Fingerprint recognition performance in rugged outdoors and cold weather conditions

Ron F Stewart, Matt Estevao, Andy Adler

Abstract— **This paper reports on tests of the performance of fingerprint recognition technology in rugged outdoor conditions, with an especial concentration on the performance in cold weather. We analyze: 1) chip versus optical fingerprint scanner technology, 2) recognition performance and image quality, and 3) user/device interaction. A outdoor fingerprint door access system was designed to capture fingerprint images and video data of user interactions. Using this device, data were captured over a period of two years, and a user survey performed. Data were analyzed in terms of biometric error rates and fingerprint quality (NFIQ) as a function of temperature and humidity. Results suggest: 1) biometric performance has no significant dependence on temperature and humidity (-30C to +20C), 2) both chip based and optical fingerprint scanners have some flaws in rugged and cold weather applications, and 3) overall fingerprint biometric technology has a good level of usability in this application.**

I. INTRODUCTION

We test and report on the performance of fingerprint recognition technology in rugged outdoor conditions, with an especial concentration on the performance in cold weather. We focus on: 1) the ruggedness of the technology itself, 2) the performance in terms of biometric error rates and image quality, and 3) the usability of the technology. We are motivated by the current context of heightened concerns with explosives security. There is significant interest from explosives manufacturers, users and regulators to develop technological controls to improve this security. Such improved security is needed throughout the hazardous chemicals and explosives industries, for applications such as access control to explosives buildings and magazines, for authorization of use of explosive equipment, such as mobile manufacturing units, and for electronic blasting. Fortunately, several emergent technologies including biometrics offer the promise of a step change in control of *what* equipment is used, by *whom*, *where* and *when* [5], [9], [10].

Biometric technologies, such as fingerprint, face and iris recognition, allow automatic identification of users [7]. However, biometric system performance is known to vary significantly depending on the environmental conditions, user training, user motivation, population characteristics and other factors.

Fingerprint technology is currently being tested for many identity applications; and some relevant tests are technology evaluations such as [1], [8], and the Seafarer's ID card interoperability tests [2]. We are not aware of any biometric operational tests performed in conditions sufficiently similar to the rugged, outdoor environment of explosives manufacturing, storage and blasting applications. We note that some anecdotal evidence suggests that there is a large basis of expertise using fingerprints in military applications, primarily in hot, desert climates. However, these results would not address our concern with low temperature performance issues.

We therefore set out to perform tests to understand the operational advantages and limitations of fingerprint biometric systems in such environments. This research was conducted in three phases: 1) requirements analysis, 2) development of prototype units, and 3) testing and evaluation. The first two phases have been published [4], while this paper focuses on testing and evaluation.

II. OPERATIONAL REQUIREMENTS

Our initial phases of research were designed to select an appropriate biometric modality for explosives security. Many different biometric technologies were explored and evaluated against a set of usability and operational requirements [4]: security, usability, ruggedness, reliability, size, form factor, temperature range, user perception, privacy concerns, ease of use, cost, and mobility.

Based on this analysis, several biometric modalities were classified as inappropriate for this application, since they do not match the required workflow or would be cumbersome to use (modalities identified as inappropriate were face, voice, iris, and signature). The main biometric modalities considered were fingerprint and finger vein pattern; of these, fingerprint was chosen because it was judged to be the technology which was best understood operationally and with a large vendor base.

Fingerprint image capture technologies were considered for the application as follows:

- *Optical sensors:* A finger is placed on a glass or acrylic plate and the reflectance image is captured by a camera. Optical sensors are relatively inexpensive and robust. Some disadvantages of optical systems are that they are 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), some manufacturers place a layer of silicone on the platen; however this silicone is less robust under heavy use.
- *Silicon chip sensors:* the finger is 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

Stewart is with Orica Canada Inc, Brownsburg, Quebec, Canada, ron.f.stewart@orica.com

Estevao and Adler are with Systems and Computer Engineering, Carleton University, Ottawa, Canada, adler@sce.carleton.ca

more expensive and have worse wet skin performance than optical sensors. Such sensors are quite resistant to environmental stresses (impacts, dirt, etc.) and have a large advertised operating temperature range ($-20\,^{\circ}$C – $+70\,^{\circ}$C).

