The Human–Biometric-Sensor Interaction Evaluation Method: Biometric Performance and Usability Measurements

Eric P. Kukula, Member, IEEE, Mathias J. Sutton, and Stephen J. Elliott

Abstract—This paper discusses the human–biometric-sensor interaction (HBSI) evaluation method that uses ergonomics, usability, and sample quality criteria as explanatory variables for the overall biometric system performance. The HBSI method was proposed because of questions regarding the thoroughness of traditional system-level performance evaluation metrics such as the failure-to-acquire (FTA) rate, the failure-to-enroll (FTE) rate, the false-accept rate (FAR), and the false-reject rate (FRR). Data were collected from 85 individuals over three visits that accounted for 25,867 user interactions with three swipe-based fingerprint sensors. The results revealed that traditional biometric metrics that focus on system-level metrics are not providing sufficient reporting details regarding the user interaction with the devices. In this paper, the systemic FTA rate of 14.38% was shown to be segmented into three metrics: false interaction (FI), failure to detect (FTD), and concealed interaction (CI). The results show that the FI accounted for 69.05% of the systemic FTA presentations, FTD accounted for 30.71%, and CI accounted for 0.24%. Overall, the HBSI evaluation method and framework for biometric interactions provided new metrics that improve the analysis capabilities for biometric performance evaluations as it links system feedback to the human–sensor interaction, enabling researchers, system designers, and implementers to understand if the issues are the result of the system, the user, both the system and the user, or some other extraneous factor.

Index Terms—Biometrics, error rates, human–biometric-sensor interaction (HBSI), measurement, testing and reporting, usability.

I. INTRODUCTION

BIOMETRIC technologies by definition recognize individuals based on behavioral and physical characteristics such as fingerprints, facial features, an iris pattern, hand geometry, a vein pattern of the palm or finger, and signature dynamics. Biometrics can be described by five desirable properties, as outlined in [1], which has been amended by many others over the years. While these five properties are described in the literature as being ideal, each deployment of biometrics is also challenged by them. First, a biometric must be universal, which means that the features are available on all people. Second, the features must be invariant, which means that the features extracted must not change over time. Third, the features must possess high intraclass variability, which means that the biometric data collected from one user are distinct from another. Fourth, the biometric features must be consistently extractable, which means that the sensor must be able to consistently and repeatedly collect and extract the biometric features over time. Last, the collection of the biometric data must be acceptable for use by the population.

This paper focuses on the latter two properties: collectability and acceptability in terms of biometric testing and reporting measurements using the human–biometric-sensor interaction (HBSI) evaluation method.

Traditional approaches to evaluate the performance of a biometric system have been focused at the system level, which means that evaluators and designers have been interested in system-reported error rates such as the failure-to-enroll (FTE) rate, the failure-to-acquire (FTA) rate, the false-accept rate (FAR), and the false-reject rate (FRR). Traditional performance evaluations have worked well to evaluate emerging technologies, new biometric modalities, and algorithm revisions. However, the focus on system-level evaluations has produced limited research focused on usability and issues relating to how humans interact with and use biometric devices. Therefore, user interaction errors have been either coded and analyzed as system-level errors or, worse, overlooked. As the community becomes more experienced in testing and evaluation, standardized testing documents and methodologies [2]–[4] and long-held assumptions about evaluation metrics need to be reexamined, as analysis capabilities have increased, allowing for system-level performance errors to be dissected into errors caused by the biometric system, the user, both the system and the user, or some other extraneous factor. The underlying question one should ask when examining a biometric system is: what affects biometric system performance? In general, performance failures can be classified into three subgroups: the users (physical, behavioral, and social factors), the environment, and the matching algorithm. While it is important to understand each of the three groups when designing a biometric system, the interrelationship between the groups is important to not only acknowledge but also measure the impact on the other subgroups during biometric performance evaluations, which is illustrated in Fig. 1.

