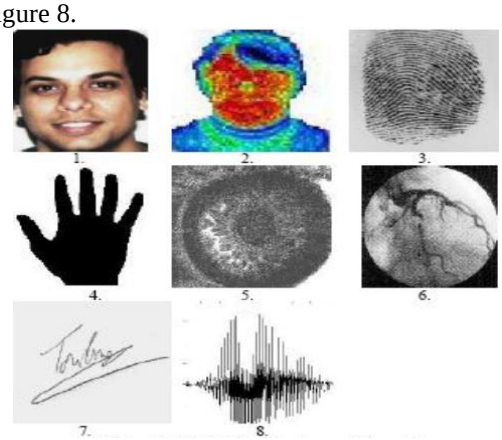

Fig 1- 8: Types of biometrics

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Facial Recognition and Thermogram – Facial Recognition systems are based on the distance between facial attributes (from pupil to pupil, for instance) or on the dimensions of the attributes themselves (such as the width of the mouth). At ach transaction, a tiny camera feeds a live image of the person to a database which compares the image to the one stored. This technology has a good impact on the user, since it seems natural and intuitive, is not expensive and works well under constrained conditions. The weakness is that it is very sensitive to variations in illumination, faces with different positions or expressions, and it performs poorly when database size increases. Face recognition in the thermal infrared domain has received relatively little attention in the literature in comparison with recognition in visible-spectrum imagery. Identifying faces from different imaging modalities, in particular from infrared imagery becomes an area of growing interest [4].

The human face and body maintain a constant average temperature of about degrees providing a consistent thermal signature. This is in contrast to the difficulties of face segmentation in the visible spectrum due to physical diversity coupled with lighting, colour, and shadow effects. At low resolution, IR images give good results for face recognition. Thermal face recognition is useful under all lighting conditions including total darkness when the subject is wearing a disguise. Disguised face detection is of particular interest in high-end security applications. Disguises are meant to cheat the human eye.

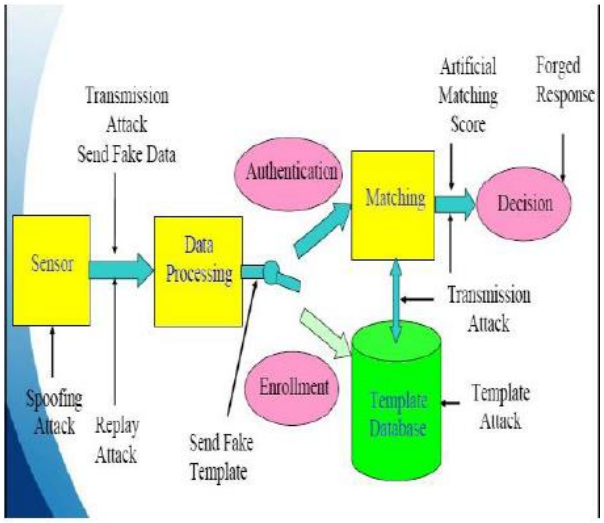

Fig 9: Biometrics authentication systems

Various disguise materials and methods that have been developed over the years are impossible or very difficult to be detected in the visible spectrum [5]. Two methods for altering the facial characteristics of a person: artificial materials, e.g., fake nose, make-up, wig, artificial eyelashes and surgical alteration.

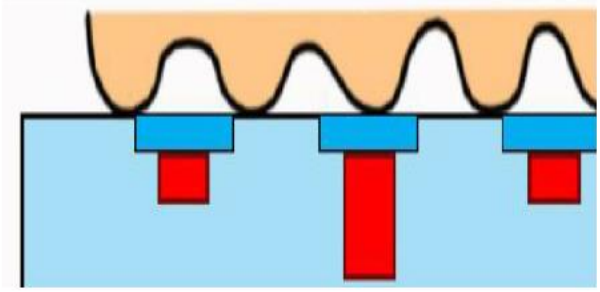

Fig 10: Thermal Sensor

Visual identification of individuals with disguises or makeup is almost impossible without prior knowledge. This technology is similar to the hand vein geometry. It also uses an infrared source of light and camera to produce an image of the vein pattern in the face.

II. BRIEF WORKING

Block diagram of proposed Thermal Biometrics Authentication [6] Fig.11 shows the block-diagram of the proposed biometric authentication system. First, images (visible and infrared) are acquired simultaneously using a scanner and a thermal camera. Scanner images are used as samples for the biometric authentication, while the IR images are used for liveliness detection. Some standard procedures are then applied in order to segment these images.

