Automatic Detection of Biometric Transaction Times

Michael E. Brockly and Stephen J. Elliott
Department of Technology Leadership and Innovation
Purdue University
West Lafayette, IN 47907, USA
mbrockly@purdue.edu and elliott@purdue.edu

***Abstract*—The purpose of this paper is to illustrate the automatic detection of biometric transaction times using hand geometry as the modality of interest. Video recordings were segmented into individual frames and processed through a program to automatically detect interactions between the user and the system. Results include a mean enrollment time of 15.860 seconds and a mean verification time of 2.915 seconds.**

Keywords—biometrics; hand geometry recognition; HBSI, transaction time

I. Introduction

This paper highlights the use of hand geometry to demonstrate a method of automatically calculating biometric transaction times. Biometrics is defined as the automated recognition of individuals based on their behavioral and biological characteristics [1]. Hand geometry refers to the process of identifying a person by the shape of his or her hand. This modality is based on taking a photograph of the user's hand while placed on a surface, finding singular points on the hand and taking measurements of them [2]. Hand geometry systems use different measurements of features such as finger length, finger width, finger thickness, finger area and palm width to perform authentication on individuals [3].

Hand geometry is commonly used in time and attendance systems or access control systems. Operationally, hand geometry has proven extremely popular in time and attendance applications [4]. There are also many different benefits that make hand geometry appealing to businesses and users. Hand geometry functions as a medium cost system since only a low/medium resolution charged-coupled device (CCD) camera is needed. It also provides fast computational speeds, low template size, and good ease of use for users [5].

During the capture process, a certain amount of time occurs when the subject is enrolling into the system and subsequently verified. This period beginning with the biometric sample presentation and ending with the biometric system decision is known as biometric transaction time [6]. Calculating these time periods help to better understand not only the system's ease of use, but also the amount of time a user's spends when using a particular biometric. This amount of time creates an understanding of which biometric is the best choice for a specific application. When implementing a biometric system, especially in a time and attendance environment, a fast transaction time is required to prevent unnecessary time costs.

II. Background

A. Motivation

The motivation for this research was to establish a way to automatically determine transaction times from recorded video, without the need for manual coding. Prior research into biometric transaction time includes using human observers to code when events occur in order to achieve time on task [7]. Other research has recommended video recording these events in order to manually record the timing data at a later time [8]. Human observers may be prone to error as they may be unable to note the exact moment when interactions occur, or note it repeatedly. Video coding is also susceptible to interrater reliability issues. Interrater reliability represents the degree to which the ratings of different judges are proportional when expressed as deviations from their means [9]. Not all video coders will report the same result and this research aims to achieve consistent reporting of transaction times without the use of humans.

B. Impact to the Community

For biometric timing terminology such as transactions, attempts, presentations, and interactions, conflicts in definitions exist in many sources [6], [10]-[13]. This research primarily follows the definitions used in [10] with the exception of interaction. A transaction is defined as "the sequence of attempts to the system on the part of the user for the purpose of enrollment, verification or identification" [10]. An attempt is defined as "the submission of one (or a sequence of) biometric samples to the system on the part of the user" [10]. A presentation is defined as "the submission of a single biometric sample to the system on the part of the user" [10]. Finally, an interaction is defined by the authors as the action(s) that take place within a presentation. Fig. 1 shows the hierarchy of these terms.

III. Methodology

The data collection used an Ingersoll Rand Handkey II as the biometric capture device. The device was positioned against a wall and located 90 centimeters above ground level. All events were recorded on a Logitech HD Pro C910 webcam. This webcam was positioned 24 centimeters above the hand geometry machine in order to completely record all lights on the top of the device. These recordings were used to monitor all

  DOI:

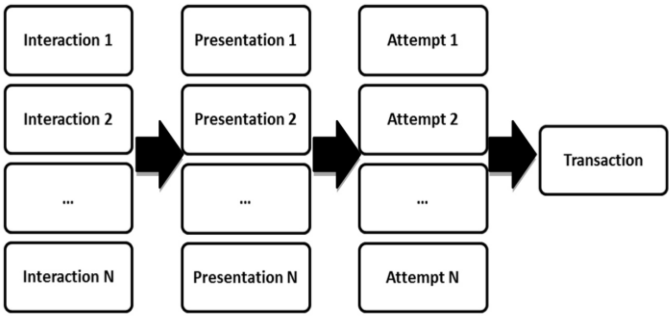

Fig. 1. Terminology hierarchy.

interactions that occurred within the biometric transaction process. The device and camera setup is displayed in Fig. 2.

