Development of Human-Biometric Sensor Interaction Model for Distinctive Assert Framework

T.Venkat Narayana Rao[1], Shiny Kannarapu[2], Khasim Shaik[3]

Professor, Computer Science and Engineering, Sreenidhi Institute of Science and Technology,
Student, Computer Science and Engineering, Sreenidhi Institute of Science and Technology,
Asst.Professor, Computer Science and Engineering, Sreenidhi Institute of Science & Technology,
Hyderabad, India

Abstract : These days Biometric technologies have acquired a distinguished element of solving digital identity and crucial security tasks. These technologies enhance identification and authentication depending on the physiological and behavioral characteristics of an individual. This made the governmental agencies to choose the technology of Biometrics as an additive for distinctive scenarios in which identification through ID cards and passports play a prominent role. Recent researches have proclaimed that Biometric Systems depends on how individuals collaborate and agree with it the responsibility of hoaxer in an Distinctive Assert Framework and has amalgamated to develop the HSBI model to a full genre which can grade likely False Asserts and Attack Presentations. This paper, reviews the work related to Human-Biometric Sensor Interaction model with respect to the initiation of tokens into the Biometric System that perform tasks relating to the security enhancement.

Keywords: *Authentication, Sensor, Biometric , security attack, framework.*

*****

1. Introduction

1.1 Biometric Technology

Biometric Identification Technology is defined as an involuntary detection or distinctive affirmation of individuals depending on their physiological and behavioral attributes. Biometric exploration focuses on five basic elemental areas: data stock, decision-making, symptom handling, conveyance, and accumulation. Every section in this technology underlies a particular provocation. Typically, the data stock segment of the General Biometric Model includes an issue of proposing their biometric specimen to the detector.

Assisting a successful biometric provocation is elemental to the success of the biometric system. False provocation by a legitimate user will result in functional measures which include throughput, costs, and performance. Unsuitable categorization of the biometric traits can also result in production of the system. Biometric trials and computations has, traditionally verified the compact among the incorrect match standard and erroneous non-match standard . However, these results do not disclose all the underlying features of biometric presentation. For an instance, when a metric such as quality is calculated, the outcome may fundamentally be different but it will be uncertain which individual is responsible for that result to change or how[1][5][6].

The system approximates and calculate the presentation of a biometric system and concentrates at the system-level. This means that the experts and engineers are focusing in the errors which are reported by systems such as Failure to Enroll (FTE) rate, Failure to Acquire (FTA) rate, False Accept Rate (FAR), and False Reject Rate (FRR) . Customary presentation verification methods have worked well to evaluate transpiring technologies, new biometric procedures, and algorithm adaptations. On a whole, error in presentations can be categorized into three subgroups: the efforts of the users or manipulators, which can be estimated based on physical, behavioral, and social factors, the environment, and the matching algorithm. Hence, the customary manipulation methods centre on the universal manipulation of biometric systems ,but disregarding specific individual effects[2][3][7].

1.2 Distinctive Assert Framework

Wide range of biometric affirmation systems mostly authorizes the authentication processes which requires the manipulator to prove themselves. This asserts that the user may need an integration of biometric statistics, samples, licenses or the entry of individual bona fides (e.g. PIN, username/password). The system will direct to organize wherever the user is the legitimate owner of the file/sample and will authorize a co-operation if fixed validations are done. After the bona fide is submitted, the individual scrutinizes his/her biometric and the captured outline is compared against only the stored outline that has been located with the bona fide. These applications strive to authenticate a traveler's assert of distinction by going through a delegated sample (usually an electronic passport or registered travelers card.) These systems are able to check the originality of such files and can spot various counterfeits and identification issues to the nearest dominance. This solution make use of its users by guarding their records and asserts, blocking probable counterfeit attacks that may be difficult to defend without the help of technology[13][9].

1.3 Human-Biometric Sensor Interaction Model

The Human-Biometric Sensor Interaction (HBSI) Model demonstrates how metrics measured from biometrics sensors (sample quality and system performance) can be merged with bio-technology (physical and emotional) and practicality (accuracy, efficiency and satisfaction) metrics to compute the entire presentation of a biometric system. Relating this model permits a complete picture to better an understanding of what influences a biometric systems presentation. The model (Figure 1) has its origins lie at the collaboration of practicality, human factors, and image standard / performance. For example, initial work of the team discussed the issue of hand placement based on evidence collected during a biometric feasibility study[4][10].

