Conference Report

Focus on New Security Technology
The 39th Carnahan Conference in Spain

Henry Oman
Editor-in-Chief Emeritus

The growing worldwide security threatening environment has motivated nations to develop successful technology for preventing breaches in security. These successes are reported in the annual *Carnahan Conference on Security Technology*, which is conducted by the IEEE Aerospace and Electronic Systems Society, and on alternative years, is held outside of the United States. The 39th Carnahan Conference was hosted by Spain and was held in the city of Las Palmas de Gran Canaria, which is on the island of Gran Canaria in the eastern part of the Atlantic Ocean, off the west coast of Africa.

Engineers from all over the world came to the 39th IEEE-AESS Carnahan International Conference on Security Technology (ICSC) to describe – in 75 papers – the latest technology they developed for solving the new and complex security problems. Their topics ranged from detecting with nanotechnology instruments the prohibited objects being carried by passengers, to protecting stored nuclear weapons. Canary Island provided a pleasant environment and comfortable well-equipped meeting rooms for holding a security conference. The island also had a unique security problem. Illegal immigrants from Africa and Asia are sneaking into the remote shores of Canary Island where they are received by illegal contractors who ship them to Spain for survival on funds supplied by charitable organizations. V. Arana described new techniques for detecting and capturing these immigrants as they approach the shore, hiding between waves [1].

A tour of the south and west shores of Canary Island followed on October 21. Many acres of huge windmills contributed to petroleum conservation by generating electric power from winds that were blowing most of the time. We walked through a huge area that contained many radar dishes and antennas that tracked overhead low-altitude satellites to receive their telecommunication traffic and relay it to stations that were, at the moment, beyond the range of the home stations of these satellites.

TECHNOLOGY MANAGEMENT IN 9-11 WORLD TRADE CENTER ATTACK

The world's security technology has entered a new era as a result of a fast rising rate of population growth and availability of new tools for threatening security. For example, the agents who demolished the World Trade Center towers on September 11, 2001, when entering the US, pretended to need airplane pilot training. Their commander communicated with them in a foreign language by e-mail. A flood of data intercepted September 10 by the US Government's National Security Agency (NSA) had contained two Arabic messages that hinted at a major event to occur the next day. However, these messages were not translated until the next day.

Money for the agents' training, travel, hotel, and living costs, totalling $400,000, and had to be supplied. Commodity importers in the United States pay for their imports with dollars which are credited to firms in the import-supplying nation. Today, we receive – almost everyday – in our e-mail offers of commissions for accepting dollars from foreign entities and delivering them to designated US agencies or persons.

A decade ago, security technology was a need that military and naval forces had to develop to prevent an enemy from succeeding with a "surprise" attack. Then on September11, 2001, the al Qaeda team crashed passenger airplanes into the World Trade Center in New York City, New York, and the Pentagon building in Washington, DC. Financial details were described on pages 95 to 104 in the October 17, 2005 issue of ***Forbes Magazine.*** Also described are the new worldwide intense research and development efforts for effective security technology, and the high-level government organizations creating security-control rules and laws.