The successful deployment of biometric systems, regardless of modality or application, needs to take into consideration
how individuals interact with the device. Failure to do so may cause degradation in the optimal performance of the biometric sensor, causing heightened error rates such as FTA, FTE, FAR, and FRR. Furthermore, if users cannot successfully interact with a biometric device, there is a potential for failure to use, which means that people will switch to using other competing technologies. Therefore, the use of biometrics will likely be dependent on individuals’ ability to not only use it more effectively but also find it more efficient than the technology that it replaces (such as the username/password combination in a computer sign-on application) and be satisfied with the experience, which are the components of usability as outlined in ISO 9241-11 [6]. Therefore, are user interaction successes and failures being properly captured with the current testing metrics? The motivation for this paper is to experimentally show how systemic FTA metrics can be segmented into more granular metrics in the HBSI framework for biometric interactions, improving the precision of biometric testing and reporting.

II. HBSI Model

Seminal research and publication in the area of usability and accessibility, which was concerned with biometric system ergonomic design, was pioneered by the User Research Group at the National Cash Register [7], [8]. Currently, there are two institutions that are working in this area, i.e., Purdue University [9] and the National Institute of Science and Technology [10]. For a review of literature that includes the seminal work, the motivation for work in HBSI, and current research in the area of biometric usability, refer to [11]. Before the framework for biometric interactions is discussed, the origins of the HBSI model and evaluation method are presented.

The HBSI conceptual model (Fig. 2) was derived from separate areas of research, namely, ergonomics [12], usability [6], and biometrics [2]. Please see [5], [11], [13], and [14] for a complete discussion regarding the HBSI conceptual model. The purpose of the model is to illustrate how metrics from biometrics (sample quality and system performance), ergonomics (physical and cognitive), and usability (effectiveness, efficiency, and satisfaction) can be used to evaluate the overall functionality and performance of a biometric system. Including metrics from the different disciplines, it is now possible to better understand what affects biometric system performance. The following three sections describe the intersections of the conceptual model in more detail.

A. Human–Sensor Intersection

The human and sensor components of the HBSI model are similar to Tayyari and Smith’s human–machine interaction model [12]. Much like that model, the human and biometric sensor components look to achieve the optimal relationship between humans and a biometric sensor in a particular environment. The intersection of these two sections is best summarized by ergonomics, examining anthropometry, training and transfer issues, and impairments.

B. Human–Biometric-System Intersection

The human and biometric system components of the HBSI model are arranged in the model to accommodate the way biometric sensors, software, and implementations occur and are presented to users. Not only must a biometric sensor be designed so that a user can interact with it in a repeatable fashion, but the sensor(s), the software, and the way the entire “system” is packaged must also be usable. According to ISO 9241-11 [6], usability is comprised of three factors: effectiveness, efficiency, and satisfaction. Each of the three metrics is distinct and important to understand for products to balance between the three. First, biometric systems must be effective, which means that users are able to complete the desired tasks without too much effort. Second, biometric systems must be efficient, which means that users must be able to accomplish the tasks easily and in a timely manner. Third, users must like or be satisfied with the biometric system, or they will discontinue its use and find alternative methods to accomplish the task.

C. Sensor–Biometric-System Intersection

As mentioned in the previous two sections, users must be able to interact with a sensor in a consistent manner over time, and users must find the entire biometric system usable. To enable this to occur, the third relationship of the HBSI conceptual model emerges—the sensor–biometric system, whose key metric is sample quality. Sample quality is the important link between these two components because the image or sample acquired by the biometric sensor must contain the characteristics or features needed by the biometric system to enroll or match a user in the biometric system. It is well documented in the literature that sample quality affects the biometric matching algorithm. Yao et al. [17] stated that, “in a deployed system, the poor acquisition of samples perhaps constitutes the single most important reason for high false reject/accept rates.” Therefore, not only does the human–sensor relationship need
to be functional and the human–biometric system need to be usable, but also the sensor–biometric system needs to be functional. An efficient sensor–biometric system only occurs if the sensor can capture and pass usable features to the biometric matching algorithm.

