FINGERPRINT VERIFICATION FOR CONTROL OF ELECTRONIC BLAST INITIATION

Ron F Stewart[1], Richard Youmaran[2], Andy Adler[3]

[1]Orica Canada Inc, Brownsburg, Quebec, Canada
[2]School of Information Technology and Engineering, University of Ottawa, Canada
[3]Systems and Computer Engineering, Carleton University, Ottawa, Canada

ABSTRACT

In the current context of heightened concerns with explosives security, there is significant interest in technological controls to improve security. It is important to be able to control what is fired, by whom, where and when. This paper describes research Orica has performed to investigate and test biometric systems to address the question of "by whom". The goal of this research is to incorporate the most suitable biometric system onto the 'blaster' unit of an electronic initiation system. This approach will ensure that only authorized personnel can initiate a blast involving electronic detonators. *Requirements analysis:* we initially explored many different biometric technologies to evaluate them against the requirements, including security, usability, ruggedness, size, form factor, privacy, and operational temperature range, This analysis identified chip based fingerprint sensors as the best candidate. *Development of prototype units:* in order to test the identified sensors, we modified standard, commercially-available, electronic blast initiation units ("blaster") to incorporate a fingerprint reader. *Testing and evaluation: Biometric* We conducted a biometric scenario evaluation in order to determine: 1) security level (measured by false accept rate (FAR)); 2) usability (measured by failure to enroll (FTE) and false reject rates (FRR)), and to 3) discover environment specific issues and challenges (such as temperature, humidity, dirt, or those related to the usage patterns of the user group). Tests were conducted at quarry sites in eastern Ontario, Canada. Results show rates of: FAR= 0%, FTE= 1.67%, FRR= 28.81%. Overall, these results suggest that this fingerprint biometric technology has a good level of usability in this application of electronic blast initiation control.

INTRODUCTION

In the current context of heightened concerns with explosives security, there is significant interest in technological controls to improve security. Fortunately, emergent technologies offer the promise of a step change in control of *what* is fired, by *whom*, *where* and *when*! The advent of electronic initiation systems especially facilitates this desirable goal [WIPO ref 1] [WIPO ref 2]. This paper concerns enhanced security of *who* fires explosives. Biometric technologies, such as fingerprint, face and iris recognition, allow automatic identification of users [Wayman, 1999]. We describe research Orica has performed to investigate and test biometric systems to enhance explosives security. Biometric system performance is known to vary significantly depending on the environmental conditions, user training, user motivation, population characteristics and other factors. The goal of this research is to incorporate the most suitable biometric system onto the 'blaster' unit of an electronic initiation system. This approach will ensure that only authorized personnel can initiate a blast involving electronic detonators.

Fingerprint technology is currently being tested for many identity applications. Some relevant tests are technology evaluations [Maio, 2002] [Wilson, 2003], and the Seafarer's ID card interoperability tests [ILO, 2004]. However, we are not aware of any tests performed in conditions sufficiently similar to

blasting applications. We therefore conducted research to investigate biometrics performance for control of blast initiation. This research was conducted in three phases: 1) requirements analysis, 2) development of prototype units, and 3) testing and evaluation which involves user enrollment, data acquisition and data analysis.

REQUIREMENT ANALYSIS

We initially explored many different biometric technologies to evaluate them against the requirements, including security, usability, ruggedness, size, form factor, and operational temperature range. Additional considerations were applicability to all potential users, and privacy concerns. Many biometric modalities exist; common examples are fingerprint, face and iris identification, but other examples include finger vein, signature, voice pattern, gait, and many others. For each modality there are multiple technology vendors, and multiple algorithms. In order to analyse the requirements, this section reviews issues in implementation and use of biometrics technology that will need to be considered.

Performance Measures

Biometrics performance measures the ability of authorized users to correctly enroll and access the system, preventing non-authorized people from access. The first group (genuine users) must first enroll into the system (an error at this stage is a failure to enroll or FTE). Later, when they use the system, it must acquire an image of the user (an error here is a failure to acquire or FTA), and then successfully identify the user (an error here is a false reject or FR). The second group (impostors) do not enroll, but (whether by error or with malicious intent) attempt to access the system. If the biometric falsely grants access, this is considered to be a false accept or FA.

If a biometric system allows multiple tries (three attempts is typical), then a FR would be the case where none of the attempts is successful. The term for a failure for single biometric match attempt is a false non-match (FNM). In a test protocol, the rate of these errors is measured to calculate the false reject rate (FRR) or false accept rate (FAR). Many biometric algorithms allow a trade-off to be made between these rates. Typically the FAR may be decreased by allowing the FRR to increase.

