Project 1.5

Biometric Identification and Surveillance[1]

Don Adjeroh, Bojan Cukic, Arun Ross – West Virginia University
donald.adjeroh@mail.wvu.edu; bojan.cukic@mail.wvu.edu; arun.ross@mail.wvu.edu

Year 5 Deliverable

Technical Report:

Research Challenges in Biometrics

and

Indexed biography of relevant biometric research literature

Donald Adjeroh, Bojan Cukic, Arun Ross

April, 2014

[1] "This research was supported by the United States Department of Homeland Security through the National Center for Border Security and Immigration (BORDERS) under grant number 2008-ST-061-BS0002. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security."

1. OVERVIEW

Every human has distinct biometric characteristics. They can be classified using biometric measurements. The ability to positively confirm the identity of people crossing international borders has always been of paramount importance. DHS has been at the forefront of the deployment of biometric systems. Current biometric systems at border crossings offer reasonably prompt, nonintrusive and accurate support for the identification of travelers. Nevertheless, given the ever-growing size of biometric datasets (visa applicants, watch lists, etc.), the question is whether current technology will be able to keep up with emerging operational needs.

The past two decades have seen a substantial increase in biometrics activity accompanied by the deployment of biometric systems in diverse applications ranging from laptop access to border control systems. The inclusion of biometric evidence in military and criminal courts necessitates a careful examination of the scientific basis for biometric recognition. In particular, there is an urgent need to systematically review the scientific literature to determine if some of the common assumptions made about biometric traits with respect to criteria such as *universality, uniqueness, permanence, measurability, performance, acceptability* and *circumvention*, is borne out in the academic literature. Thus, the purpose of this study is to:

(a) Identify gaps in existing research and the implications on operational system risks; and
(b) Provide recommendations for further research and deployment scenarios.

2. INTRODUCTION

Human recognition and identification are challenging problems, with diverse practical applications. Biometrics has become an active research field with many unresolved questions. A fundamental requirement of any biometric recognition system is a specific human trait, which should have several desirable properties such as universality, distinctiveness or individuality, and measurability. Universality means every individual in the considered population should possess the trait. Distinctiveness, sometimes termed individuality, means the trait should be sufficiently different across individuals in the population. Measurability means that it should be possible to acquire the biometric trait by a physical system and transform it into digitized features without causing undue inconvenience to the individual. Compared to the other properties, the distinctiveness of a given trait is difficult to verify due to the enormous number of individuals in the world. Some biometric traits, such as fingerprints and iris, are generally considered as being unique to an individual based primarily on empirical results, and on a few theoretical studies. Recently the term individuality has been used to describe the distinctiveness or uniqueness of a given biometric trait. The underlying scientific bases for individuality of biometric traits have been studied using different methods. In Section 3, we offer an overview of the recent research results on individuality of strong biometric modalities and their measurability, followed by the discussion of distinctiveness of soft biometric modalities in Section 4. Section 5 provides a short overview of computational challenges in the development of modern large scale biometric systems. We conclude with the recommendations for further research and innovation directions in Biometrics in Section 6.

3. INDIVIDUALITY OF FINGERPRINTS, FACE AND IRIS BIOMETRICS

A. Individuality of Fingerprints

The fingerprint individuality problem was first addressed by Galton in 1892 [1], which is defined

as the probability of a specific fingerprint configuration. Galton assumed that a full fingerprint can be covered by 24 independent square regions on average, each spanning 6 ridges. He further assumed 1/2 to be the probability to reconstruct any region by looking at the surrounding ridges; 1/16 to be the probability of occurrence of a specific fingerprint type; 1/256 to be the probability of occurrence of the correct number of ridges entering and exiting each of the 24 regions. Thus, the probability of a particular fingerprint configuration is:

$$p = \frac{1}{16} \times \frac{1}{256} \times \frac{1}{16} \times \left(\frac{1}{2}\right)^{24} = 1.45 \times 10^{-11} \qquad (1)$$

A number of subsequent models [2], [3], [4], [5] consider the probability of a particular fingerprint configuration based on the number of minutiae features *n*, and a fixed probability of their occurrence *p*. Assuming complete independence between the minutiae points, this gives:

$$P = p^n \qquad (2)$$

Different *p* and *n* are used in different models. Although the above models are rather straightforward, a significant weakness is that they are based on ideal conditions, where the realistic problems such as partial matching and intra-class variations are not considered.

