NASIOROWSKA, B. Improving safety and security in platinum mining by utilizing the newest facial recognition technology. *The 4th International Platinum Conference, Platinum in transition 'Boom or Bust',* The Southern African Institute of Mining and Metallurgy, 2010.

Improving safety and security in platinum mining by utilizing the newest facial recognition technology

B. NASIOROWSKA
Interoptic Networks CC

The theft of platinum, gold or diamonds poses a substantial threat to the economy of any country where the above industry exists. Mines provide employment for local and migrant workers and it is their employees that hav against illegal miners and product theft. Additionally, the safety of genuine mine employees is at risk as they are exposed to threat and corruption from the illegal miners. The most successful access control system existing in one of the South African gold mines has introduced a facial recognition system that has been used since 2001 to verify mine employees. Currently the mine group has implemented the facial recognition system employed by the mine. This technologically advanced solution has helped to deny access to non face features of the person at the access point. Face2Face Access takes an image of a person, evaluates his characteristic features and sends information into its database. An employee only has to look into the 'mirror' at the access point to be allowed into the premises. A name is connected to the individual's face.

Theis paper will analyze different biometric technologies and their suitability to be implemented at different mines.

Introduction

The theft of platinum, gold or diamonds poses a substantial threat to the economy of any country where the mining of beneficiation industry exist. Mines provide employment for local and migrant workers and it is their employees that have to be protected against illegal miners and product theft. Additionally, the safety of genuine mine employees is at risk as they are exposed to threat and corruption from the illegal miners.

Currently used security precautions and measures include: access control systems with cards (proximity or barcode) for time and attendance, physical security guards, CCTV solutions, metal detectors. The above security measures still allow unauthorized access; therefore, new technological systems have to be introduced.

The implementation of biometric technologies in the mining industry has been taking place over the last ten or more years in South Africa. There has been continuous search for the 'perfect' biometric system to fulfil the stringent requirements and challenges of the mines. Systems such as hand geometry, fingerprint, iris and facial recognition provided varied results.

In the international markets where focus is on the governments' requirements to control borders and prevent international terrorism, three biometric modalities have been identified as the preferred biometric solutions. Facial recognition came up as the ICAO/ISO standard for passport applications and fingerprint and iris recognition as the additional biometric solution that governments can utilize. Therefore all efforts in the international markets have been directed towards standards development and improvement of these technologies.

The question remains: could the above choices also be the most suitable for the mining industry? All biometric modalities have specific qualities that make them special but at the same time there exist certain elements that are not suitable for implementation in the very specific mining environment.

It is imperative to choose the best possible biometric technology for the application needed to analyse the strengths and weaknesses of a particular modality.

Biometric technologies strengths and weaknesses

Table I highlights the main commonly identified properties of the three major biometric technologies.

Facial scan–how does it work?

The facial scan technology process consists of the following steps:

- Image acquisition
- Image processing
- Distinctive characteristic location
- Template creation
- Matching.

Image acquisition

A facial image can be acquired ideally through a highest quality camera. Best results for verification 1:1 and identification 1:N can be achieved when users can stand at a fixed distance from a camera with fixed lighting and the same background.

