Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 4th, 2012

Biometric Discrimination Power: Is It Mostly Hype?

Naomi Jordan Cook, Raman Asati, Thomas Bryla, Lara Roth-Biester, and Roshan Shaikh
Pace University, Seidenberg School of CSIS, White Plains, NY 10606, USA
{nj54121w, ra71498n, tb13382n, lr43748n, rs95452w}@pace.edu

Abstract

This study explores whether the reputation of biometric products is well deserved or based on hype. We focus on two types of biometric systems—fingerprint and face—in our investigation of the accuracy of those systems, as reported by both biometric companies and the media. After reviewing the phenomenon of the "hype cycle", we evaluate the claimed power and accuracy rates of various fingerprint and face products by examining how these accuracy claims were reached, and by determining whether claimed accuracy matches real-world performance. Finally, results from our testing of one freeware face product and one commercial fingerprint scanner are given.

1. Introduction

There are two main categories of biometrics—physiological and behavioral. For physiological biometrics, authentication is the automatic verification of individuals using one or more distinguishing biological traits, such as finger and palm prints, hand and earlobe geometry, retina and iris patterns, and DNA.

By reputation, biometric authentication systems carry the promise of increased security, greater assurance and accountability, convenience, and potential cost savings. The United States' US-VISIT immigration and border management system, as well as several European governments' expressions of interest in biometric national identity cards, have raised the public profile—and, by extension, the credibility—of biometrics considerably.

With stiff competition in this still-emerging field to produce better, smarter, and more efficient and economical systems, there is a tendency by designers and manufacturers to overstate the accuracy of their system. They do so by defining accuracy in rather loose, ambiguous terms. However under stricter scrutiny, tighter definitions, and rigorous testing using precise measurements, many systems prove themselves unable to live up to their hype.

1.1. Literature Review

Blackburn et al [1] believe that in spite of advances in face recognition technology over the past few years, greater accuracy is nevertheless needed. Five years later the Society of Photo-Optical Instrumentation Engineers [2] holds a similar view, concluding that identifying individual faces in uncontrolled environments remains the biggest challenge in face recognition reliability.

Nor is fingerprint technology without its weaknesses, despite enjoying a longstanding reputation as an advanced technology offering relatively high accuracy at relatively low cost. Bolle et al [3] discuss recent challenges to the premise of fingerprint uniqueness, as well as the large variation in the quality of fingerprints over populations, technical problems relating to hardware, and other disadvantages that bring the accuracy of fingerprint technology directly into question. Ross, Shah, and Jain [4] find that while some vendors of fingerprint systems deny that it is possible to "trick" the technology, "our preliminary results show that minutiae templates are indeed vulnerable to the masquerade attack." Simon A. Cole's extensive examination [5] of the real-world consequences of fingerprinting errors is also abundant with examples of the weaknesses to which the technology is prone.

For several years, consultant and academic Roger Clarke has been emphasizing the need for greater oversight in biometrics, saying in 2008 that "biometrics tackles a very difficult challenge, and a host of factors have to be confronted that undermine quality. The scope for error is vast." [6] He went so far as to say in 2002 that "(the) biometrics industry is mythical. Publicly-available, independent evaluation of technologies and products is extremely rare. Three available reports show that most of the technologies and products don't work. Technologies, products and suppliers continue to appear and disappear at a rapid rate. Pilots almost never proceed to the next stage. Anecdotally, installations are so ineffectual that they're a great embarrassment to everyone concerned." [7]

Pato and Millett (2010) describe human recognition systems as "inherently probabilistic" and therefore inherently fallible. While they recognize that error rates can be made small, they cannot be eliminated. "The field of biometrics would benefit from more rigorous and comprehensive approaches to systems development, evaluation, and interpretation." [8]

What is clear from the available literature is that no biometric system is flawless or invulnerable, and that different technologies possess different weaknesses and strengths recommending them to certain, but not all, applications. This picture is quite different from the one most commonly painted by vendors, developers, and government officials wishing to portray biometric systems as nearly perfect.