In Pankanti and Jain's work [6], the individuality is described in a more realistic manner: for a given input fingerprint containing *n* minutiae points, the individuality is the probability that an arbitrary fingerprint in a database containing *m* minutiae will have exactly *q* corresponding minutiae with the input. It is easy to deduce that if there are *q* or more matches, the two fingerprints are considered sufficiently similar and thus should belong to the same person.

$$P(M,m,n,q) = \sum_{p=q}^{\min(m,n)} \left(\frac{\binom{m}{\rho}\binom{M-m}{n-\rho}}{\binom{M}{n}} \times \binom{\rho}{q} l^{\rho} (1-l)^{\rho-q} \right) \qquad (3)$$

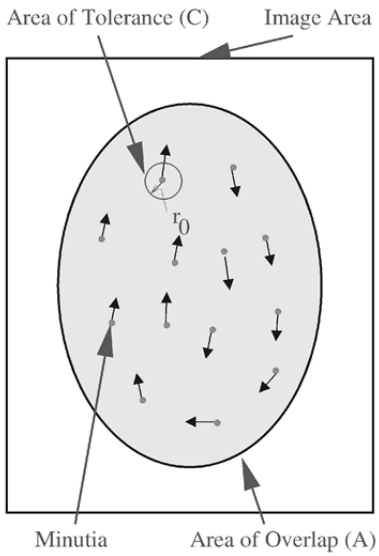

Figure 1. Parameters used in defining fingerprint individuality [6]. Alignment of minutia points must be established in an input fingerprint image prior to matching it with a template.

In Equation (3), the ratio $M = A/C$, where A is area of overlap and C is the total area of the fingerprint (Figure 1). 'l' is the probability of two position-matched minutiae having a similar direction. One weakness of Pankanti and Jain's work is that the assumption of uniform distribution of minutiae features may not always be satisfied in practice. This problem is later addressed by Dass et al. [7], using a family of finite mixture models, which better represent clusters of features observed in fingerprint images compared to the uniform distribution. The estimates of fingerprint individuality are obtained using the probability of a random correspondence (*PRC*), which is defined as follows: Let Q denote the query fingerprint image and T denote the template for the given fingerprint. Let m be the total number of minutiae points in Q and n be the total number of minutiae points in T. Let p_m be the probability of a random minutiae feature from T matching one of the m minutiae features of Q. Then the PRC is the probability of obtaining exactly k matches between Q and T (Equation 4):

$$PRC = \binom{n}{k} p_m^k (1 - p_m)^{n-k}. \qquad (4)$$

A small *PRC* value indicates it is unlikely that the query and template fingerprint image belong to the same person. To calculate *PRC*, p_m has to be properly estimated based on the statistical distribution of the template database. Another weakness of Pankanti's work is that it does not consider all possible discriminatory information that is embedded in fingerprints. Only ridge endings and ridge bifurcations are considered. Other fingerprint features, such as pattern type (Level 1) and pores (Level 3 features), are not included. In a later study, Chen and Jain [8] developed a more complex model to incorporate all three levels of fingerprint features. The correlation between features and the feature distribution are also considered. However, in the related work we consider here, the image quality is not explicitly taken into account for individuality. In practice, fingerprint image quality, age, gender and other attributes have been demonstrated to exhibit a significant impact on the system's ability to match fingerprints and develop useful large scale applications [48][49].

B. Individuality of Iris

Iris is considered to be a highly individualized pattern [14], [15]. However, the individuality of iris is currently not well defined or quantified [16]. Unlike fingerprint, the iris information is usually represented as 2 dimensional binary code, called Iris Code. Two such codes can then be compared using certain distance measures (Hamming distance, Euclidean distance, etc). To address the individuality of iris, Yoon et al. [17] proposed a dichotomy solution, which transforms the distances into two categories: intra-class distances and inter-class distances. That is, given two Iris Codes, they either belong to the same person (thus their distance is intra-class) or not (thus their distance is inter-class). Regardless of the types of features, the feature distance vectors are numeric values that can be sent to a proper classifier for recognition. Eleven models based on different features, distance types and classifiers have been developed and compared, which provide a strong background for this and future studies. Unfortunately, the key question: "what is the individuality of iris" has not been explicitly answered.

Daugman [15] suggests that the iris recognition system could yield a zero false-match rate, on a large database that contains 632,500 iris images of 316,250 persons spanning 152 countries. However, this rate is predicated on high quality iris images, which are obtained under strict supervision. Low quality images in that data set had been omitted. In practice, the image quality can be affected by various factors, which becomes a major concern that is related to the

discrimination capability of an iris recognition system. In Kalka et al.'s work [18], the effect of various quality factors has been analyzed, including de-focus blur, off-angle, occlusion/specular reflection, lighting, and iris resolution. A fully automated iris image quality evaluation block is developed to estimate the factors. This work shows that after removing the poor-quality images selected by specific quality metrics, a considerable improvement in recognition performance is achieved. They further provide an upper bound on the computational complexity required to evaluate the quality of a single image.

Kalka's work shows that the performance of an iris recognition system can be significantly compromised by the image quality. Thus, to build a realistic model for the individuality of iris, the error impact should be taken into account. This interesting problem is still open for future study.

C. Individuality of Face

Unnikrishnan [19] used the notion of unusual features to study individuality in face recognition. Here, an unusual feature is defined as a feature whose metrics lie below the 5^{th} or above the 95^{th} percentiles for that feature. Those features could be nose length, inter pupillary distance, upper lip length, shape of forehead, prominence of the chin, etc. Note that these are shape features, not appearance features. The author further indicated that a face with *100* independent features will have *10* unusual features on average. It is easy to compute the probability of a particular face configuration with *10* unusual features:

$$P = 0.05^{10} = 9.8 \times 10^{-14}. \quad (5)$$

In other words, this simple model suggests that the combination of these *10* unusual features can distinguish 10^{13} different faces. Perrett et al. [20] identify 224 shape features on the frontal face. If all these features can be acquired by an automatic identification system, then this system can distinguish $\sim 10^{29}$ faces.