Both types of sensors were considered for testing. It was decided to consider only full size fingerprint sensors and not swipe action fingerprint sensors, in which the user moves the finger across the sensor and an image sequence is captured, from which the complete fingerprint image is subsequently reconstructed. Such swipe sensors are lower cost (using less sensor area), but suffer from a larger false rejection rate and training requirement for users.

Based on our requirements analysis, a biometrics scenario evaluation [3] was performed to determine the effectiveness of the biometrics system and identity issues in the technology, implementation, user training, and other human factors relevant to use of fingerprints in this application. Three key research questions were elaborated, to determine:

- *hardware/sensor performance issues:* including reliability of fingerprint technologies, failure modes, effects of dirt and weather on sensors.
- *fingerprint physiology performance issues:* including the variability in fingerprint performance with temperature and humidity.
- *usability factors:* with a focus on human factors that can be addressed in user training or design/configuration of the fingerprint unit.

III. EXPERIMENTAL CONFIGURATION

A biometric scenario test was conducted in a door access configuration at two sites near Ottawa, Canada. This location shows a large variability in temperature ($-35\,^{\circ}$C – $+30\,^{\circ}$C, during the test period). Two different fingerprint sensor types were used, one capacitive and the other optical, each for a period of one year. The data collected from these tests included: fingerprint images and match results, video images of users interacting with the sensors, user surveys, and weather data. The experimental protocol was reviewed and approved by the university's human research ethics board.

A. Biometric sensors

Tests were performed on a capacitive scanner (TCS1, UPEK, Emeryville, CA, USA) and an optical scanner (FS88, Futronic, Hong Kong). The electronics of each sensor were rated for $0\,^{\circ}$C – $70\,^{\circ}$C. For the external interface, the capacitance sensor itself is rated to $-30\,^{\circ}$C, while the optical sensor uses an acrylic window which can also withstand similar cold temperatures. In order to provide a rugged enclosure with heating and weather sealing, each sensor was mounted into an insulated high density lexan enclosure which contained the device and indicator lights (Fig. 1). The fingerprint sensor was weather sealed into the enclosure. A similar box was made to mount the camera above the fingerprint scanner. Red and green indicator LEDs were installed in this box to communicate system status to the user.

Both devices have USB type connectors which were passed to a controller computer inside the building. The enclosure was insulated and heated to maintain operating temperature with a thermal switch ($+10\,^{\circ}$C) connected to power resistors giving 13W heating power. During the coldest days, this heating made the fingerprint sensor feel slightly warmer than the outside air.

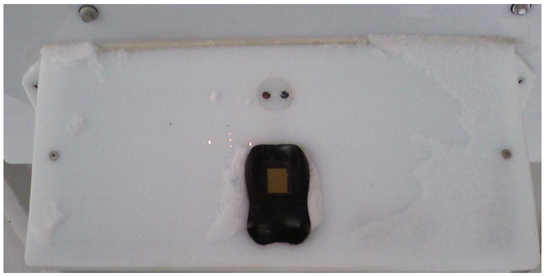

Fig. 1. Fingerprint sensor (UPEK TCS1) placement in a heated box. The snow had been partially cleared from the sensor by users.

Fingerprint matching was performed using a custom application based on the Verifinger SDK, version 5.0 (Neurotechnology Vilnius, Lithuania). The system operated in *identification* mode, in which each presented print was accepted if it matched any enrolled print. Thus, users did not need to present any card or ID number. Fingerprints matching authorized users at the 1:10,000 security level were given access. All presented fingerprints were saved to disk and were subsequently post-processed for data interpretation.