2. Biometric Hype and the "Hype Cycle"

Biometric hype comes in two distinct forms: hype generated by the media, and hype generated by manufacturers to push their own products. Sometimes these two forms feed off each other to create an even higher level of hype. Such is the case of biometrics, which reached the apex of its hype following the terrorist attacks of 9/11: biometrics was seen as the answer—or, at least, part of the answer—to the world's fears about terrorism. It is telling that the majority of articles relating to biometrics as a counterterrorism measure date to 2002, the year following 9/11.

Much touted as the future of security following the September 11 attacks, several states implemented different strategies involving face recognition scanning. Boston's Logan airport, where 10 of the 19 9/11 terrorists boarded planes, conducted trials with face scanners in 2002. The system correctly detected 153 volunteer "terrorists," but failed to detect 96 of them. That same year Palm Beach airport ran its own face recognition trial, and got similar results, failing to detect its targets more than half of the time.

While biometrics showed promise in 2002, the technology was unable to match the hype. Further, these earlier systems were trying to pull a Minority Report-style scan as people passed in front of security cameras. Plucking identities from video is a biometrics task infinitely more ambitious than identifying a stationary, properly-positioned person three feet away in ideal lighting [9].

The hype cycle, a term coined [10] by Gartner, Inc., comprises five phases in the life of a new technology:

1. The Technology Trigger is the breakthrough phase for the technology. Media attention drives publicity, but no working products exist yet.
2. During the Peak of Inflated Expectations, a frenzy of publicity generates over-enthusiasm and unrealistic expectations. Some early successes—accompanied by many more failures—are reported.
3. The Trough of Disillusionment occurs when the technology fails to meet expectations and becomes unfashionable. Media attention wanes.
4. The Slope of Enlightenment sees some businesses persisting with the technology, and experimenting with it in order to understand its benefits and practical applications.
5. The Plateau of Productivity is reached when the benefits of the technology become widely demonstrated and accepted. The technology becomes increasingly stable and evolves in second and third generations. The final height of the plateau varies according to whether the technology is broadly applicable or benefits only a niche market [10].

Prior to 9/11 biometrics had almost reached Phase 2 of the Hype Cycle [11]. It is certainly more than probable that the events of 9/11 and their aftermath triggered the inflated expectations of biometrics. By 2005 biometrics had reached the "trough of disillusionment".

Now, in 2011, biometrics is theoretically at the end of the fourth phase and reaching the fifth. As a class of disruptive or discontinuous technology, biometrics has not completed its development cycle, and yet is now subject to significant innovation. In other words, just as biometrics is beginning to stabilize and deliver on past promises, current expectations continue to be driven by "next generation" technologies [12].

3. Research Methodology

3.1. Classification

Biometric verification is the one-to-one comparison of a biometric to verify a known individual. This method attempts to answer the question, "Am I who I say I am?" Biometric identification is the one-to-many comparison of a biometric against a database to identify an unknown individual. This method attempt to answer the question, "Who am I?" Our research focuses on products that use biometric verification for access control.

Classifying a biometric device as high- or low-end depends on a number of factors: how the device is used, the setting in which it is used, scale of implementation, intended population size, and cost per unit. For our purposes a product qualifies as high-end if

it is fast and reliable enough to be suitable for use in high-risk or high-population areas, such as nuclear power plants or border control. A low-end product will tend to be suitable for low-risk, low throughput environments, such as server rooms and offices, and therefore need not be as fast or powerful as its high-end counterpart. For simplicity, we used price as the sole indicator of high-end versus low-end, and set the threshold at $450: that is, anything above was determined to be high-end, and anything below low-end.

3.2. Methodology

We began our research by contacting around 40 U.S.-based biometrics companies specializing in either face or fingerprint verification. Out of that original pool, six face and seven fingerprint companies were willing to participate in our research and allow us to collect data on their products.