Although Unnikrishnan's work presents promising modeling results, it is still preliminary. The critical fact is that, when referred to face recognition, the facial features are usually not extracted from actual faces, but from 2D face images. Several issues need to be addressed before we can develop a realistic face individuality model: (1) Although there are many effective facial feature extraction techniques, no standard organization is currently established to group the facial information into feature categories. (2) The quality of image can be significantly compromised by pose, illumination, expression, and aging. (3) The statistical inter-dependence between facial features of a single individual may not be negligible.

Klare and Jain [21] proposed a taxonomy which categories facial features into 3 levels: Level 1 features are those global features of a face that can be extracted from low resolution face images (those with inter-pupilary distance (IPD) less than *30* pixel), such as gender, ethnicity and general age group. Level 2 features are explicit to face recognition and require more detailed face observations. These are local features, usually only relevant for face recognition, including features extracted using elastic bunch graph matching (EBGM) [22], local binary patterns (LBP) [23], SIFT feature descriptors [24], [25], metrological features [26], and so on. Level 3 features contain micro level features on the face such as scars and facial marks [27]. Klare's work may serve as a starting point for the future studies on the individuality of faces and its consequences for face recognition.

In the past two decades, a number of preprocessing methods have been developed to improve image quality. Blanz and Vetter [28] proposed a 3D morphable model that allow users to adjust the initial alignment between the input 2D image and the 3D morphable facial model, then change the pose of the input image to frontal and set the illumination to ideal ambient condition. The model is trained by a set of face images to learn the distribution of 3D facial shape and texture in a parameterized feature space. Gao et al. [29] proposed a pose normalization approach based on fitting active appearance models (AAM). In this work, profile faces with different rotation angles in depth were warped into shape-free frontal view faces. Bronstein et al. [30] present a 3D face recognition approach that is invariant to expressions. Their algorithm is a representation of the facial surface that is invariant to isometric deformations. Chen and Lovell [31] proposed a face recognition method which is robust to illumination and expression. In this work, adaptive principal component analysis (APCA) is used to construct a subspace of image representations, which are then warped according to inter-class and intra-class sample covariance, respectively. Park et al. [32] proposed a generative 3D aging modeling to simulate the facial aging process. In this work, the input image is projected into the parametric 3D aging pattern space. A new face image at target age is then simulated. For low-resolution face images, Bourlai et al. [33] proposed a method that applies a number of tools such as image filtering, linear de-noising, and thresholding based nonlinear de-noising methods to enhance the quality of the low resolution images. All these preprocessing methods can considerably improve the recognition accuracy.

D. Capacity Approach

In data analysis, we often assume that the data is drawn independently and identically distributed (i.i.d.). However this assumption is not always true in practice. Sometimes we can accept an approximate independence. Sometimes, the dependence cannot be ignored. In that case we usually have two options. The first option is to eliminate the effect of dependence either by applying a de-correlation method [34], or by considering an informative feature subset, which involves a feature selection problem that can be solved in various ways [35], [26]. The second option is to incorporate the dependence information into the model. For fingerprint analysis, Dass et al. [7] proposed a mixture model in which minutiae are first clustered and then independently modeled in each cluster. A similar approach is applied by Chen et al. [8] when developing a mixture model based on 5 major fingerprint classes to evaluate fingerprint individuality. R. Kwitt et al. [36] proposed a joint statistical model for texture image retrieval problem, in which a copula-based method is applied to capture the associations among coefficients. These methods may be adapted for studies that involve different type of features.

One may argue that in Unnikrishnan's work [19], a specific number of rare features may not be guaranteed for each individual. Alternatively, if we represent each feature using a binary symbol (such as 'long (1)' or 'short (0)'), and consider each feature as i.i.d. Bernoulli random variables over the population with $P_r(f_i = 1) = 0.5$ for $i = 1, 2, \ldots, n$, then the probability of a particular face configuration is $1/2^n$. That means 8.59×10^9 individuals (which is more than the world population), can be distinguished using *33* features.

In practice, however, most human faces are remarkably similar, which means the variations in the relative sizes and distances among these features could be subtle. However the embedded noise in the face information could be overwhelming due to the large variations in pose, illumination, expression, occlusion, camera parameters, and background. Similar problem can

apply to other biometrics, such as measurements on the human body. Thus, to study the general performance of a biometric system, we need to address a more challenging problem: the impact of the noise. This problem can be addressed by adopting the concept of capacity from information theory.