B. Application configuration

The application was designed to allow access to the main facility at Orica Canada's explosives distribution center at Greeley, Ontario, Canada. This facility manages filling of transport vehicles for delivery to clients. The tests began in August 2007, and a second site was added in December 2008. Data captured until May 2009 are analyzed in this paper. At the main site (9 users), a device was built to allow video capture of user interactions with the fingerprint sensor, as shown in Fig. 2. A USB webcam is focused downward at the fingerprint sensor to capture the movement and positioning of users hands. At the second site (4 users), only the fingerprint sensor was placed (without video capture).

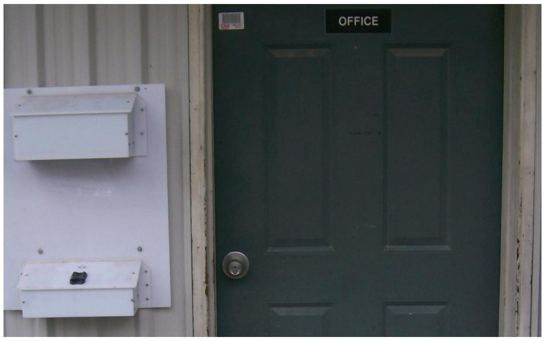

Fig. 2. Fingerprint scanner (lower white box) and video camera (upper white box) at Greeley, Ontario site.

Cables and controller wires from the sensors were fed inside the building to a controller PC based on Windows XP. Custom software allowed user enrollment and performed data capture. Door access was provided by controlling a magnetic door lock through a relay. Video data were captured continually, whenever motion was detected. If a fingerprint event was detected during this interval, then the video stream was saved to disk; otherwise, the recording was deemed to be spurious, and discarded. In order to provide for resistance against power outages at the site, battery backup was provided for the system.

The use of Windows as an operating system platform caused numerous difficulties, mostly due to the way in which errors occurring with the fingerprint sensors which were handled (by "popping up" an error message, which blocked the application and confused the site users). We strongly recommend against using such a desktop operating system for a biometric implementation, although it was deemed necessary to allow collection of the research data in this application.

User enrollment was performed on the same device used for access. The custom software provided an enrollment interface which would allow enrollment of new users and removal of previously enrolled users (if required) under control of the site manager. For training, users were given a brief description of fingerprint technology and a demonstration of finger placement. After six months of use, a survey was performed of site users based on open ended questions about user's perceptions of the biometric technology.

C. *Weather information*

Hourly weather information covering the testing period was downloaded from Environment Canada for the weather stations closest to the test sites. The weather data for temperature, windchill, dew point, and relative humidity were extracted for further analysis.

IV. DATA ANALYSIS

A. *Usage Patterns*

Video data of participants was analyzed manually. Each recorded event was reviewed to determine whether it constituted a "normal" or "unusual" usage pattern. Based on such analysis, two unusual usage patterns were identified. These patterns were discussed with the participants in order to clarify what circumstances were happening.

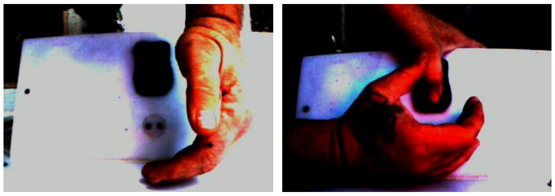

Fig. 3. Unusual usage pattern #1: cupping hands around fingerprint sensor

The first unusual pattern was a cupping of the hands around the fingerprint sensor. This occurred primarily during the day, but also occurred at night, as shown in Fig. 3. Participants reported that this was because indicator lights were not sufficiently bright, so that it was not easy to tell whether the fingerprint had been accepted. This was especially true in bright sunshine. This feature was corrected by placing higher intensity lights during a hardware upgrade.