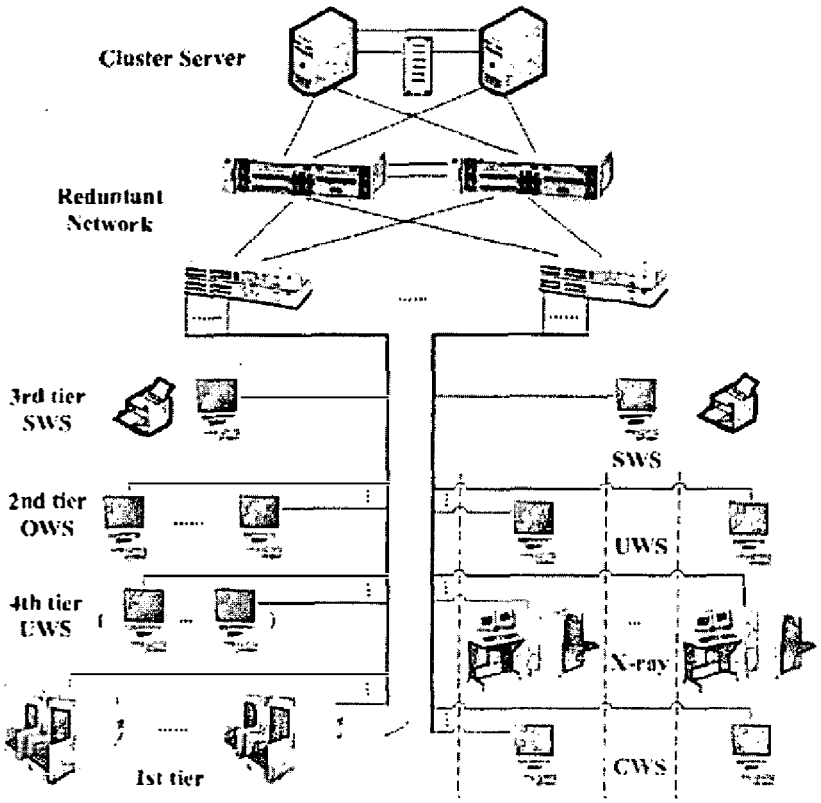

Fig. 1. Baggage at a China airport is x-rayed to produce a contents-image displayed to skilled observers as well as the baggage checker. The left side of the system is for checked baggage, while the right side of the system is for carry-on baggage inspection

SYSTEMS ENGINEERING TERMINATES AIRPLANE HIJACKING IN CHINA

China provided an example of quickly solving a security problem. The first mainland airplane to be hijacked was on its way to Taiwan on May 5, 1983. Another plane was hijacked on May 12, 1988. A hijacked airplane crashed in Baylun Airport in Guangzhou in 1990 and hundreds of people died as a result. A total of 12 airplanes were hijacked between April 6 and June 6, 1994. Then China's government took effective action that ended the hijacking of passenger-carrying airplanes. The success of this technology was described in the paper, *"Review of Security Inspection Networking System Development in China Airports and its Trend in the Future,"* presented by Dong Li at the Carnahan Conference [2].

By 1994, China's government evolved into a system in which a Politburo Standing Committee makes important decisions. Of this committee's eight members: five are electrical or electronic engineers; and the rest are hydraulic, mining, and power engineers. A first step in systems engineering on a development program is to evaluate the alternatives. The team determined that their first step was to find out what techniques other nations were taking to stop airplane hijacking, and how effective these techniques were.

The variation of deaths caused by drunk drivers illustrates the variation of effective achievements by different nations. For example, in a typical month the drunk drivers in the United States kill more people than were killed by the hijacked airplanes that crashed into the World Trade Tower in New York City. In contrast, the annual death rate from drunk-driver-caused accidents is nearly zero in Finland. There the police frequently set up roadblocks where every passing driver must deliver a breath of air into an alcohol sensor. When alcohol vapor is detected, the driver immediately loses his driver's license for a period up to one year and a subsequent offense could cause a lifetime license loss.

At the Carnahan Conference, Li described the systems engineering steps taken in China to end the hijacking of passenger-carrying airplanes in China. At that time the "big sheepfold" of baggage screening had been adopted all over the world. An arriving passenger's hand-carried bags were X-ray screened when the passenger entered the airline's terminal. The passengers then carried their baggage to check-in counters. This "uncontrolled" zone was a large area extending from the rear of the gates to the fronts of the check-in counters. The "uncontrolled" zone needed to be extended to the back of the check-in counter. This was achieved in China with a Flow Renovation of Security Inspection (FRSI), which kept checked baggage from passenger access after inspection. Performance was improved with new X-ray inspection machines, supplemented by explosive detection systems. The Civil Aviation Administration of China developed and quickly deployed the new FRSI system for 100% baggage screening at many airports in China.

Further development in China produced the Multi-tier Management System (MTMS-1) which was successfully installed at the Baiyun airport in Guangzhou, and Taoxian airport in Shenyang in 1995:

- The first tier contains enhanced dual-energy X-ray equipment of single and double tunnel types adapted to check-in counters in islands (Figure 1).
- The second tier is the Operating Workstation (OWS) which is deployed in one or more security-screening rooms.
- The third tier is the Supervisor Workstation (SWS) that provides many management functions such as re-inspection and on-duty performance check.
- The fourth tier is Unpacking Work Station (UWS) that provides, when needed, a centralized hand-search process in the passenger's presence.