In information theory, a communication channel (or channel), refers to a physical or logical transmission medium that can be used to transfer an information signal from one or more transmitters to one or more receivers. The transfer process is subject to uncontrollable ambient noise and the imperfection of the signaling process itself. The communication will not be successful unless the transmitter and receiver agree on what was sent. In information theory, the channel has a very important characteristic, called *channel capacity*, which is defined as the tightest upper bound on the amount of information that can be reliably transmitted over a communication channel. A channel is said to be memoryless if the probability distribution of the output depends only on the current input and is conditionally independent of previous channel inputs or outputs. The channel capacity of a memoryless channel is defined as [37]

$$C = \max_{p(x)} I(X;Y), \tag{6}$$

where $I(X;Y)$ is the mutual information of the input X and output Y and the maximum is taken over all possible input distributions. The mutual information is given by:

$$I(X;Y) = \int p(x,y) \log \frac{p(x,y)}{p(x)p(y)} \, dxdy, \tag{7}$$

Or equivalently,

$$I(X;Y) = h(X) - h(X|Y) = h(X) + h(Y) - h(X,Y). \tag{8}$$

E. Recognition capacity

The noise problem in a biometric authentication system can be considered as a noisy channel problem in communications. The noise comes either from the errors that are inevitably involved during the feature extraction process, or from intended security intrusion behaviors [38] such as spoofing. Thus, after a noisy feature extraction process, the subject is represented by a series of features. These features are further used to distinguish subjects. The quality, complexity, and variability of the features can be attributed to a recognition channel. An example of this approach has been introduced and characterized by Schmid et al. in [39], [40]. Similar to a communication channel, a recognition channel is also characterized by its capacity, called *recognition capacity*. The recognition capacity of a biometric system is considered as the maximum number of classes that can be successfully recognized asymptotically with probability of recognition error close to zero when the number of informative samples gets large. To achieve the expression of recognition capacity, the feature extraction process is modeled using a parallel Gaussian channel. In Schmid's and Nicollo's work [34], the input $X = (x_1, \ldots, x_n)$ is considered as a set of independent features, which is obtained by feature selection and de-correlation operation PCA or ICA. Assume there is additional i.i.d. Gaussian noise $z_i \sim Gaussian(0, N_i)$ generated by the environment for each feature x_i $(i = 1, \ldots, n)$. Finally, let the output be $Y = (y_1, \ldots, y_n)$. The original parallel Gaussian channel capacity for X is given by [37]:

$$C = \max_{\sum E[x^2] \le P} I\,(x_i\,;y_i\,) = \sum_{i=1}^{n} \frac{1}{2} \log_2(1 + \frac{P_i}{N_i})\ bits, \quad (9)$$

Where $P_i = E\left[x_i^2\right], P = \sum P_i$ are the power constraints. The equality is achieved if $x_i \sim Gaussian\,(0, P_i)$ for each i. Schmid [34] used a variation of the channel capacity in Equation 9 to derive the recognition capacity density for a biometric system based on PCA-encoding (Equation 10):

$$C = \sum_{i=1}^{n} \frac{1}{2n} \log_2(1 + \frac{\lambda_i}{N_i})\ bits\,, \quad (10)$$

where the input X is encoded as a series of principal components and λ_i is the ith eigenvalue in the principal component analysis. Other efforts on channel capacity applications include Barni et al.'s watermark channel analysis [41] and Wyner's photon channel analysis [42].

While these modeling approaches open the door for the analysis of performance and scale in biometric systems, none of them has been developed based on the strong empirical foundation, which would confirm the realism of the assumptions and the robustness of modeling methodology. For this reason, such modeling approaches remain aspirational in terms of their impact to practice. The performance indicators we receive from the largest biometric data collection and deployment in the World, India's UIDAI, which reports False Positive and False Negative identification rates around 0.1% for a population of about 600 million users through multimodal system with 10-fingers and both iris [50], appear to be the state of the art.

4. DISTINCTIVENESS OF SOFT BIOMETRICS

Soft biometric traits are those characteristics that provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals [43]. Soft biometric traits include gender, ethnicity, age, eye color, hair color, weight, etc.

Jain et al. [43] showed that 3 soft biometrics (gender, ethnicity and height) can improve fingerprint recognition by around 6%. Other soft biometrics such as freckle, mole, scar, pockmark, dark skin color and wrinkle can also improve the face-recognition performance of a state-of-the-art commercial matcher [27]. Scheirer et al. show that that the collection of 10 soft biometrics and 10 context attributes can boost the face identification system over the baseline by over 30% [44]. Furthermore, the possibility for human recognition based solely on a bag of soft biometric traits has been studied and promising preliminary results have been demonstrated by Dantcheva et al. [45]. Kumar et al. [46] also showed the collection of 65 attributes extracted from face images can be used in a stand-alone feature model. Compared to the current state-of the-art for the Labeled Faces in the Wild (LFW) data base, this model reduces the error rates by 23.92% in face verification.

Strength of soft biometric traits is that they contain additional discriminatory information which can be used in concert with primary traits such as fingerprints and iris. The attributes are usually binary values, which means the computational time and space based on the attributes will be small. However, the measurability of a large number of attributes will be low. The automatic extraction of the attributes still remains a challenge. A large training sample may be required, which will be expensive and time consuming to collect.