III. HBSI Evaluation Method

To evaluate the model, the central intersection in Fig. 2 has been expanded to reveal the HBSI evaluation method (Fig. 3), which outlines the measurements for each intersection. Since the conceptual model is derived from different disciplines, each component (usability, ergonomics, and biometrics) produces a unique output. Thus, final conclusions based on the HBSI evaluation method will likely be dependent upon the goals, objectives, and criteria of the researcher or designer. The research in [11], which this paper is based upon, sought to find relationships within the HBSI evaluation method and report back new insights to consider when designing and ultimately testing biometric devices. Additionally, the authors acknowledge that the metrics used in this evaluation method may produce a tradeoff between performance and usability. As aforementioned, the focus of this paper is on metrics emerging from the research in [11] that linked the interaction between the human and the sensor, instead of relying solely on the system-generated performance metrics. This paper proposes that the systemic FTA metrics can be segmented into more granular metrics outlined in the HBSI framework for biometric interactions, improving the precision of biometric testing and reporting, as the errors can be labeled according to the source: the biometric system, the user, both the system and the user, or some other extraneous factor.

IV. Presentation and Acquisition Metrics

The FTA rate is typically defined as the proportion of verification or identification attempts for which the system fails to capture or locate an image or signal of sufficient quality [2]. In traditional biometric testing, FTA has been the de facto “usability” metric. Moreover, in these traditional biometric performance evaluations, interactions with a biometric system are traditionally viewed as a binary system; presentations either become successfully acquired samples (SASs) or result in an acquisition failure (FTA). This binary paradigm has impeded the system designers’ ability to understand how users interact with a biometric system and how the biometric system responds to this human–sensor interaction, as all acquisition errors have been treated the same. In this paper, the expansion of FTA was named the HBSI framework for biometric interactions (Fig. 4). This framework was developed to better understand what common correct and incorrect movements or behaviors typically occur with biometric devices. An incorrect or erroneous presentation is an interaction with the sensor that can be classified in three ways: defective interaction (DI), false interaction (FI), or concealed interaction (CI). Correct presentations are interactions with the sensor that can be classified as a failure to detect (FTD), failure to extract (FTX), or SAS. The sum of these six classifications is equal to all the human–biometric-sensor interactions with the system being evaluated. The following sections will highlight sections of the HBSI framework for biometric interactions. The DI classification was not included in this analysis as it emerged during the development and subsequent presentation of [18], long after the methodology and data analyses strategies were completed in [11]. For a complete discussion on the background of the framework and its derivation, refer to [11] and [19] respectively.

A. CIs

CIs occur when an erroneous presentation is made to the sensor that is detected by the biometric system but is not correctly handled or classified as an “error” by the biometric system. Therefore, CIs are accepted as SASs even though it was from an erroneous presentation. In other words, CIs are those attempts where the user presents a biometric characteristic(s) to the sensor but used the wrong biometric characteristic, yet the sensor recorded the interaction as an SAS. An example with fingerprint recognition would be a user that is instructed to use the sensor but used the wrong biometric characteristic, yet the sensor recorded the interaction as an SAS. Another example of a CI is a user that inadvertently interacts with the sensor with their fingertip or interphalangeal joint when the expected or desired characteristics were the volar pads of the fingers. A CI is recorded because the system records this inadvertent interaction as an SAS.

B. FIs

FIs occur when a user presents his or her biometric features to the biometric system, which are detected by the system and is correctly classified by the system as erroneous due to a fault
or errors that originated from an incorrect action, behavior, or movement executed by the user. FIs are concerned with presentations in which a user does not properly interact with the sensor and the biometric system correctly recognizes the attempt as a problematic or erroneous presentation. An example involving fingerprint recognition would be a user swiping their right index finger over the sensor too quickly and the system detects the interaction and provides feedback for the user to slow down.

