ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Multimodal Biometric Algorithm using Normalized Score Level Fusion Rules with Support Vector Machine Optimization

[1]A.E. Sujatha and [2]B. Dr.A.Chilambuchelvan

[1]E.Sujatha B.E.,M.Tech.(GOLD MEDAL), M.B.A.,(Ph.D.,) Research Scholar, Associate Professor, Department of Computer Science and Engineering, Jaya Engineering College, Chennai, India.
[2]Dr.A.Chilambuchelvan, B.E.,M.E.,Ph.D., Professor, Department of Computer Science and Engineering, R.M.K. Engineering College, Chennai,India.

ARTICLE INFO

Article history:
Article Received 12 January 2015
Revised 1 May 2015
Accepted 8 May 2015

Keywords:
Multimodal Biometrics, Score Level Fusion, Neural Networks, Normalization, Support Vector Machine.

ABSTRACT

Multimodal Biometric Algorithm which integrates Iris, Fingerprint, Vein Thermo gram, Hand geometric biometric traits to provide high security. This paper presents Multimodal Biometric Algorithm using Score Level Fusion Rules and the normalization techniques that concludes with the optimized technique among multimodal biometrics for matching decision. Neural Network based Algorithms are used for recognizing each biometric traits.

To Cite This Article: A.E. Sujatha and B. Dr.A.Chilambuchelvan., Multimodal Biometric Algorithm using Normalized Score Level Fusion Rules with Support Vector Machine Optimization. ***Aust. J. Basic & Appl. Sci.,*** *9(21): 47-51, 2015*

INTRODUCTION

Biometrics is used to provide high level security for authentication, verification and identification. Multimodal Biometrics is an integration of more than one biometric trait to enhance security.

This paper presents a solution for the high security level needed in all levels of vulnerable system using multimodal biometrics. Multimodal Biometrics enhances matching performance, anti spoofing, increases population coverage by reducing Failure to Enroll rate (Kalyan Veeramachaneni, Lisa Ann Osadciw, 2003; Woodward, J.D. Jr., 2000). Unimodal Biometrics suffers from noisy data, intra-class variations, non-universality, spoof attacks, unacceptable error rates, lack of individuality, inter-class similarities, and susceptibility to circumvention (Multimodal Biometrics: 2004; Biometric Recognition: 2003).

Identifying and Verifying a human being is done in into three ways: something you possess as in an ID card, something you know, and something unique about you (Hong, L. and A. Jain, 1998).

In all real time Scenarios such as identifying a person to verify its claimed identity, ID card is used. Credit Card, Mails, Login processing, the PIN is used. The Security level using these ways leads to the following demerits (Biometric Recognition: 2003).

(i) Keys can be easily lost, forged, or duplicated.

(ii) PIN number or Passwords can be forgotten as well as shared, stolen, or guessed easily by hackers (Kalyan Veeramachaneni, Lisa Ann Osadciw, 2003).

To choose a complex PIN and Password, possession of Smart card etc., are not the permanent solution for security in the real world. Every year the amount of costs, time spends for the security is not affordable. So, introducing Biometric technologies can automate the identification of people by one or more of their distinct physical or behavioral characteristics by something they are called Multimodal Biometric Security Solution.

1.1 Characteristics of Biometrics:

Universality: Each person should posses a valid biometric trait.

Uniqueness: Each biometric trait exhibits distinct features.

Permanence: It must be sufficient invariant over a period of time.

Measurability: Biometric trait should not cause inconvenience to the individual.

Performance: The biometric trait should be accurate.

Acceptability: The trait must be accepted by a target population that utilizes the application.

Corresponding Author: A.E. Sujatha, E.Sujatha B.E.,M.Tech.(GOLD MEDAL), M.B.A.,(Ph.D.,) Research Scholar, Associate Professor, Department of Computer Science and Engineering, Jaya Engineering College, Chennai, India
E-mail: sanjaymohankumar@gmail.com

Circumvention: It shows how easily the chosen biometric trait can spoofed using artifacts (Biometric Recognition: 2003).

1.2 Identification:

Identification systems are done with 1: N (one-to-N, or one-to-many) matching to verify who that is claimed identity in the template.