How can we determine the discrimination ability of a soft biometric system? There are number of terms related to discrimination ability, such as individuality [6], recognition capacity [34], reliability [47], etc. To the best of our knowledge, only a few theoretical studies of the discrimination ability of soft biometric traits exist. The discrimination capability of soft biometric systems is currently neither well defined nor systematically studied. Given the characteristic of soft biometric traits, instead of trying to address the discrimination capability of single soft biometric trait, it may be more reasonable to consider the discrimination capability of the collection of a number of soft biometrics. In other words, we investigate whether a given number of features (including soft biometric features) is sufficient to distinguish individuals.

Although we currently do not have a standard for measuring the individuality of soft biometrics, we observe that the Probability of a Random Correspondence (*PRC*) [7] can be considered a generic formulation for soft biometric traits. Using Equation 4 the feature set needs to satisfy all or part of the following assumptions: (1) The features are scalar variables; (2) A match between two features is always aligned. That is, x_i will only be compared with y_i for all i; (3) All matches are independent and equally likely; (4) All features are sufficiently accurate and, as a consequence, no uncertainty should be associated with a match based on the quality of features.

Schmid et al.'s capacity driven approach [34] could be adapted to soft biometric systems, for example, body measurements. Unfortunately, in practice, the distribution of some soft biometric traits, such as gender and ethnicity, are not continuous, not Gaussian as required by the model. Also, the distribution of some measurements might have long tails. Another relevant consideration proposed by Dantcheva et al. [47] is the notion of reliability of a multi-trait soft biometric system (SBS). In practice, it is possible that the subjects will share similar facial and body characteristics. This is called cross subject interference. The reliability of a SBS captures the probability of false identification of a randomly chosen person out of a random set of N subjects. If we denote the number of categories by ρ, the feature space by $v = (v_i, \ldots, v_N)$, the number of non-empty categories by $F(v)$($1 \leq F(v) \leq N$), the reliability is modeled by the probability $P(F)$ that a randomly drawn N-tuple of people will have F active categories out of a total of $\min\{\rho, N\}$ possible active categories (Equation 11):

$$P(F) = \frac{F^{N-F}}{(P-F)!(N-F)!\sum_{i=1}^{N}\frac{i^{N-i}}{(N-i)!(\rho-i)!}} \tag{11}$$

Given ρ, the reliability of authentication averaged over the subjects in v is a function of the number of nonempty categories $F(v)$, and independent of the distribution of categories.

5. System Engineering Issues in Large Scale Biometrics

Cloud computing-based biometric databases offer a long-term, scalable solution to a variety of emerging challenges facing current biometric architectures. These challenges include rapidly growing data volumes, increased system usage, costs associated with specialized hardware, and growing administrative costs.

The number of biometric data records — typically fingerprints, but increasingly iris and facial images, and especially video clips and voice recordings — has greatly expanded as a variety of

user communities and government agencies are called upon to use the latest authentication (identification and verification) technologies. Some of the most common applications of biometric data are to reliably and quantifiably establish identity of people who want to enter the country, have committed crimes, or are on a watch list. The number of biometric data records has recently expanded on a massive scale due to new requirements for governmental agencies to use the latest identification and verification technologies. This data is being expanded to support tasks that include border security, criminal justice, and terrorist watch list monitoring. Eventually, hundreds of millions of identities, amounting to petabytes of biometric data, will be housed in databases operated by the government or private organizations. Many of these agencies will require their systems to identify individuals in near real-time with a high degree of accuracy. At the same time, shrinking budgets are necessitating a reduction in the cost-per-match while demanding increases in both accuracy and in the number of matches performed. The systems currently deployed by these agencies are reaching their upper limits in terms of storage capacity and have not yet produced tenable results in providing peta-scale solutions. What is needed is a system composed of inexpensive, preferably commodity-like components that provides accuracy, performance, scalability, reliability, availability, and interoperability.

The researchers at the Center for Identification Technology Research (CITeR), an NSF I/UCRC, have been issued a challenge by the center's Industry Advisory Board, to investigate possible approaches that will enable the scale up of operations of biometric and identity management systems and operations. The scale-up challenge faced by CITeR's industry and government affiliates is remarkable. Over the next few years, biometric databases for the Federal Bureau of Investigations (FBI) [1], Department of State (DoS) [9], Department of Defense (DoD) [10], and the Department of Homeland Security (DHS) [11] are expected to grow to accommodate hundreds of millions of identities. For example the DHS Automated Biometric Identification System (IDENT) database, as of 2010, hosts 110 million identities and enrolls or verifies over 125,000 individuals per day [12]. Another example is the national identity cards program for India's 1.2 billion-plus citizens, called "Aadhaar" and run by the Unique Identification Authority of India, (UIDIA) [13] which also demonstrates the geometric progression of the number of identities expected in new systems that process biometric data. In early 2014, having enrolled over 600 M users, India's UIDIA processes more than 400 trillion biometric matches per day using an equivalent of 3 Automated Biometric Identification Systems (ABIS). These operations require about 30 TB of input / output every day [50].