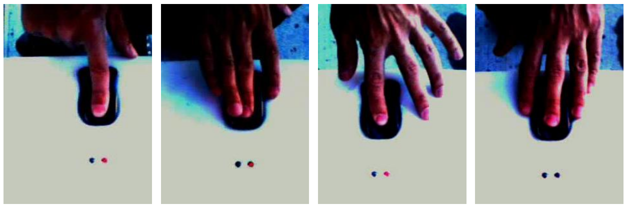

Fig. 4. Unusual usage pattern #2: rapid alternation of finger presentation. A single user made these presentations within 83s.

The second usual pattern was from participants placing multiple different fingerprints in rapid succession, as shown in Fig. 4. In one case a single user placed four different fingers within less than 1.5 minutes. This type of behavior was most prominent near the beginning of the tests. The explanation given by the participants was that they had forgotten which finger was enrolled. We suspect that this is partially due to the delay in system operation. There is a 2.0 second average delay between initial finger placement and the door opening, resulting from 1.0 second of scanning time, and 1.0 second of biometric processing time. As users become habituated, it appears that this delay becomes expected. However, for new users, it sometimes causes difficulties, as they expect immediate response from the system and will make additional placements too soon.

Another usage pattern was reported by participants but not recorded in the video data. In the early afternoon, when exposed to bright sunlight, the capacitive sensor became unbearably hot to touch. This problem only occurred with the capacitance sensor; the lexan on the optical sensor did not heat in the same way. Interestingly, participants did not feel that the cold was a similar barrier. Removing gloves to use the sensor was reported to be somewhat inconvenient, but was perceived to be roughly equivalent to use of keys.

B. *Biometric Performance*

Data captured were stored by time and date for subsequent post processing. All saved fingerprint files were inspected to remove non-fingerprint images that may have been captured, such as ghost images (due to sun shining through latent print oils on the sensor surface) or images of condensation on the sensor. Each file was then processed to calculate the maximum match score against all enrolled users, and this was compared against the software threshold setting defined for 1:10,000 match error rates. Since we do not have a verified identity of each fingerprint attempt, it is not possible to distinguish between false and true matches and non-matches. Therefore, we define the following rates:

- *Accept Rate: (AR)* an image is accepted against any enrolled user

- *Reject Rate: (RR)* an image is not accepted against any enrolled user. This occurs most commonly due to poor finger placement or dirty or wet fingers.
- *Failure to Acquire Rate: (FTAR)* the sensor detects the presence of something, but a fingerprint image is not registered. This occurs most commonly due to early finger removal.

The following rates were determined over the course of the study: AR= 66.4%, RR= 20.0%, FTAR= 15.5%. This indicates that about $\frac{2}{3}$ of presented fingers were accepted. Examples of rejected fingerprints are shown in Fig. 5

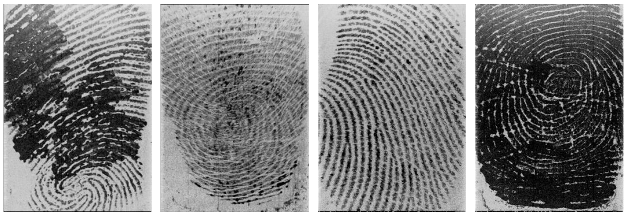

Fig. 5. Examples of rejected fingerprint images: (*from left to right:*) fingerprint covered with liquid; fingerprint moved during scanning (blurred image); fingerprint incorrectly placed; fingerprint applied with too much pressure (blurring features).

We were especially interested in the role of weather on variations in determining the performance of fingerprint access systems in outdoor applications. In particular, cold weather is suspected to result in dry and stiffer fingerprint physiology. Such changes would result in poor performance both on the optical scanner (due to decreased compliance of the fingerprint ridges onto the platen) and the capacitance scanner (due to increased impedance of the dry skin).

In order to address this issue, we compared fingerprint performance to the temperature and humidity. Fig. 6 shows RR a function of temperature (°C) for the optical scanner. A correlation coefficient of $r = -0.101$ is calculated, indicating a very weak relationship between Temperature and RR.