At China's biggest airports, like Beijing and Shanghai, the deployed system contains as many as 100 X-ray machines installed behind 200 check-in counters in 8 islands. About 30 operating window systems are deployed during the rush hours of flight. In most circumstances, ten screeners are enough for daily screening work. A cluster server with redundant configurations supports logical control service and data storage service. All systems are based on a local-area network (LAN), which provides a platform for high-speed communication and data transfer.

The first generation of the Multi-Tier Management System (MTMS) developed naturally from checked baggage and screening activity at an airport. The system satisfied the urgent requirement of front-line securing inspection responsible for anti-hijacking, so it was promoted for use at more and more airports in China. The performance and functions of MTMS have been advanced by the development of newer versions of MTMS; for example, operator responses to a random fictional image threat are recorded to evaluate the performance of a single or multiple operators. Analyzing these responses will determine if a single operator needs new training, or if an improvement plan should be developed for future operator training.

Li concluded that the remaining challenge is building a networked security inspection-managed system for all enforcement departments in an airport. Development of the combined-threat machine will reduce their size, weight, and price. Then more combined-threat machines will be deployed because this machine has many advantages such as high detection rate, low false-alarm rate, and the capability to detect all contrabands.

More work is still needed in the broad analysis and deepness processing of all of the information collected. Useful information underneath the raw data could be discovered and used to guide the security inspection process, and could be sent to other enforcement departments for profiling.

One of the two major lessons in the report on the 9-11 attack on the World Trade Towers in New York is that some terrorist information held by intelligence agents had no way of being shared by the security department at the nearest airport. Building a security system network that fulfills all requirements in every aspect coming from the front line of security to counter-terrorism is the "target to approach." This lesson, acquired by blood and life, proves the need.

DETECTING INTRUDERS AT CRITICAL LOCATIONS

Armed guards, who are on duty continuously 24 hours in everyday of the year, are protecting high-value and dangerous assets. However, the guards are costly, and an intruder could accomplish his objective when the guard is napping or has gone to a bathroom. Consequently electronic sensors were developed for sensing an intruder in a prohibited area, and reporting his presence to a human authority. Electronic and photonic sensors are currently used to detect intruders who climb over or cut through fences.

A user who needs to install a detector of a perimeter invasion has many options offered to him. They include the following, which were listed by Douglas Armstrong [3]:

- **Buried systems**: magnetic anomaly, fluid-filled, electromagnetic, fiber optic, microphonic, and seismic.
- **Fence-mounted vibration**, linear (microphonic cable), single point, geophone.
- **Fence-mounted proximity:** electromagnetic, capacitive.
- **Fence-mounted gross attack:** continuity, fiber optic, taut wire.
- **Free-standing fixed line:** microwave fence, active infrared beam, laser beam.
- **Free-standing single ended:** Doppler microwave, passive infrared.
- **Other types of technology:** laser scanning, radar, and video base.

To enable a user to select the perimeter-intruder detector, Armstrong has undertaken evaluation of intruder detection systems against specific customer requirements to determine whether those systems are fit for the specified purpose. This

