A Survey of Synthetic Biometrics: Capabilities and Benefits

Nicholas M. Orlans  
The MITRE Corporation  
7515 Colshire Drive  
McLean, VA 22102

Douglas J. Buettner  
The Aerospace Corporation  
P.O. Box 92957 – M1/112  
Los Angeles, CA 90009-2957

Joe Marques  
The MITRE Corporation  
7515 Colshire Drive  
McLean, VA 22102

Abstract

Computer generated “synthetic” biometrics are not widely used within the biometrics community beyond their current use as a research tool. Yet they offer a number of potential advantages that can be developed further to support the science and practical use of biometrics. They can be used to improve the understanding of a biometric system’s robustness and as an engineering tool to predict system performance. This paper surveys the state of synthetic biometrics generation, provides a glimpse at some benefits that can be obtained from their use, and discusses the issues retarding their adoption by the biometrics community.

1. Introduction

This survey explores the current state of computer generated (synthetic) biometric images, and discusses areas where synthetic biometrics can provide added value to the biometrics community and ultimately to the public and private sector interests that it serves. Also discussed are the areas of research that need to be conducted before their possible widespread adoption and use by the biometrics community.

1.1 Synthetic Biometrics

Synthetic image generation, as shown in Table 1, has been achieved for the most widely recognized image-based biometrics of fingerprint, face, and iris [1, 2, 3, 4, 5, 6].

Table 1. Synthetic Biometric Data Generation

<table>
<thead>
<tr>
<th></th>
<th>Fingerprint</th>
<th>Face</th>
<th>Iris</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synthetic image generation</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Statistical feature model</td>
<td>yes - level 2 minutiae</td>
<td>yes - (method)</td>
<td>yes – (theoretical)</td>
</tr>
<tr>
<td>Validated model</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Environment effects</td>
<td>partial</td>
<td>partial</td>
<td>partial</td>
</tr>
</tbody>
</table>

Within the Association for Computing Machinery (ACM) Special Interest Group on Computer Graphics (SIGGRAPH) community, a long-standing goal has been held for photo-realism in the generation of synthetic images—a goal that some feel has been achieved [7]. This body of work, spanning over three decades, documents achievements in modeling, animation, and rendering human subjects. The visual products range from feature films, commercial art, to video games.

The most advanced synthetic images come from the movie industry and have yet to be fully adapted to suit biometric needs. A synthetically rendered face is illustrated in Figure 1.

Figure 1. Rendering Of A Synthetic Face.¹

The quest for realistic computer-generated artificial-persons has created an art and science that includes physics-based models to control physical form, motion and illumination properties of materials [8]. Today, computer generated characteristics address detailed aspects of facial features, skin, hair, gait, as well as body and eye movement [3, 4, 5, 8, 9, 10, 11, 12, 13, 14].

Statistical feature models are empirical or mathematical models that provide a statistically valid method for a computer algorithm to generate

¹ Image Source: http://graphics.ucsd.edu/~henrik/papers/face_cloning/ reproduced with permission from the author.
biometric features across a target population. Statistical feature models should, in general, be derived from the physics. However, they can also be generated from empirical methods. For example, the optimal statistical derivation model for fingerprints would be derived from the biological factors that create the unique friction ridge and pore patterns in the human fetus. The method of empirically determining equivalent statistical parameters however suffices, where the analysis of anthropometric, fingerprint or other private/public databases of biometrics can be utilized [15, 16, 17, 18, 19, 20, 21]. The Pankanti et al. derivation of fingerprint uniqueness was for fingerprint minutia from ridge flow [22]. No statistical derivation has been proposed for finger ridge/trough patterns or “level 3” information [21, 22]. Level 3 information includes pores and more subtle details about friction ridge width, shape and deviation. Hence for fingerprints, a partial theoretical mathematical model and empirical data exist that could be used to validate the synthetic model generator.

Methods for empirically deriving statistical shape models for the face or body exist [23, 24]. Daugman has published treatments addressing the statistical uniqueness of the human iris [25, 26].

