A Survey of Synthetic Biometrics: Capabilities and Benefits

Nicholas M. Orlans, Douglas J. Buettner, Joe Marques (IC-AI ’04)

Abstract - a 2004 survey of synthetic biometrics

Synthetic biometrics are not widely used beyond research

- May offer a number of potential advantages to support science *and* practical use of biometrics

Synthetic biometrics may be useful to

- Improve our understanding of the robustness of a biometric system
- Predict the performance of a system a priori

Survey of the current state

- A glimpse at benefits that may obtained (e.g. parametric systems testing, enhancing privacy, cost)
- A discussion of issues retarding the adoption in the biometrics community

Synthetic biometrics

A goal of SIGGRAPH is photo-realism in generated synthetic images

- D. P. Greenberg et al., “A Framework for Realistic Image Synthesis”, 1997
- Develop physically based lighting models
- Light reflectance models, light transport, perception

Synthetic image generation achieved for most widely recognized image-based biometrics

- Fingerprint
- Face
- Iris

Figure 1. Rendering Of A Synthetic Face.[1]

Synthetic biometrics

An art and science of physics-based models to control physical form, motion and illumination

- Facial features, skin, hair
- Gait, body and eye movement

Statistical feature models

- Empirical or mathematical models to provide statistically valid biometric generation
- Based on physics and/or generated from empirical methods

An example: the fingerprint model

- Ideally derived from biological factors that create pore patterns in a fetus
- However, equivalent statistical parameters can be obtained empirically with analysis of databases
- No model for friction ridge width, shape and deviation: partial mathematical model

Synthetic biometrics

Method

- Empirically deriving statistical shape models

Theoretical

- Addressing the statistical uniqueness

Table 1. Synthetic Biometric Data Generation

	Fingerprint	Face	Iris
Synthetic image generation	yes	yes	yes
Statistical feature model	yes- level 2 minutiae	yes - (method)	yes – (theoretical)
Validated model	no	no	no
Environment effects	partial	partial	partial

Synthetic biometrics - model validation

Compare statistical distribution to that of real biometrics

Fingerprints

- University of Bologna Fingerprint Verification Competition (FVC) tests
- Tests that use synthetic images from University of Bologna's SFinGe

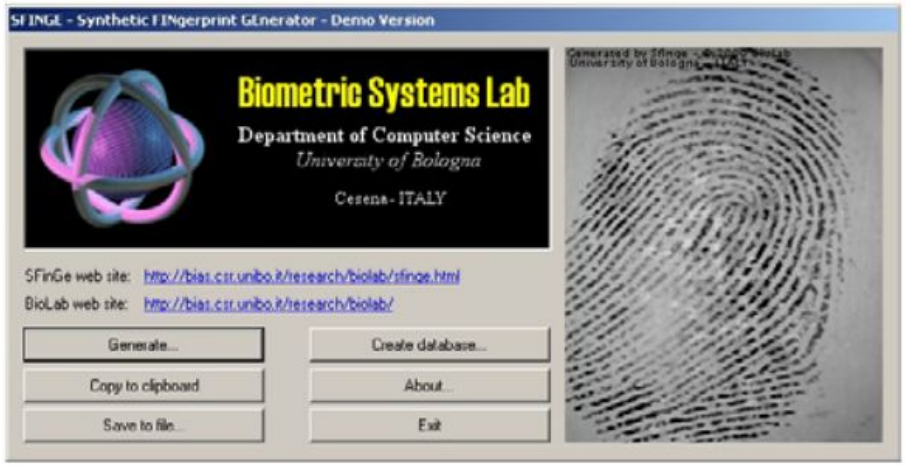
Face

- National Institute of Standards (NIST) Facial Recognition Verification Tests (FRVT)

Iris

- None; limited number of vendors

SFinGe


SFinGE - Synthetic FINgerprint GEnerator - Demo Version
Biometric Systems Lab
Department of Computer Science
University of Bologna
Cesena - ITALY
SFinGe web site: http://bias.csr.unibo.it/research/biolab/sfinge.html
BioLab web site: http://bias.csr.unibo.it/research/biolab/
Generate...
Create database...
Copy to clipboard
About...
Save to file...
Exit