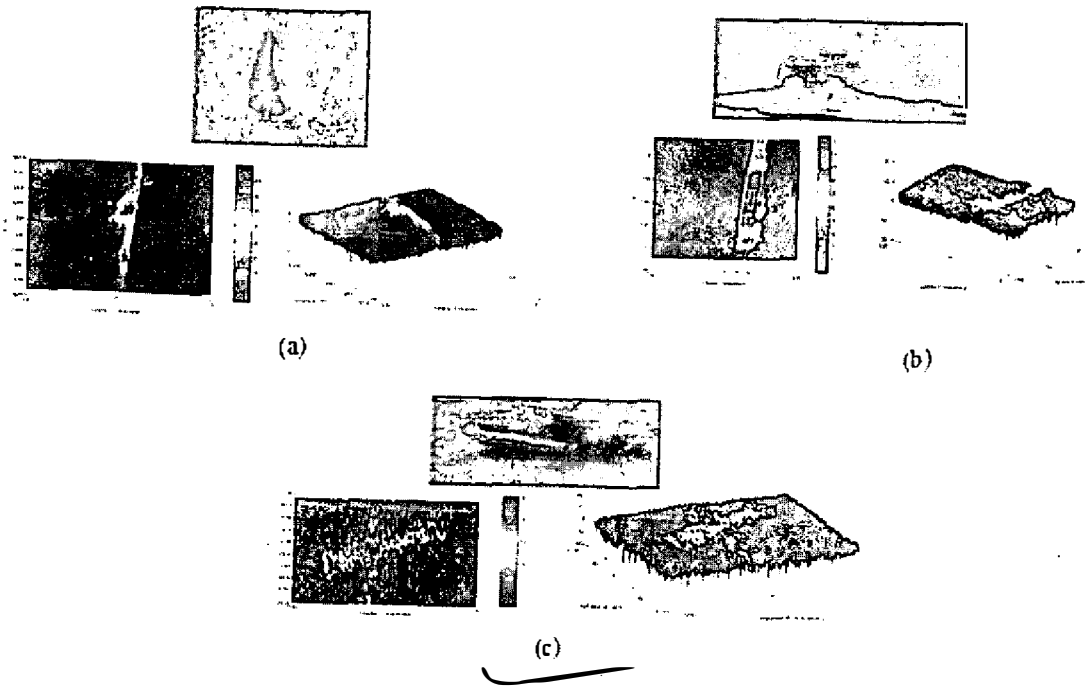

Fig. 2. Photos and Doppler images produced by CWFM radar are shown for three types of vessels:

Fig. 2A. sailing boat; Fig. 2B. ferry; and Fig. 2C. zodiac

project is developing a series of perimeter-intruder-detection system performance standards, with supporting documentation on issues such as specification, installation, commissioning, and maintenance.

SENSING INTRUDERS AT HIGHEST CRITICALITY SITES

Modern sensors can detect an intruder who enters a critical area, provided that the sensor is supplied with operating power. At the 38th Carnahan Conference we toured the Oak Ridge National Laboratory where even nuclear warheads were stored. There, in critical areas, were battery-powered sensors that could detect and report the slightest movement of the critical object being protected. Their latest sensor had such a low power consumption that it could operate for years before its battery wore out!

Banks are establishments where huge sums of money are kept on hand and a depositor can command on the Internet that designated sums from his account be transferred to another account. An eavesdropper could capture the depositor's computer code and extract money from his account. F. Puenti found that this possibility is real, and evaluated alternatives for protecting an account from this kind of theft [4]. They propose a device similar to a pocket calculator that can receive data from the bank's computer, either through the computer screen, USB, or Bluetooth. The device accepts the user's digital signature and passes the signature back to the bank's computer so it can be attached to the transaction data. The main idea is that by signing the data digitally outside of the computer the message cannot be affected by viruses or malicious software.

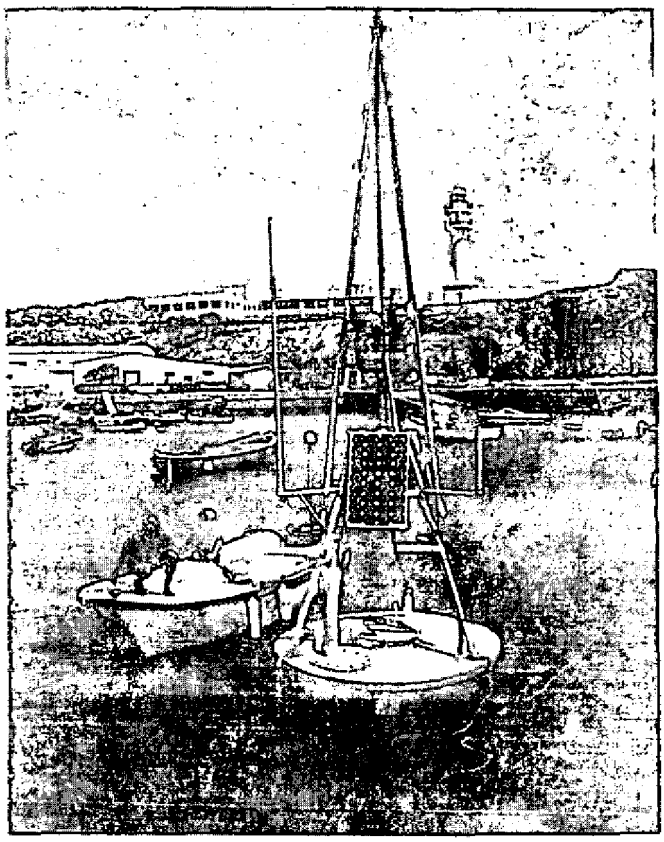

Fig. 3. Two batteries with a charging module, an aerogenerator, and three solar panels power the Oceanographic Buoy which delivers images and data to a coastal network