Table I
Biometric technologies strengths and weaknesses

	Strengths	Weaknesses
Fingerprint recognition	**Capable of high levels of accuracy** Fingerprint recognized as a distinctive identifier **Ergonomic, easy-to-use devices** Placement of finger is an easy process **Ability to enrol multiple fingers** 10 fingers' scan provides more information **Range of deployment environments** Small devices Variety of solutions for logical and physical access control	**It is not an ideal solution for every situation** **Inability to enrol some users** Manual labourers, elderly population, certain ethnic and demographic groups, children **Performance deterioration over time** Some systems' error rates have gone from non-existent to 25% over 6 weeks because of daily wear **Association with forensic applications** General public association with criminal fingerprinting **Need to deploy specialized devices** Fingerscan devices must be at a protected location **Physical contact required** Users are concerned about germs
Facial recognition	**Ability to leverage existing equipment** Mostly software-based technology capable of using existing high quality CCTV cameras and photo ID systems **Ability to enrol static images** In large-scale facial-scan deployments there is an existing database of facial images Surveillance applications need only one **Ability to operate without physical contact** The only biometric solution capable of identification without subject co-operation	**Acquisition environment effect on matching accuracy** Direct lighting, camera position and quality can reduce accuracy **Changes in physiological characteristics that reduce matching accuracy** Changes in appearance might have an impact on some systems that are not robust. Eyeglasses, hats and scarves can cause users to be falsely rejected in some systems
Iris recognition	**Resistance to false matching** Potential for high level of accuracy **Stability of characteristic over time** Iris does not change over a person's lifetime	**Difficulty of usage** Enrolment and verification require fairly precise positioning of the head and eyes. **False rejection failure to enrol** A percentage of users are unable to enroll in iris scan systems because they cannot provide adequate enrolment images. **User discomfort with eye-based technology** Concern that exposure to the technology may damage eyesight

Robust facial recognition systems can handle deviations from the norm but surveillance is still a worst-case scenario as images are acquired from non-cooperating subjects at different angles and on the move.

Locating the face within the frame is the first task of a system by sensing multiple cues such as:

- Motion
- Facial or head shape
- Skin colour
- Facial features such as two eyes.

Image processing

After acquisition images are cropped and normalized but are usually converted to black and white, so that initial comparison based on grayscale characteristics can be done. Normalization of images allows for similar size and variations in orientation and distance to be overcome. Eyes are located and the facial image can be related to straighten it along the horizontal axis. Rapid image processing is essential to the system operation.

Template creation

Enrolment templates cannot be used to recreate original images and are created from multiple processed facial images.

Template matching

Match templates are compared against enrolment templates using proprietary methods. The match result depends on the score level assigned. If the score surpasses a predefined level, then the comparison of the templates is a match. In a 1:1 verification the system is attempting to verify if the person is the person he/she claims to be. A rejection in a facial scan system is often defined as a failure to match.

A 1:N identification will require a high number of match attempts and the best performing facial recognition systems can handle tens of thousands of identification comparison per second.

Facial-scan technologies—feature attraction

Various facial scan systems are suitable for different applications, such as access control, surveillance or

forensics. The most popular methods used by leading facial-scan vendors are Eigenface, Principle Components Analysis (PCA), Linear Discrimination Analysis (LDA) and Elastic Bunch Graph Matching (EBGM).

Principle components analysis (PCA)

A facial image is created by overlaying 'Eigenfaces' (two dimensional grayscale faces) on the raw data like filters. See Figure 1. A full frontal image of a face is required and any change in a simple facial feature requires recomputation of the Eigenface components.

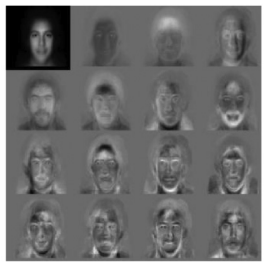

Figure 1. Eigenfaces

Linear discrimination analysis (LDA)

The LDA requires a large database and a frontal image. It discounts differences in lighting and facial expression. Pixel values in a face scan are calculated, distributed and plotted. Linear relationships between variations that occur between individual A and individual B raw data are analysed. The 'Fisherface' is generated. See Figure 2.

Figure 2. Fisherface. (Source: Peter N. Belhumeur *et al*. 'Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection.' *IEEE Transactions on Pattern Analysis and Machine Intelligenc*e, July 1997)

Elastic bunch graph matching (EBGM)

EBGM addresses non-linear aspects of the face, such as illumination shadows, pose angle and expression. As a result, a facial graph is created. EBGM can handle images that are not full frontal. See Figure 3.