This study involved the data collection of thirty-five subjects enrolling into a hand geometry system and subsequently verifying their hand in the system immediately afterward. The enrollment process consisted of the test administrator entering a PIN and the subject placing their hand three times on the surface of the device to create a biometric template. Once enrolled in the system, the test administrator entered the PIN again and the subject placed their hand on the surface one more time to verify. The verification process was repeated four times.

After the data collection finished, videos were split into individual frames using freely available software called FFmpeg [14]. The video recordings were segmented into fifteen frames per second. These frames were then analyzed using the Hand Geometry HBSI Tool developed at the Biometrics Standards, Performance and Assurance (BSPA) Labs at Purdue University. This program, created in Java Standard Edition (SE) 1.7, automatically detects when lights change on the device, determining when interactions occur. As

Fig. 2. Recording configuration.

Fig. 3. Hand geometry lights.

the frames are analyzed, any light changes from off to on and vice versa are noted. A listing of all possible lights is shown in Fig. 3. The red lights near the hand in Fig. 3 show when an interaction occurs. There is also a green and red light at the top of the sensor that when illuminated, denotes either a successful or unsuccessful attempt.

The program works by responding to color changes at specific groupings of pixels in the video recordings. The program user will load in the video frames into the program and crop out only the selected area of interest (Fig. 4). Before analyzing the data, the authors established a model shown in Fig. 5 to determine the timing schema. This model was created in accordance with the Operational Times Model shown in [6]. This research is primarily concerned with the biometric transaction time. The time begins when the lights are first all on, until the time that they are all off and the green or red light is illuminated. Subject interaction time was not used for this research since the test administrators entered the PIN for each of the subjects.

Once the enrollment and verification times were determined, failed presentations were analyzed in terms of Human-Biometric Sensor Interaction (HBSI) errors. Displayed in Fig. 6, the HBSI error framework is used to determine

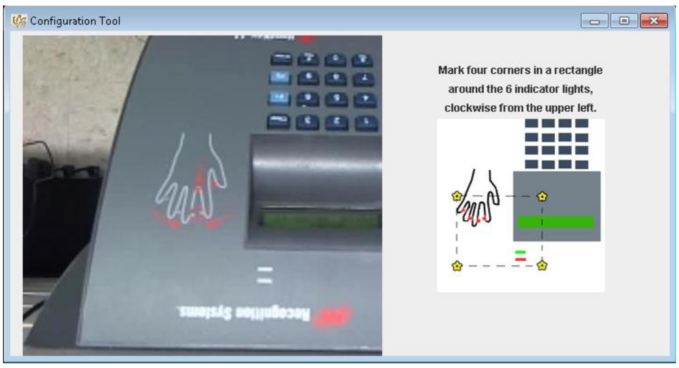

Fig. 4. Hand geometry HBSI tool.

  DOI:

