Executive Summary of RAND Issue Paper IP-218[*]

BIOMETRICS: FACING UP TO TERRORISM

by John D. Woodward, Jr.[†]

As the nation recovers from the attacks of September 11, 2001, we must rededicate our efforts to preventing any such terrorist acts in the future. While there is no easy, foolproof technical fix to counter terrorism, the use of biometric technologies might help make America a safer place.

Biometrics refers to the use of a person's physical characteristics or personal traits to identify, or verify the claimed identity, of that individual. Fingerprints, faces, voices, and handwritten signatures are all examples of characteristics that have been used to identify us in this way. Biometric-based systems provide automatic, nearly instantaneous identification of a person by converting the biometric, for example a fingerprint, into digital form and then comparing it against a computerized database.

This RAND Issue Paper discusses how biometric technologies could be used to impede terrorism in three critical areas:

1. Controlling access to sensitive facilities at airports,
2. Preventing identity theft and fraud in the use of travel documents, and,
3. Identifying known or suspected terrorists with a proposed counterterrorist application known as FaceCheck.

CONTROLLING ACCESS

Sensitive areas of the nation's ports of entry, particularly airport facilities, need to be safeguarded so that only authorized personnel can gain access to them. Currently, badges and tokens, such as a key or pass card, are used to identify authorized personnel and to control access to these areas. The system assumes that whoever possesses the badge or the pass card is the person who should be granted access, when in reality, badges and tokens are easily forged, stolen or misplaced.

Security can be enhanced, however, by combining something a person must physically possess with something a person must know (such as a password or a personal identification number, PIN). The system is still easily compromised, however, because given the profusion of PINs and passwords and our difficulty remembering them, PINs are often written down on the card itself or on a piece of paper stored in close proximity to the card.

Access control to sensitive facilities can be further improved by using biometric-based identifiers. In other words, instead of identifying an individual based on something the person has (a badge), or something he knows (a password or a PIN), that person will be identified based on something he is. For example, instead of flashing a badge, airline staff with a need to access sensitive areas of airports could be required to present a biometric, for example, their iris, to a sensor. From a foot away and in a matter of seconds, this device captures the person's iris

---

[*] RAND issue papers explore topics of interest to the policymaking community. Although issue papers are formally reviewed, authors have substantial latitude to express provocative views without doing full justice to other perspectives. The views and conclusions expressed in issue papers are those of the authors and do not necessarily represent those of RAND or its research sponsors.

[†] John Woodward, a former CIA operations officer, is a RAND senior policy analyst. To obtain a copy of this Issue Paper, please contact RAND's Washington External Affairs office by email at wea@rand.org or call 703.413.1100 extension 5431.

image, converts it to a template, or computer readable representation of the iris, and searches a database containing the templates of authorized personnel for a match. A match confirms that the person seeking access to a particular area is in fact authorized to access that area.

PREVENTING IDENTITY THEFT AND FRAUD

Like badges and tokens, passports, visas and boarding passes can also be forged, misplaced or stolen. By placing a biometric template on such a document, for example, putting a template of one's fingerprint (or other biometric) on a bar code, chip or magnetic strip on the document, we make it more difficult for someone to adopt a false identity or create a forged travel document. To ensure security, the biometric should be encrypted and inserted into the document by a digital signature process using a trusted agent, such as a U.S. embassy's visa section.

IDENTIFYING KNOWN OR SUSPECTED TERRORISTS WITH FACECHECK

We need a better way to identify individuals, whom we know or suspect to be terrorists, when they attempt to enter the United States. Biometric facial recognition systems could be immediately deployed to help thwart future terrorist acts. Such a FaceCheck system can be implemented in a way that uses public safety resources effectively and efficiently and minimizes inconvenience and intrusiveness for the average traveler.

In general, facial recognition systems use a camera to capture an image of a person's face, as a digital photograph. This image is manipulated and reduced to a series of numbers that represent the image in relation to the "average" face. These numbers are often referred to as a template, which is instantly searched against a "watchlist," or computerized database of suspected terrorists' templates. This search seeks to answer the question, "Is this person in the watchlist database?" A computer-generated match or "hit" alerts the authorities to the presence of a potential threat.

The technology, however, is not perfect, and it has yet to be fully vetted in real world, operational settings. Although human beings generally can perform facial recognition processes fairly well, these activities are still very challenging for technological systems. Unless the photograph is captured under very controlled conditions, the system may have difficulty identifying the individual or even detecting his face in the photograph. The system works best when environmental factors such as camera angle, lighting, facial expression and others, are controlled to the maximum extent possible.