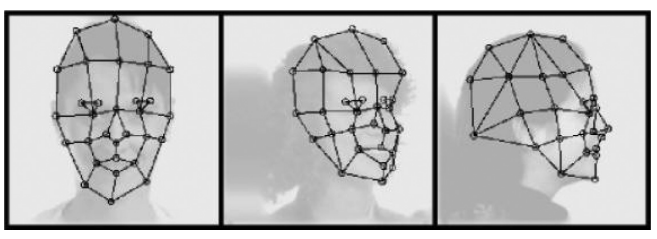

Figure 3. Elastic bunch graph matching. (Source: National Science and Technology Council, 'Biometric Foundation Documents.')

What is the best biometric technology for access control in the mining environment? A South African example

One of the gold mine groups in South Africa had an innovative approach already ten years ago to find a solution for access control with a view to improving safety and security at their premises.

Access control systems utilize tokens, such as cards, with additional CCTV cameras and security guards. All of the above mentioned measures will not be enough to prevent unauthorized access because the above systems do not identify or verify individuals, but rather use PIN numbers (of the cards) or rely on decisions made by humans that are not reliable or are open to collusion.

A stringent analysis of possible implementation of fingerprint, iris and facial recognition provided thorough understanding of what can be expected from the performance of the available solutions.

After a thorough investigation and based on hands-on experience of other installations of hand geometry, fingerprint and iris recognition, the final verdict on what is the best biometric technology in the mining industry turned out to be facial recognition.

Facial recognition access control system—Why?

- It is very accurate with very fast throughput of hundreds of persons (the station camera takes a picture of the person requiring access, and the image is recognized within 0.3 seconds)
- It is easy to use, nonintrusive and friendly as miners only have to look at their own reflection in the mirror where the camera works in the background.
- No contact is required to acquire biometric features (fingerprint is not suitable due to dust on fingers and cuts, and possible germ contamination due to touching the finger scanner)
- Reliability and scalability
- No possibility of clocking fraud
- Log file generated from attempts of deception (time and date stamped).
- Audit report on individuals with live face verification proof
- A name is connected to the individual's face.

The above facial recognition system was chosen and has been used since 2001 to verify mine employees at the gold plants. Currently, the mining group has implemented the facial recognition system at the shafts and bank areas in order to verify all miners employed. The system has around

Figure 4. Facial recognition access control system used in gold mines in South Africa

20 000 employees in the database and on a daily basis there are around 15 000 miners using the facial recognition access control system.

Facial recognition systems can be utilized to automatically verify persons without an opportunity for collusion. The facial recognition access control system installed in this particular gold mine helped to alert the security personnel when two different faces appeared with the same name.

The question posed was: Has the identity been stolen from a genuine employee and was an imposter trying to gain access with the other person's access card? Or are there two different individuals with the same name? In this case, the facial recognition system helped alert the management of the gold mine to a possible identity theft and the individuals in question could be further investigated by means of proof of identity. If a fingerprint system were used in the above case, security management could have assumed it was a duplicate enrolment of a person as the human eye cannot tell fingerprints apart once they become a template.

There is another example which proves why facial recognition rather than fingerprint, iris, etc. is a better choice in a case of two persons who look alike. A continuous study conducted by Interoptic Networks, concerning faces of twin children to test facial recognition systems in real life applications, provided results which prove that a high threshold assigned to a facial recognition system for acceptance or rejection will guarantee correct differentiation between twins and lookalikes.

Automated biometric facial recognition systems can replace tokens or work with tokens that provide access to doors, gates, turnstiles and other entrances. The above can work as a stand-alone or a networked system. Networked solutions can be used in larger applications such as controlling access to multiple buildings with multiple doors used by a large number of people.

The future of biometric facial recognition systems in the mining industry

Different types of facial recognition systems can be implemented in the mining environment, not only for access control. Surveillance is one such. Also, facial recognition systems can be deployed in a variety of forms, e.g. mobile hand-held units, cell phone applications with facial verification capabilities, as well as suitcase size mobile systems.