We attempted to elicit information on the advertised accuracies of each company's system or systems. Of particular importance was the use of three parameters to direct the evaluation of each product:

1. System performance based on EER (equal error rate)
2. Number of users the system is designed to handle
3. Quality of the data samples required for the system to work satisfactorily

Additionally, each company representative was asked the following ten questions, the answers to which we believed would yield exactly the sort of the data that would help us separate hype from reality:

1. How much does the product cost?
2. What is the product's expected accuracy rate?
3. What is the product's tested accuracy rate?
4. What population size was used to test the product?
5. What system /software is used for the product?
6. Is it the same system / software that is used for the product?
7. What facial / fingerprint features does the product detect?
8. What algorithm does the system use?
9. What is the detection time in milliseconds?
10. What is the dpi of image capture resolution?

4. Product Evaluations: Fingerprint

Both high-end and low-end fingerprint verification products match prints to stored images using one of two major classes of algorithm: minutiae-based matching and pattern matching. Minutiae-based matching compares several specific details within the ridges of a fingerprint. Pattern matching, compares both individual points and the overall characteristics of the fingerprints.

Although each company we interviewed uses their own combination of hardware and proprietary software, the flow of the fingerprint scanning process is essentially the same for all products, whether high-end or low-end:

1. Sample acquisition: capture of a person's fingerprint using a sensor
2. Feature extraction: sample is transformed into reference template.
3. Quality verification: Steps 1 and 2 are repeated as many times as necessary to ensure data is captured correctly.
4. Storage of reference template
5. Matching: compares real-time input data from an individual against the reference template
6. Decision: authenticated or not authenticated

Basic information on both high-end and low-end fingerprint products are provided below. See Appendix A for a detailed breakdown of company and product data.

Table 1: Key Fingerprint Product Data

Company	Product	High/ Low end
Biometrics Direct	AET 60 BioCARDKey	High
Neuro Technology	VeriFinger SDK	High
Integrated Biometrics	IBISDK/IBISCAN4	High
Zvetco Biometric	Authasas	Low
Griaule Biometrics	Fingerprint SDK	Low
Fulcrum Biometrics (distributor)	Fingerprint Extractor	Low

4.1. Results from initial company queries

Initial results from our conversations with these companies yielded mixed results. Some companies were happy to promptly share product data, while others would only do so after several attempts at contact and interview.

Those companies from which we successfully obtained data invariably reported accuracy rates of between 99% and 99.99%. Prices for low-end products ranged from $60 to $820, while prices for high end products ranged

from $800 to $5,000. Testing populations ranged from 500 to 100,000.

Most companies use their own algorithm and software, however pattern-based matching is the most common fingerprint technique used.

Most accuracy rates are determined using high quality fingerprint images. Maximum DPI ranged from 200 DPI to 512 DPI. No detection speeds were given. (See Appendix A.)

Figure 2 shows a definite, but slight, correlation between price and accuracy. And it is of course impossible to discern a relationship between algorithm and accuracy, since every company uses the same general class of algorithm. (See Appendix A.)

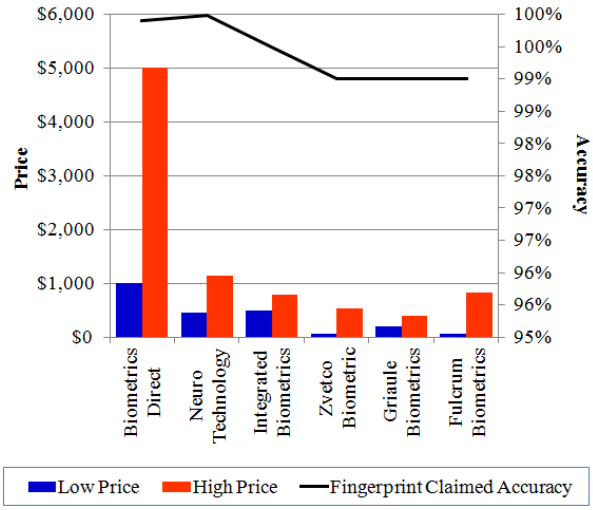

Figure 2: Price of fingerprinting products vs. accuracy

5. Product Evaluations: Face Verification

Both high-end and low-end face verification products match facial images to stored images using one of a great many classes of algorithm. The companies we interviewed use the following algorithms:

Table 2: Face Verification Algorithms by Company

Company	Product	Algorithm
Ex-Sight	Face Engine	AMII algorithms
Animetrics	Anim SDK	Face dot EF5
Image Metrics	Metrics	Face matching
Attrasoft	Facetree	Pattern
Cognitec	FaceVACS-SDK	Incorporates B5T8, A14T8(2D) & B5L5T8(2D/3D)
Attrasoft	API	Face pin
Genex	3D Capture	Human Form Research
Cyberextruder	Aureus 3D SDK	ADM tracking

All face verification technology works fundamentally the same general way: verification algorithms create a point-to-point map of the face, and convert that map to binary. A one-to-many matching process compares a query face image against all the template images in a database to determine the identity of the query face. The verification of the test image is done by locating the image in the database that has the highest similarity with the test image. The verification process is a closed test, which means the sensor takes an observation of an individual that is known to be in the database.

Basic information on both high-end and low-end face verification products are provided below. See Appendix B for a detailed breakdown of company and product data.

Table 3: Key Face Verification Product Data

Company	Product	High/ Low end
Ex-Sight	Face Engine	High
Animetrics	Anim SDK	High
Image Metrics	Metrics	High
Attrasoft	Facetree	High
Cognitec	FaceVACS-SDK	High
Attrasoft	API	Low
Genex Technologies	3D capture	Low
Cyberextruder	Aureus 3D SDK	Low

5.1 Results from initial company queries

As with the fingerprint results, initial results from our conversations with facial biometric companies yielded mixed results. Some companies were reluctant to share data with us.

Again, as with fingerprinting companies, claimed accuracy rates were very high, with only one reporting any rate below 98% (Cognitech, 95%).

Prices for low end products ranged from $100 to $800, while prices for high end products ranged from $1,000

to $2,0000. The sizes of test populations ranged from 500 to 5,000.

Most products used a measurement of the distances between facial features as the primary method of detection, and used either a 3D or a 2D facial modeling convention. Most companies develop and use proprietary algorithm and software.
Maximum DPI ranged from 200 DPI to 450 DPI
Detection time ranged from 14 to 20 milliseconds. (See Appendix B.)

Figure 3 (below) yields little in the way of helpful information. We can draw no correlation between price and accuracy, and again, as with our fingerprint research, the claimed accuracies are so high and so similar to each other as to make any possible pattern too slight to be of much import.

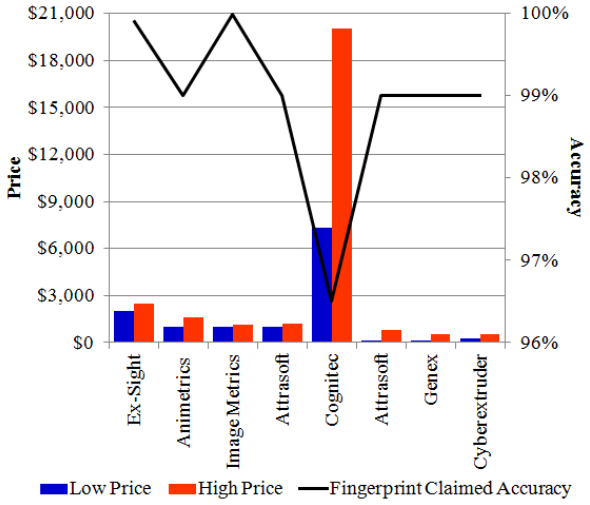

Figure 3: Price of face verification products vs. accuracy

6. Product Testing: Results

6.1. Fingerprint

The iGuard LM Series Fingerprint Scanner is a verification product that scans fingerprints for comparison with fingerprint images stored in its database. We used it as a standalone unit with an internal database, although it has the ability to be set up on a network with an SQL server and database or Microsoft Access. As a standalone, the unit can handle up to 1,000 users, and is expandable to 20,000 users with a "Supermaster" upgrade. Training the unit was straightforward. All the unit needs is to scan two of your fingers twice each, then an ID number. Once trained, the unit recognizes you as either "Authorized" or "Unauthorized".