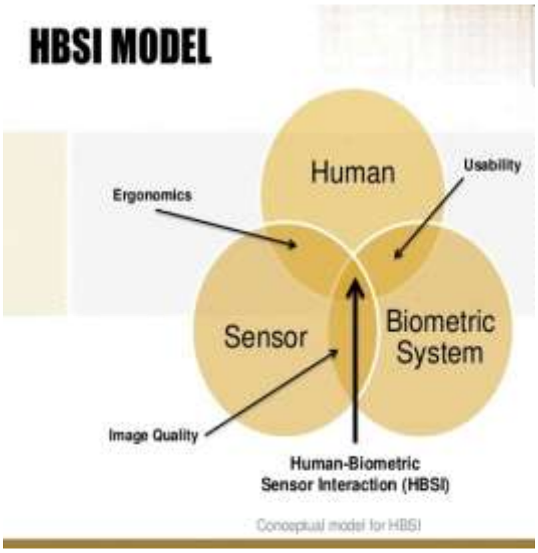

Figure 1.The Original HBSI model

The model has been validated against several modalities. The next generation of the model has adapted to take into account intelligent sensors that have some signal processing / image standard / feature extraction intelligence during detection and accession. Six different types of metrics were evolved based on the HBSI model. Defective interaction (DI), concealed interaction (CI), and false interaction (FI), are based on erroneous presentations only [14].

Concealed interactions take place when the subject proposes an erroneous biometric sample, and it is accepted by the system as a correct sample. A false interaction is when the system provides a report to the user of an erroneous presentation. The system correctly manages the sample as an error and generally provides an error notification. The HBSI model also records errors related to capable presentations, such as failure to detect (FTD). This is when an exact presentation has been made, but the sensor does not recognize the interaction. Other measures involve Failure to Process (FTP), and Successfully Processed Sample (SPS). An FTP is an exact presentation that does not enter the system due to low standard or a failed feature removal. SPS is a detected presentation with no perceptible errors that is correctly allowed into the biometric system.

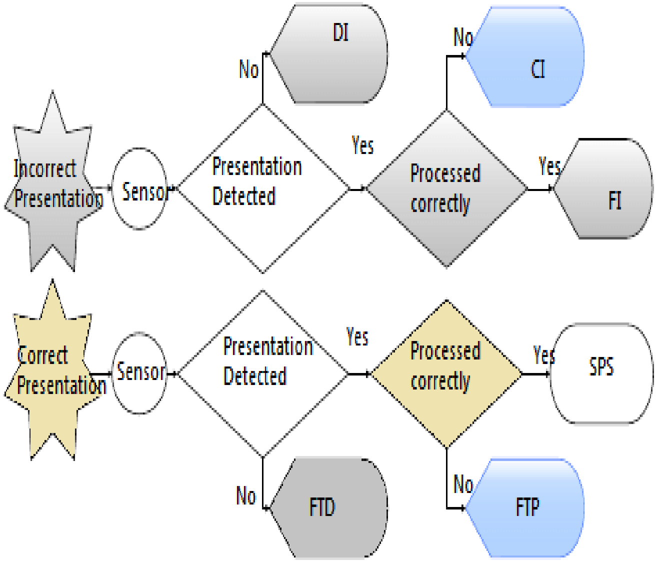

Figure 2.HBSI Presentation Framework

2. The Full HBSI model

To provide practitioners and investigators with elements that allow the appraisal of erroneous asserts, thrashes, token presentations a new sub-configurations have been evolved. These new configurations have been expanded comfortably within the HBSI Presentation Framework to produce the full HBSI model, allowing a wide range of classifications which are to be deployed within a distinctive assert framework Future work will investigate applying the Operational Times model to the Full HBSI Model. This full HBSI model, as shown in Figure 2 and figure 3 accounts for systems that permit for one or more aspects of authentication. This version of the model works to include token, attack and erroneous presentations, iterating to the beginning of the process (if required) once a process of authentication has been done. Latest technologies that execute anti-spoofing or animation detection components and the capability to standardize potential attacks to a figure of dominance for successive processing, were originally not considered in the original implementation of the HBSI Model as shown in figure 4. Hence, an advantage of using the full HBSI model permit the classifications of potential erroneous asserts and attack presentations[11][14].