CONTROLLING IMMIGRANT ENTRY INTO SPAIN

The world's population grows at a rate that could re-populate a metropolis the size of New York City every six weeks. Diminishing resources in Africa and Asia are generating new national and international security problems. An example of a new security problem is the effective delivery of illegal immigrants from Asian and African nations into Spain where they can find low-paying jobs or live off of unemployment payments. These immigrants are carried in the ship to the zone where they can be transferred to small boats for delivery into shallow waters off of the coast of Spain's Gran Canaria Island. They then immigrate through waves to the beach where a local agent gathers them, bypasses local immigration offices, and sends them on to Spain on buses and passenger-carrying ships.

New radar technology and coastal monitoring technology has been developed for detecting this illegal immigration activity. For example, the new Continuous Wave Frequency Modulated (CWFM) radar, that was described by Christina Duarte, presents some interesting advantages for immigration control and coast surveillance [5]. It achieves low probability of interception, high resolution, and does not present "blind spots." In this application optics and infrared sensors are frequently used, but they can be disabled by haze and fog. Such atmospheric conditions reduce the CWFM radar's range, but the system continues to operate.

The CWFM radars, which are simpler and cost less than pulse radars, do not present "blind spot" limitations because simultaneous transmission and reception exist continuously. The transmitted bandwidth uses a low sample frequency, and the radar has a low probability of interception. The radar transmits in the 28-29 GHz band, with a bandwidth of 2 GHz, which gives a 0.075 meter resolution. A Doppler processor produces moving images displays, as shown in Figure 2, for the observer who can identify the type of ship being scanned.

ACOMAR BUOY GATHERS OFF-SHORE DATA

A new tool for surveillance of offshore activity is a buoy that has been developed to deliver data to the ACOMAR RED network. European agencies need this data for solving many problems in areas such as sea security, sailing, water quality management, hydrocarbon and natural gas production, and management of life in sea resources. The meteorological data delivered by the buoy include wind speed and direction, air temperature and humidity, solar radiation, and atmospheric pressure. Oceanographic data delivered by the buoy include the water's temperature, conductivity, dissolved oxygen, pH, turbidity, chlorophyll and hydrocarbon content, water-flow direction and speed, and wave activity.

V. Arana described the current status of the ACOMAR RED network and the buoy that gathers and delivers needed data [6]. Power for operating the anchored off-shore ACOMAR buoy could not be reliably delivered by an on-shore utility because storm waves could break the buoy's power-supplying cable. Therefore, a battery in an isolated container powers the buoy's radar and other sensors, as well as its transceiver. A solar panel keeps the battery charged (Figure 3).

BIOMETRIC IDENTIFICATION OF PERSONS PROGRESSES

Criminals that enter into US prisons are fingerprinted so they can be subsequently identified positively. Once, the kidnapper of Lindberg's baby was identified from fingerprints, and he was executed. Consequently people in the United States, associate fingerprints with criminals, and they object to the use of their fingerprints for controlling the entry into their workplaces or other areas where entry is controlled, mostly by guards. Entry-control failures have been attributed to inattentive guards.

Progress in other nations on fingerprint identification-accuracy was reported at the 39th Carnahan Conference. For example, J. Fierrez-Aguilar compared two options that a computer could be commanded to use in searching recorded fingerprints for the contributor of a sample fingerprint that is offered. One approach was to compare minute details of the prints. The better technique is to fill in missing segments in the lines of the offered fingerprint, and then use the line shapes and positions in the search for the recorded fingerprint that matches [7].

HAND GEOMETRY FOR ADMITTANCE TO PURDUE RECREATIONAL SPORTS CENTER

The need in the United States for alternatives to fingerprints for accurately identifying persons has motivated testing of alternatives at Purdue University. To enter Purdue University's Recreational Sports Center, a student has to display his identification card. Eric Kukula reported the results of a test in which hand geometry replaced the identification card for admission to the Center [8]. Initially, 453 participants were surveyed to determine their usage of the Center and thoughts about the current access control system. The results indicated that 55% of the participants thought that fingerprint recognition was the least intrusive, followed by hand geometry (36%), eye iris and retinal imaging (7%), and face imaging (6%).