Biometric performance depends strongly on the population using the system. Issues are:

- *Biometric placement:* Correct positioning is essential for high quality images. For example, for fingerprints, the finger must be placed consistently with a consistent pressure. Correct placement can be helped with training, motivation or by supervision.
- *Training and motivation:* Training can typically be done very quickly (in a few minutes) but must be done before the enrollment process (otherwise the enrolled image will be of poor quality). Motivated users are those who see the biometric technology as a benefit to themselves. This can be ensured by a well thought out design of the entire system to minimize any inconveniences to the users from the technology.
- *Biometric image quality:* Image quality varies dramatically between samples (see Fig. 2 for example). Certain occupations, such as construction and farming, are known to damage fingerprint details over time, which dramatically increases error rates [Maio, 1997]. It is quite likely that mine/quarry work also has this effect, although we are unaware of any studies of this population.

- *Environmental Factors:* Most applications of biometrics are in place which are relatively clean and at room temperature. Outdoor applications, such as the one considered here, introduce many difficulties, such as dirt and wide changes in temperature and humidity. These factors are known to decrease biometric performance.

Failure to Enroll

As mentioned in the previous section, a certain fraction of fingerprints do not have enough detail to be enrolled, resulting in a failure to enroll (FTE). FTE depends on the application, although rates of as 2 percent are common. There are several possible solutions to FTE: 1) a user may attempt to enroll each finger to find one that has sufficient details, and 2) some fingerprint algorithms allow presentation of multiple fingers in order to combine details from each. If there are users for which neither strategy works, it may be necessary to provide a card or key to override the system. Such an override mechanism is likely necessary in any case, for the possibility the biometric sensor fails.

Usability and user perception

Usability issues are important for biometric technology, especially due to the recent media focus in the context of national security systems. Successful biometric implementations need to show clear benefit to the users and to be clear about the use and storage of private data. From a commercial point of view, biometric systems have been most successful in physical access, time and attendance, and network security applications.

Security level requirement

The security level of a biometric system is measured by the FAR - the probability of successful access by an impostor. The security level requirement must be established by considering the level of threat of an impostor. In many cases a very low FAR (below 1:1000) is not very important, because a malicious impostor may be able to take other approaches to access the system.

Security level varies with the number of enrolled users per device. For example, a typical FAR level may be 1 in 10,000. If 100 users are enrolled onto a single device, then each presented image is compared against each enrolled fingerprint (called 1: N biometric operation). This results in an overall FAR of approximately 1 in 100. If required, it is possible to improve the FAR by requiring each user to present a code or ID in order to be compared against only themselves (called 1:1 biometric operation).

Cost

Costs of deploying and operating biometrics technology in an electronic blaster are from many sources, including: the biometrics sensor, interface electronics to blaster support technology to manage user enrollment and training.

Control of Enrolment and Privacy

Biometric privacy is a sensitive issue in many applications. This is especially true for fingerprints, mostly because of the criminal connotations of fingerprinting. It is generally reported that the best way

to manage privacy issues is have a clear policy and information on the use and storage of biometric images. Since blasting is a high security operation, it is likely that users have already provided fingerprints to obtain permits, and will be less concerned about the privacy issues.

We consider two possible enrolment scenarios.

- *Site level control:* the local site manager has the software to enroll users onto each electronic blaster unit. Local procedures are established to add and remove users from the lists of permitted operators. Enrolled fingerprints would be stored in the local computer which is used for enrolment and would not be available outside the site.
- *Corporate level control:* the blasting equipment vendor would enroll users as they complete a course on the use of the electronic blasting system. Software would allow each local site to interact with the list of approved users and to download fingerprints to the blaster units as required. In this scenario, fingerprints would be stored by equipment vendor.

Legal compliance

It is clearly important to comply with local laws, especially with respect to privacy and policing issues. One biometric specific issue is whether technology should implemented to make it efficient to comply with a court order to give stored fingerprints to police.

Biometrics standards and interoperability

The international standards organization (ISO) has numerous standards and draft standards within WG1-SC37 that are relevant to biometrics implementations, especially if interoperability is a concern. On the other hand, if the implemented system will operate in isolation, and does not need to interact with any other biometric system, then there is no need for standards compliance.

BIOMETRIC TECHNOLOGY

Biometric technology has matured dramatically in the past 10 years, and many modalities and devices are available. The choice of an appropriate biometric technology for this application should consider security, usability, ruggedness, reliability, size, form factor, temperature range, user perception, ease of use, cost, and mobility.