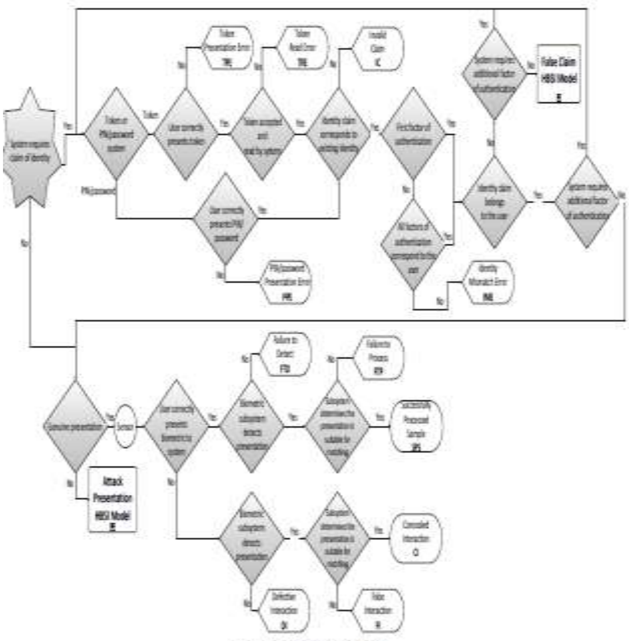

Figure 3: The Full HBSI Model

Figure 3.The Full HBSI model

2.1 The Erroneous Assert Model

In the case of an ABC system, workforce are employed and instructed to look after multiple synergies and to handle irregularities where ever applicable. For an instance, if an erroneous assert is made (e.g. an accidental swapping of the passport) and the system is capable to detect and subsequently raise the claim to the border guard, then workforce will interfere and initiate action on the sample as either a Refused Sample or a Forwarded Sample. It will be significant for systems to be able to classify false claims as this could lead to breach of security[11].

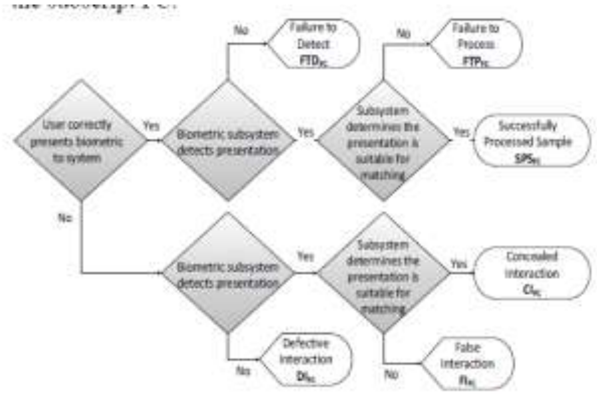
User correctly presents biometric to system
Yes
No
Biometric subsystem detects presentation
Yes
No
Failure to Detect
FTD_{EC}
Subsystem determines the presentation is suitable for matching
No
Failure to Process
FTP_{EC}
Yes
Successfully Processed Sample
SPS_{EC}
Biometric subsystem detects presentation
Yes
No
Defective Interaction
DI_{EC}
Subsystem determines the presentation is suitable for matching
Yes
Concealed Interaction
CI_{EC}
No
False Interaction
FI_{EC}

Fig 4. Erroneous Assert Model

2.2 Attack Presentation Framework

Systems which involve kind of attacks such as of anti-spoofing or liveliness detection will grasp the Attack Presentation HBSI Model (figure 5). The HBSI Attack Presentation Model make sure that the exact biometric sample is been recognized, ventures to categorize it as an attack sample, and determines if the presentation is suitable for combining to save the sample. If the biometric subsystem categorizes the presentation as an attack, it either ensigns and forwards the sample to then respective dominance or simply ensigns the sample and refuses it. If the presentation is not classified as an attack, it can achieve one of three attack HBSI erroneous metrics. Whilst improvements to hardware and software are continuously being developed to counter specific threats and types of attacks in large scale biometrics systems, there is the underlying issue of the possibility of identity attacks[16].