We used 24 test subjects, scanning two sets of fingerprints each. Training for each subject took approximately one to two minutes. Recognition of authorized fingerprints took between one and three seconds. Rejection of unauthorized fingerprints took between three and five seconds. Out of 100 different fingerprint tests, of which 50 were authorized and 50 were unauthorized, we had a 100% accuracy rate.

We were unable to generate any false acceptances. Our attempts to generate false rejections succeeded, but only under extreme conditions: i) moistening the finger before scanning, ii) tilting the finger 30°, iii) wrapping the finger in Saran, and iv) removing the finger before scanning is complete. Given the small sample size, we conclude reservedly that this product lives up to its accuracy claims. A more definite conclusion requires that the unit be put through its paces with a much larger group.

6.2. Face

Facile Face Labeling, or FaceL, is a face processing and labeling tool that labels faces in a live video from an iSight camera or webcam. [13] It can handle only a small number of users ("don't try the whole school or neighborhood"). [14] Training FaceL was straightforward. When the subject sits in front of the webcam, the program's face detector identifies the subject's face immediately by drawing a blue rectangle around it on-screen. After enrolling each subject using multiple expressions and poses, each of which is saved with a unique enrollment ID (a name, for example), the "Train Labeler" function teaches FaceL to identify a subject's face.

We used 15 test subjects. Training for each subject took between five and 30 seconds per subject. Verification of each subject was instantaneous: that is, the moment FaceL detects a face it instantly assigns and displays a name, whether correct or incorrect. FaceL's accuracy is high when the subject remains still and directly faces the camera, but is noticeably less accurate when the subject moves around, squints their eyes, or doesn't sit face-on.

FaceL's accuracy rate is difficult to measure since its verification process involves cycling through several identity labels for a single test subject as expressions change, the head tilts, or the subject moves around. That said, out of our 15 test subjects, we estimate that FaceL verified correctly 99% of the time under ideal conditions, and 95% of the time under imperfect conditions.

7. General Conclusions: Fingerprinting & Face Verification

High-end companies that produce devices for biometric fingerprinting and face verification do not seem to be substantially different from low-end companies performing the same service. Some low-end companies even use the same software as their high-end counterparts, like VeriFinger by Neurotechnology, which is also used by the Fulcrum Biometric Distributor.

While each company may use distinct or proprietary software for common devices, the differences in the accuracy of each seem not to be dramatic. Algorithms for face verification are not uniform, however it is true that each fingerprinting product employs the pattern matching algorithm.

Each company within their own field (fingerprint or face) establishes a similar minimum standard DPI for accurate verification. It is worth noting that, for both face and fingerprint scanners, increased dpi is known to result in reduced accuracy and increased computational complications [15].

Image quality, too, can affect performance and accuracy. Image quality, as distinct from dpi, refers to the quality of the image obtained—is the image clear? Are all the required points visible? Is the image unobstructed? Poor quality biometric images diminish the matching performance of biometric verification systems, result in false matches and false non-matches, and increase search times [16].

The uniformity of stated result and accuracy among companies strongly suggests that further study is needed. If it is at all possible to determine the real-world accuracy (assuming it is different from its stated accuracy) of the biometric products we examined without the ability to extensively test products themselves, it seems the logical next step is to obtain data from customers who use the products in the real world.

7.1. Recommendations for Future Work

We believe that the logical next step is to reach out to organizations that use these products in the real world. We have already begun to make some progress towards this goal, but a much more comprehensive and in-depth study of customer-reported data is needed.

Table 4: Company responses to requests for references of customers using their face verification products

Company	Contacted	Willing to provide references	Notes
Cyberextruder	Yes	Maybe	Will respond soon
Attrasoft	Yes	No	No response to emails/phone calls
Genex	Yes	Yes	Waiting to hear
Animetrics	Yes	No	Not policy
Ex-Sight	Yes	Yes	Waiting to hear
Image Metrics	Yes	No	Not policy

Table 5: Company responses to requests for references of customers using their fingerprinting products

Company	Contacted	Willing to provide references	Notes
Biometrics Direct	Yes	No	
Neuro Technology	Yes	Maybe	Waiting to hear
Integrated Biometrics	Yes	No	Need more info to answer questions
Zvetco Biometric	Yes	No	
Griaule Biometrics	Yes	Maybe	Waiting to hear
Fulcrum Biometrics	Yes	No	Sent product to test

8. References

[1] D. Blackburn, C. Miles, B. Wing, et al, *Face Recognition*, National Science and Technology Council, Subcommittee on Biometrics, 7 August 2006.