In this section, we briefly summarize the technologies were that were considered for this application:

- *Fingerprint: Optical Sensors* A finger is placed on a glass or acrylic plate and the image is captured by a camera. Optical sensors are relatively inexpensive and robust. Some disadvantages of optical systems are that the physically larger, and work less well with dry skin, and may be easier to spoof. In order to improve dry skin performance (which is be most severe at low temperatures), most manufacturers place a layer of silicone on the platen; however this silicone is less robust to heavy use.
- *Fingerprint: Silicon Chip Sensors* Such field scanners require the finger to be placed directly onto a silicon chip which images the electromagnetic interaction between the chip and the live finger surface. Such scanners are physically smaller but tend to be more expensive and have

worse wet skin performance than optical sensors. Such sensors are quite resistant to environmental stresses (impacts, dirt, etc.) and allows a largest operating temperature range (-20° C to +70°C). Silicon chip sensors were recommended as the likely most reliable technology for initial evaluation.

- *Fingerprint: Swipe based fingerprint readers* In order to achieve lower cost, fingerprint image technologies can be implemented in a swipe construction. The user will move the finger across the sensor and a video image is taken, from which the complete fingerprint image is subsequently reconstructed. This allows cheaper sensors, but suffers from a larger training requirement for users, since it is important to learn how to reliably swipe the finger across the imaging area.
- *Finger vein pattern* Near-infrared light from LEDs penetrates the finger. Veins absorb the light and appear dark in the image. Compared to fingerprint sensors this technology is claimed to be less resistant to dirt and spoofing. However, it is relatively new and less well understood at this stage.

Technologies not considered: Face, Voice, Iris, Signature Biometric technologies such as face, voice, iris, signature, and gait are not appropriate for this application system because they do not match the required workflow or would be cumbersome to use. For example, Iris based biometrics require an infra-red camera and a specific placement of the user with respect to the system which is inconvenient. Signature biometrics would be difficult to integrate with the current blasting workflow.

PROTOTYPE UNITS

Hardware: In order to test these fingerprint chip readers, we developed a number of prototype units in which fingerprint reader and verification hardware was inserted into a standard, commercially-available, electronic blast initiation unit ("blaster") and sealed for environmental ruggedness (Fig.1). The fingerprint sensor was placed ergonomic prototype system in order to simulate realistic usage patterns, since the configuration of this unit will have a significant impact on device usability, impacting test results. Based on these prototypes, internal demonstrations were conducted to obtain feedback on possible implementation issues.

Software: The image capture software was designed to provide a user interface to supervise and enroll users, online validation to ensure proper finger issue for repeat enrolment, and Database to store all capture fingerprints for offline analysis.

Figure 1: Fingerprint capture unit mounting on electronic blasting unit. The fingerprint sensor is shown at bottom left.

TESTING AND EVALUATION

The testing protocol was reviewed and approved by the Human Research Ethics Board at the University of Ottawa. Tests were designed to follow the guidelines for a *Scenario Evaluation* according to the recommendations of *Best Practices in Testing and Reporting Performance of Biometric Devices* [Mansfield, 2002], [ISO 2006]

Tests were conducted at 4 different quarries in Eastern Ontario. Data were gathered shortly after the blasting was performed. Weather was dry and warm (15−30°C) throughout the tests. A numerical ID is assigned to each user during the first enrollment in the database, in order to protect user identity. During the data acquisition phase, we collected biographical data of the participants to allow repeat enrollment. Once the data acquisition was complete there was no need to link the database of fingerprints with personal information. However, it was necessary to be able a set of prints from a specific participant in order to determine the security level and usability.

The data collection protocol was as follows: at each site, on each visit, users were asked to place all 10 fingers (one at a time) onto the prototype unit, and the fingerprint images captured for later analysis. Users were asked, on command, to place and to remove their fingers on the fingerprint sensor integrated on the Orica blaster unit. Fingerprint placement was not monitored at this stage since it is intended to be an operator independent process. Also, fingerprints were collected under challenging conditions such as humidity, temperature, dust, and dirt. Users were asked to repeat the described process twice at each visit. If at any time during the gathering process, a user did not place or remove their finger properly on the sensor, an error message is seen and the procedure was repeated for that finger.

In total, 170 images were captured on 8 test days on 6 different participants. User collaboration was good; they were patient and understanding through the entire process, and understood the data gathering procedure and were sympathetic to the aims of the research.

RESULTS

The gathered data is used to conduct a biometric scenario evaluation in order to determine: 1) *security level* (measured by false accept rate); 2) *usability* (measured by failure to enroll (FTE) and false reject rates (FRR), and to 3) *discover environment specific issues and challenges* (such as temperature, humidity, dirt, or those related to the usage patterns of the user group).