Mobile ID devices have been deployed for a variety of non-stationary applications where access to traditional implementation of full-sized live scan fingerprint readers and photo capture stations with set-ups adhering to standards are not possible. Facial recognition is a new addition to the above mobile devices and 'mug shots' for comparison with reference databases are most common

There is a great need to do 'spot checks' of individuals present on the mining premises in order to identify them and check whether they are employees, subcontractors or visitors allowed to access the premises. Therefore implementation of new mobile ID devices with facial recognition would be most beneficial.

New biometric facial recognition technology has raised the scope and effectiveness of surveillance and the human ability to recognize a person. Covert surveillance can now be carried out. Placing a biometric facial recognition system at the entrances where they can be easily seen may be designed to prevent access of unwanted persons. Covert surveillance with facial recognition allows for spotting faces of criminals or suspects by automatic comparison of live faces to a database of wanted individuals. Security personnel are alerted by being made aware of faces that are similar to reference images of suspects or wanted or banned individuals.

There is continuous improvement and innovation of facial recognition systems. One of the questions that comes up regularly is, whether a facial recognition solution can verify a face over a long period of time, e.g. over a period of 5 to 10 years.

A South African example of testing biometric facial recognition systems–Interoptic Networks facial recognition twins project

In September 2004, Interoptic Networks launched a biometric facial recognition project that would involve the study of the faces of twin children. The aim was also to be able to use the results of this study for software development in the area of facial scan technology. One of the goals is to see if a computerized facial recognition system could successfully distinguish between the twins themselves at the time of using the system as well as over a period of 5 years as they aged.

This project is a world first and promises to provide valuable information that will help improve facial recognition software systems worldwide as well as assist future users in assessing existing products.

In addition, the project aims to focus on gathering images of the children's faces for analysis of anthropological landmarks, dimensions and angles to quantify facial characteristics and proportions. Annual results are compared providing information on how the computerized system is coping with physical changes of twin children's faces.

The approach was taken to obtain photographs of different sets of twin children located in South Africa over a minimum period of five years, with an extension to ten years, as well as to conduct live operational testing of facial recognition products once a year.

This face database has the following properties:

- Twin siblings
- Ageing
- Varying ethnicity.

These aspects are critical when analysing the quality of face recognition products as they deal with three of the most concerning issues surrounding face recognition.

Before face recognition was ready for industrial application, the issue of varying ethnicities was the major concern for researchers and developers. This problem has since been solved, and skin tone no longer plays a role in the success rate of recognition algorithms, including those which make use of visible light only. However, a face database of ethnic twin children was not available.

Since the maturity of face recognition technology, two new concerns have been raised. For the general public, ageing in face recognition systems is an issue and a critical measuring stick for the evaluation of face recognition systems. Despite the prevalence of face databases available, none include sufficient ageing and none include the ageing of young children.

The issue of twins originated due to security concerns, for example at a bank where there might be twin siblings making use of the same branch.

There is a continuous need in all industries and criminal

justice systems around the world to find facial recognition solutions that would distinguish look alike persons. Therefore an automated facial recognition system can play a huge role in verifying/identifying persons that look the same to the human eye. A famous case occurred as far back as 1901 in the USA where two unrelated men with similar names who were in the same prison had almost identical facial features.

Testing results

Two separate types of testing were performed, a static image-to-image facial recognition system and a live facial surveillance system recognition system.

Static image-to-image test

Some general observations can be shared in this paper (it is not this paper's main objective to provide detailed results of the Interoptic Networks Twins Project).

Various tests were conducted using the twins database as a reference, simulating real life scenarios.

- General ageing: images from 2005 used to probe a database trained with images from 2004
- New reference images with old probe images: images from 2005 used to probe a database trained with images from 2006
- Duplicate analysis: determining whether or not the systems can differentiate between the twin siblings.

Research and analysis

General observations

The images were received in different resolutions. The images from 2004 were 640 × 480, while the images from 2005 and 2006 were in much more detailed (3072 × 2304). The images from 2005 and 2006 were thus resized to 640 × 480, to ensure an accurate test.