Empirical and mathematical models are validated by comparing their statistical distributions to the statistical distributions from real biometrics. The closest testing that approaches what is needed to validate synthetic biometrics generators against real biometrics is the University of Bologna Fingerprint Verification Competition (FVC) Tests [27, 28]. These tests use synthetic images from the University of Bologna’s SFinGe tool (shown below in Figure 2) [29]. Very realistic images simulate a low-cost sensor with rotation, displacement and distortion characteristics approximating images from real biometrics.

Figure 2. The SFInGe Fingerprint Generation Tool

The National Institute of Standards and Technology’s (NIST) Facial Recognition Verification Tests (FRVT) are equivalent to the FVC tests; the NIST tests, however, do not utilize synthetic faces [30]. There is no equivalent public testing of iris recognition vendors due to the limited number of vendors.

Environmental affects not only refer to the ability to control through parametric means (while maintaining calibrated results) the effect of nature on acquired biometric image data, it also refers to the influences from the image acquisition physics. As an example, SFInGe, contains controls for pressure, moisture, skin elasticity, and the ability to choose specific sensor types to mimic sensor specific image acquisition affects [1, 2, 27].

Methods for synthesizing potential environmental affects on the acquisition of synthetic face and iris images can be gleaned from the radiosity and global illumination methods [8, 31]. Additional models for environmental factors such as temperature on human subjects can eventually be used to account for the effects of physical changes like sweat on biometrics [32]. Complete accounting for image acquisition affects is also possible using physical optics theory and the physics of the response by the imaging device to electromagnetic radiation. Image processing methods exist for measuring image acquisition distortion among other effects [see for example http://www.mitre.org/tech/mtf/].

1.2 The Biometrics Community

Within the biometrics community, the use of synthetic biometric images for research and testing is not a new concept or practice. As previously discussed, research groups have utilized synthetic biometric images for testing and parametrically controlled data generation [27, 28]. Of the mainstream biometrics, synthetic fingerprint and facial images have perhaps received the most attention by biometrics researchers [1, 2].

Using synthetic biometrics is generally not considered a best practice for testing biometrics systems [27, 33]. Additionally, the requirements of Common Criteria testing provide a further roadblock to the adoption of these methods [34]. Common Criteria requires the use of real images obtained from the sensor in an operational scenario for security certification testing, as the focus is on operational security. Hence, using synthetic images is not desirable in this case since they are not integrated into the biometric system; where the fully operational system’s security vulnerabilities need to be uncovered.
Another issue retarding the adoption of synthetic biometrics pertains to the availability of real biometrics from engineering staff members working on the development of these systems, and from the understandable desire to simply use biometrics from real people captured by the actual system.

Finally, the current synthetic biometric generation systems do not fully mimic real sensors, and do not provide statistically valid representations of real populations.

Hence, despite the availability of cost-effective commercially available tools to synthesize complete human subjects, their use has not been fully realized within the biometrics community. This brings up the fundamental question of how these issues retarding their adoption can be removed to facilitate their use within this community. For example, how could the biometrics community best incorporate these tools to potentially further refine the testing and evaluation of any system, which incorporates biometrics (a.k.a. biometric systems)? What are the benefits?

This introduction has provided some initial background into the state of computer generated (synthetic) biometrics. We now review the hurdles facing the adoption of synthetic biometrics within the biometrics community and ponder some potential advantages for using synthetic biometrics within that community.

2. Benefits for Biometric Systems

While not a substitute for the biological diversity provided by live biometrics, computer generated biometrics do offer several advantages. The potential benefits for using synthetic biometrics, as well as research areas that should be explored are provided in this section.

2.1 Parametric Biometric Systems Testing

The Common Criteria testing issue, mentioned in section 1.2, is circumvented if the use of synthetic images for testing biometric systems is restricted to testing the artificial intelligence underpinnings (i.e. the image processing algorithm’s robustness factors and environmental boundaries). The system’s biometric inputs are synthetically generated up front using any number of carefully controlled parameters. The synthetic images are then processed in a simulated operational mode, where the biometrics processing logic that will be employed by the operational system remains intact.