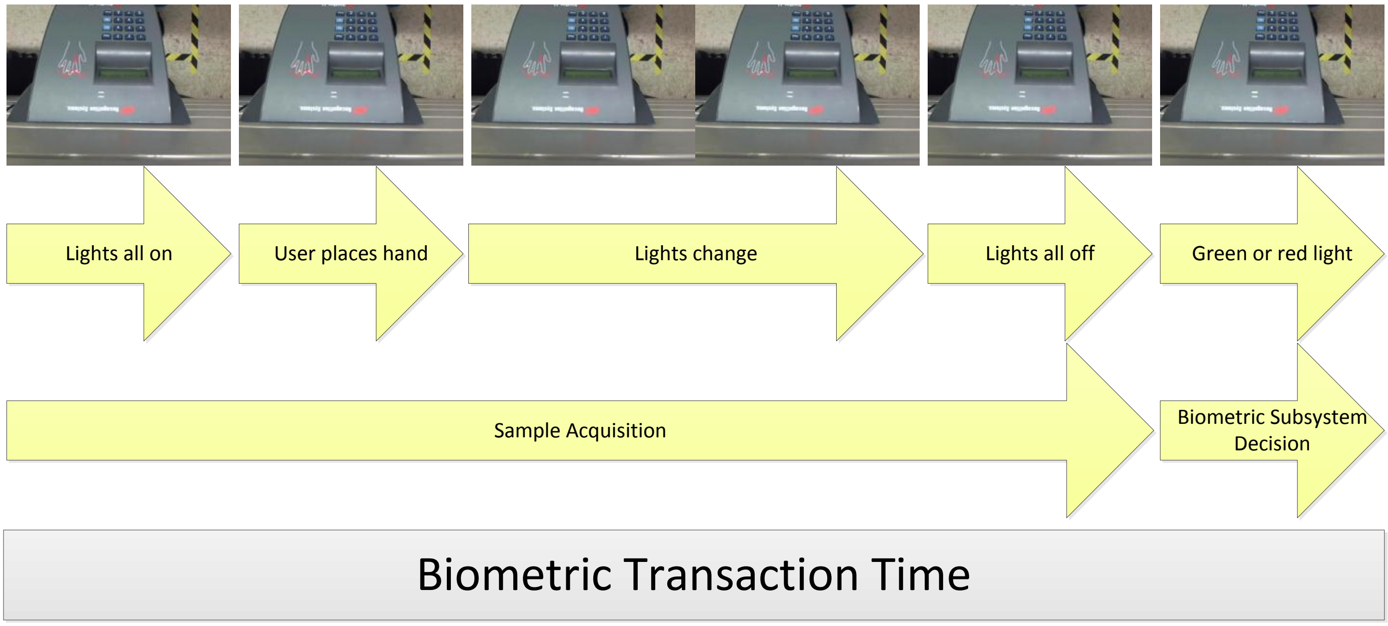

Fig. 5. Biometric transaction time model.

different classifications of errors that occur when a human interacts with a biometric system. Originally designed for a swipe fingerprint sensor, the HBSI methodology applies to many biometric systems including dynamic signature verification, iris recognition, and in this case hand geometry.

IV. Results

The methodology was used to determine transaction times for both the enrollment transaction and the verification transactions.

A. *Transaction Times for Enrollment*

Each subject began the data collection by following the enrollment procedure. Prior to collection, subjects were assigned a specific PIN number that was entered by the test administrator. After the PIN was entered all four of the hand lights on the device were illuminated. Once illuminated, the enrollment time started. Subjects inserted their hand and touched all the pins in the device with their fingers to extinguish all of the lights. After the lights were out, the subject repeated this process two more times in order to complete the process. Once three presentations occurred, the biometric template was created and the subject was successfully enrolled into the system.

All thirty-five subjects were successfully enrolled into the hand geometry system with three presentations. The shortest enrollment time was 5.802 seconds and the longest enrollment