Comparisons of Biometric Technologies (Biometrics: 2006; Biometric Recognition: 2003)

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Fingerprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Hand Geometry	M	M	M	H	M	M	M
Face	H	H	M	M	L	H	H
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H
Palm Print	M	H	H	M	H	M	M

1.3 Verification:

Verification is to verify that a person is claimed identity. After an every individual provides a biometric trait the biometric system extracts features and generates a template. Then it compares the template with this person's reference template stored during enrollment, to determine whether the individual's trait is matched with stored template. Verification is done as 1:1 (one-to-one) matching.

1.4 Performance Evaluation:

FAR- False Acceptance Rate: It measure the proportions of imposters Accepted.

FRR-False Rejection Rate: It measures the proportions of Genuine Users Rejected.

FTE- Failure to Enrolment Rate: It measures the proportion of individual that are unable to generate repeatable templates and unable to reproduce their biometric feature consistently.

FTA-Failure to Acquire Rate: It measures the proportion of individual that the system is unable to capture or locate quality image.

FME- False Match Rate and FME- False Non Match Rate: They measure the accuracy of matching process. Performance of the biometrics is evaluated by visually representing the relationships between errors rates. By adjusting the decision criteria there can be trade-off between false match and false non-match errors (Mansfield, T., *et al*., 2001; Biometric Recognition: 2003).

II. Proposed Multimodal Biometric Design:

This paper integrates four multimodal biometric traits: Iris recognition, Finger Print, Vein Thermogram, and Hand Geometry.

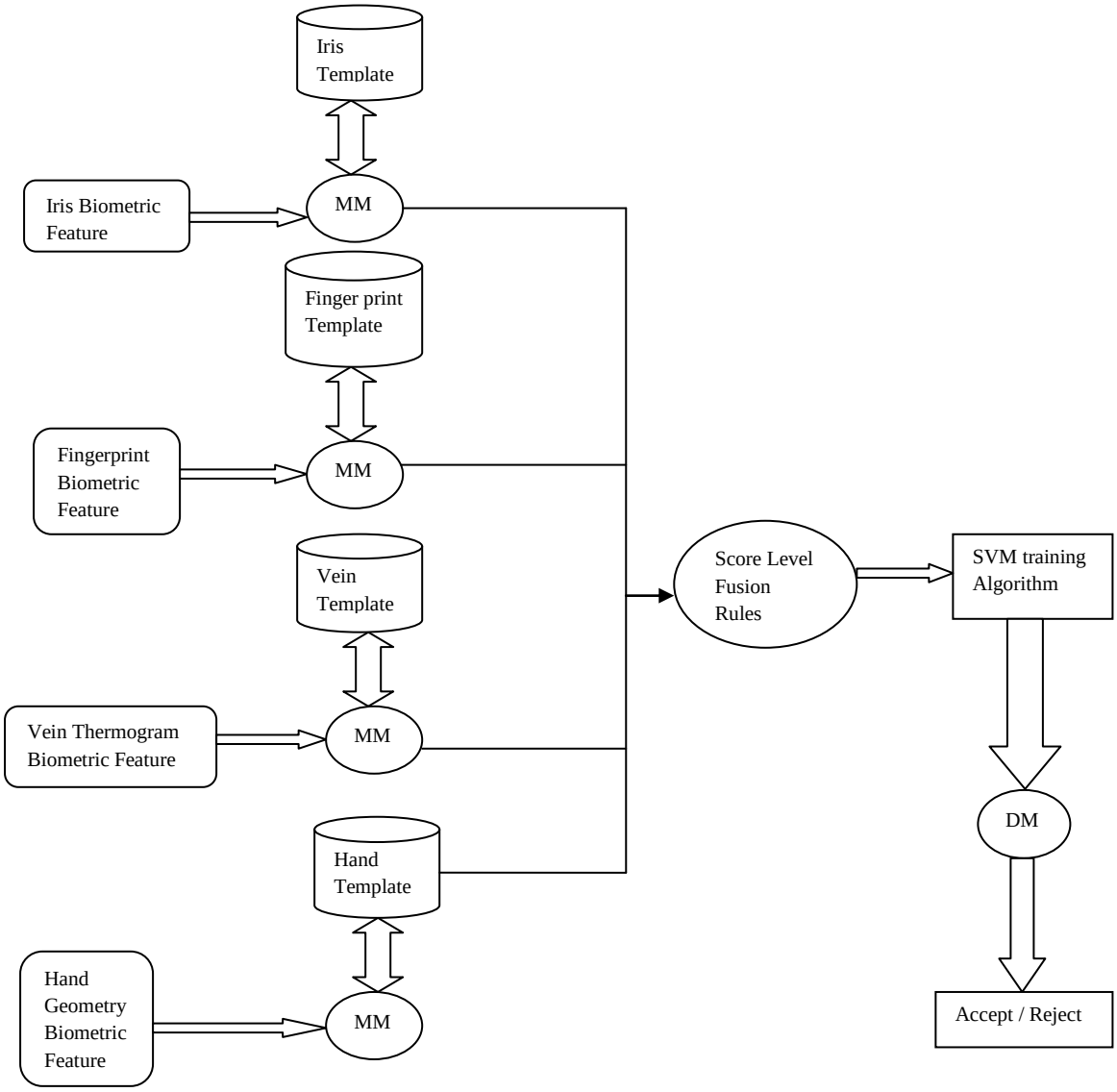
2.1 Iris Recognition:

