Role of biometrics in port security

David B McIntosh, Chief Executive Officer, OmniPerception Limited & Chairman of the International Association for Biometrics, Guildford, UK

Professionals operating in the maritime sector are well aware of the heightened concerns about the safety and security of ships, ports and the communities surrounding them. Since 9/11, fear of a similarly catastrophic event occurring in the maritime context has loomed large.

The need to tighten security in all areas is apparent, but in the context of port security the scale of the task is somewhat overwhelming.

Personal identity

Improved identity management is key to tightening security. Having confidence in who you are dealing with is crucial. Yet fraudulent access gained by staff impersonation is currently the single most common cause of perimeter and secure area breaches in airports, ports and harbours. If someone steals whatever ID tag or card is required to gain access, they can go where they like and pretty much do what they want. Existing systems – generally the plastic photo ID card – are not good enough to prevent this. Even if such an ID card has a PIN or password associated with it, it becomes only marginally more difficult to steal and use effectively.

Verification

The situation then is far from satisfactory, but what is to be done? Can new technology solve our problems in identity management? Are such systems relevant to real life activity in ports and harbours all around the world?

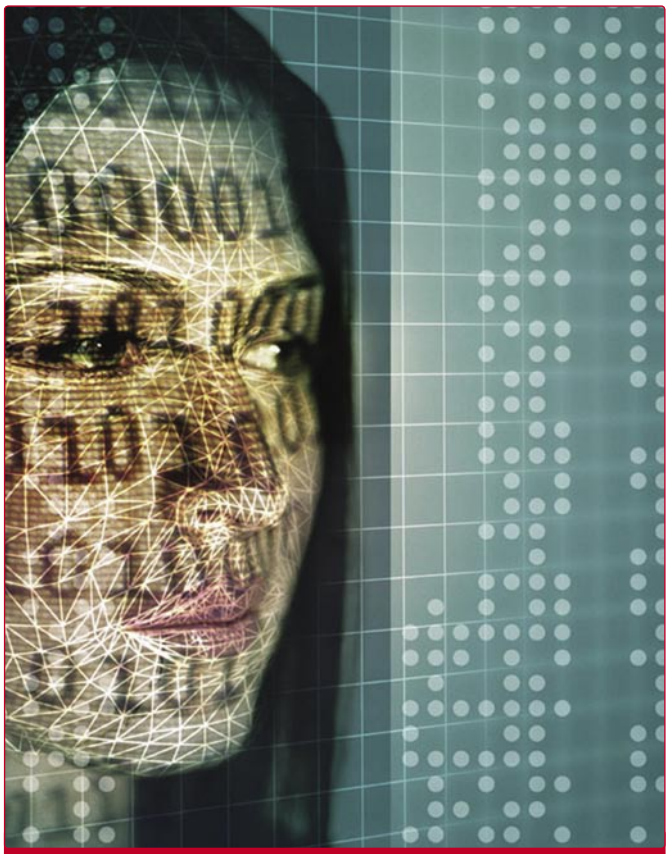
Biometric technology can indeed be of assistance in providing viable solutions to port security and this is already being adopted in other areas of the transport sector. The Department for Transport has decided to insist on biometric ID for all staff access air-side at UK airports – likely to be mandatory in the very near future. The biggest problem airports have is impersonation of staff going airside when they shouldn't. By having a biometric ID card requiring a positive facial match, airports can be sure of allowing access to the right people in the right place. UK ports and harbours are unlikely to be far behind.

With identity theft now being the fastest growing crime in the West, the ports and harbours community needs a new identity checking system that is reliable, quick and more convenient than non-biometric alternatives. It should be pointed out that such technology can only ever be part of the answer. Human vigilance and professionalism are also needed more than ever before.

