Biometric Data Using Score Fusion Through Stegnography

Muntha Raju [1] Dr. Ashutosh Verma [2]
[1].Research Scholar ,Maharishi University of Information
[2].Department of Computer Science and Engineering, Maharishi University of Information

Abstract:- Multi-biometrics, or the fusion of more than one biometric modality, sample, sensor, or algorithm, is quickly gaining popularity as a method of improving biometric system performance and robustness. Despite the recent growth in multi-biometrics research, little investigation has been done to explore the possibility of achieving multi-modal fusion from a single sensor. This approach to multi-biometrics has numerous advantages, including the potential for increased recognition rates, while still minimizing sensor cost and acquisition times. In this work, experiments are presented which successfully combine multiple samples of face and iris biometrics obtained from a single stand-off video sensor. Several fusion techniques are explored to test the e activeness of multi-modal and score level fusion, with the best recognition rates achieved by using a Borda count of face and iris modalities. The nal results out-perform either single-modality approach, and the proposed multi-biometric framework represents a viable and natural extension to many commercial stand-off iris sensors.

Keywords:- Multimodal Biometrics, Modes of Fusion, Security Services.

1. Introduction

There are three general ways to identify a person to a computer system, based on what you know, what you have, or who you are. "What you know" approaches such as passwords and PINs have less reliability because they can be lost, stolen, or guessed. "What you have" technologies such as RFID cards and e-tokens also can be stolen. Biometrics belong to the "who you are" class and can be subdivided into behavioral and physiological approaches. Behavioral biometric include signature recognition, voice recognition, keystroke dynamics, and gait analysis. Physiological biometric include fingerprints, iris, retina scans, hand, finger, face, ear geometry, hand vein, nail bed recognition, DNA and palm prints. As biometrics can't be borrowed, stolen, forgotten, and forging is

practically impossible, it has been presented as a natural identity tool that offers greater security and convenience than traditional methods of personal recognition. Biometric system is an enabling technology with the potential to make our society safer, reduce fraud, and lead to user convenience by providing the functionalities [1] like verification, identification, screening and enrolment. Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic such as face, fingerprints, finger knuckle print, voice and iris. Because such characteristic are physically associated to the user, biometric recognition is a natural and more reliable mechanism for ensuring that only authorized users are able to enter a facility, access a computer system, or cross international restrictions such as border of any country. It is basically a pattern-recognition system that is used to identify or verify a human beings or users.

If we talk about the computer security there are three levels of computer security schemes. Firstly a person carries, such as an identity proof with a photograph. Secondly relies on something a person knows, such as a password or a code number. Finally the third and highest level relies on something that is a part of a person's biological makeup of behavior, such as a fingerprint, a knuckle print, a facial image, or a signature etc.

Characteristics of an ideal Biometrics

On the above study of biometric methodologies there are some characteristic of ideal biometrics which are as follow:

i.Universality: It means that every person should possess the biometric traits.

ii.Uniqueness: It indicates that no two persons should be the same in terms of the traits.

iii.Permanence: It means that the traits should be invariant with time. A cue that changes significantly over time is not a useful biometric.

iv.Collectability: It means that it should be possible to acquire and digitize the cue using

suitable devices without causing any inconvenience to user.

v.Performance: It refers to the achievable recognition accuracy, speed, robustness, and the resources required to achieve the accuracy and speed.

vi.Acceptability: It indicates the extent to which people are willing to accept a particular biometrics in their daily life.

2. Related Work

The research has focused on the single biometric trait for recognition and authentication. The palm is the inner surface of the hand between the wrist and the fingers. Early works in automatic palm print recognition utilized palm print images obtained off-line , while the newer systems typically obtain palm print image by using a scanner [6] or a CCD camera [5,7].Biometric trait like palm print has advantage like Noise Interference is less.

Several methods like Gabor filter, Sobel method, and Wavelet packet Transform, Fourier transform are available in the literature to extract. Shunyu Yang [1] proposes a real time personal identification based on Fourier transform for palm print recognition in which segmentation of hand gesture is done on which Fourier transform is applied for image processing. David Zhang[2] have used 2D Gabor algorithm in which lines and points are extracted from palms and it is considered as a texture image so an adjusted Gabor filter employed to capture the texture information on palm prints. Xiangqian Wu [3] used detectors to extract the line of palms in different direction and irregular lines are represented in this using chain code and palm prints are matched by matching the points on their palm lines.[4] helped in increasing overall system accuracy by reducing the (FAR) False Acceptance rate.

Securing the data and implementation of the system:

The processes involved at sender are explained in The actual confidential data is secured by following the steps given below:

· All users' cryptographic keys generated from their own fingerprint biometric are shared among the users

· A mean image generated from all users' facial images using Eigen face-based recognition algorithm is shared among the users.

Multimodal systems

To over fulfill the mentioned problems and limitations the multimodal systems are used, leading to the improvement of the system's performances and the increase of the number of enlisted population in the systems and discouragement of fraud.