6. FUTURE RESEARCH RECOMMENDATIONS

In this study, we systematically reviewed the scientific literature to determine if some of the common assumptions made about biometric traits with respect to criteria such as universality, uniqueness / individuality, permanence, measurability and performance, are borne out in the academic literature. This report discusses some of our observations with respect to some strong biometric modalities (fingerprints, face and iris) and offers preliminary insights into soft biometric atteributes. We provide recommendations for future research activities that can strengthen the fundamentals of biometrics from a scientific perspective.

Individuality

The uniqueness of a biometric *trait* can be evaluated using different types of models. These models fall under three different categories:

- Biological models: In this approach, the anatomical aspect of the trait is modeled based on a biological understanding of the trait.
- Feature models: In this approach, the capacity of the "template" or the feature set used to characterize the biometric trait is used to assess the uniqueness of the trait.
- Score models: In this approach, a biometric matcher is used to compare biometric samples and the resulting match scores are analyzed in order to understand the distinctiveness of the biometric trait.

Biological models for fingerprint generation have been proposed in the literature. However, these models have not been used to quantify the uniqueness of the biometric trait. In the case of iris, most studies focus on match scores and attempt to model the distribution of scores in order to understand the uniqueness of iris patterns.

Research gap 1: In order to quantify the uniqueness / individuality of a trait, it is necessary to independently develop three types of models: biological models, feature set models and score models. Further, the relationship between these models has to be systematically established[2]. This research activity will help the scientific community to quantify the notion of uniqueness as it pertains to individual biometric traits.

Permanence

The impact of aging on the performance of biometric algorithms has been studied in the context of face recognition. Several aging models have been developed by face recognition researchers in order to account for the changes in an individual's facial structure and texture over a period of time. However, such studies have not been extensively conducted in the context of fingerprint and iris. While recent research has examined the degradation in match scores when matching time-lapsed data, the biological underpinnings for this observation has not been established.

Research gap 2: The impact of age on biometric traits has not been rigorously studied. The face recognition community has published a few datasets that can be used to facilitate such studies. However, the fingerprint and iris recognition researchers do not have easy access to time-lapsed data (where biometric data from an individual has been collected over a long period of time – e.g., 10 – 20 years). This calls for two lines of research activities: (a) begin assembling datasets that capture the biometric traits of individuals over a large span of time; (b) develop models that account for changes in a biometric trait with respect to age[3].

Research gap 3: The impact of diseases on biometric traits has not been systematically analyzed. Most biometric datasets available for scientific research contain data acquired from

[2] For example, in the case of fingerprints, the degree of uniqueness as established by minutiae points should be consistent with that established using a biological model for generating fingerprints.

[3] Besides age, the impact of nutrition and environment should also be established.

reasonably healthy individuals[4]. Consequently, a preponderance of scientific publications report performance of biometric algorithms on healthy subjects, i.e., subjects whose biometric traits may not exhibit a great deal of anomaly. Access to operational data may be instructive for furthering our understanding of the robustness of biometric algorithms to pathological variations in the general population.

Research gap 4: The availability of cosmetic surgical procedures to modify an individual's appearance poses a challenge to biometric algorithms. Recent research has analyzed the impact of cosmetic plastic surgery on face recognition algorithms[5]. However, a more rigorous study is required to understand the various types of cosmetic alterations that are available and their impact on biometric algorithms. These cosmetic alterations are socially acceptable and are not intended to deliberately defeat a biometric system. Collaboration with the medical community will be necessary to perform this research in an effective manner.

Systems

With respect to biometric systems and their quality, the recent study from the National Academies [58] states that "if it is determined that biometric systems and technologies are the most appropriate (...), then our understanding of the underlying science and technology must be robust enough to support the applications." Unfortunately, to date we found no studies which analyze possible internal flaws (faults, performance limitations, zero-effort failures) in the development of any biometric system. This does not imply there were none. It does indicate that these systems are rather immature. Further, large-scale biometric systems appear not to be open to scientific scrutiny. Rather, such systems are large black boxes inaccessible for independent verification and validation.

Research gap 5: With respect to improvements in accuracy we recommend studying the new concepts of self-adaptation [59]. The self-adaptive software engineering paradigm would allow biometric systems to change over time and, in such a way, better accommodate changes in scale, periodic quality shifts, a variety of modalities, etc. Further, such systems would be able to monitor operational environments and choose algorithms and / or security defenses deemed the most appropriate for the given emerging threat. With respect to improvements in cost / time computational effectiveness and privacy preservation, we acknowledge ample evidence of the leap towards systems with billion(s) of users. This prompts the need to study fundamental biometric search and retrieval techniques, and effective winnowing (partitioning and indexing) techniques, with provable accuracy, that reduce penetration rates by orders of magnitude. Such a research direction would calibrate concerns related to highly decentralized biometric services (clouds).

---

[4] As an example, we are not aware of any fingerprint datasets available to the research community at large, which contain data from individuals with skin diseases. Similarly, we are not aware of iris datasets containing ocular images of individuals with eye diseases.

[5] Similarly, the appearance of an iris can be impacted by the introduction of cosmetic contact lenses.

REFERENCES AND THE INDEXED BIOGRAPHY OF RELEVANT BIOMETRIC RESEARCH LITERATURE

[1] F. Galton. Finger Prints. London: McMillan, 1892.