Iris recognition is done on the pupil of the eye. Iris is an elastic connective tissue and it a very rich source of biometric data because it has 266 distinctive characteristics and used 173 out of it. Iris is formed during the 8th month of gestation and stable throughout life, except in cases of injury. Iris recognition can be used in both verification and identification systems. High-quality camera captures high-resolution Iris image. It defines the boundaries and coordinates of the iris, zones. In the proposed Algorithm Neural Network Iris Recognition is to be implemented with one or few of the following factors: (i) furrows, (ii) freckles (iii) carona, (iv) ridges, (v) dark spots / rings. CASIA (Institute of Automation of the Chinese Academy of Sciences) Database is to be utilized for recognition and experimental results.

2.2 Finger Print Recognition:

Fingerprint recognition is commercialized in 1970s and more than 75 fingerprint recognition technology (Hong, L. and A. Jain, 1998) companies are currently used in law enforcement applications due to more reliable, accurate biometric trait (Hong, L. and A. Jain, 1998; Prabhakar, S. and A. Jain, 2002). Fingerprint recognition technology extracts features from impressions made by the distinct ridges. The fingerprints are either flat or rolled. A flat fingerprint captures impression of the central area between the fingertip and the first knuckle; a rolled print captures ridges on both sides of the finger. A fingerprint is captured by a scanner, enhanced, and stored into a template. Scanner technologies are optical, silicon, or ultrasound technologies. Ultrasound is the most accurate and used widespread. Noise is caused during enhancement by dirt, cuts, scars, and creases or dry, wet, or worn fingerprint is reduced. In the proposed Algorithm new fingerprint recognition algorithm is to be implemented on CASIA (Institute of Automation of the Chinese Academy of Sciences) Database.

Australian Journal of Basic and Applied Sciences, 9(21) Special 2015, Pages: 47-51



2.3 Vein Thermogram:

Hand Vein geometry is based on the veins under the skin absorb infrared light and a darker pattern on the image of the hand taken by an infrared camera. The system identifies a person using the patterns of veins in the back of the hand with visible veins. A person's vein patterns are highly stable throughout their life. They are developed before birth and even differ between twins of all types. Vascular pattern recognition technology is developed to minimize the disadvantages of commercially available biometric systems and to have the benefits of impeccable security, usability, reliability, accuracy, and user acquiescence (AVIATION SECURITY). In the proposed Algorithm new Vein Thermogram recognition algorithm is to be implemented on CASIA (Institute of Automation of the Chinese Academy of Sciences) Database.