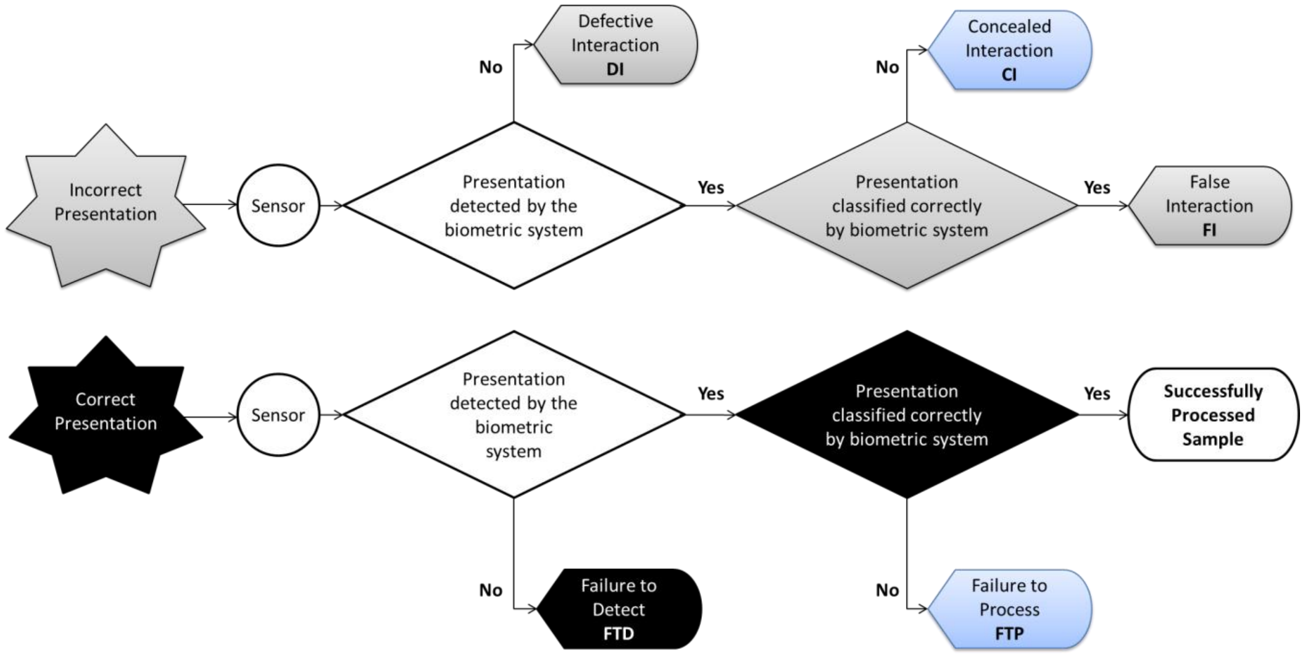

Fig. 6. HBSI error framework.

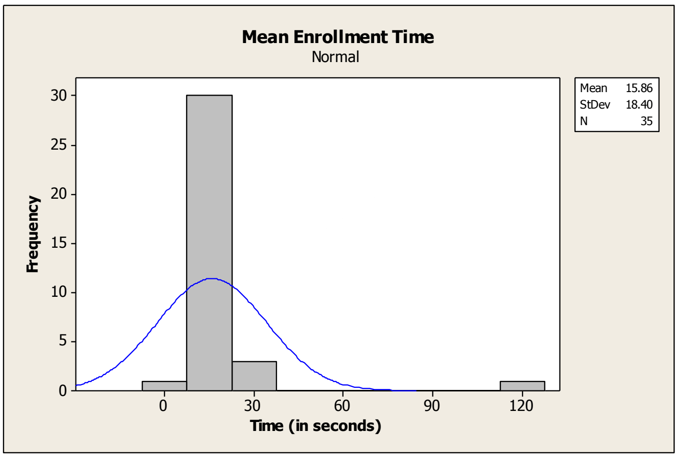

Fig. 7. Mean enrollment time.

time was 116.142 seconds. Although the user with 116.142 seconds was an outlier, they did not achieve a system timeout and were successfully enrolled. The mean enrollment time was 15.860 seconds. Fig. 7 displays the histogram of mean enrollment time.

B. *Transaction Times for Verifications*

Once enrolled into the system, each subject was verified against their template four times. The test administrator entered the PIN for the subject and again all four lights were illuminated. Once the lights came on, the verification time started, as did the transaction time. Subjects inserted their hand and touched all the pins in the device with their fingers to extinguish the lights. Once all the lights were extinguished, the device used either a green or red light to denote a successful to unsuccessful transaction respectively. Thirty-three subjects were able to complete four successful transactions and only two subjects required five attempts to do so.