C. FTD

FTD classifications involve correct presentations to the sensor that are not detected by the biometric system. FTDs are presentations to the sensor that are observed by test personnel as being a correct interaction but are not detected by the biometric system. During presentations that are classified as FTDs, the biometric system remains in the same state as it did before the user interaction took place. For example, with fingerprint recognition, users correctly position their finger on the sensor, but the system fails to respond and/or does not detect the presence of the fingerprint being on the sensor, i.e., the biometric system remained in the same state as before the interaction. Another example of an FTD with face recognition, iris recognition, or hand geometry would be if a light source is in the field of view of the device, the biometric system will not be able to detect the presence of the biometric characteristic(s). Due to factors beyond the user and the biometric system, the presentation cannot be detected.

The FTD rate provides data to system designers, revealing the user interactions the system did not detect, regardless of the cause. The FTD rate exposes user interactions that have typically not been collected during performance evaluations. Understanding these issues will enable system designers to further improve devices and algorithms and reduce the frustration of those who believe that they are correctly interacting with the sensor, yet the sensor does not detect their features as being present.

D. FTX

FTX involves samples from the data collection module that are unable to be processed completely. FTXs may occur for a number of reasons, such as problems in segmentation, feature extraction, or quality control. Determining the cause of incomplete processing may be difficult to differentiate in “black box” systems, thus the generic grouping metric FTX was established. FTX is a system error and is generated by the biometric system and typically reported in a log file. An example of this error would be when the biometric system acquires a fingerprint sample from the data collection module, but cannot process the sample into biometric features and returns an error.

E. SASs

As the name implies, an SAS occurs if a correct presentation is detected by the system and if biometric features are able to be created from the sample. SASs result from presentations where biometric features are able to be processed from the captured sample, which are then passed to the biometric matching system.

F. HBSI Framework for Biometric Interactions

After reading about the framework, the following question may emerge: is this level of detail really needed in biometric performance evaluations? The authors would argue yes because the HBSI framework for biometric interactions provides additional explanatory power for the evaluation of biometric systems. For example, take throughput time, which is a common metric for measuring efficiency for biometric access control systems. If the HBSI framework for biometric interactions is used, the throughput time data will be more compelling, as system designers and implementers are able to measure and subsequently understand the interactions that go along with a given throughput time to use a biometric device. For example, a user correctly presents his or her right index finger to the sensor ten times, but only one presentation is detected by the system. The result from the HBSI evaluation method is nine FTDs. However, if an evaluator was using traditional reporting metrics and was also measuring efficiency or task time, the evaluator may question why one attempt took so long but would have no supporting data to analyze and determine cause. Reporting FTDs in this case provides the data to support why efficiency was so poor for this individual, which, in this case, was due to the additional interactions the user performed that went unnoticed by the biometric system.

V. METHODOLOGY

A. Fingerprint Devices

The experiment to test the usefulness of the HBSI evaluation method investigated three swipe-based fingerprint sensors (Fig. 5). One commercial swipe sensor and two alternative swipe sensor designs derived from the research in [11] were used. The goal of the evaluation was to compare the usability and biometric performance results from three different swipe sensor form factor designs and two different interaction techniques. Summarizing the three designs and two techniques, the commercial sensor and PULL sensor utilized the same human–sensor interaction technique that required users to place their finger on the sensor and pull toward the body. Alternatively, the PUSH design had a different human–sensor interaction technique that required users to start with their finger...
on the sensor and slide it away from the body. Please see [11] for a complete discussion regarding the literature, design, and fabrication of the swipe sensor form factor devices and a discussion of the interaction techniques.

B. Data Collection

To evaluate the swipe sensor form factors using the HBSI evaluation method, the capacitance fingerprint sensor used for all three swipe sensors and fingerprint capture algorithm was the same, enabling the form factor design to be the independent variable. Each subject had one transaction to provide ten successfully acquired fingerprint images for each sensor used in this paper. Each participant was allowed 30 presentations to produce ten SASs, which means that the fingerprint images exceeded the quality control threshold. Regarding the systematic FTA metrics, the transaction-level FTA rate was the proportion of transactions that failed to produce any of the required ten images, whereas the presentation-level FTA rate was the proportion of presentations that failed to produce an acquired sample. The latter was the focus of this paper.