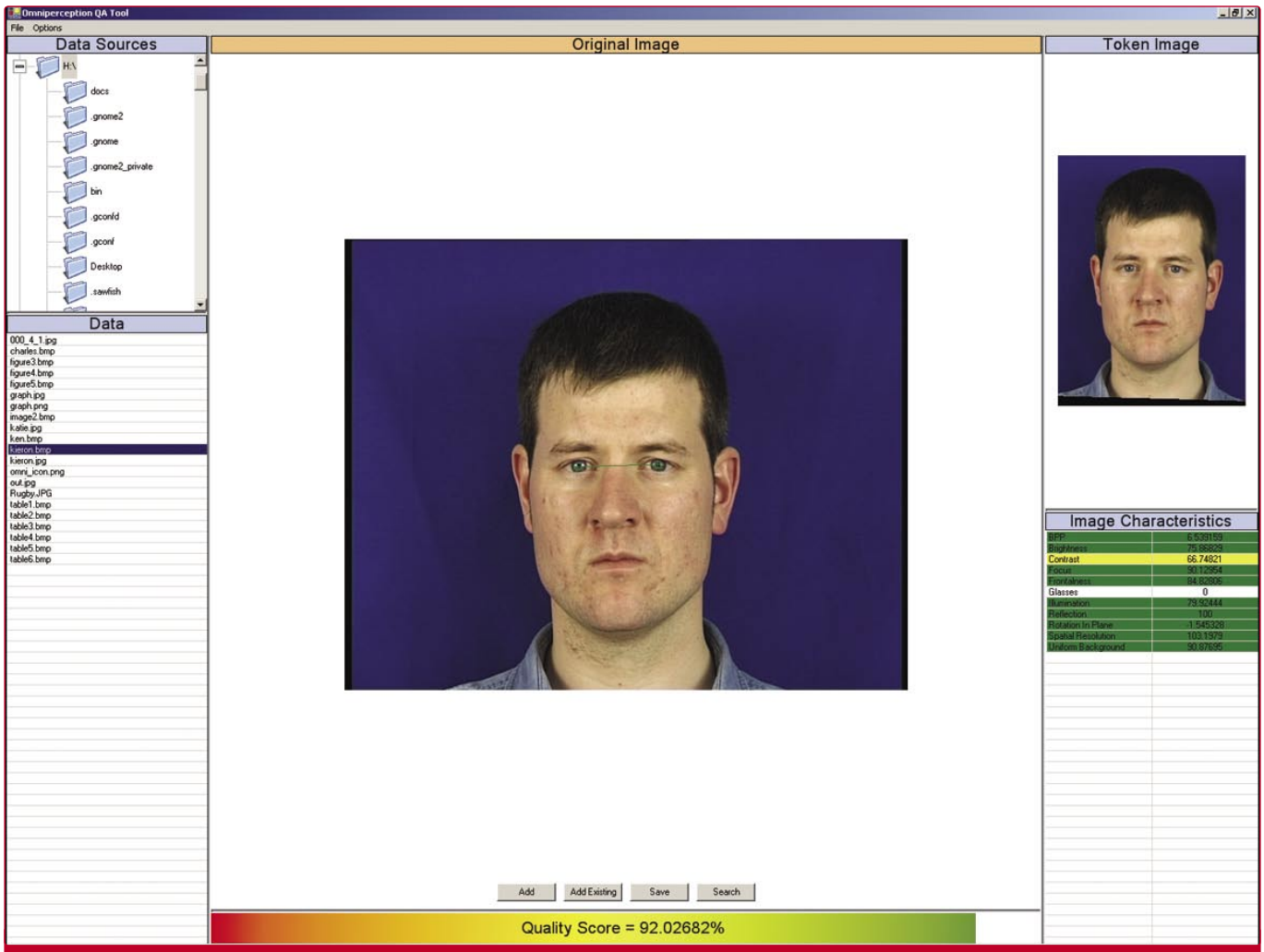
Biometrics is just what the name implies – a biological measurement of some kind. The term tends to be used today to imply a measurement that is not only biological but also unique, or at least highly distinctive, to one individual person. Whenever it is necessary to establish beyond reasonable doubt someone is in fact who they say they are, some form of biometric is likely to be involved. The biometric community call this 'closing the loop' – physically tying the identity directly to the real human being.

Two biometric techniques that have been used by the criminal justice community for many years are DNA testing and fingerprint matching (the latter having seen service in three centuries). Beyond police work, the use of these are limited. DNA is unlikely to catch on in a wider security context; it is hard to imagine clocking in for work using spittle samples.

Example of facial recognition system that could easily be used for port staff and dockyard workers. A 1-to-1 match takes less than a second to confirm an identity match and grant access to approved staff.



A unique FacialPIN™ is created via complex algorithms. It becomes a person's biometric identity reference – a number so long that no one could ever remember it but one that is with them at all times.