During the testing, the program responded almost immediately when doing enrolments and recognitions. Thus, there is no timing information in the results. See Table II.

- Number of images: the number of images from each year. '20' indicates a full complement of images.
- Dimensions: the resolution of that year's images, in pixels.
- Average size of file: average memory occupation of each image file in the corresponding year.

When testing facial recognition, the issue of background noise is critical. Consistency of image colour and quality should be relatively similar throughout databases (this cannot always be the case, but when photographs are taken in controlled conditions, it should be possible). Table III shows a breakdown of the quality of images used in the twin database.

From Table III it is clear that the images captured in 2005 are most suitable for recognition purposes, whereas the images from 2006 are of sufficient quality to be used in such tests. However, the images from 2004 are problematic, with inconsistent lighting throughout and a wrinkled background. The fact that these images are less suitable for this type of a test is confirmed in the results throughout.

Table II
General observations

Year	Number of Images	Dimensions (in pixels)	Average size of file
2004	20	640 × 480	140 kB
2005	20	640 × 480	170 kB
2006	18	640 × 480	167 kB

Live facial recognition surveillance test

In the live test with a facial recognition surveillance system used for a 5-year period the following observations were noted:

The faces of the twin children were distinguished from year to year in all cases where lighting conditions were similar. The hairstyle, weight gain, and change in facial appearance due to growth had no impact on the positive results of distinguishing the twins. Only when striking sunlight was introduced during testing did it cause certain identification discrepancy in some of the twin sets.

The live facial surveillance system tested works utilizing a highly successful matching algorithm. It was the leading system at the time and one of the first commercially available, and was incorporated in a computerized system. The conclusion after the first 5 years of testing was that this particular system was robust enough to be used in real-life applications and that it outperforms the human ability to immediately tell apart lookalike persons.

During consecutive tests, the operator of the facial recognition system could not distinguish the children, therefore name tags were introduced to be worn during the testing period.

This again proves that the computerized system was more efficient in conducting the above experiment.

Facial recognition for e-Passport, e-Visa and ID document applications

Facial recognition is a chosen biometric technology for e-Passport and e-Visa applications. Currently, it is also being introduced in national ID schemes, as well as border control watch-list surveillance systems all over the world. The mining industry can easily adopt the recommended biometric technology for capturing and producing of ID cards by the respective companies HR departments.

ISO/IEC biometric standards provide guidelines for face image capturing as well as face image quality. Additionally, ICAO (International Civil Aviation Organization) specifies guidelines on how photographs should be taken for travel document purposes. Some recommendations by ISO/IEC and ICAO on how to take photographs for e-Passports, e-Visas or ID Documents are mentioned below:

Table III
Image quality and background noise

Year	Colour consistency	Background colour	Texture
2004	Inconsistent: brown lighting and blue lighting	Grey (9/20) brown (11/20)	Plain, wrinkled
2005	Consistent	Grey	Plain
2006	Consistent	Grey	Plain, wrinkled

Full frontal facial image

This type of a facial image type includes the full head with all hair in most cases, as well as the neck and the shoulders. This type is suitable for storage of the facial information and is applicable to portraits for passports, drivers licenses and 'mugshot images'.

Token facial image

A facial image type specifies frontal images with a specific geometric size and eye positioning based on the width and height of the image. This image is suitable for minimizing the storage requirements for computer face recognition tasks, such as verification, while still offering vendor independence and human verification capabilities.

Factors that affect the facial recognition system's performance are categorized as concerning the Environment and the user (subject). In the acquisition and capture process of a face, elements such as variation of lighting and extreme or weak illuminations, as well as camera characteristics (sensor resolution), play a role in performance. Current facial recognition standards for e-Passports allow for limited facial expressions and behaviour such as closed eyes and subject position.

In the analysis of the facial image quality, different aspects have to be considered. The most obvious are:

- The size of the image and its resolution
- Image exposure and noise
- Lighting or background
- The behaviour of the person (subject) whose photo is being taken.