2.4 Hand Geometry:

Hand geometry systems are 30 years old in accessing control to facilities ranging from nuclear power plants to day care centers. Hand geometry technology focuses 96 measurements of the hand, including the width, height, and length of the fingers; distances between joints; and shapes of the knuckles (AVIATION SECURITY). Optical camera and light-emitting diodes with mirrors and reflectors are used to capture two orthogonal two-dimensional images of the back and sides of the hand. Although the basic shape of an individual's hand remains relatively stable over one's lifetime, natural and environmental factors can cause slight changes. The shape and size of our hands are reasonably diverse, but are not highly distinctive. Thus, hand geometry is not suitable for performing identification matches. In the proposed Algorithm new Hand geometry recognition algorithm is to be implemented on CASIA (Institute of Automation of the Chinese Academy of Sciences) Database.

III. Fusion Approaches:

3.1 Fusion Rules:

Problem:

Classify input pattern Z into one of m possible classes (c1, …., cm) based on evidence provided by R classifiers

Let xi be the feature vector for the I classifier derived from Z; X's are independent

Assign Z → c, if g(c) ≥ g©, 1≤ k≤m, k≠j

Product Rule: g(Cr) = $\prod_{i=1}^{R} P(C_r \mid x_i)$

Sum Rule: g(Cr) = $\sum_{i=1}^{R} P(C_r \mid x_i)$

Max Rule: max P(Cr | xi)

Min Rule: min P(Cr | xi)

3.2 Levels of Fusion:

The Levels of fusion are Feature level, Sensor level, Match Score level, Decision level. Multimodal biometric traits are integrated as multiple instances, multiple sensors, and multiple traits, multi algorithms by sensor level, feature level, match score level and decision level. The amount of the information available for fusion decreases after each level of processing in a biometric system (Kalyan Veeramachaneni, Lisa Ann Osadciw, 2003; Prabhakar, S. and A. Jain, 2002).

3.2.1 Match score level fusion:

In the proposed Algorithm each recognition score is obtained and fusion rules are constructed to integrate Iris, Fingerprint, Vein thermo gram, Hand geometry recognition techniques (Hong, L., *et al*., 1999). Match score is used to measure the similarity between the input and template biometric feature vector. In match score level fusion, the match score obtained from different matchers are combined (IJCA, 2010).

Since scores obtained from different matchers are not homogeneous, score normalization technique is followed to map the scores obtained from different matchers on to a same range set. Score level fusion is independent of biometric system. It is used after signal, image processing. It requires lower communication bandwidth.

3.3 Score Normalization Techniques:

Min-max:

Matching Score for min-max is

$$s' = (s - \min\{s_k\})/(\max\{s_k\} - \min\{s_k\})$$

Decimal scaling:

Scores are represented in a logarithmic fashion

$$s_i' = \frac{s_i}{10^n}$$

with

$$n = log_{10} max_{i=1}^{N} s_i$$

Z-score:

Z-Score normalization is measured as:

$$s' = \frac{(s - median)}{MAD}$$

$$MAD = median\ (|\{s_k\} - median\ |)$$

Median and MAD:

Median and Median Absolute Deviation can be used for score distribution instead of average and standard deviation. It is more robust against outliers, and used only if distributions are close to Gaussian. MAD score distribution is:

$$M = median_{i=1}^{N} |s_i - m|$$

Double sigmoid:

It is identical to Sigmoid score normalization only if it allows tweaking parameter.

$$s_i' = \begin{cases} \dfrac{1}{\left(1 + \exp\left(-2\dfrac{(s_i - \tau)}{\alpha_1}\right)\right)} & if\ s_i < \tau \\ \dfrac{1}{\left(1 + \exp\left(-2\dfrac{(s_i - \tau)}{\alpha_2}\right)\right)} & if\ s_i \geq \tau \end{cases}$$

where α_1 and α_2 are linear indicators.

Tanh-estimators:

Tanh score normalization is:

$$s_i' = \frac{1}{2}(\tanh(0.01\ (s_i - \mu_{GH})/\sigma_{GH}\ ) + 1$$

3.4 Optimization:

After Score level normalization the decision is to be made on the claimed identity is whether genuine or imposter. In order to make decision, Support Vector Machine is adapted for comparative experimental analysis.