If a person (including a terrorist) is coming to the United States from overseas, he or she likely passes through an immigration checkpoint at the port of entry. From the perspective of counterterrorism, this checkpoint is a chokepoint where the would-be terrorist is most vulnerable. This is the first and likely only place in the U.S. where he will be closely scrutinized by trained federal officials. Here is how FaceCheck can make the checkpoint a more formidable bastion. (See Figure 1 on the next page.)

An individual processing through an immigration checkpoint at a port of entry should be subject to a FaceCheck whereby he or she would be required to pose for a photograph under completely controlled conditions. This way we minimize facial recognition's technological imperfections, which derive in large measure from the system attempting to find a face in a crowd. The photograph would then be processed by the facial recognition system and run against a watchlist database of suspect terrorists. If the system indicates a match, this result would be confirmed by visual inspection by the authorities, and the person could be taken to a secondary interview for heightened scrutiny.

Facial recognition systems do not necessarily have to be implemented to process every individual seeking to enter the United States. Rather, the authorities should use FaceCheck in a more strategic way. This would include using FaceCheck randomly; in targeted ways; and in conjunction with other information. Testers, or human guinea pigs, whose images have been entered into the watchlist database should be included in the immigration processing to rigorously evaluate the system—how well did FaceCheck do in identifying suspects?

Moreover, while we do not have to use FaceCheck on all passengers entering the United States, we should consider setting up FaceCheck stations at ports of entry and have passengers pose for photographs as if we are using FaceCheck. In this way, we keep terrorists guessing as to where the systems are actually deployed or in use. We should also experiment with FaceCheck systems using closed circuit surveillance cameras to capture images clandestinely at certain ports of entry. In this way, we can learn how well such systems work in realistic operational environments and gain information to improve their technical capabilities. We also need to consider using FaceCheck for visa processing at our embassies and consulates overseas. We could easily require a visa applicant to submit to a photograph taken under controlled conditionsand then run a search against the watchlist database before issuing a visa.

Dedicated, highly-trained terrorists may be able to defeat facial recognition systems, but at least we force terrorists to take additional steps that drain their resources and keep them on the defensive.

CONCLUSION

There is no high tech silver bullet to solve the terrorism problem. But to the extent we can improve access control at sensitive facilities such as airports, reduce identity theft and immigration fraud, and identify known or suspected terrorists with FaceCheck, then we make terrorism more difficult in the future. Biometrics is one technology that can help us achieve the goal of a safer America.

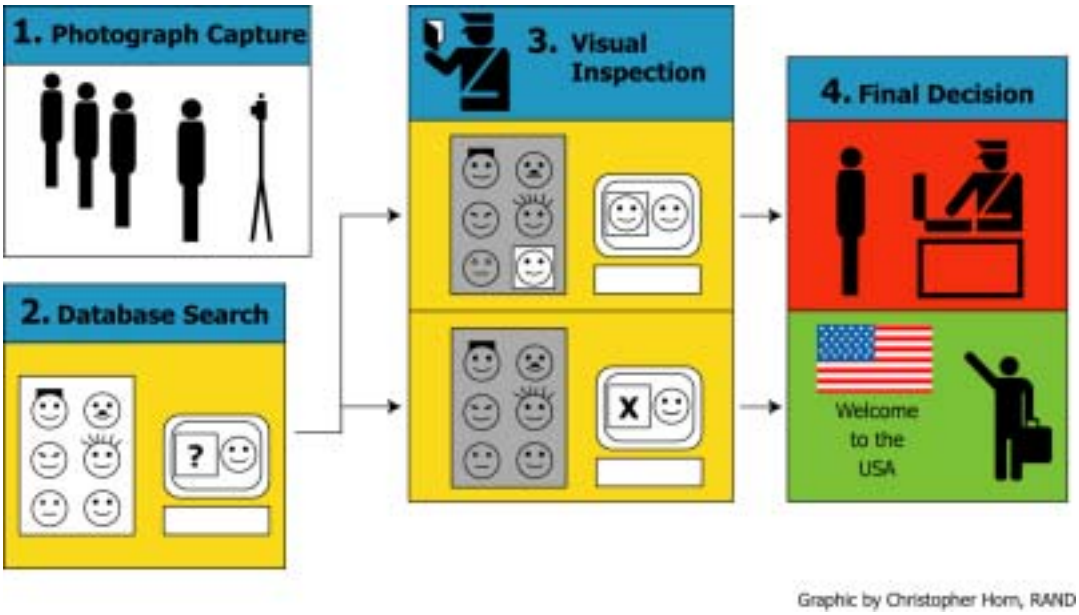

Figure 1 - **Countering Terrorism with FaceCheck**