System robustness issues can be investigated from the parametric control provided by these synthetic ‘scenes’. For example, synthetic face images for facial recognition tests can include carefully controlled changes to pose angle, illumination, expression, and obstructions [35]. Additional relevant parameters include motion and location information.

Differences in biometric recognition performance across demographic populations and sub-populations (such as age) have been reported in recent tests, but the causes are not always fully understood [36]. Synthetic techniques may play a role in isolating demographic differences and associated specific parameters, which might play a role in effecting biometric recognition performance [37].

Figure 3. Synthesized Aging Sequence

The illustration in Figure 3 is an example of using “hybrid” synthetic images to study aging, where a photographic image of a live person is added to a 3D face model. In this example, the model is aged forwards and backwards in a progressive sequence using the FaceGen application from Singular Inversions, Inc. [36]. In the case of fingerprinting, friction ridge quality and finger size correlations to age, ethnicity and gender effects on performance could be readily tested using validated synthetic images.

Differences across environments and sensors are known to result in differences in performance. Some biometric systems address some of the environmental or sensor differences. However, the majority of systems have yet to effectively account for all differences. Here, the ability to parametrically control environmental difference is a necessary step towards the ability to account for (or cancel) its particular influences.

2.2 Operational Scenario Testing

Synthetic scenes with injected biometrics provide the potential to construct arbitrary representations of real-world scenarios using a fixed
set of model "subjects" or randomly generated populations of subjects and scenarios. Ground truth, that is, the actual layout of the potential operational location, is known in advance, eliminating the need to re-identify and re-orient human subjects or physical objects. Variations on a basic theme, such as a video of subjects walking through a chokepoint, can be systematically modeled with parametric settings. Parameters range from global, environmental factors such as illumination and camera angle, to local aspects such as hair length, pose angle, and facial expressions. Furthermore, specific behavioral outliers to normal chokepoint transit behavior can be examined to reveal system vulnerabilities. Biometric systems engineers could run a vast array of operational scenario tests to define the optimum layout of biometrically enabled security devices by testing the system in the computational realm prior to deployment.

As biometric systems are deployed in support of national security, border control, and immigration applications, understanding the affects of international populations becomes very significant. Countries with population groups that lack sufficient diversity in age and ethnicity for thorough testing of border management applications would certainly benefit. For example, the FaceGen software permits control of several ethnic characteristics [36]. A recognition system’s inability to properly discriminate between controlled variations in ethnic or racial attributes for example, suggests there may be an inadequate body of system training data used to fine-tune the system or a fundamental problem with the recognition algorithms.

2.3 Enhancing privacy

Another important benefit for synthetic biometrics is their lack of association with a specific individual’s identity. Hence, they provide the unique ability to be anonymous in origin by design and thus allow researchers to simulate populations without having to worry about security arrangements for the handling and use of biometrics from real people [38].

An example that highlights the touchy subject of biometrics use by governments in the area of privacy was the proposed use of biometrics in a Department of Defense anti-terrorism total information awareness system that attracted congressional and public scrutiny concerning privacy, policy, and potential abuse issues. Those concerns, ultimately led to the cancellation of that program, are summarized in a December 2003 audit report from the Inspector General of the U.S. Department of Defense [39].

Synthetically generated biometrics provide a benefit to security systems testing by providing a privacy sensitive method, where synthetics are not subject to the same privacy and legal issues that must be addressed when personal data is collected and maintained. Moreover, there should be few if any restrictions for distributing, publishing, and sharing synthetic datasets. There are these types of issues, however, when attempting to analyze real datasets from private or government sources. With fewer restrictions, there are additional benefits for information sharing for research as well as cost reductions from storage and data handling.

2.4 Cost and Time

Once necessary software is in place and control parameters are configured, synthetically generated biometrics can be quickly produced. Typically, database production times are on the order of minutes or hours as opposed to months or even years for the collection of the same number of natural images. The synthetic fingerprint generator, SfinGe, reportedly generates 10,000 realistic prints in ten hours using a single Pentium IV CPU [1]. A MITRE experiment experienced similar generation times for face images [36]. Synthetic generators are functionally capable of scaling to produce very large databases or simply generating large numbers of randomly selected biometrics from the specified parametric controls.