Table 1 shows the mean transaction times for each of the four verifications along with an overall mean verification time. The two unsuccessful attempts with transaction times of 5.132 seconds and 2.066 seconds were excluded from the results. Verification transactions three and four had the lowest mean transaction times. Verification transaction four, although having a 0.056 second longer mean time than transaction three, had the lowest standard deviation. This trend indicates that the range of individual transaction times is being reduced, and subjects may be becoming habituated to the verification process. Boxplots of verification times are included in Fig. 8; overall the four verification transaction times are not statistically significant from each other.

TABLE I. MEAN TIMES

Category	Mean Time	Standard Deviation
Enrollment	15.860 seconds	18.40
Verification 1	3.040 seconds	1.297
Verification 2	3.119 seconds	2.192
Verification 3	2.723 seconds	1.076
Verification 4	2.779 seconds	0.963
Verification Mean	2.915 second	0.8460

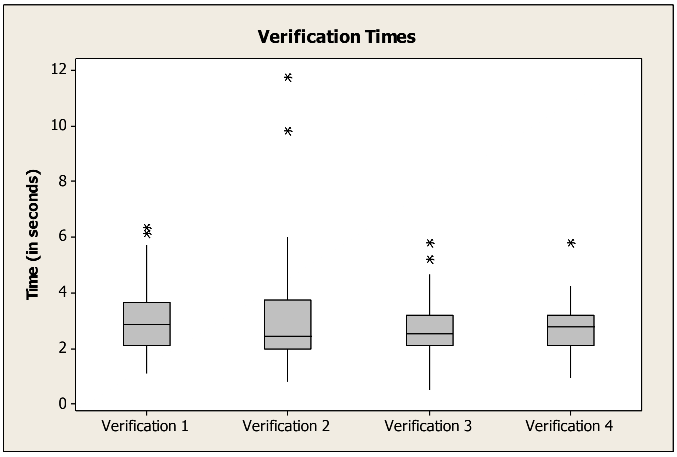

Fig. 8. Boxplot of verification times.

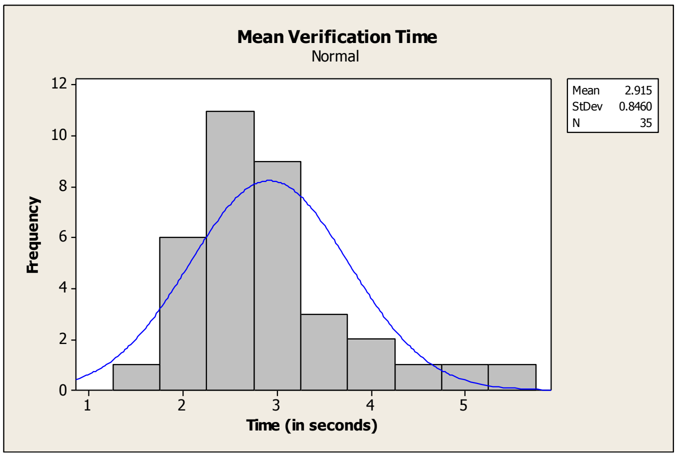

Fig. 9. Mean verification time.

C. *HBSI Errors*

Using the terminology outlined in Fig. 1, the vast majority of presentations were classified as successfully processed samples (SPS). All enrollment attempts were successful, showing no HBSI errors in the enrollment phase. Out of the 140 verification presentations, only two presentations were not classified as SPS. Two subjects each had one failure to process (FTP) during their four verification attempts. These subjects were both able to extinguish all of the lights and receive feedback from the system that the quality was not high enough to be accepted. Each of these subjects' other three verification presentations were SPSs.

V. CONCLUSIONS

This paper has shown that videos can be automatically coded post-hoc to determine transaction times without the use of a human operator. Transaction times in this research are accurate to one-fifteenth of a second. This allows for very accurate timing data as soon as events in the biometric system occur. Automatically coding data allows researchers to spend less time coding data and more time analyzing it. This method eliminates interrater reliability and human bias when coding.