The evaluation consisted of collecting fingerprint images from 85 individuals, of which 48 were female and 35 were male. The evaluation included training, enrollment, and matching. Table I shows the schedule over the three visits.

<table>
<thead>
<tr>
<th>Sensor Type</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Training</td>
<td>4</td>
<td>15</td>
<td>4</td>
</tr>
<tr>
<td>1 Enrollment</td>
<td>10</td>
<td>30</td>
<td>10</td>
</tr>
<tr>
<td>1 Matching</td>
<td>10</td>
<td>30</td>
<td>10</td>
</tr>
<tr>
<td>2 Matching</td>
<td>10</td>
<td>30</td>
<td>10</td>
</tr>
<tr>
<td>3 Matching</td>
<td>10</td>
<td>30</td>
<td>10</td>
</tr>
</tbody>
</table>

Table I: Data Collection Methodology

Key: 
- S = # of successful presentations desired
- A = # presentations allowed per sensor

To compare proportions for a particular factor and determine if statistically significant differences exist in all possible pairs of proportions, the Marascuilo procedure for multiple proportions was used. The procedure is outlined in [22] and consists of three

C. Statistical Analysis

To evaluate the data, a chi-square ($\chi^2$) test of independence was used. According to [21], the $\chi^2$ test of independence examines relationships between two discrete variables. The paper explored the HBSI framework for biometric interactions to see if a particular sensor form factor is related to a particular type of presentation outcome. The goal of the $\chi^2$ test was to see if significant relationships exist between the presentation outcome and the form factor sensor type. The hypothesis was given as follows: $H_0$: the presentation outcome is independent of the form factor design and $H_a$: the presentation outcome is not independent of the form factor design, with the test statistic shown in

$$\chi^2 = \sum_{i=1}^{k} (O_i - E_i)^2 / E_i$$  \hspace{1cm} (1)

where $O_i$ is the observed frequency for bin $i$, and $E_i$ is the expected frequency for bin $i$. The expected frequency is calculated by $E_i = N[F(Y_u) - F(Y_l)]$, where $F$ is the cumulative distribution function for the distribution being tested, $Y_u$ is the upper limit for class $i$, $Y_l$ is the lower limit for class $i$, and $N$ is the sample size [22].

Furthermore, if $\chi^2$ is small, which means that the observed frequencies are similar to the expected frequencies, the null hypothesis is retained, and the conclusion that the two variables are independent holds [21]. However, if $\chi^2$ is large, the two variables are said to be related, and the null hypothesis is rejected.

To compare proportions for a particular factor and determine if statistically significant differences exist in all possible pairs of proportions, the Marascuilo procedure for multiple proportions was used. The procedure is outlined in [22] and consists of three
steps. First, it takes samples of size \( n \) from \( k \) populations and computes the differences \( (p_i - p_j) \), where \( i \neq j \) among all \( k(k-1)/2 \) pairs of proportions. The absolute values of the computed differences are the test statistics. The second step uses the \( \chi^2 \) table to find the critical value based on the number of factors and the significance level to compare it with the computed critical values computed from (2). The final step is to compare all \( k(k-1)/2 \) test statistics against the corresponding critical value at the defined significance value [22]

\[
\chi^2_{ij} = \sqrt{\chi^2_{a,k-1}} \sqrt{\frac{p_i(1-p_i)}{n_i} + p_j(1-p_j)} / n_j.
\]

VI. RESULTS

The results presented in this paper are only a subset of the full HBSI evaluation method (Fig. 3) analysis performed in [11]. The measurements included three separate metrics for usability: the user feedback (satisfaction), the time on task (efficiency), the number of errors made and level of assistance (effectiveness). Measurements for human factors included anthropometric measurements, fingerprint sample quality, and fingerprint image size and contrast. The third section of the HBSI evaluation method analyzed traditional biometric system performance metrics, i.e., FTA, FTE, FAR, and FRR. The focal point of this analysis is the expansion of the traditional biometric system performance measurement for FTA using the HBSI framework for biometric interactions to analyze acquisition errors using four metrics: FI, FTD, CI, and FTX.

