Summary of NIST Patriot Act Recommendations

1. One-to-One Matching (Verification) -- NIST recommends one face and two index fingerprints for verification. All three biometrics should be in image form. The face image should conform to the ANSI/INCITS 385-2004 standard. The fingerprint images should conform to the ANSI/INCITS 381-2004 standard with 500 dots per inch (dpi) scan resolution.
2. One-to-Many Matching (Identification) -- NIST recommends ten slap fingerprint images stored in type 14 ANSI/NIST-ITL 1-2000 formatted records for enrollment and checking of large databases. Face images are not recommended for identification applications. With available fingerprint scanning technology, the acquisition of 10 slap fingerprints should take only slightly more time than the acquisition of two flat fingerprints.

Both of these recommendations are identical to the recommendations made in the joint report to Congress titled "Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents" [1] dated February 2003. Since this report was issued, extensive testing of biometric systems has been carried out by NIST that continue to support these recommendations.

VERIFICATION

For verification applications, the conclusions of the report sent to Congress dealing with the comparison of face and fingerprint accuracy should be updated in light of the following. First, NIST has recently found that the NIST-developed fingerprint matcher [2] is substantially less accurate than commercial systems. Second, the data used for tests in the report has lower quality than the data presently being collected by the US-VISIT program. Third, the face images used in these tests [3] are of higher quality than those in most operational government data sets.

When all these factors are combined, the comparison of face and fingerprint accuracy needs to be revised [4]. Contemporary fingerprint systems are substantially more accurate than face recognition systems. This conclusion holds even for face and fingerprint images categorized as high quality. This should be qualified by the observation that any advances in face recognition technology since the Face Recognition Vendor Test (FRVT) [3] have yet to be evaluated.

The two-fingerprint accuracy (or true accept rate (TAR)) at 0.1% false accept rate (FAR) for the US-VISIT two fingerprint matching system [4] is 99.6% while the best 2002 face recognition TAR at 1% FAR was 90% using controlled illumination [4]. When outdoor illumination was used in 2002 [3], the best TAR at 1% FAR was 54%. Even under controlled illumination, which is not currently used in US-VISIT, the error rate of face recognition is 25 times higher than the two-fingerprint results using US-VISIT data [4] that has 10 times lower FAR. If the case of uncontrolled illumination is considered, this factor would be 115. This means that face recognition is useful only for those cases where fingerprints of adequate quality cannot be obtained. The fingerprint matching

accuracy achieved with two fingers by US-VISIT is the best that can be achieved with current verification technology [5].

IDENTIFICATION

For identification applications, extensive testing on COTS fingerprint systems has confirmed the requirement for ten slap fingerprints. Eighteen different companies' products were tested, and thirty-four systems were evaluated [6]. Different data subtests measured accuracy for various numbers and types of fingerprints, using operational fingerprint data from a variety of U.S. Government sources. 48,105 sets of fingerprints (393,370 distinct fingerprint images) from 25,309 individuals were used for analysis.

For all systems, the accuracy increases as the number of fingers increase. The improvement is both large and consistent. Although the actual benefits were found to vary by dataset and by system, the general trend was quite consistent. The accuracy of searches using four or more fingers was higher than the accuracy of two finger searches, which was higher than the accuracy of single-finger searches.

These results are strongly dependent on fingerprint image quality. For the US-VISIT fingerprint matching system, using Department of State (DOS) Mexican visa Border Crossing Card (BCC) data, the true accept rate (TAR) using index finger pairs is independent of background database size over the range from 100,000 entries to 6,000,000 entries. Using the operational thresholds of (1300, 1880), the TAR is 96% [4]. If however image quality rather that database size is the controlling factor, then for low quality data, Cogent image quality 8 (the lowest image quality identified by the Cogent matcher), the TAR falls to 53.6%. With high quality images, Cogent image quality 1, the TAR is 99.6%. Image quality is important since the image quality of most archival law enforcement databases is lower than the image quality of the data presently being collected by US-VISIT and will remain so for some time into the future. The only tested method for improving matching accuracy for databases with lower image quality is to increase the number of fingers used. Typical 10-finger true accept rate (TAR) for the most accurate COTS system tested exceeded 99.95% at a false accept rate (FAR) of 0.01% [6].

REFERENCES

[1] "Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents – Appendix A;" PDF document at http://www.itl.nist.gov/iaui/894.03/fing/fing.html; November 2002.

[2] C L Wilson, C I Watson, M D Garris, A Hicklin; "Studies of Fingerprint Matching Using the NIST Verification Test Bed (VTB)" NISTIR 7020; National Institute of Standards and Technology; Gaithersburg Maryland; 07 July 2003

[3] P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and M. Bone, 'Face recognition vendor test 2002, NIST IR 6965, National Institute of Standards & Technology, Gaithersburg Maryland, March 2003.

[4] C. L. Wilson, M. D. Garris, and C. I. Watson, Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints, NISTIR 7110, National Institute of Standards and Technology, (May 2004).

[5] C. Watson, C. Wilson, K. Marshall, M. Indovina, R. Snelick, Studies of one-to-one fingerprint matching with vendor SDK matchers, NISTIR 7119, National Institute of Standards and Technology, (May, 2004).

[6] C.L. Wilson, R. Austin Hicklin, Harold Korves, Bradford Ulery, Melissa Zoepfl, Mike Bone, Patrick Grother, Ross Micheals. Steve Otto and, Craig Watson, Fingerprint vendor technology evaluation 2003: summary of results and analysis report, NISTIR 7123, National Institute of Standards and Technology, (June 2004).