170 images in total for 6 different people were obtained during this experiment. 60 images are used for enrollment purpose and the remaining fingerprints for identification. Out of 60 images, only one finger did not enroll properly and was rejected. The user did not have a sufficiently good fingerprint image quality and only 9 fingers were used for enrollment. The acquired images were analyzed using the Neurotechnologija MegaMatcher version 1.0.0.1 software [Neurotechnologija]. This software performed well (4th place) in the FVC2004 fingerprint tests [Maio, 2002], and is designed to function with the images from the selected fingerprint sensor.

Overall, the following results were obtained:

- Failure to enroll rate (FTE) of 1.67%
- False accept rate (FAR) of 0%
- False reject rate (FRR) of 28.81%

Results show that fingerprint quality was high for most participants. One finger could not be enrolled, but this individual could enroll the other fingers. On the other hand, the FRR rate was large. Subsequent analysis shows this to be largely a finger placement issue. Fig. 2 illustrates a representative sample of possible concerns with finger images that were captured in this study. (Participants whose finger images are shown agreed to such disclosure).

Figure 2: Fingerprint images of various possible concerns with finger images. Numbered from right to left: 1) Finger placement, 2) Poor quality ridges on finger, 3) cut on finger, 4) and 5) Dirt or poor quality ridges on finger. All of the images shown here can still be processed with the software.

DISCUSSION

Overall, these results suggest that fingerprint biometric technology has a good level of usability in this application of electronic blast initiation control. Biometric security appears to be good, as no False accept events were detected. Dirt did not appear to be a significant problem in this study. In most cases the sensor worked with dirty fingers. When it did not, users would typically wipe fingers on their clothes with a good effect. (No specific instructions were given for dirt.) Overall, user perception was good.

Users understood the need and value of the technology. There was one user who did not want to participate (he did not want to give out his fingerprints). Some users were concerned that the technology may be inconvenient to use.

From the usability point of view, it appears that fingerprint quality was high for most participants. However, the FRR was high, largely due to finger placement errors. Currently, we are preparing a phase II study which will address this issue. Fingerprint placement is understood to be a training issue, in which performance can be improved by 1) better initial training to sensitize users to the issue, and 2) better feedback to users as they use the device. Phase II tests will incorporate both of these elements. Trials have also begun on the use of this kind of technology to enhance other aspects of the security of the explosives supply chain.

Conclusion: overall results to date show that this fingerprint biometric technology has a good level of usability in the application of electronic blast initiation control. We plan to continue to investigate biometric technology to enhance blasting security as well as other aspects of the security of the explosives supply chain.

REFERENCES

- "Blasting Methods and Apparatus with Reduced Risk of Inadvertent or Illicit Use" WIPO International Publication WO2006/086844
- International Labour Organization, *ILO Seafarers' Identity Documents Biometric Testing Campaign Report* Part 1: Technical Report, 2004 www.ilo.org/public/english/dialogue/sector/papers/maritime/sid-test-report1.pdf
- ISO/IEC 19795-1:2006, *Information technology. Biometric performance testing and reporting. Principles and framework* ISO, 2006.
- Maio, D., Maltoni, D., 1997, "Direct gray-scale minutiae detection in fingerprints" IEEE Trans. Pattern Analysis and Machine Intelligence, 19(1), pp. 27-40
- Maio, D. Maltoni, D. Cappelli, R. Wayman, J.L. Jain, A.K., 2002, "FVC2000: fingerprint verification competition", IEEE Trans. Pattern Analysis and Machine Intelligence, 24(3), pp. 402-412
- Mansfield A.J., Wayman J.L., *Best Practices in Testing and Reporting Performance of Biometric Devices (Version 2.01)* Centre for Mathematics and Scientific Computing, National Physical Laboratory, UK, August 2002 www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf
- Neurotechnologija Inc. Megamatcher SDK, www.neurotechnologija.com
- Wayman J.L., 1999, "Fundamentals of Biometric Authentication Technologies," Proc. Card Tech/Secure Tech. also: www.engr.sjsu.edu/biometrics/nbtccw.pdf
- Wilson C., Hicklin R.A., Korves H., Ulery B., Zoepfl M., Bone M., Grother P., Micheals R., Otto S., Watson C., *Fingerprint Vendor Technology Evaluation 2003* National Institute of Standards and Technology, 2003 fpvte.nist.gov/report/ir_7123_summary.pdf
- "Security Enhanced Blasting Apparatus with Biometric Analyzer and Method of Blasting" WIPO International Publication WO2006/086843