Facial biometric systems are designed to verify the identity of bona fide individuals wishing to enter a secure area (a 1-to-1 match). These systems help avoid undesirables that are impersonating bona fide individuals gaining entry fraudulently.

Fingerprinting has a much wider applicability than DNA sampling, but not everyone has a readable fingerprint and the problem – known as 'failure to enrol' – is a significant disadvantage for such a method to be used successfully in everyday life. Also, in the maritime industry, both at sea and ashore, the use of protective clothing and all weather gear often render finger-based identity checking impractical. For example, if dockyard workers were required to give a fingerprint to gain access they would have to put down anything they were carrying and take off work gloves, hardly a speedy solution.

New biometric developments now emerging are much more appropriate, in particular automatic face-recognition. Police offices are already using automatic face-recognition on a daily basis and say that it is rapidly becoming the 'third forensic science' alongside fingerprinting and DNA analysis.

Biometrics as a verification tool

How would facial recognition biometrics work in a maritime industry environment? A unique 'FacialPIN™' is established for everyone with right of access, done at the same time as the normal ID photograph is taken and adding less than 30 seconds to the process. The FacialPIN™ is created via complex algorithms designed specifically for the purpose; these are easily installed on the kind of standard hardware likely to be already in use.

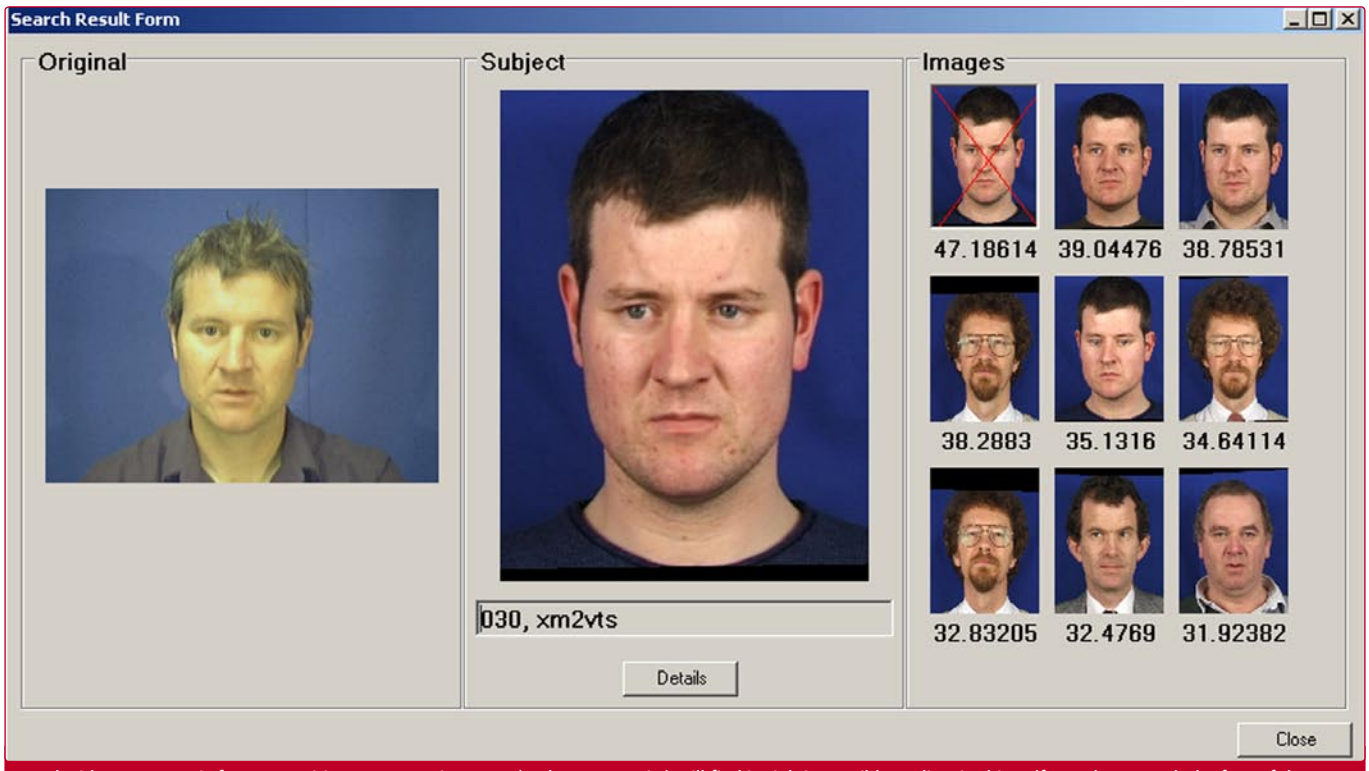
For those with international ID cards, the facial biometric will be stored on the card itself and this can also be done for local identity card systems. Alternatively, the FacialPIN™ can be stored on a network and recalled for reference by the system when required. In either case, the FacialPIN™ is a unique number based on the person's own facial characteristics. It becomes that person's biometric identity reference – a number so long that no one could ever remember it, but one that is with them at all times.