Synthetic biometrics - environmental effects

SFinGe - the effect of nature

- Pressure
- Moisture
- Skin elasticity

SFinGe - the effect of image acquisition physics

- Choose sensor types for image acquisition effects

Leveraging physics

- Synthesization of effects can be gleaned from radiosity and global illumination methods
- Temperature can be used to account for physical changes like sweat
- Image acquisition effects with optics theory and response to electromagnetic radiation

The biometrics community

Use of synthetic biometric images for research is not new

- Testing and parametrically generating data, e.g. FVC and FRVT

However, generally not considered best practice to use synthetic biometrics

- Common Criteria (ISO/IEC 15408) requires the use of real images for security certification testing
- Availability of real biometrics and the desire to simply use these
- Current synthetic biometric generation do not fully mimic real sensors
- May not provide statistically valid representations of real populations

Benefits - parametric biometric systems testing

Common Criteria can be circumvented if synthetic images are restricted to testing AI underpinnings

- Generate biometric inputs synthetically up front, using controlled parameters
- Processed in a simulated operational mode, the operational system remains intact

Investigate system robustness from parametric control in synthetic ‘scenes’

- Pose angle
- Illumination
- Expression
- Obstructions

Synthetic techniques may play a role in isolating demographic differences

Synthetic aging - FaceGen, Singular Inversions

FaceGen

The easy way to create realistic faces

- 3D human faces & heads from 1 or more photos or at random
- Adjust age, race, gender and 150 other controls
- Meshes for animation, 3D printing and compatibility with other software

Benefits - operational scenario testing

Potential to construct arbitrary representations of real-world scenarios

- Fixed set of model subjects or randomly generated populations of subjects/scenarios
- Ground truth is known in advance
- Variations on a theme can be modeled with parametric settings

One can test the system in the computational realm prior to deployment

- E.g. countries lacking sufficient diversity in age and ethnicity for border management
- More adequate body of system training data for fine-tuning the system or recognition algorithm

Boston's Logan Airport failed to match the identities of 38% of a test group of employees

- Test synthetically, avoid publicity debacle

Benefits - enhancing privacy

Synthetic biometrics lack association with a specific individual's identity

- Provide the ability to be anonymous by design
- Worry less about security arrangements when handling biometrics

Example: use of biometrics in a Department of Defense anti-terrorism information awareness system

- Congressional and public scrutiny concerning privacy and policy
- Led to the cancellation of the program
- Synthetic biometrics would provide a privacy sensitive method

Fewer, if any, restrictions for distributing, publishing and sharing synthetic datasets

Benefits - cost and time

Once software is in place, synthetically generated biometrics can be produced quickly

- Typically producing database in minutes/hours instead of months/years
- SFinGe generated 10,000 fingerprints in ten hours, using a **Pentium IV**
- Scale to produce large database with parametric controls

Real biometrics are expensive and challenging to obtain

- Gathering is expensive
- Resorting to private or government databases restrict publication visibility

However, it is of course directly dependent on the availability of valid statistical models

Statistical modeling

Statistical models

- Mathematical equations or empirically derived algorithms
- Fed randomly generated numbers to create data statistically equivalent to real data
- Provide the ability to predict performance of larger populations based on smaller populations

Distributions are dependent on the conditions of test and subjects used

- High humidity and temperature causes sweat
- Models can be combined with Monte Carlo simulations

Conclusions

- The ability to increase reliability and accuracy of biometric systems is critical
- The lack of statistically valid models remains a main problem
- Demonstrations of transforming real biometrics transformation, e.g. illumination is achievable
- An good example of where the tech can be used is border management, wide range of operational conditions
- Ultimate scalability hinges on the statistical models, the creation, formalization and assessment of such models are important next steps

References

- Orlans, Nicholas M, Douglas J Buettner, P O Box, and Joe Marques. “A Survey of Synthetic Biometrics: Capabilities and Benefits,” n.d., 7.
- Greenberg, Donald P, James Arvo, Eric Lafortune, Kenneth E Torrance, James A Ferwerda, Bruce Walter, Ben Trumbore, Peter Shirley, Sumanta Pattanaik, and Sing-Choong Foo. “A Framework for Realistic Image Synthesis,” n.d., 18.