Image resolution and size

For the full frontal image type, the recommended standard (ISO/IEC) is 180 pixels of resolution of the width of the head or roughly 90 pixels from the eye to the centre of the face.

Image exposure or noise

Different processes that are required in producing a digital image contribute to noise in facial images. Noise can be generated by the CCD sensor of a camera, an image scanning device or an image compression algorithm (e.g. JPEG).

Lighting and background

The best results to enhance machine-assisted face recognition performance are achieved when photographs are taken against a background of gray, plain, smooth surface. No unnatural colour should be introduced. Grayscale photographs should be produced from common incandescent light sources. Colour balancing techniques should be used for colour photographs (high colour-temperature flask with standard film or tungsten-balanced film with incandescent lighting).

The behaviour of the person (subject)

Examples of characteristics related to the person's behaviour include the following:

- Behaviour of eyes, e.g. closed eyes
- Closed or open mouth
- Any kind of expression, e.g. smiling or neutral
- Head pose, e.g. frontal or rotated in any direction.

Best practices for use of full frontal image on travel documents ISO/IEC biometric data format

Face image data

Photographic Quality requirements:

- Close-up of your head and shoulders so that your face takes up 70–80% of the photograph
- In sharp focus and clear
- Show you are looking directly into the camera
- Show your natural skin tones
- Have appropriate brightness and contrast.

See Figure 5.

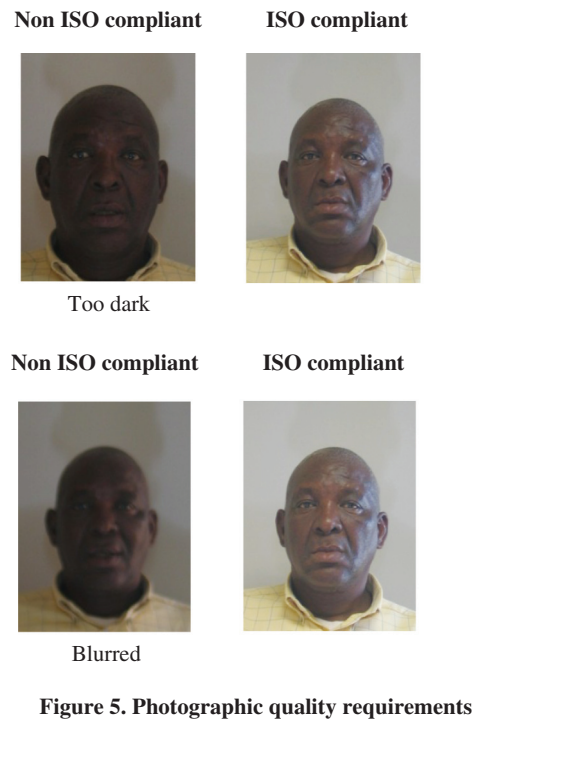

Figure 5. Photographic quality requirements

Photograph style and lighting must be:

- Colour neutral
- Show your eyes open and clearly visible—no hair across your eyes
- Be taken with a plain light-coloured background

Figure 6. Photograph style and lighting

- Be taken with uniform lighting and not show shadow or flash reflections on your face
- No red eyes.

See Figure 6.

If you wear glasses:

- The photograph must show your eyes clearly with no flash reflection off the glasses.
- No tinted lenses; lighter framed glasses are preferred.

See Figure 7.

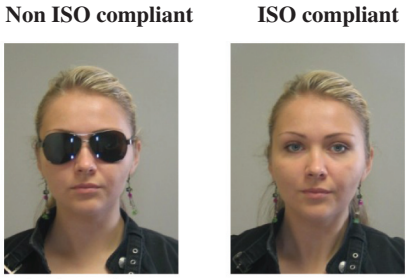

Figure 7. Glasses

If you wear a head cover:

- These are not permitted except for religious reasons, but your facial features from bottom of chin to top of forehead and both edges of your face must be clearly shown. See Figure 8.