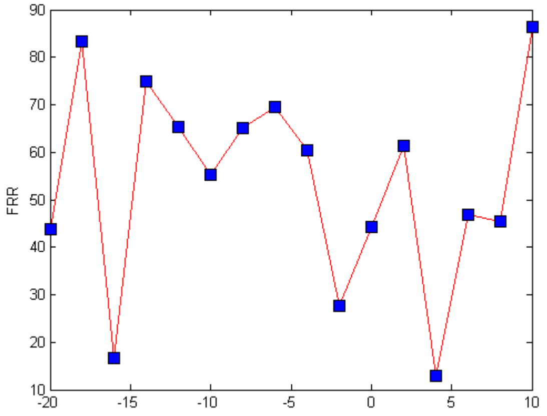

Fig. 6. Reject Rate (RR) vs. Temperature (°C) for the optical scanner.

C. Fingerprint Image Quality and Weather

Since the match rates were a function of the vendor SDK algorithm, and of both the enrolled and live fingerprint images, we wanted to find a measure more sensitive to the presented fingerprint image quality. We choose to use the NIST fingerprint image quality (NFIQ), which is "intended to be predictive of the relative performance of a minutia based fingerprint matching system.[6]" This algorithm gives an integer rating for fingerprint image quality using a 1–5 scale. A rating of 1 indicates a very good quality image, while 5 indicates very poor.

Based on NFIQ measures, we first validated that NFIQ values did predict biometric performance in this case (Fig. 7).

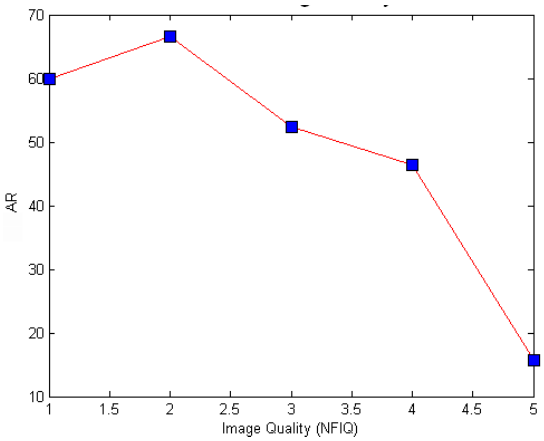

Fig. 7. Acceptance Rate (AR) versus NFIQ for the optical scanner.

Next, NFIQ was analyzed as a function of temperature (Fig. 8) and humidity (Fig. 9) for each fingerprint image captured. A very weak relationship is shown between these environmental variables and fingerprint quality or match performance.

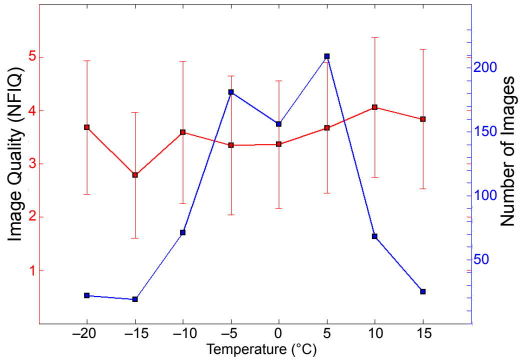

Fig. 8. Average NFIQ (±SE) vs. Temperature (°C) for the optical scanner. Each Temperature on the horizontal axis indicates a range of ±2.5 °C.

D. Survey of Participants

The survey of participants showed broadly positive results. Participants were largely not concerned with privacy issues; however, in order to obtain explosives permits, employees require police fingerprinting and background checks, so there is a familiarity with security requirements. Survey questions and a summary of responses are shown in the following list:

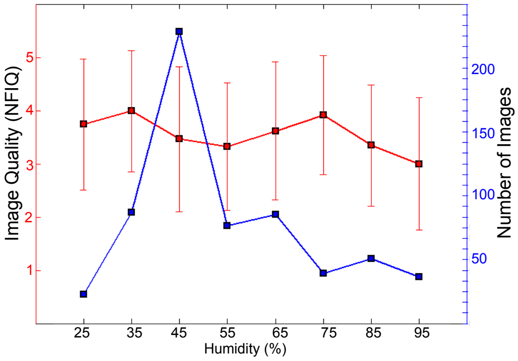

Fig. 9. Average NFIQ (±SE) vs. Humidity (%) for the optical scanner. Each humidity value on the horizontal axis indicates a range of ±5%.