[2] E. Henry. Classification and Uses of Fingerprints. London: Routledge, 1900.

[3] B. Wentworth and H. Wilder. Personal Identification. Boston: R.G. Badger, 1918.

[4] H. Cummins and C. Midlo. Fingerprints, Palms and Soles. Philadelphia : Blakiston, 1943.

[5] S. Gupta. Statistical survey of ridge characteristics. Int'l Criminal Police Rev., 218, 1968.

[6] S. Pankanti and A. K. Jain. On the individuality of fingerprints. IEEE TPAMI, 24, 2002.

[7] S. C. Dass, Y. Zhu, and A.K.Jain. Statistical models for assessing the individuality of fingerprints. Information Forensics and Security, 2(3):391–401, 2007.

[8] Y. Chen and A. K. Jain. Beyond minutiae: A fingerprint individuality model with pattern, ridge and pore features. In ICB, 2009.

[9] Moss, Frank E. Testimony of Frank E. Moss, Deputy Assistant Secretary for Passport Services Bureau of Consular Affairs. Travel.State.Gov. [Online] December 2, 2005. [Cited: March 7, 2011.] http://travel.state.gov/law/legal/testimony/testimony_2921.html.

[10] Sun Microsystems. Secure Identity Management at the U.S. Department of Defense. Sun Microsystems Website. [Online] May 2003. [Cited: March 27, 2011.] http://www.sun.com/software/whitepapers/wp-dmdc/wp-dmdc.pdf.

[11] Department of Homeland Security. DHS Exhibit 300 Public Release BY10 / NPPD - US-VISIT . Department of Homeland Security Website. [Online] April 17, 2009. [Cited: March 7, 2011.] http://www.dhs.gov/xlibrary/assets/mgmt/e300-nppd-usvisit-ident2010.pdf.

[12] Graves, William. US VISIT : The world's largest biometric application. National Institute of Science and Technology Website. [Online] March 4, 2010. http://biometrics.nist.gov/ibpc2010/pdfs/Graves_William_The_future_of_IDENT.pdf.

[13] Sharma, Amol. India Launches Project to ID 1.2 Billion People. *Wall Street Journal.* September 29, 2010.

[14] J.Daugman. Recognizing people by their irispatterns. Technical report, University of Cambridge UK.1998.

[15] J.Daugman. New methods in iris recognition . IEEE Trans. Systems, Man, and Cybernetics, Part B, 37(5):1167-1175,2007.

[16] A.Ross .Iris Recognition: The path forward. Computer, 43(2):30-35,2010.

[17] S.Yoon, S.-S. Choi, S.-H Cha,Y.Lee, and C. C.Tappert. On the Individuality of the iris biometric. GVIP, 5,2005.

[18] N.D. Kalka , J.Zuo, N.A. Schmid, and B.Cukic. Estimating and fusing quality factors for iris biometric images . IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, 40(3):509-524,2010.

[19] M.Unnikrishnan. How is the individuality of a face recognized? Journal of Theoretical Biology, 2009.

[20] D.I. Perrett, K. A. May, and S.Yoshikawa. Facial shape and judgements of female attractiveness. Nature, 368:239-242,1994.

[21] B.Klaire and A.K. Jain. On a taxonomy of facial features. In BTAS,2010.

[22] L. Wiskott, J. M. Fellous, N. Kruger, and C. von der Malsburg. Face recognition by elastic bunch graph matching, in proc. ieee int. conference on image processing, vol. 1, p. 129, 1997. Pattern Analysis and Machine Intelligence, 19(7):775–779, 1997.

[23] T. Ahonen, A. Hadid, and M. Pietik ¨ ainen. Face description with local binary patterns: Application to face recognition. Pattern Analysis and Machine Intelligence, 28(12):2037–41, 2006.

[24] D. G. Lowe. Object recognition from local scale-invariant features. In ICCV, 1999.

[25] E. Meyers and L. Wolf. Using biologically inspired features for face processing. Int. Journal of Computer Vision, 76(1):93–104, 2008.

[26] D. Cao, C. Chen, M. Piccirilli, D. Adjeroh, T. Bourlai, and A. Ross. Can facial metrology predict gender? In IJCB, 2011.

[27] U. Park and A. K. Jain. Face matching and retrieval using soft biometrics. TIFS, 5(3):406–415, 2010.

[28] V. Blanz and T. Vetter. Face recognition based on fitting a 3d morphable model. Pattern Analysis and Machine Intelligence, 25(9):1063–74, 2003.

[29] H. Gao, H. ı m Kemal Ekenel, and R. Stiefelhage. Pose normalization for local appearance-based face recognition. In ICB, 2009.

[30] A. M. Bronstein, M. M. Bronstein, and R. Kimmel. Expression-invariant 3D face recognition. AVBPA, pages 62–69.

[31] S. Chen and B. C. Lovell. Illumination and expression invariant face recognition with one sample image. In ICPR, 2004.

[32] U. Park, Y. Tong, and A. Jain. Age invariant face recognition. Pattern Analysis and Machine Intelligence, 32(5):947–954, 2010.