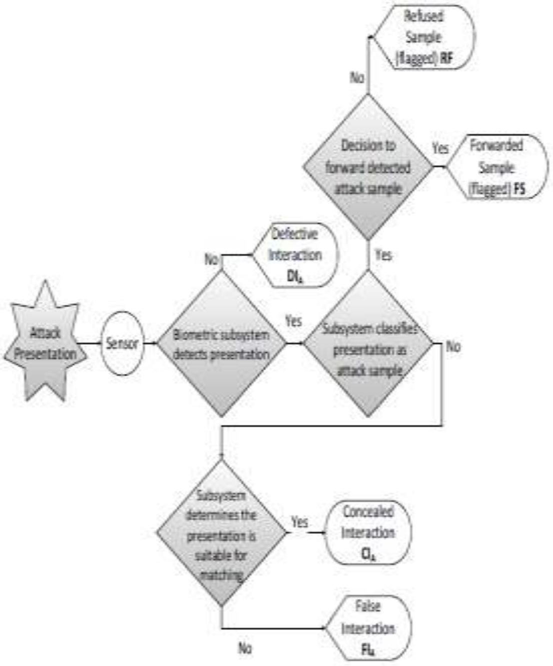
Refused Sample (flagged) RF
No
Decision to forward detected attack sample
Yes
Forwarded Sample (flagged) FS
Defective Interaction
DI_A
No
Yes
Attack Presentation
Sensor
Biometric subsystem detects presentation
Yes
Subsystem classifies presentation as attack sample
No
Subsystem determines the presentation is suitable for matching
Yes
Concealed Interaction
CI_A
False Interaction
FI_A
No

Fig 5. Attack Presentation Model

3. Assessing Distinctive Assert Framework

Developing the HBSI Model for distinctive assert framework requires auxiliary processes so the full interaction, be it a genuine, erroneous presentation, can be fully understood. Applying these supplementary models will allow researchers and designers to analyze the full token and biometric interaction, which will be key for the development of these systems. Categorizing these presentations that involve an assert of distinction which allows the capability to compute metrics beyond traditional rates in acquisition and decision-making, enabling a full account on the evaluation of usability, bio-technology and sample quality in these systems.

In an attack situation where the system decides that no supplementary authentication is needed for the sample but is assessed as a non-genuine presentation through liveliness/anti-spoofing components (for example, it may not detect movement in the presentation of the face) then this interaction will be forwarded to the Attack Presentation Model. If the system detects the sample and then determines an attack, then this sample may be then ensign as either Refused or Forwarded, allowing dominance to handle the irregularity and guide the user out of the process.

The noble case would be for presentations to result in a Successfully Processed Sample but using this model it will allow a wide range of metrics to be obtained, categorizing all types of presentations giving the ability for a system to highlight potential areas in the system which may need Development[12].

4. Applications

i) Border Control/Airports

Border Control/Airport Biometrics play a key area of application for biometric technology is at the border. Anyone who has travelled by air can tell you security checkpoints border crossings which are some of the most frustrating places to have to move through. Now, biometric technology is helping to automate the process. Trusted passenger screening initiatives are being automated.

ii) Consumer/Residential Biometrics

Recent innovations in mobility and connectivity have created a demand for biometrics in the homes and pockets of consumers. Smartphones with fingerprint sensors, apps that allow for facial and voice recognition, mobile wallets: these are the popular ways that consumers around the world are finding biometric in their lives[8].

iii) Finance sector

Financial sector is one of the vital key area where in biometrics can benefit the financial transactions for decision making. With recent implementations of mobile and online payments protected by biometrics, it’s very clear that the security and convenience are welcomed by the consumer when it comes to buying goods and those benefits are gradually making their way into the higher risk world.

iv) Fingerprint &Biometric Locks

These electronic systems take a digital picture of the fingerprints and then transmit them into a source for verification. The use of biometrics offers a much higher level of security than passwords or keys, as it is effortless for an unauthorized individual to steal another's key or password and thus gain access to a restricted area. Biometric physical access control solutions are stronger authentication methods than keys, key cards and PINs for a simple reason that can be expressed as “ they’re what you are, not what you have”.

v) Healthcare Biometrics

Healthcare Biometrics brings security and convenience wherever they’re deployed, but in some instances they also bring increased organization. In the field of healthcare this is mostly true. Health records are some of the most valuable personal documents out in reality, doctors need access to them quickly, and are ought to be they to be accurate[14][15].

vi) Time and Attendance

Biometric time and attendance solutions exist to keep track of who is where and when they’re there. In its most basic form, time and attendance tracking is a schedule, in which workers, volunteers can be traced [20].

vii) Other Applications

Other Biometric Applications such as cyber threats continue to rise and connectivity begins to grow all facets of life around the globe other biometric applications that are not listed in our showcase section rise to meet the demand[10].