- *How would you describe your understanding of biometrics technology before this study?*
  None (75%). Pretty good familiarity (25%)
- *Did you have any concerns about this project and usage of fingerprints?*
  None.
- *Overall, what did you like about fingerprint access technology?*
  In order of frequency: 1) Ease of use, 2) Not needing keys, 3) Convenient, 4) "Knowing system recognizes me"
- *Overall, what did you dislike about fingerprint access technology?*
  In order of frequency: 1) It doesn't work sometimes, 2) Takes a long time to analyze print and make decision 3) Too hot to use in sunshine in summertime
- *Do you have any other concerns such as for the privacy or security of the system?*
  Most participants had no concerns. One was concerned about identity theft: "What if thieves stole fingerprint system?"

E. Sensor reliability and errors

One key research concern was to identify issues and reliability problems with the fingerprint hardware, most of which were due to the physical environment of the scanners. It is important for an implementation of this type that issues affecting reliability be addressed, since the main area of user dissatisfaction identified in the survey was device unreliability.

During testing several hardware issues were noted:

- *Failed capacitive sensor:* Two capacitive sensor units failed (and were replaced). Both failures occurred on cold winter days (although not colder than the vendor specification (−30 °C). On one unit a short on the circuit board due to condensation was identified, but no obvious electronic problem was identified on the other.
- *Hot surface of capacitive sensor:* In summer the capacitive sensor surface became unusably hot in direct sunlight.
- *Condensation in optical scanner:* condensation was discovered collecting under the scanner lexan optical window. This occurred on a wet snowy January day (Fig. 10). The problem was solved be adding a fan in front of the heating resistors to keep the air circulating in the box.

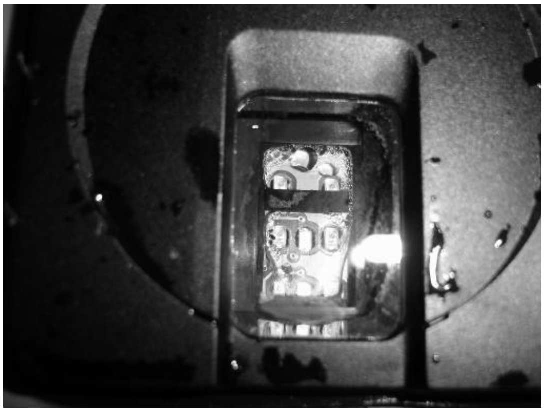

Fig. 10. Condensation build-up under optical scanner window.

- *Capture of "ghost" images* The optical scanner showed several examples of false images. Occasionally, latent fingerprints would become illuminated by the sun shining directly on the scanner unit (Fig. 11). This would be captured by the scanner, resulting in a false accept.

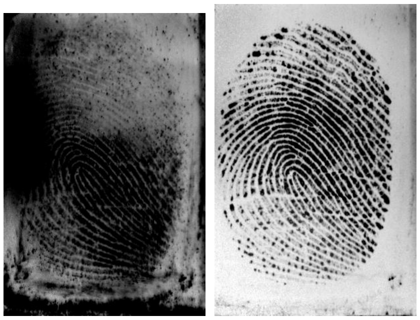

Fig. 11. "Ghost" image (right) caused by direct illumination of a latent print and fingerprint (left) of the previous user.

  A similar issue is the detection of condensation on the optical scanner. In this case, the scanner detects a fingerprint, makes a comparison, and (correctly) rejects the finger. The operational disadvantage, however, is that this results in a large number of reject events being inserted into the biometric log file. An example is shown in Fig. 12
- During the testing, the scanner modules were found to loose their USB connection with the controller computer relatively frequently (approximately weekly and not a function of temperature). The Windows OS used to control the application was, in many cases, not able to reconnect over a USB bus in this state, requiring a reboot.