### A. FTA Results

The experiment’s 85 participants interacted with the three swipe sensors 25 867 times, of which 22 148 (85.62\%) interactions produced SASs, with the remaining 3719 presentations classified as acquisition failures, resulting in a traditionally reported attempt-level FTA rate of 14.38\%. The Marascuillo procedure for comparing multiple proportions was used to compare the presentation outcome for the PUSH design (sensor 2) and PULL design (sensor 3) with the results of the commercial swipe design (sensor 1), which were described earlier in Section V.

Table II summarizes the results of the FTA analysis as it is traditionally reported, without regard to FI, FTD, and CI. Table II reveals that the total number of FTA attempts by the left and right index fingers had negligible differences. The results in Table II show that there is no difference between sensors 3 and 1 with the left index finger, but sensor 3 had a significantly lower FTA rate with the right index finger than sensor 1. With respect to sensor 2, the FTA rate was significantly different to that of sensor 1 for both fingers.

### B. HBSI Framework for Biometric Interaction Results

Table III extends the systemic FTA analysis (Table II) to include the HBSI framework for biometric interactions. Note that the full HBSI framework for biometric interactions as presented in Fig. 4 had six categories, but at the time of the experiment, it only consisted of FI, CI, FTD, FTX, and SAS, as no grossly incorrect presentations, or Defective Interactions (DI) were witnessed during data collection. The aggregate of the acquisition error bins of the framework, i.e., FI, FTD, and CI, equals the total number of FTA attempts listed in Table II for the respective sensor and finger. For example, Table II lists the total number of FTA errors for the left index finger as 1865.

This is equivalent to the summation of FI (1237), FTD (627), and CI (1) for the left index finger, shown in Table III. More importantly, the framework accounts for all presentations in this paper, which means that the cumulative percentages from each bin for each sensor equal 100\%. Examining the frequency counts for FTD and CI in Table III, it is apparent that there is a significant relationship between the presentation outcome and the sensor factor.

As discussed in Section V, data collection occurred over three visits, thus data analysis occurred offline. To assess performance for the dataset, Neurotechnologija’s VeriFinger 5.0 algorithm was used. In order for the sample (fingerprint image) to enroll in the system, a minimum of 10 minutiae had to be present, as well as exceed a quality threshold of 39\%, which were the system default values. Since the system did not disclose what parameter failed in the case of an enrollment failure, these instances were reported as a FTX. The results for FTX are shown in Table IV.

VII. CONCLUSION

Traditional biometric testing and reporting results from [11] revealed that the overall average FRR was 0.52\% for all three
TABLE IV

<table>
<thead>
<tr>
<th>Sensor</th>
<th>N</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>179</td>
<td>2.410%</td>
</tr>
<tr>
<td>2</td>
<td>295</td>
<td>4.089%</td>
</tr>
<tr>
<td>3</td>
<td>248</td>
<td>3.324%</td>
</tr>
</tbody>
</table>

Failure to Extract (FTX) Results

Fig. 7. Proportion of FI, FTD, and CI presentation classifications related to 3719 acquisition failures labeled as systemic FTA attempts.

TABLE V

Summary of the HBSI Framework for Biometric Interactions

<table>
<thead>
<tr>
<th>Successfully Acquired Samples</th>
<th>False Interaction (FI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>%</td>
</tr>
<tr>
<td>22,148</td>
<td>85.62%</td>
</tr>
<tr>
<td>Concealed Interactions (CI)</td>
<td>Failure to Detect (FTD)</td>
</tr>
<tr>
<td>N</td>
<td>%</td>
</tr>
<tr>
<td>9</td>
<td>0.05%</td>
</tr>
</tbody>
</table>

Removing the FTD and CI presentation outcomes, which accounted for 30.95% of the original systemic FTA errors, means that 9.93% of the presentations in this paper still resulted in an FI, which is significant. However, the tools used in the HBSI evaluation method enables researchers to further understand the human–sensor interaction because of the explanatory power gained from the streaming video analysis of the user interaction and feedback from the biometric device. In this paper, this additional explanatory power improvement was 4.44% of the acquisition errors.

