ISSN No. 0976-5697

Volume 6, No. 4, June 2015 (Special Issue)

International Journal of Advanced Research in Computer Science

TECHNICAL NOTE

Available Online at www.ijarcs.info

Automatic Verification System

Dr. Ritu Bhargava
*Lecturer:*Dept. of Computer Science, Aryabhatt International College, Ajmer,India
drritubhargava@yahoo.com

Prafull Chandra Narooka
Research Scholar: Dept. of Computer Science ,MJRP University, Jaipur
Jaipur, India
narooka.on.web@gmail.com

*Abstract:*We introduce a multi model biometrics technologies, these technologies are used to verify human characteristics for security. It can be used to overcome the some of the limitations of a single biometrics. Physical biometric patterns identified for security reason the identity established by a face recognition, eye recognition, fingerprint verification and voice recognition systems. The advantages of biometrics to verify/authenticate a human identity. We introduce a multimodal biometrics system which integrates face recognition, eye recognition, fingerprint verification or speaker verification in making personal verification.

Keywords: automatic, verification, system

I. INTRODUCTION

biometrics technology refers to automatic verification system. The automatic verification of the identities of individuals is becoming an increasingly important requirement in application. Automatic systems that uses measure physical characteristics to recognize the identity.

A biometrics system is defined as "a system which automatically recognizes a person as individual and unique information a combination of hardware and pattern algorithms. Based on certain physical and behavioral characteristics that are belonging to that person."

Person authentication for access system control to a prohibited area or for identification in many network areas or social service area, some physical characteristics that are used in biometrics include face recognition, eye recognition, fingerprint verification and voice recognition, hand geometry, DNA etc. it is the requirement of an application which determine and check the choice of a specific biometrics indicator.

If a user cannot provide a nice or clear fingerprint due to dry finger and cuts then face and voice may be better biometric indicator. If in the current palace environment noise available then voice is not a suitable biometric indicator, the face location algorithm, May not work properly, if the background of the user's face is cluttered

II. ATTACKS ON BIOMETRICS SYSTEMS

Biometrics systems provide and offer many advantage over traditional taken (as key) or knowledge (as password) which based on authentication and verification systems or schemes. There are many attacks which can be grouped into following nine categories.

Type 1 attack

Attacking the biometric sensor present a fake biometric to the system that mimic as an authorized user example are fake gelatin finger, picture of an iris and voice recording.

Type 2 attack:

Attacking communication from the biometric sensor. Not always an option biometric sensor and feature extractor are some time combined. Attacks can intercept data send by sensor. Attacker could send malicious data to the feature extractor as replay attack. Examples are hill climbing attacks and decoding intercepted WSQ files to make fake fingerprints.

Type 3 attack:

Manipulating/overriding feature extraction and template creation prances usually an attack on software or firmware. Example generating a template preselected by the attacker and steal template generated by the system.

Type 4 attack:

Attacking the communication channel between template creation unit and comparison unit. Large threat when templates are compared on a remote system. Example: intercept a user template for later use, inject a malicious template, and inject a malicious template to brute force the system.

Type 5 attack:

Attacking the template companion unit, close equality makes some attacks possible here, template must be in the clear when they are compared, can be an attack on software, firmware or configuration. Example: modify matching software to produce artificially low or high scans and change threshold for a successful match.

Type 6 attack:

Attack or temper with stored templates some system support more than one template per user (beware of duress templates). Example: steal a template, associate a malicious template with an already enrolled user and enroll a malicious user.

Type 7 attack:

Attacking the transmission of stored templates, data can be corrupted; intercepted, or modified, traffic is after unencrypted. When send over Ethernet or serial network template stored on cards or taken (replay attacks on proximity cards). Example: sniffing traffic to steal template and injecting templates to falsely authenticate a malicious user.

Type 8 attack:

Overriding the final decision and if the final match. Decision can be overriding by an attacker that the system has been defeated.

CONFERENCE PAPER National Conference on
"Internet Technology and Cyber Crime"
On 11 January 2015
Organized byPraful Narooka and
Sponsored by Agarwal College, Merta City (Nagpur)

Type 9 attacks:

Attacking the transmission of enrollment template to the storage location similar to attacks at point 4 but with potential longer lasting effects. Could permanently add malicious template into the system.