The Handkey II was tested as a hand geometry replacement for identification cards. Participants were trained with a 5 to10 minute briefing that included the purpose of the project, a technology overview, a hand placement tutorial, and instructions on specific enrollment and procedures to follow. Kukula described in detail the problems that needed to be solved to get the hand-geometry system working. He reported that an analysis of the survey revealed that 93% liked using hand geometry, 98% thought that it was easy to use, and 87% preferred it to the existing card-based system. System performance achieved a three-try match rate of 99.02% when "gaming" and potential imposter attempts were removed from the analysis. The failure-to-enroll rate was zero.

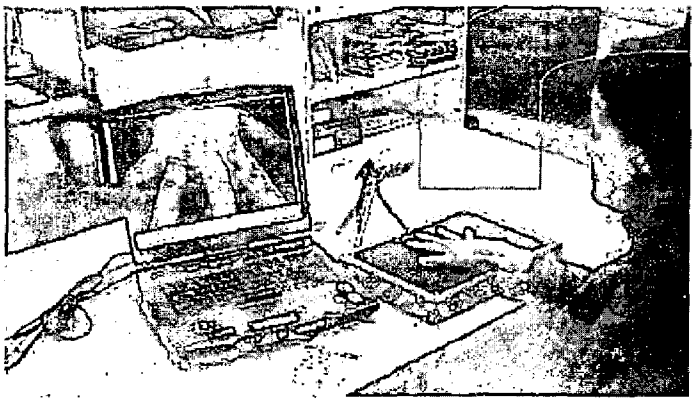

Fig. 4. This hand imager produces a repeatable photograph of a hand that is placed on a base on which pins that guide the position of the hand's fingers

USING HAND AND KNUCKLE TEXTURE FOR BIOMETRIC IDENTIFICATION

Hand geometric systems use an optical camera to capture two-dimension images of the palm and sides of the hand, offering a balance of reliability and ease of use. They typically collect more than 90 dimensional measurements, including: 1) finger width, height, and length; 2) distances between joints; and 3) knuckle shapes. Although the basic shape and size of an individual's hand remains relatively stable, the shape and size of our hands are not highly distinctive. The system is not well-suited for performing one-to-many identification matches.

Hand geometry readers can function in extreme temperatures and are not impacted by dirty hands, as fingerprint sensors can be. Hand geometry devices are able to withstand wide changes in temperature and function in dusty environments. They are commonly used for access to control facilities, time clocks, and controlled areas. The Columbia Legislature uses a hand-based system to confirm voting members prior to conducting votes. The US Immigration and Naturalization Service uses a similar system to verify the identity of travelers at border crossings. The University of Georgia uses hand-based systems to restrict cafeteria access to students enrolled in the university's meal plan. These systems are also used in a number of workplaces to keep track of employee time and attendance.

For an alternative to taking hand and finger measurements along fixed axes, as in hand geometry-based systems, researchers have investigated using the contour of the hand's silhouette as a biometric feature. This system captures the hand image and removable platen from the known position. Next, the hand contour was extracted from the hand image using a mean-shift unsupervised segmentation. The five pairs of fingers to be compared were extracted from the contours and aligned separately.

Hand-palm-based authentication systems have also been proposed. This system acquires the hand-palm image by

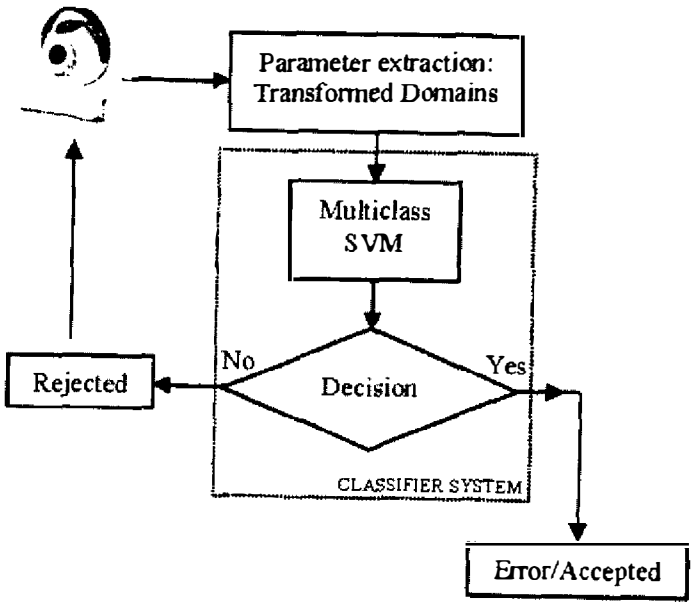

Fig. 5. The Olivetti Research Laboratory has developed a face scanning and biometric processing system which produced a false-acceptance rate of 0% and a success rate of 90.2% in face identification