3.4.1. Support Vector Machine:

Support Vector Machine solves linear separable problem such as XOR problem. It classifies the outlier data which is non-linear and unable to model mathematically. It trains the scores of the multimodal biometric trait information. It can be implemented at all stages of fusion approaches. SVM accepts linear, polynomial, sigmoid functions from user and it trains the data and selects support vectors along with the surface of the hyper plane to fit. SVM do not require less number of features in order to avoid over fitting. It has ability of fault tolerance in producing errors. Speed, Scalability is the specialty of SVM and does not depend on the dimensionality of feature space.

IV. Research Issues:

4.1 Challenges in Multimodal Biometric System:

i. Selecting the multimodal biometric source is very challenging since it depends upon the scenario and cost and leads to cultural and gender dimensions under universality (IJCA, 2010).

ii. The information acquired from different sources can be processed either in sequence or parallel. So it is quite challengeable to decide about the processing architecture depends upon the application and the choice of the source. It leads to complexity in memory and computations.

iii. Choosing the level of fusion has direct impact on performance and cost.

iv. It is very hard to find the optimal fusion approach.

v. To implement in a real time (Panikanti, S., *et al*., 2000; Frischholz, R.W. and U. Deickmann, 2000).

4.2 Design Issues:

The Design Issues are

(a) The choice and number of biometric traits and its justification

(b) The levels of fusion

(c) Optimal fusion rules adopted to integrate the information

(d) The cost versus matching performance (Multimodal Biometrics: 2004)

In the proposed algorithm these research factors are considered at all stages of algorithm and final conclusion is derived.

Conclusion:

This paper presents neural network based security solution for multimodal biometrics with normalized score level fusion rules and SVM optimization technique.

This paper presents State-of-the-art Algorithm in Security for identification, verification and authentication.

ACKNOWLEDGMENT

I would like to express my gratitude to the almighty god and visible god Parents who supports morally and my Husband Mr. D. Mohankumar for his motivation and my dear son M.S.Sanjay for his encouragement to pursue my Ph.D. degree.

REFERENCES

"An Adaptive Multimodal Biometric Management Algorithm" Kalyan Veeramachaneni, Lisa Ann Osadciw, *Senior Member, IEEE*, and Pramod K. Varshney, *Fellow, IEEE* "A. Ross, A.K. Jain, "Information Fusion in Biometrics", Pattern Recognition Letters, Sep. 2003

Woodward, J.D. Jr., 2000. "Biometrics: Facing up to terrorism," presented at the Biometrics Consortium Conf., Arlington, VA, Feb.

Hong, L. and A. Jain, 1998. "Integrating faces and fingerprints for personal identification," *IEEE Trans. Pattern Anal. Machine Intell.*, 20(12): 1295-1307.

Prabhakar, S. and A. Jain, 2002. "Decision-level fusion in fingerprint verification," *Pattern Recognit.*, 35: 861-874.

Panikanti, S., R.M. Bolle and A. Jain, 2000. "Biometrics: The future of identification," *IEEE Comput.*, 33(2): 46-49.

Frischholz, R.W. and U. Deickmann, 2000."BioID: A multimodal biometric identification system," *IEEE Comput.*, 33: 2.

Hong, L., A.K. Jain and S. Panikanti, 1999. "Can multibiometrics improve perfomance?" in *Proc. AutoID*, Summit, NJ, pp: 59-64.

IJCA, 2010. *Special Issue on "Recent Trends in Image Processing and Pattern Recognition" RTIPPR,*.

AVIATION SECURITY, United States General Accounting Office

Multimodal Biometrics: 2004. An Overview*Arun Ross And Anil K. Jain Appeared* in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp: 1221-1224.

Mansfield, T., G. Kelly, D. Chandler and J. Kane, 2001."Biometric product testing final report, computing," Nat. Phys. Lab., U.K.

Biometrics: 2006. A Tool for Information Security Anil K. Jain, *Fellow, IEEE*, Arun Ross, *Member, IEEE*, and Sharath Pankanti, *Senior Member, IEEE* IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 1: 2.

An Introduction to Support Vector Machines, 2000. Nello Cristianini and John Shawe-Taylor, Cambridge University Press.

Biometric Recognition: 2003. Security and Privacy Concerns IEEE SECURITY & PRIVACY March/April Salil Prabhakar, Sharath Pankanti, Anil K. Jain