[2] M. Crawford, "Facial recognition progress report", Society of Photo-Optical Instrumentation Engineers, 28 September 2011.

[3] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, *Guide to Biometrics*, Springer Professional Computing, New York, NY, 2004, p. 146.

[4] A. Ross, J. Shah, A. K. Jain, "Towards Reconstructing Fingerprints From Minutiae Points", Proc. SPIE Conference on Biometric Technology for Human Identification II, Vol. 5779, (Orlando, USA), March 2005.

[5] S. A. Cole, "More Than Zero: Accounting for Error in Latent Fingerprint Identification", The Journal of Criminal Law & Criminology, Vol. 95, No. 3, Northwestern University School of Law, 2005.

[6] R. Clarke, "The Mythologies of 'Identity Management'", Xamax Consultancy Pty Ltd., 2008.

[7] R. Clarke, "Personal Notes on Computers, Freedom & Privacy", Xamax Consultancy Pty Ltd., San Francisco, CA, 2002.

[8] J. N. Pato and L. I. Millet, *Biometric Recognition: Challenges and Opportunities*, National Research Council of the National Academies, Washington, DC, 2010, pp. 1-2.

[9] "Heathrow Airport To Adopt Face Scanners To Screen Passengers." Internet: http://singularityhub.com/2011/08/06/heathrow-airport-to-adopt-face-scanners-to-screen-passengers, August 6, 2011, accessed November 2011.

[10] "Interpreting Technology Hype." Internet: http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp, 2011, accessed November 2011.

[11] "Twitter Backlash Foretold." Internet: http://blogs.reuters.com/commentaries/2009/08/11/twitter-backlash-foretold/, August 11, 2009, accessed November 2011.

[12] "The Future of Biometrics Market - Forecasts 2009 to 2017." Internet: http://techbiometric.com/biometric-market/biometrics-market-forecasts-2017/, 2011, accessed November 2011.

[13] "FaceL: Facile Face Labeling." Internet: http://sourceforge.net/apps/mediawiki/pyvision/index.php?title=FaceL:_Facile_Face_Labeling, 20 January 2010, accessed November 2011.

[14] "FaceL: Facile Face Labeling - Bring on more people - but not too many." Internet: http://www.youtube.com/watch?v=0oUXtVQmcUc, May 1, 2009, accessed November 2011.

[15] D. Zhang, Xiaoyuan Jing, and Jian Yang, *Biometric Image Discrimination Technologies*, Computational Intelligence and Its Application Series, Idea Group Publishing, Hershey, PA, May 24, 2006, P. 84.

[16] "Biometric Image Quality Measurement Algorithms and Tools Development." Internet: http://www.biometrics.dod.mil/Files/Documents/Collaborations/BCF2010_DoD_Biometrics_Collaboration_Forum.pdf, accessed November 2011.

http://www.employeetimeclocks.com/articlepageX.aspx?artid=2

Appendix A

High-end Fingerprint Companies Comparison Chart

Company Name	Price ($)	Expected Accuracy	Tested Accuracy	Population Tested	System/Software	Method of Detection & Characteristics Detected	Algorithm Used	Detection time (ms)	Maximum DPI
Biometrics Direct	1,000–5,000	99.90%	99.90%	1,000	AET60 BioCARDKey	Print should be clean/ distinguishable	Pattern matching	NA	508
Neuro Technology	447–1,134	99.99%	99.90%	NA	VeriFinger SDK	Straightforward matching of the to-be-identified fingerprint pattern against many already known fingerprint patterns would not work well due to high sensitivity to errors in capturing fingerprints. Extract features of minutiae points from the fingerprint image, and any matches between these sets of very specific fingerprint features are noted	Verification/ pattern matching	0.1-0.2	250
Integrated Biometrics	499–795	99.50%	99.50%	10,000	IBISDK/IBISCAN4	Allows sloppy finger placement with lowest False Reject Rate. Efficient processing enables one-to-many performance for large user populations. Highest accuracy and usability securely enables biometric only operation	Pattern matching	NA	512