VIII. Future Work

The results in this paper provided the necessary data to further explore biometric testing and reporting measurements. In this paper, only swipe-based fingerprint sensing technology has been examined. Future work is already underway to evaluate ten-print fingerprint capture [23]. Additionally, further evaluations using the HBSI framework for biometric interactions are planned for other biometric modalities. Additionally, the results of the HBSI framework for biometric interactions indicate a relationship between usability (primarily effectiveness) and biometric system performance. Thus, future work needs to be done to further examine and revise the HBSI evaluation method.
REFERENCES


[22] e-Handbook of Statistical Methods, NIST, Gaithersburg, MD, 2006.


Eric P. Kukula (M’03) received the B.S. degree in industrial distribution and management, the M.S. degree in technology and information security, and the Ph.D. degree in technology and computational science from Purdue University, West Lafayette, IN, in 2002, 2004, and 2008, respectively.

During his graduate work, he was a National Science Foundation Graduate Teaching Fellow in GK-12 Education for two years. He is currently a Visiting Assistant Professor and Senior Researcher with the Biometric Standards, Performance, and Assurance Laboratory, Department of Industrial Technology, Purdue University, where he teaches a graduate-level course in automatic identification and data capture (AIDC) technology. His research interests include how humans interact with technology, specifically the human–biometric-sensor interaction (HBSI), which involves how humans, sensors, and environmental conditions impact the design and underlying performance of biometric devices and systems. He has been involved with biometrics research for more than seven years. He is a Coeditor of ANSI Technical Report—Information technology—Biometric Performance Testing and Reporting—Part 7: Framework for Testing Methodologies for Specific Modalities. His research has led to publications in international books, journal articles, and conference proceedings. He is also a strong supporter of outreach education.

Mr. Kukula has been an active member of the International Committee of Information Technology Standards (INCITS) task group M1.5—Biometric Performance Testing and Reporting since 2003. He is the INCITS/M1.5 International Representative and the Head of US Delegation for WG5 Biometric Performance Testing and Reporting for ISO/IEC JTC1 SC37 Biometrics.

Mathias J. Sutton received the B.S.I.Ed. degree in industrial education, the M.S. degree in industrial technology, and the Ph.D. degree in industrial technology curriculum and instruction from Purdue University, West Lafayette, IN, in 1983, 1986, and 1990, respectively.

He has 22 years of experience in military logistics as a U.S. Air Force Logistics Readiness Officer. He is currently an Associate Professor with the Department of Industrial Technology, Purdue University, where he has been actively involved in mentoring graduate students, particularly in the Weekend Master’s Program—a program designed for working professionals in industry. His research and teaching interests include automatic identification and data capture (AIDC) technologies, production cost analysis, and statistical methods in technology research. His research in AIDC and statistical methods has led to publications in several journals and refereed conference proceedings.

Stephen J. Elliott received the B.Sc. degree in political science from Iowa State University, Ames, in 1993, the M.Sc. degree in transport planning and management from the University of Westminster, London, U.K., and the Ph.D. degree in industrial technology/automatic identification and data capture from Purdue University, West Lafayette, IN, in 2001.

He is currently an Associate Professor and the Assistant Department Head with the Department of Industrial Technology, Purdue University, where he is also a University Faculty Scholar and the Director of the Biometric Standards, Performance, and Assurance Laboratory. He has spoken at several conferences and is active in biometric standard initiatives. He is the Editor of ANSI/INCITS Information Technology—Biometric Performance Testing and Reporting—Part 5: Framework for Testing and Evaluation of Biometric System(s) for Access Control. He has written numerous articles on biometrics and published more than 14 journal articles and 37 conference proceedings. His research interests include the testing and evaluation of biometric systems and dynamic signature verification.