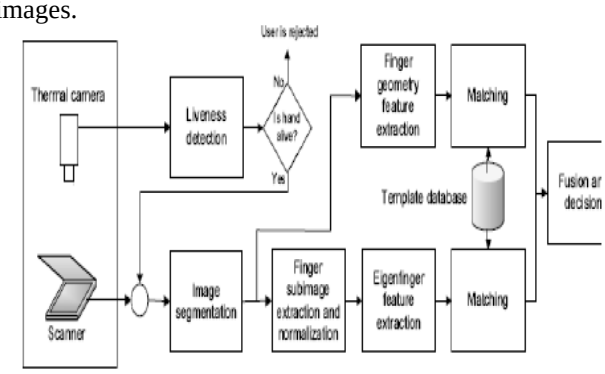

Fig 11: Block diagram of proposed Thermal Biometrics Authentication

In the next phase, the liveliness detection is performed on the segmented infrared image. If the liveliness detection module claims the hand is alive, the biometric system proceeds with extraction of the biometric features from the scanner image. Otherwise, the process is terminated and the user is rejected.

Two kinds of biometric features are extracted: (i) Eigen finger features extracted by means of the transform applied to the previously extracted and normalized finger sub images; (ii) Finger geometry features extracted from the hand contour. Each of these features is matched to the templates stored in the database. Matching scores are combined using fusion at the matching score level, and finally, an authentication decision is made by threshold.

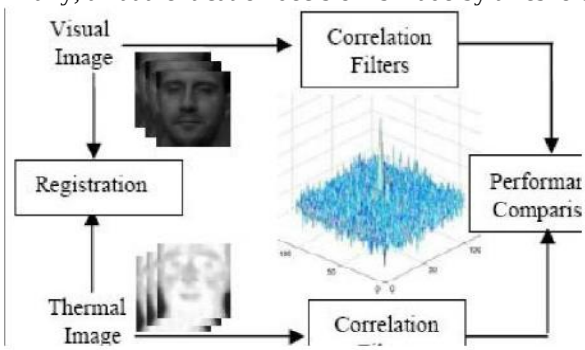

Fig 12: Visual and Thermal Recognition using Correlation Filters.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

III. THERMAL FACE RECOGNITION

The face recognition techniques in practical applications, recognition based only on the visual spectrum has difficulties performing consistently under uncontrolled operating environments. Performance of visual face recognition is sensitive to variations in illumination conditions. The performance degrades significantly when the lighting is dim or when it is not uniformly illuminating the face. Even when a face is well lit, differences in the angle of view can affect manual or automatic locating of feature points. Shadows, glint, makeup, and disguises can cause greater errors in locating the feature points and deriving relative distances. Thermal infrared images represent the heat patterns emitted from an object. Since the veins and tissue structure of a face is unique, the infrared images are unique. Thermal IR imagery is independent of ambient illumination since the human face and body is an emitter of thermal energy. The passive nature of the thermal infrared systems lowers their complexity and increases their reliability. Used in conjunction with passports and drivers' licenses, thermograms will positively identify individuals to immigration and police officials. In addition, correction Facilities can use thermograms to process suspects and inmates, ensuring exact identification and reducing the possibility of prisoners switching places while participating in work release programs.

The evaluated system consists of three main modules performing (i) data pre-processing and registration, (ii) glasses detection and (iii) fusion of holistic and local face representations using visual and thermal modalities. The facial appearance of a person changes substantially through use of simplistic disguise such as fake nose, wig. The individual may alter his/her facial appearance via plastic surgery. Both of these issues are critical for the employment of face recognition systems in high security applications. The thermal infrared spectrum enables us to detect disguises under low contrast lighting [7]. Symptoms such as alertness and anxiety can be used as a biometric that is difficult to conceal as redistribution of blood flow in blood vessels causes abrupt Changes in the local skin temperature.

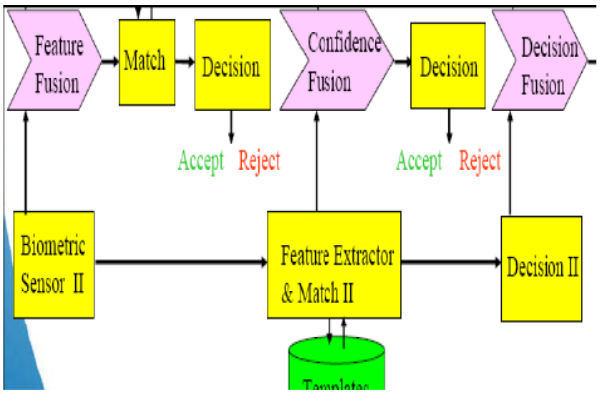

Fig 13: Multi-Modal Biometric Fusion

IV. APPLICATIONS

The various applications of the biometrics system are as follows:

1. Financial services: The banking sector uses voice recognition for telephone banking [3].
2. Defence/nuclear centres: Such places use robust authentication systems, such as retina scans, to control access to the facilities [6].
3. Computer security: Typical deployments are based on voice or finger pressure, and the like, for granting access to personal computers [7].
4. Access Control: One of the most traditional of applications for biometrics, accessing buildings, offices, cars, and even homes are applications for biometric implementations [7]. Applications for this technology include any activity where absolute identity verification is necessary. On a personal level, facial thermograms can replace house keys and automatic teller machine cards. Entering a locked house or conducting financial transactions will involve stepping up to a camera and punching in a PIN. The lens will capture the facial thermogram and compare it with a registered image for the number. A match will allow access.