Collecting medium to large databases of biometrics from real people for testing (or any purpose) is expensive and challenging. Actual costs vary according to the collection protocol and logistics of the target population. Most collections undertaken by universities tend to incorporate small numbers of test subjects for the test population, typically from the young university population [17, 18]. Larger government or industry sponsored collection efforts, on the order of thousands or tens of thousands of images are extremely costly. The only alternative to carefully controlled biometrics collection protocols for research is use of private or government databases. This use restricts the publication visibility of the research results, due to privacy concerns.

The ultimate scalability to large quantities of valid synthetic images hinges not only on the ability to create realistic synthetic biometric images, but also is directly dependent on the availability of valid statistical models.

3. Statistical modeling

Statistical models are essentially mathematical equations or empirically derived algorithms, which
are fed randomly generated numbers to create data that are statistically equivalent to real data. Mathematical models provide researchers and engineers with the ability to predict the performance of larger populations based on the modeled performance of smaller populations [40, 41].

Match score distributions from biometric systems contain many underlying behavioral and physical population uncertainties. Figure 4 shows the match score distributions from a corpus of input images (see [42] for details on the corpus).

![Figure 4. A Fingerprint Algorithm’s Raw Scores](image)

The distribution is dependent on the conditions of the test and the subjects used. For example, high humidity and temperature causes sweat, where low humidity causes dry skin. This environmental influence on our skin, in turn influences the acquisition of the fingerprint image differently for different types of fingerprint sensors. Even though the corpus in Figure 4 was accumulated in a climate controlled indoor environment, some of the younger test subjects provided sweaty fingerprints. Future physics-based or empirically derived models from biometric technology testing can be combined with Monte Carlo simulations. This provides a powerful tool for scientists and engineers working with biometric systems, in the same manner that these methods help researchers in other disciplines [43].

4. Conclusions and recommendations

It is evident that the realm of biometrics is exploding and the integration of various biometrics into sophisticated and robust models is occurring. The ability to increase the reliability and accuracy of these systems is critical, as biometrics become an essential part of law enforcement and security communities. The use of synthetic biometrics by researchers in simulations provides a potential method for testing these systems in a privacy-enhancing manner.

Simulations provide controlled statistical sampling through the use of a model. The models in turn are used to provide an approximation about complex, multi-variable problems. The lack of statistically valid models remains one of the main problems faced by the biometrics community. The authors recommend that targeted studies and prototyping efforts be conducted to progress the state of the art as presented previously in Table 1. Additionally, a demonstration of how real biometrics samples can be accurately transformed across two or more diverse synthetic environments is an important and achievable next step for the advancement of biometrics. For example, face images with indoor illumination versus outdoor illumination can be simulated and then used to accurately compensate for the undesired variances from live images.

An example of a biometrics deployment that may have benefited from the use of synthetic biometrics is an operational scenario test of the highly publicized face recognition system test at Boston’s Logan Airport. The deployment reportedly failed to match the identities of 38% of a test group of employees [44]. Had this deployment been modeled and checked synthetically, by a third party, this highly public failure with its associated publicity debacle may have been avoided.

A much better example of where the technology could be utilized in the future is in the testing of border management scenarios where there is a wide range of atmospheric and operational conditions. The U.S. alone must contend with the extreme cold wintertime conditions in Alaska to the hot humid summertime conditions in Florida [45].

As discussed, the ultimate scalability to large quantities of valid synthetic images hinges directly on the statistical models underpinning the generated data, and this is an area where questions remain. A synthetic generator for biometric data must contain a model, where currently it must make assumptions about the distinguishable phenomenology of the biometric trait, its natural variances, and also its responses to the environment. The creation, formalization and assessment of such models are important next steps towards allowing an understanding of performance derived from testing with synthetic biometrics.
Bibliography

17. The AR Face Database, available online at http://rvl1.ecn.purdue.edu/v1/ARdatabase/ARdatabase.html
18. The Yale Face Database, available online at http://cvc.yale.edu/projects/ylafacesB/ylafacesB.html
26. J. Daugman and C. Downing, “Epigenetic randomness, complexity, and singularity of