Low-end Fingerprint Companies Comparison Chart

Company Name	Price ($)	Expected Accuracy	Tested Accuracy	Population Tested	System/Software	Method of Detection & Characteristics Detected	Algorithm Used	Detection time (ms)	Maximum DPI
Zvetco Biometric	60–530	99.00%	99.90%	100,000	Authasas Enterprise Edition/Utility Software – ID check	Before the matching process begins, the candidate image must be aligned with the template coordinates and rotation. Features from the candidate image are then extracted and compared with the information in the template. Depending on the size of the input image, there can be 10-100 minutia points in a template. A successful match typically only requires 7-20 points to match between the two fingerprints.	Pattern matching	NA	508
Griaule Biometrics	200–400	99.00%	99.00%	500	Fingerprint SDK 2009	"The fingerprint is acquired from a fingerprint scanner."	Pattern matching	NA	NA
Fulcrum Biometrics (distributor)	65–820	NA	NA	NA	Fingerprint Extractor	"Image is improved by better contrast and distinctness."	Pattern matching	NA	500

Appendix B

High-end Face Verification Companies Comparison Chart

Company Name	Price ($)	Expected Accuracy	Tested Accuracy	Population Tested	System/ Software	3D / 2D	Method of Detection & Characteristics Detected	Algorithm Used	Detection time (ms)	Maximum DPI
Ex-Sight	2,000–2,500	99.90%	99.90%	5,000	Face Engine		The system translates the template into a unique code. This coding gives each template a set of numbers to represent the features on a subject's face.	AMII algorithms	14	430
Animetrics	1,000–1,570	99.00%	98.00%	5,000	Anim SDK	3D model has the ability to recognize a face even when it is turned 90 degrees away from the camera. Moreover, they are not affected by the differences in lighting and facial expressions of the subject.	Once it detects a face, the system determines the head's position, size and pose. As stated earlier, the subject has the potential to be recognized up to 90 degrees, while with 2D, the head must be turned at least 35 degrees toward the camera.	Face dot EF5	18	200
Image Metrics	1,000–1,100	99.99%	99.90%	1,000	Metrics		"Distance between the eyes Width of the nose Depth of the eye sockets The shape of the cheekbones The length of the jaw line"	Face matching algorithms	17	256
Attrasoft	1,000–1,200	99.00%	99.00%	5,000	Facetree		The system then makes use of a person's facial features – its peaks and valleys and landmarks – and treats these as nodes that can be measured and compared against those that are stored in the system's database.	Matching Algorithm/ Pattern	20	356
Cognitec	7,300–20,000	95– 98%	99.90%	5,000	Face Engine		FaceVACS allows you to pick and choose what modules you want for your system. Intensity and shape data information,portrait characteristics module, encoding module, face tracker module, verification module, identification module.	Incorporates B5T8, A14T8(2D) AND B5L5T8(2D/3D)		

Low-end Face Verification Comparison Chart

Company Name	Price ($)	Expected Accuracy	Tested Accuracy	Population Tested	System/Software	3D / 2D	Method of Detection & Characteristics Detected	Algorithm Used	Detection time (ms)	Maximum DPI
Attrasoft	$100	99.00%	98.00%	500	API		Distance between the eyes; width of the nose; depth of the eye sockets; shape of the cheekbones; length of the jaw line	Face pin algorithms	18	250
Genex Technologies Inc.	$100	99.00%	99.00%	1000	3D capture	3D	Overall facial structure, including distances between eyes, nose, mouth, and jaw edges. These measurements are retained in a database and used as a comparison when a user stands before the camera	Genex's Human Form Research - Algorithms	20	250
Cyberextruder Inc.	$250	99.00%	99.00%	1000	Aureus 3D SDK		Overall facial structure, including distances between eyes, nose, mouth, and jaw edges	ADM tracking algorithms	18	450