This paper has also validated the terminology expressed in section II. Through frame segmentation and analysis with the hand geometry tool, individual interactions with the system are demonstrated. These interactions can be quantified further than simply transaction times. Future research will now be able to report exactly how many interactions, presentations, etc. occur with complete confidence. In the metric of hand geometry, the tool can also detect the number of interactions needed to perform an enrollment or verification. Each time one of the lights change on the device, a new interaction is recorded. Recording which lights remain on the longest can help to improve the device or improve the instructions to the subject.

Outside of hand geometry, the same logic may be applied to other biometric modalities. Individual interactions occur in every biometric process. When video is recorded, it can be processed through a similar tool to record whenever pixels in the recording change. Future research includes using this methodology on other biometric modalities such as fingerprint recognition and iris recognition. These modalities can be analyzed for both biometric transaction times as well as the number of interactions, presentations, or attempts needed to successfully complete a transaction.

The methodology can also be replicated in order to detect Human Biometric Sensor Interaction (HBSI) errors. In the event of an error, metrics can be automatically assigned based on a set of conditions. For example, in hand geometry, if the red light is shown to denote an unsuccessful attempt, the presence of the other red hand lights can be used to justify a specific error metric such as a concealed interaction (CI). HBSI error detection can also be replicated onto other modalities in order to quantify error metrics. This will be validated in future research.

REFERENCES

[1] International Organization for Standardization (ISO), Information processing systems – Vocabulary – Part 37: Harmonized Biometric Vocabulary, ISO/IEC DIS 2382.37, 2010.

[2] R. Sanchez-Reillo, “Hand Geometry,” Encyclopedia of Biometrics, Springer US, 2009. doi: 10.1007/978-0-387-73003-5_251

[3] D. Zhang and V. Kanhangad, “Hand Geometry Recognition,” Encyclopedia of Cryptography and Security, Springer US, 2011. doi:10.1007/978-1-4419-5906-5_1377

[4] S. Liu and M. Silverman, “A practical guide to biometric security technology,” IT Professional, vol. 3, no. 1, pp. 27–32, 2001. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=899930

[5] R. Sanchez-Reillo and A. Gonzalez-Marcas, “Access control system with hand geometry verification and smart cards,” Aerospace and Electronic Systems Magazine, IEEE, vol. 15, no. 45, pp. 45–48, 2000. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=825671

[6] R. T. Lazarick, E. P. Kukula, and S. J. Elliott, (2009, July). “Operational Times,” Encyclopedia of Biometrics, Springer US, July 2009. doi:10.1007/978-0-387-73003-5_114

[7] M. Theofanos, B. Stanton, S. Orandi, R. Micheals, and N. Zhang, NISTIR 7403 Usability Testing of Ten-Print Fingerprint Capture, NISTR, pp. 1-56, March 2007. http://zing.ncsl.nist.gov/biousa/docs/NISTIR-7403-Ten-Print-Study-03052007.pdf

[8] B. P. Bailey, J. A. Konstan, and J. V. Carlis, J. V, “Measuring the effects of interruptions on task performance in the user interface,” Proc. IEEE Int. Conf. on Systems, Man and Cybernetics, pp. 757–762, 2000. doi:10.1109/ICSMC.2000.885940

[9] H. E. A. Tinsley and D. J. Weiss, “ Interrater Reliability and Agreement of Subjective Judgments,” J. of Counseling Psychology, vol. 22, no. 4, pp. 358–376, 1975.

[10] International Organization for Standardization (ISO), Biometric Performance Testing and Reporting – Part 1: Principles and Framework, ISO.IEC FCD 19795-1, 2005.

[11] International Organization for Standardization (ISO), Information technology – Biometric performance testing and reporting – Part 6: Testing methodologies for operational evaluation, ISO/IEC FCD 19795-6.2, 2011.

[12] R. Micheals, B. Stanton, M. Theofanos, and S. Orandi, A Taxonomy of Definitions for Usability Studies in Biometrics, Gaithersburg: NIST, 2006.

[13] ILO Seafarers’ Identity Documents Biometric Interoperability Test (ISBIT-4) Report, ILO, vol. 2003, pp. 1-162, 2009.

[14] FFmpeg (Ver. 1.2). http://www.ffmpeg.org