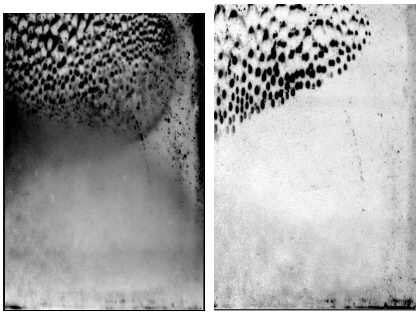

Fig. 12. "Ghost" images caused by rain droplets on the optical scanner. Such images are correctly rejected, but may fill a biometric log file.

V. DISCUSSION

In the current context of heightened concerns with explosives security, there is significant interest in technological controls to improve security. In earlier work, we determined that automatic fingerprint recognition was the best candidate biometric technology for explosives security from an analysis of the requirements: security, usability, ruggedness, size, form factor, privacy, and operational temperature range [4]. One important unknown was the usability and performance of fingerprint technology in rugged outdoors environments, especially in cold weather.

In this paper, we report on tests to determine outdoor and cold weather effects of: 1) chip versus optical fingerprint scanner technology, 2) fingerprint recognition and quality, and 3) user/device interaction. A outdoor fingerprint door access system was designed to capture fingerprint images and video data of user interactions. Using this device, images and video data were captured over a period of two years, and a user survey performed. Data were analyzed in terms of biometric error rates and fingerprint quality (NFIQ) as a function of temperature and humidity. Results suggest:

- biometric performance has no significant dependence on temperature and humidity ($-30\,^\circ$C – $+20\,^\circ$C),
- both chip based and optical fingerprint scanners have flaws in rugged and cold weather applications,
- fingerprint biometric technology has a good level of usability in this application. Users are broadly satisfied with use of this technology. Their key concerns are that it is somewhat slow, and occasionally unreliable. Users need to be assured of the security of their biometric data, based on technological and policy implementations.

REFERENCES

[1] R. Cappelli, D. Maio, D. Maltoni, J.L. Wayman and A.K. Jain, "Performance Evaluation of Fingerprint Verification Systems", IEEE T Pat. Anal. Mach. Intel., 28:3–18, 2006.

[2] International Labour Organization, *ILO Seafarers Identity Documents Biometric Testing Campaign Report Part 1: Technical Report* 2004.

[3] R. Bolle, J. H. Connell, S. Pankanti, N.K. Ratha, A.W. Senior *Guide to Biometrics*, Springer, 2004.

[4] R.F. Stewart, R. Youmaran, A. Adler "Fingerprint Verification for control of Electronic Blast Initiation" Conf. Int. Soc. Explosives Eng., Nashville, TN, USA, Jan. 2007.

[5] South African Patent Office *Improving the Security of the Explosives Supply Chain* Applications 2006/03013 and 2007/03129.

[6] E. Tabassi, C. Wilson, C. Watson, *Fingerprint Image Quality* National Institute of Standards and Technology, Publication, 2004.

[7] J. Wayman, A. Jain, D. Maltoni, D Mario, *Biometric Systems – Technology, Design and Performance Evaluation* Springer-Verlag, London, 2005.

[8] C. Wilson, R.A. Hicklin, H. Korves, B. Ulery, M. Zoepfl, M. Bone, P. Grother, R. Micheals, S. Otto, C. Watson, *Fingerprint Vendor Technology Evaluation 2003* National Institute of Standards and Technology, 2003. `fpvte.nist.gov/report/ir_7123_summary.pdf`

[9] WIPO International Publication WO2006/086844 *Blasting Methods and Apparatus with Reduced Risk of Inadvertent or Illicit Use*.

[10] WIPO International Publication WO2006/086843 *Security Enhanced Blasting Apparatus with Biometric Analyzer and Method of Blasting*.