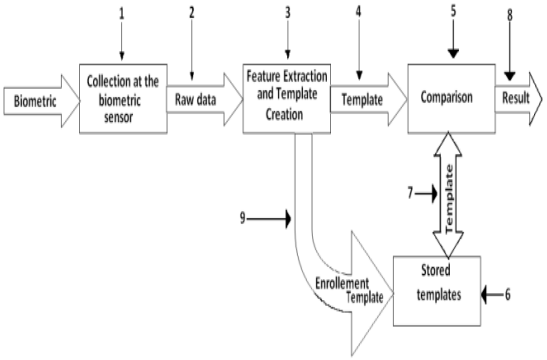

Fig. Attack point in biometric system

III. MULTI MODEL BIOMETRIC SYSTEMS

Every single biometric in to our multi model system has different characteristic and different matching schemes. The optimal biometric system is having some properties of universal, acceptable, collectable and secured but there is no single biometric identifier which has all of these properties so there is a solution multiple biometric identifier system. As an example a multi model biometric system may use both face and iris recognition to identify a person.

Multi model biometric system are used in real world application are the traditional unimodel systems.

IV. LEVELS OF FUSION

The literature shows that there are four type/level of fusion are is used for integrating all data from two or more biometric systems these are the sensor level, the future level, the matching score level and the decision level.

Fusion at the sensor level:

The raw data from different sensors are fused. Means acquired from sensing the biometrics characteristics with two or more sensors. An example of the sensor fusion level is sense a speech signal simultaneously with two microphones it can be used for multi model biometrics system because the incompatibility of data from different modalities

Fusion at the feature extraction level:

Fusion at this level can be applied to the extraction of different type features from the same modality or different multi modalities. For example a unimodel system is the fusion of instantaneous and transactional spectral information for speaker recognition; in feature level fusion we use some feature extraction algorithm or different future extraction algorithms on different modalities. As example in different cases the given feature might not be compatible due to differences in the nature of modalities.

Fusion at the matcher score level:

At this level, it is possible to combine scores obtained from the same biometrics characteristics or different ones. Scores are obtained as example of matcher level on the basis of the proximity of future vectors to their corresponding reference material. The scores obtained from different matchers are not homogenous for this purpose score normalization is followed so a scale fused scored is obtained by normalizing the input matching.

Fusion at the decision level:

At this level output of the multiple classifiers are combined. In this a vote majority scheme can be used to make final decision, different biometrics system can only output only the final decision thus decision level fusion is very appropriate for those biometric systems. The available information for these fusion methods in the binary form, which allowed very simple operation for fusion.

V. TYPES OF MULTI MODEL SYSTEMS:

Depend on the traits, sensors and features sets many types of multi model systems are there:

Single biometrics traits, multiple sensors:

Multiple sensors are used for recording the same biometric trait, for each training the raw biometrics data are obtained from different sensors. The raw data observed from different type of sensors then is combined at the feature level.

Multiple biometric traits:

Multiple biometrics traits like fingerprints and face or face and voice can be combined. Different type of sensors is used for every biometrics characteristic. A commercial product BIODL is used for voice lip motion and face of a user to verify identity.

Single biometrics trait, multiple units:

Two or more finger of a person can be used like biometric trait. It is an inexpensive way of improving system performance, as it does not require multiple sensors or incorporating feature extraction for modules.

Multiple snapshots of single biometric:

In this multi model system more than one instance of the same biometric is used for the verification. For example multiple impression of the same finger or multiple samples of the voice.

VI. DESIGN ISSUES IN MULTI BIOMETRICS

The types of facts should be considered when designing a multi model biometric system these include –

- The chaise and number of biometric identifier (indicator).

CONFERENCE PAPER National Conference on
"Internet Technology and Cyber Crime"
On 11 January 2015
Organized byPraful Narooka and
Sponsored by Agarwal College, Merta City (Nagpur)

- The level in the biometric system at which information provided by multiple traits/indicator should be integrated.
- Decision (votes majority).
- The fusion methodology adopted for integrating the data information.
- The cost versus matching performance trade off.
- Verification system versus identification system.

VII. APPLICATION OF MULTI MODEL BIOMETRICS

The defense requires high level security system for boarder management; civil application and interface to terrorism and first responder validation are the major area. Which use the multi model biometric, personal information data and work transaction needed fraud prevent solution that increases security and user familiar interface? Multi model biometric provide great solution to all other areas where the high security is require.

VIII. CONCLUSION

Multi model biometrics system can overcome some of the limitation of unimodel systems. As an example the problem of non-universality is addressed since multiple traits can ensure sufficient population coverage

Biometric technology adds a new layer of security by ensuring secure verification or identification and authentication.

We have developed a multi model biometric system which integrates decision made by face recognition, finger print verification and voice verification to make user identification.

CONFERENCE PAPER National Conference on
"Internet Technology and Cyber Crime"
On 11 January 2015
Organized byPraful Narooka and
Sponsored by Agarwal College, Merta City (Nagpur)