V. FUTURE SCOPE

Biometric verification based on a single feature does not yield a very low error rate. In order to further reduce the error rate, many researchers have turned their attention to the use of multi-feature verification. Several literatures discussing this topic have been published and good results have been achieved. In this paper, we also extract multiple features to decrease the verification error rate. Equation reveals that the temperature T of the skin surface is the only variable which dominates the contrast and quality of thermal images. Moreover, heat conduction affects the temperature distribution on the skin surface. According to the Fourier law (heat conduction law) the temperature gradient will vary over the same object surface. The temperature gradient direction changes slowly that is from high to low. Where Ql is the rate of heat flow through area A in the positive direction, and constant k is the thermal conductivity of the material. The law means that the rate of heat flow due to conduction in a given direction is proportional to the area and the temperature gradient in that direction [12].

VI. CONCLUSION

The main conclusion of thermal biometrics is that one must be cautious when evaluating the value of an imaging modality for a specific recognition task. Ideally, this question should be framed as that of estimating the Bayes optimal error for a classification problem.

Biometrics system is used for High-quality identification of users it means that the systems use all possible way to get corrected identification. As in this system the user has to store the biometric data and only after corrected processing of the access to system is possible it means the biometric data is nothing but part of human body or it may be the behaviour of the individual which is unique from person to person. Also this unique property of individual cannot be copied, lost as well as shared by the persons hence there is very less chance that any person can get access to another system easily. Although there are some limitations while using the single biometric system hence the multi biometric systems are prefer over single system .As there are various different techniques of biometric system available hence one technique can be used to replace other.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

But still the researches are going on to introduced more secure and less complex biometric systems which are more secure and more beneficial. Biometrics system is used for High-quality identification of users it means that the systems uses all possible way to get corrected identification. As in this system the user has to store the biometric data and only after corrected processing of the access to system is possible it means the biometric data is nothing but part of human body or it may be behaviour of the individual which is unique from person to person. Also this unique property of individual can not be copied, lost as well as shared by persons hence there is very less chance that any person can get access to another system easily. Although there are some limitations while using the single biometric system hence the multi biometric various different techniques of biometric system available hence one technique can be used to replace other. But still the researches are going on to introduced more secure and less complex biometric systems which are more secure and more beneficial.

REFERENCE

1. D. A. Socolinsky and A. Selinger, “A comparative analysis of face recognition performance with visible and thermal infrared imagery,” in Proceedings ICPR, Quebec, Canada, August 2002.
2. D.A. Socolinsky and A. Selinger, “Face recognition with visible and thermal infrared imagery,” Computer Vision and Image Understanding, July - August 2003.
3. Joseph Wilder, P. Jonathon Phillips, Cunhong Jiang, and Stephen Wiener, “Comparison of Visible and Infra-Red Imagery for Face Recognition,” in Proceedings of 2nd International Conference on Automatic Face & Gesture Recognition, Killington, VT, 1996, pp. 182
4. X. Chen, P. Flynn, and K. Bowyer, “Visible-light and infrared face recognition,” in Proceedings of the Workshop on Multimodal User Authentication, Santa Barbara, CA, December 2003, to appear.
5. B. Abidi, “Performance comparison of visual and thermal signatures for face recognition,” in The Biometrics Consortium Conference, Arlington, VA, September 2003.
6. F. J. Prokoski, “History, Current Status, and Future of Infrared Identification,” in Proceedings IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications, Hilton Head, 2000.
7. P. Jonathon Phillips, Hyeonjoon Moon, Syed A Rizvi, and Patrick J. Rauss, “The FERET Evaluation Methodology for Face-Recognition Algorithms,” Tech. Rep. NISTIR 6264, National Instituite of Standards and Technology, 7 Jan. 1999.
8. X. Chen, P. Flynn, and K. Bowyer, “PCA-based face recognition in infrared imagery: Baseline and comparative studies,” in International Workshop on Analysis and Modeling of Faces and Gestures, Nice, France, October 2003.
9. Yael Adini, Yael Moses, and Shimon Ullman, “Face Recognition: The Problem of Compensating for Changes in Illumination Direction,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 721–732, July 1997.
10. P. J. Phillips, D. Blackburn, M. Bone, P. Grother, R. Micheals, and E. Tabassi, “Face recognition vendor test 2002 (FRVT 2002),” Available at http://www.frvt.org/FRVT2002/default.htm, 2002.
11. Authors, “Thermal face recognition in an operational scenario,” in Submitted to CVPR 2004.
12. A. Ross and A. Jain,”Information fusion in biometrics. Pattern Recognition Letters”, 2003.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)