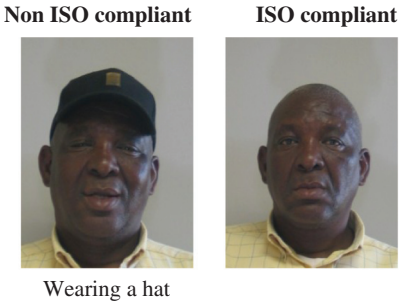

Figure 8. Head cover

The above specifications can be utilized as guidelines in other applications such as taking photographs of new and existing employees for the purpose of including them in access control ID cards, and later utilize those ISO-compliant face images in facial recognition search engines used for identification of persons. See Figure 9.

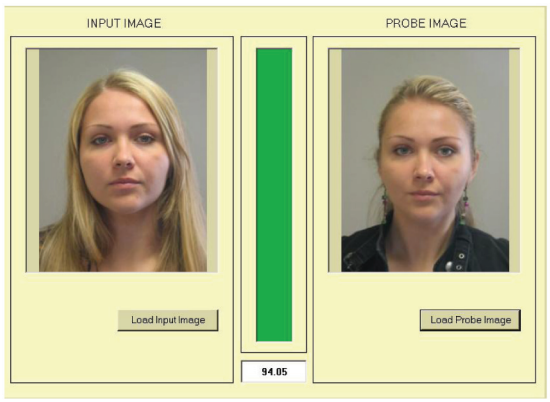

Figure 9. Example of correct ISO image, verification achieved by a facial recognition system

Conclusion

Following the 'popular' fingerprint biometric technology is not always the best for the mining environment.

Based on real-life experience and results achieved in the South African mining environment, a facial recognition access control system implemented in one of the gold mine groups has proven to be the most successful from the perspective of its effectiveness, reliability and user co-operation, based on day-to-day operations.

The system has given the best results based on the following evaluation criteria:

- Resistance to deceit
- No possibility of counterfeiting the artifact (it was tested by attempting to enter a photograph of a person, which proved unsuccessful)
- Extremely fast time to achieve recognition
- High convenience to the user
- Cost of recognition device and of its use as it can operate for a long time without changing the scanner element
- Easy interfacing of the device with the existing time-and-attendance card system, turnstiles and doors
- Short time and little effort involved in updating (adding and deleting users, issuing new passwords, keys, etc.)
- Long-term reliability and maintainability (some systems have been working for 8–10 years already).
- No cost of protecting the device (the face of the imposter or damaging it is registered on the system)
- Low cost of distributing and logistical support, as it can be done via the internet network.

Facial recognition systems are the biometric technology new market leaders of the 21st Century.

References

ISO/IEC JTC1 SC 37 Standing Document 2—Harmonized Biometric Vocabulary.

Basia Nasiorowska

CEO, Interoptic Networks

Basia Nasiorowska is a founder of Interoptic Networks and has been involved in the IT and Telecoms Industry over the last 20 years. She has been instrumental in shaping some of the critical aspects of the South African ICT market over the past two decades.

In the Telecommunications sector she has been involved with Telecommunications Skills Development Forum (TSDF) since the introduction of the Skills Development Act (Dept. of Labour) in South Africa. She was the Chairperson of TSDF.

Basia was also the driving force behind the formation of the SABS Committee SC74 Fibre Optics in 1996 and has actively participated over the years in the important work of this Committee.

For the past 10 years, Basia has been focusing on Biometric Technologies and has been involved in the ISO/IEC work concerning Biometrics.

She is a member of SABS SC71Q, the South African working group on Biometrics, which is represented in ISO/IEC JTC 1 SC 37 Biometrics. She is also involved in the work of StanSA TC 71 Information Technology which follows the work of ISO/IEC JTC 1/SC 17 and SC 31.

Basia has introduced state-of-the-art Facial Recognition systems to the South African market which have successfully benefited her customers and the market as a whole.

Her interest in Biometrics, and in particular Facial Recognition Systems, has turned into a passion that allowed her to gain experience and expertise in the Facial Scanning Technologies world-wide.