extracting and normalizing from a binarized image the hand-palm region of interest. This image contains the rectangular section of the palm whose corners are the base of the little finger, the base of the index finger, the base of the thumb, and the fourth corner, to complete the parallelogram.

A drawback of these hand-based systems is that the hand must be pressed on glass to acquire the hand palm image. During image acquisition the glass gets dirtier as each hand is scanned. The dirt can absorb illumination, making the resulting images difficult to correlate with recorded images. Thus the time duration between required glass-cleanings can vary.

Miguel A. Ferrer described the Sony DSC-8P sensor that captures a hand's image in a 2048 by 1536 24-bit color intensity image in JAPEG format [9]. The sensor is positioned about 12 cm (4.68 inch) above a board that has been covered with a black piece of cardboard that contains three pegs. The subject is instructed to place his or her right hand flat against the table with the first peg between the index and hart finger, the index finger pointing toward the second peg, the hart finger pointing toward the third peg, and the rest of the fingers naturally spread. The image is captured by focusing the sensor on the knuckle of the hart finger (Figure 4). The subject is then instructed to remove his or her hand from the board and then return it to the same position. In this preliminary work, 160 images were collected from 20 subjects.

The images were preprocessed using MATLAB programming code, and classified with a hidden Markov model and a support vector machine, just to compare the performance of both systems. The performances of both systems are similar, and their error rate is around 0.094.

EAR CONTOUR, A POTENTIAL BIOMETRIC IDENTIFICATION TOOL

Although the ear is a newcomer in the biometrics field, ears have long been used as a means of human identification in the forensic field. Traditional and manual methods of describing ear features and identification have been developed for more than 14 years. Just like fingerprints, the history of the use of ear shapes and marks suggests their use for automatic human identification. At the 39th Annual Carnahan International Conference, Lui Alvrez described the potential of ear contours for identification in the security environment, and showed a mathematical model of these contours that his team developed [10].

Every person's ear has a unique shape and dimensions that differ from those of the ears of everyone else. This uniqueness differs from the unique line-shapes in fingerprints, which can be easily compared with those stored in files. However, optic-electronic tools and mathematical processes are now available for developing equations that clearly define the features of a given ear in terms that can be stored in computer memory, and compared with data from other recorded identified ears. Furthermore, a person's ear can be scanned without touching the person.

Alvarez defined the method for establishing the contour of the edges of an ear in its image, and then establishing an identifiable point from which lines of reflected-light scans can radiate. A mathematically-described ovoid image can then be defined and quantified in terms of reflected light at points on the lines radiating from the point. He pointed out that the proposed technique to estimate the ear contour and ovoid is the first step in ear analysis. In his next step, he will test a new technique in an ear-image database in order to evaluate the performance of methods for ear identification.

STRATEGY FOR IMPROVING THE RELIABILITY OF FACIAL IDENTIFICATION

Carlos M. Travieso cited reasons why face recognition is a latent field in which much research and commercial development is going into improving the product [11]. Objectives include the guaranteeing of security in precincts and following the movement of people. He cited the great number of scientific papers that show facial identification is a wide-open field in constant evolution. Continued improvements are motivated by the increasing requirements of security in our society. He described simple, robust, and novel errors – detection features which can be applied to the Olivetti Research Laboratory (ORL) Face Database that stores 400 images (Figure 5).

Travieso cited the capability of being retrained as an important aspect inside a system of facial recognition. Biometric characteristics of people change with time, and the biometrics of the face are no exception. Therefore we have to re-train the system so that it adapts to these changes. The redesigned system must detect when the face of a person is who he says he is. In case of doubt it must ask for a new face image, or reject the proposed identification. The key to evaluating a rejection is determining the significance of the cause for rejection. It could be a simple thing like a wart or pimple on one place on the skin. This cause for rejection could be delivered to a higher authority. On the other hand, a wrong-face overall configuration would cause reject.