5. Conclusion

Enclosing the full HBSI model will allow the integration of the framework to large-scale applications such as Automated Border Control and biometric identity solutions used in the likes of banking and in healthcare. The importance of these models will be seen through the expansion of HBSI to real applications. In this paper, the additional frameworks to the HBSI model has been discussed in detail, which allow the categorizations of likely attacks and erroneous asserts are advised to be fed to the biometric system. Future works would focus on introducing experimental data to the models, further allowing the ability to highlight areas where the proposed integrations are possible.

The work in this domain is already in progress i.e. the application of involuntary identification using the Human Biometric Sensor Interaction model to identify presentations in real-time, which will contribute to the success of manipulating overall system performance in terms of usability and sample quality. Moreover, merging the full HBSI model and the Operational Times model will prove beneficial to understanding presentations with respect to the transaction times. The evaluations of complex multi-model systems will enhance the observation of testing techniques, where the environment in which these systems would usually operate in must be replicated to the highest possible detail. Thus, therefore intensifying the capability to extend the model to new technology and the ability to assess and report on the latest trends in the biometric world.

References

[1] J. Wayman, A. Jain, D. Maltoni and D. Maio, "An Introduction to Biometric Authentication Systems," inBiometric Systems, Springer, 2005, pp. 1-20.

[2] A. Mansfield and J. Wayman, "Best Practices in Testing andReporting Performance of Biometric Devices," NPL,Teddington, 2002.

[3] S. Li, J. Lai, T. Tan, G. Feng and Y. Wang, Advances inBiometric Person Authentication, Guanzhou: Springer,2004.

[4] E. Kukula, M. Sutton and S. Elliott, "The Human-BiometricSensor Interaction Evaluation Method: Biometric Performance and Usability Measurements," IEEETransactions on Biometrics Compedium, vol. 59, no. 4, pp.784-791, 2010.

[5] C. Wilson, "Devices and Applications," in Vein PatternRecognition: A Privacy-Enhancing Biometric, Hoboken,2010, pp. 116-117.

[6] J. Pato and L. Millet, Biometric Recognition: Challenges andOpportunities, Washington, D.C.: National Research Council of the National Academics, 2010.

[7] M.Nuppeney, "Automated Border Control - State of Playand Latest Developments," in NIST IBPC 2014,Gaithersburg, 2012.

[8] Frontex Europa, "Best Practice Operational Guidelines forAutomated Border Control (ABC) Systems," Frontex,Warsaw, Poland, 2012. 9. Frontex, "BIOPASS II Automated Biometric Border

[9] Crossing Systems based on Electronic passports and facialrecognition," Frontex, Warsaw, Poland, 2010.

[10] R. Amin, T. Gaber, G. Taweel and A. Hassanien, "Biometricand Traditional Mobile Authentication Techniques:Overviews and Open Issues," in Bio-inspiring CyberSecurity and Cloud Services: Trends and Innovations,Springer, 2014, pp. 423-446.

[11] U.Uludag and A.Jain, "Attacks on Biometric Systems: ACase Study in Fingerprints," in SPIE-EI 2004, Seucirty, Seganography and Watermarking of Multimedia Contents VI, 2004.

[12] A.Tiwari, R.Agarwal and S.Goyal, "Biometric Authentication for Mobile Banking Seucirty," SSRN, India, 2014.

[13] B. Samuel and O. Abass, "An Overview of Biometric Identifiers with Emphasis on the Concepts And Applications of Finger Vein Recognition," International Journal ofComputer Science and Mobile Computing, vol. 2, no. 8, pp. 257-261, 2013.

[14] A. Omotosho, O. Adegbola, B. Adelakin and A. Adelakun, "Exploiting Multimodal Biometrics in E-Privacy Scheme for Electronic Health Records," Journal of Biology, Agricultureand Healthcare, vol. 4, no. 18, pp. 22-33, 2014.

[15] S. Elliott, E. Kukula and N. Sickler, "The Challenges of the Enviroment and the Human/Biometric Device Interaction on Biometric System Performance," in HBDI and EnviromentProceedings, 2004.

[16] E. Kukula, "Understanding the Impact of the Human-Biometric Interaction & System Design on Biometric Image Quality," in NIST Biometric Quality Wortkshop II Fingerprint & Quality Calibration, Gaithersburg, MD, 2007.