[33] T. Bourlai, A. Ross, and A. Jain. Restoring degraded face images: A case study in matching faxed, printed and scanned photos. TIFS, 6(2):371–384, 2011.

[34] N. A. Schmid and F. Nicolo. On empirical recognition capacity of biometric systems under global PCA and ICA encoding. TIFS, 3(3):512–528, 2008.

[35] L. Song, A. Smola, A. Gretton, J. Bedo, and K. Borgwardt. Feature selection via dependence maximization. Journal of Machine Learning Research, 13:1393–1434, 2012.

[36] R. Kwitt, P. Meerwald, and A. Uhl. Efficient texture image retrieval using copulas in a Bayesian framework. IEEE Trans. on Image Processing, 20(7):2063–2077, 2011.

[37] T. M. Cover and J. A. Thomas. Elements of Information Theory. Wiley, New York, 2006.

[38] P. Tuyls and J. Goseling. Capacity and examples of template-protecting biometric authentication systems. Biometric Authentication, LNCS,3087:158–170, 2004.

[39] N. A. Schmid and J. A. OSullivan. Performance prediction methodology for biometrics systems using a large deviations approach. IEEE Trans. Signal Process., Supplement on Secure Media, 52(10):3036–3045, 2004.

[40] N. A. Schmid and J. A. O'Sullivan. Face Biometrics for Personal Identification: Multi-Sensory Multi-Modal Systems, chapter Performance Prediction Methodology for Multi-Biometric Systems, pages 213–230.Berlin, Germany: Springer-Verlag, 2007.

[41] M. Barni, F. Bartolini, A. D. Rosa, and A. Piva. Capacity of the watermark-channel: How many bits can be hidden within a digital image. In SPIE, 1999.

[42] A. D. Wyner. Capacity and error exponent for the direct detection photon channel. IEEE Trans. Inform. Theory, 34(6):1449–1461, 1988.

[43] A. K. Jain, S. C. Dass, and K. Nandakumara. Can soft biometric traits assist user recognition? In SPIE, 2004.

[44] W. J. Scheirer, N. Kumar, K. Ricanek, P. N. Belhumeur, and T. E. Boult. Fusing with context: A Bayesian approach to combining descriptive attributes. In IJCB, 2011.

[45] A. Dantcheva, C. Velardo, A. D'Angelo, and J.-L. Dugelay. Bag of soft biometrics for person identification - new trends and challenges. Multimedia Tools Appl., 51(2):739–777, 2011.

[46] N. Kumar, A. C. Berg, P. N. Belhumeur, and S. K. Nayar. Attribute and simile classifiers for face verification. In ICCV, 2009.

[47] A. Dantcheva, J. Dugelay, and P. Elia. Soft biometrics systems: Reliability and asymptotic bounds. In BTAS, 2010.

[48] S. Mason, I. Gashi, L. Lugini, E. Marasco, B. Cukic. Interoperability between Fingerprint Biometric Systems: An Empirical Study, In DSN 2014.

[49] S. Mason, I. Gashi, "Deployment Strategies for Diverse Fingerprint Biometric Systems: Technical Report", http://www.csr.city.ac.uk/people/ilir.gashi/DSN2014/

[50] R. Mashruwala & V. Raghavan."Massive Scale Biometric Authentication System: *Reimagining role of biometrics in National ID programs", in IBPC 2014.*

[51] M. Kucken. On the formation of fingerprints. Ph.D. Thesis, University of Arizona, 2004.

[52] M. Kucken and A. C. Newell. Fingerprint formation. Journal of Theoretical Biology, 235, pp. 71- 83, 2005.

[53 J. Daugman. "The importance of being random: Statistical principles of iris recognition." Pattern Recognition, 36(2), pp 279-291, 2003.

[54] J. Daugman and C. Downing. "Epigenetic randomness, complexity, and singularity of human iris patterns." Proceedings of the Royal Society, B, 268, Biological Sciences, pp 1737 – 1740, 2001

[55] S. Baker, K. Bowyer, P. J. Flynn, "Empirical Evidence for Correct Iris Match Score Degradation With Increased Time Lapse Between Gallery and Probe Images," International Conference on Biometrics, pp. 1170-1179, June 2009.

[56] FG-NET Aging Database: http://www.fgnet.rsunit.com/index.php

[57] Jinli Suo, Song-Chun Zhu, Shiguang Shan, Xilin Chen, "A Compositional and Dynamic Model for Face Aging," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 3, pp. 385-401, March 2010.

[58] Joseph N. Pato and Lynette I. Millett (eds). "Biometric Recognition:Challenges and Opportunities", Whither Biometrics Committee; National Research Council, The National Academies Press, 2010.

[59] B. H. Cheng, R. de Lemos, et.al., "Software Engineering for Self-Addaptive Systems: A Research Roadmap," in Software Engineering for Self-Adaptive Systems, B. Cheng et al. (eds), Lecture Notes in Computer Science, Volume 5525/2009, Springer Berlin / Heidelberg, 2009, pp. 1-27.