Travieso cited the greatest success rate that could be achieved with their biorthogonal spline wavelet family. This simple and robust facial identification system achieved a false identification rate of 0% and a success rate of 90.8%. Thus, the false rejection rate was 9.2%.

POPULATION LIMITED FACE RECOGNITION

The ability to find and accurately distinguish one person's face from a computer memory containing recordings of all human faces in the world is not yet possible with today's technology. For example, the measured distances between points on a face change as a person smiles or frowns. The iris diameter changes after a person enters a darkened booth from a brightly lit room. The skin color darkens when sunshine tans a person in the summer. A huge data-storage facility would be required for storing all possible expressions in every face of a large population of stored face images. Josep Roure described the significance of these factors with an easily understandable example [12]. The limits were illustrated by his method that accurately identified faces in a group of 40 people, but would make too many errors in a data base of 1000 people.

40th ANNUAL IEEE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY

On October 16-20, 2006, the 40th Annual IEEE International Carnahan Conference on Security Technology will be held at the Radisson Plaza Hotel in Lexington, Kentucky – the city where the Carnahan Conferences began.

Forty years ago, after US President Johnson declared "War on Crime," Professor Robert Cosgriff thought that electrical countermeasures could help this program. He invited local police officials to discuss this possibility with members of his staff. Their meeting, held in the Carnahan House of his University of Kentucky, was so successful that they decided to meet periodically. This started the *"Carnahan Conference,"* which grew to a national Carnahan Conference on Security Technology, and today is the IEEE International Carnahan Conference on Security Technology.

Authors of proposed papers for the 40th Carnahan Conference are invited to submit abstracts to the conference's Organizing Committee at: International Carnahan Conference on Security Technology, PO Box 8294, Lexington, KY 40533-8295, USA.

REFERENCES

[1] Arana, V., Cabrera, F., Dorta, P., Jimenez, E., Villar, I., Deniz, A., Miranda, A., Beres, J., Holgado, E. and Rodriguez, R.,

Experimental Network of Marine Environmental Observation, Surveillance and Control in the Canary Islands Waters (RED ACOMAR), pp. 230-233.

[2] Li, Dong and Chen, Huimin, Review of Security Inspection Networking System Development in China Airports and its Trend in the Future (First Research Ministry of Public Security in China), pp. 178-181.

[3] Armstrong, Douglas and Peile, Carinna, Perimeter Intruder Detection Systems Performance Standard, Home Office Scientific Development Branch, United Kingdom, pp. 33-36.

[4] Puenti, F., Sandoval, J.D., Hernandez, P. and Molina, C.J., Improving On-Line Banking Security with Hardware Devices, pp. 174-177.

[5] Duarte, Cristina Carmona, Naranjo, B. Pablo Dorta; Lopez, Alberto Asensio and del Campo, Alvaro Blanco, High Resolution CWLFM Radar for Vessel Detection and Identification for Maritime Border Security, pp. 304-307.

[6] Arana, V. and Associates, Experimental Network of Marine Environment Observation, Surveillance, and Control in the Canoary Islands Waters (RED ACOMAR), pp. 230-233.

[7] Aguilar, J. Ferrez and Associates, On the Effect of Image Quality Degradation on Minutiae and Ridge-Based Automatic Fingerprint Recognition, pp. 79-82.

[8] Kukula, Eric and Elliott, Stephen, Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance, pp. 83-88.

[9] Ferrer, Miguel A., Travieso, Carlos M. and Alonso, Jesus B., Using Hand Knuckle Texture for Biometric Identification, pp. 74-78.

[10] Alvarez, Luis, Gonzalez, Esther and Mazorra, Luis, Fitting Ear Contour using an Ovoid Model, pp. 145-148.

[11] Travieso, Carlos M., Alonso, Jesus B. and Ferrer, Miguel A., Strategy for Improving the Reliability in the Facial Identification, pp. 149-152, (Dpto. De Senales y Communicaciones, Universidad de Las Palmas d Gran Canaria).

[12] Roure, Josep and Faundez-Zanuy, Marcos, Face Recognition with Small and Large Size Databases, pp. 153-156.