At any access control point that an identity claim is necessary, the person presents their face to a camera. The 'claim' can be via a swipe card, smart card, RFID method or via a simple key pad where a numerical PIN is entered. In each case the camera, the system or the card itself compares the identity claimed with the face presented and a 'yes/no' decision is made. This normally takes less than one second and creates minimum interference with the flow of people or the supervision of the system. The dockyard worker does not need to remove gloves or put down what he is carrying.

In some professions such as bricklaying, fingerprints are often unusable so a facial recognition booth can recognise workers to allow them access to a site and can even be used for clocking-in and attendance. Few people realise that thousands of construction workers clock-in for work every day in Britain with facial recognition systems of this kind (introduced to prevent people claiming bogus overtime and clocking other people in). There is no reason why such a system could not be used for dock workers and port staff.

Facial biometrics – the myths dismissed

To make the best use of facial biometrics those who are to deploy it need to understand it better. The biggest confusion is over the difference between 'impersonation' and 'disguise'.



Faced with an automatic face-recognition system an imposter (such as a terrorist) will find it nigh impossible to disguise himself exactly to match the face of the person whose identity he has stolen. When he tries to gain entry the system will spot his poor impersonation immediately and access will be denied.

Facial biometric systems are designed to verify the identity of bona fide individuals wishing to enter a secure area (a 1-to-1 match). These systems help avoid undesirables, who are impersonating bona fide individuals, and gaining entry fraudulently. A well-designed biometric system will spot impersonation easily and quickly.

Faced with an automatic face-recognition system an impostor (such as a terrorist) will find it nigh impossible to disguise himself exactly to match the face of the person whose card, password or PIN he has stolen. When he tries to gain entry the system will spot his poor impersonation immediately and access will be denied. However, the system will not have spotted him, as such, only that he is not the one it was looking for.

Some people criticise facial biometric systems because they are easy to 'fool'. This complaint is levelled at the 'disguise' version, not impersonation (when it is not a 1-to-1 search) and those issues are not relevant to the requirements of secure access control as you know who your staff are.

ABOUT THE AUTHOR

David McIntosh is Chief Executive Officer (CEO) of OmniPerception, leading face-recognition and computer vision company. He joined the company from the broadcast industry in February 2003 to take it into a phase of rapid expansion and development: his remit, to take the advanced biometrics R&D conducted at the University of Surrey and oversee its development into a next-generation facial recognition solution.

David is driving forward the company's strategy of seeking discrete markets for OmniPerception's innovative technology, focusing initially on identity screening and surveillance applications. With long experience in the successful commercialisation of intellectual property, David's particular areas of expertise include the application of biometrics and advanced image processing to airport security, civil ID and the prevention of fraud and identity theft.

ABOUT THE COMPANY

OmniPerception is one of Britain's most advanced computer vision companies, specialising in unique facial biometric technology and other highly advanced image processing. Originally founded by top research engineers from the University of Surrey's Centre for Vision, Speech and Signal Processing and still closely linked with the Centre's innovative output, the company is now established as a leading supplier of facial biometrics and advanced image processing solutions for customers world-wide.

OmniPerception's proprietary Affinity™ biometric technology is widely recognised as taking automatic face-recognition to new higher levels of accuracy and effectiveness. The company's powerful intellectual property portfolio and its commitment to on-going in-house Research and Development drives a growing range of products in global markets, in the field of machine readable travel and identity documents, access control solutions and other advanced image processing applications.

ENQUIRIES

For more information, visit: www.omniperception.com