Multimodal biometric systems that have been proposed in references may be classified using four parameters:

-architecture;

- Sources that provide multiple evidence;

- Level of fusion;

- Methodology used for integrating the multiple verifiers.

Overview of SDES algorithm:

For encrypting the plain text a simple cryptographic algorithm, say, Simplified Data Encryption Standard (Stallings, 2010) is used. Even though the other algorithms like DES,

AES and packet encryption system as specified in (Sengan and Pandian, 2012), are stronger than SDES the overhead also more compared to this and so we used SDES and the encryption and decryption

algorithms are demonstrated . The algorithm involves five functions: an Initial Permutation (IP); a Complex Function (CF) which involves both permutation and substitution operations depends on a key input; a simple permutation function (SW) that switches the two halves of the data; the Complex Function (CF) again; and finally a permutation function that is the inverse of the Initial Permutation (IP–1). The formula

for encryption is: Ciphertext = IP-1 (CFK2 (SW (CFK1 (IP (Plain text)))))) and decryption is essentially the reverse of encryption:

Plain text = IP-1 (CFK1 (SW (CFK2 (IP (Ciphertext)))))

In the original version of S-DES, it depends on the

use of a 10-bit key shared between sender and receiver. From this key, two 8-bit sub keys are produced for use in particular stages of the encryption and decryption algorithm. But in our proposed MBSASS model, the fingerprint based cancellable key, which is shared between the sender and receiver is used for encryption and decryption. Even though the algorithm is simple in nature to make it complex different 10-bit keys are used for different encryptions.

Conclusion

In this paper we have shown drawbacks of existing authentication system. In future, it will provide high security for user to share the important information over internet.

Steganography will improve the drawbacks and provides the high security for the user. The proposed system is very secure and at same time mutual authentication can takes place between the user and bank. The future enhancement we can do is speech recognition , thump impression, iris scan, and keystroke.

Reference

[1] Wendy S. Yambor Bruce A. Draper J. Ross Beveridge, "Analyzing PCAbased Face Recognition Algorithms: Eigenvector Selection and DistanceMeasures", July 1, 2000. Available at:http://www.cs.colostate.edu/~vision/publications/eemcvcsu2000.pdf

[2] Peter Belhumeur, J. Hespanha, David Kriegman, "Eigenfaces vs.fisherfaces: Recognition using class specific linear projection", IEEETransactions on Pattern Analysis and Machine Intelligence, 19(7):771 –720, 1997.

[3] L. Breiman. Bagging predictors. Technical Report Technical ReportNumber 421, Dept. of Statistics, University of California, Berkeley,1994.

[4] D. Swets and J. Weng, "Hierarchical discriminant analysis for imageretrieval", IEEE Transactions on Pattern Analysis and MachineIntelligence, 21(5):386–401, 1999.

[5] Wendy S. Yambor, "Analysis of PCA Based and Fisher Discriminant-Based Image Recognition Algorithms", M.S. Thesis, July 2000(Technical Report CS-00-103, Computer Science).

[6] Kyungnam Kim, "Face Recognition using Principle ComponentAnalysis", International Conference on Computer Vision and PatternRecognition, pp. 586-591, 1996.

[7]http://scien.stanford.edu/class/ee368/projects2001/dropbox/project16/

[8]http://www.irc.atr.jp/%7Emlyons/pub_pdf/fg98-1.pdf

[9] http://www.kasrl.org/jaffe.html

[10] James R. Parker, J R Parker, "Algorithms for Image Processing andComputer Vision", John Wiley & Sons, 1996.

[11] Sankar K. Pal, AshishGhosh, Malay K. Kundu, "Soft Computing forImage Processing", Studies in Fuzziness and Soft Computing, Vol. 42,2000.

[12] Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing",Pearson Publications, 2000.

[13] Image Processing Handbook by John C. Russ

[14] Handbook of Pattern Recognition and Image Processing by K.S. Fu andT.Y. Young

[15] Li Ma , Tieniu Tan , Yunhong Wang , Dexin Zhang " PersonalIdentification Based on Iris Texture Analysis" , IEEE Transactions onPattern Analysis and Machine Intelligence , Vol. 25 No. 12, December2003.

[16] John Carter, Mark Nixon, "An Integrated BiometricDatabase",availableat:ieeexplore.ieee.org /iel3/1853/4826/00190224.pdf.

[17] Arun Rose, Anil Jain and SharatPankanti, "A Prototype HandGeometry Based Verification System", 2nd International Conference onAudio and Video Based Person Authentication, Washington D. C., pp.166-171, 1999.

[18] Boreki, Guilherm, Zimmer, Alessandro, "Hand Geometry FeatureExtraction through Curvature Profile Analysis", XVIII BrazilianSymposium on Computer Graphics and Image Processing, SIBGRAPI,Brazil, 2005.