White Paper

Facial Recognition Under the Microscope

The Future of Automatic Facial Recognition – TODAY!

A technical and practical look at the latest developments in Facial Recognition technology and how to maximise it.

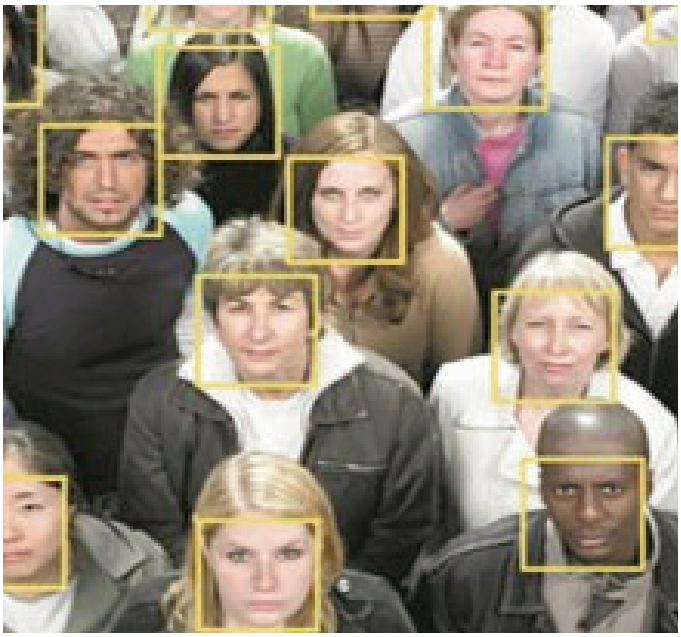
John Downie - Sales Director
Visual Management Systems Ltd.
Professor Jeremy Levesley
Department of Mathematics,
Leicester University

Contribution:
Professor Ivan Tyukin
Leicester University

Introduction

What we would like to do in this document is to look at some of the real-life issues that everybody faces when using artificial intelligence in a facial recognition environment. Artificial Intelligence is a term that is very current and topical. So, we are going to try and look under the hood at some of the things that are actually AI and how to utilise artificial intelligence for Automatic Facial Recognition (AFR).

At the outset we will need to establish exactly what AFR means in the context of this document. The role of AFR in the application we are discussing is that of detection and identification whereby faces are detected in a multi subject environment and matched with a known pool of individuals be they "the bad guys" or VIPs.



About Visual Management Systems Ltd.

Established in 1996, Visual Management Systems Ltd. is one of the UK's leading providers of integrated IP CCTV and PSIM (Physical Security Information Management) systems including hardware, software and video wall applications. The flagship product is TITAN VISION, an Integrated Security Management suite which delivers complete situation awareness, integration of all security subsystems, unified configuration across the network, programmable logic for automating response, workflow management to guide user response, and complete audit, reporting and forensic tools. Our customers include: airports, military bases, museums, city centres, national borders, oil and gas assets and critical national infrastructure.

© Copyright Visual Management Systems Ltd. 2019 All rights reserved

Back to Basics... The truth about Artificial Intelligence

There is a rush to over-market as AI, anything that involves computation with data. Things advertised as "AI" today may have no intelligence of their own at all.

With true AI, you get to use knowledge in a very different way to solve real-world problems. Algorithms allow the system to learn from its mistakes as a human does, this allows complex classification tasks, recognising a face from a non-face for example.

It is our understanding of very high dimensional information that allows us to perform tasks quickly and accurately at the edge.

Crucially it must be done in a practical way to solve problems in the outside world. Spending millions of pounds on hardware and it taking 75 hours to give you a single result would not be considered a practical answer.

A comment from Prof. Levesley.

"Ten years or so ago, people would have said what do you do? I would have replied, approximation theory or numerical analysis, but slowly over the period of the last ten years or so, new terms like Neural Networks, Machine Learning and Artificial Intelligence have all started to come in and I am sure that we have all heard of those. Yet are they the same thing or are they different?"

"From our point of view, there are some subtle differences between these things. We are using them in different ways to try to produce the facial detection, capture and recognition system. We have been engineering proper solutions to the problems that you really have".

How does AI Detect a face?

Prof. Levesley explains.

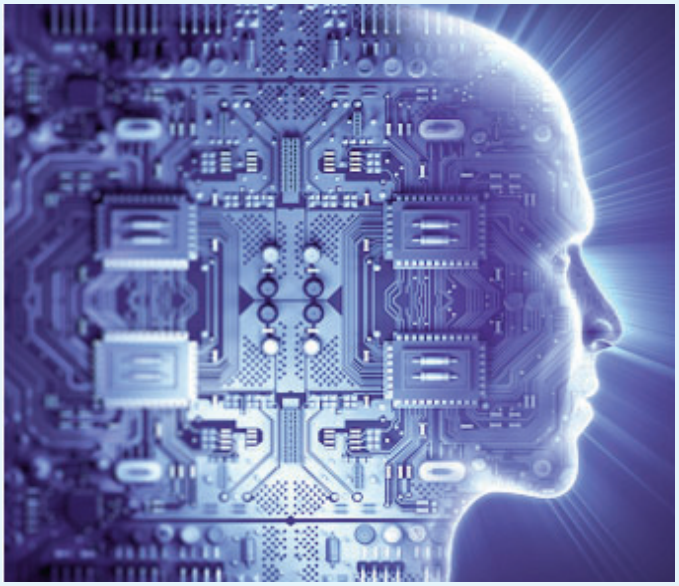
"The hard part is being able to tell what is a face and what is not a face. The thing that we are using is a thing called Histogram of Oriented Gradients (HOG). What that does essentially, the algorithm will scan across the picture and it will say a HOG of a face in that capture. This is the fundamental principle.

Once you have detected the face you know that this is the part of the scene that you are interested in and hence you reduce the amount of data you need to process from the whole image to only very small parts of the image. So when it comes down to the recognition process, you know that you are only dealing with the facial data".

Can Neural Networks really learn?

Prof. Levesley summarises.

"Another capability is to be able to do fast matching of faces using the Convolutional Neural Network (CNN) – once that part of the process is complete you may say it's still not working well enough. No Problem – we can take some of your data in order to improve the system. Machine learning capability as with humans will improve with practice. Machines are much better at doing certain things, robots won't be taking over our lives. There are millions of tasks that humans are poor at, that machines are very good at, comparing and matching numbers is one of them. Let



machines do what they do well and let humans do what we do well.

What the solution should do, is give you probabilities of faces being the ones that you are looking for and to allow a human to make the final decision – we may not want to leave this to the machine!"

What is a Face? An Academic Viewpoint

When using AI, what is a face and how do you distinguish from other things?

Prof. Levesley responded. *"A Face is simply an example of something that you present for the artificial intelligence to learn about, it happens to be a human face, essentially the machine has to learn from millions of examples of these so that it can say what is the distinguisher of a face as opposed to anything else".*

Adding *"From our point of view, we don't make any particular judgement about that, but of course we do when developing a product, but from a mathematician's point of view, we want to understand anything that you require. For example, you want to identify these 'things', they may be bottles, bags, anything it's just an example that you are providing us, that we can distinguish from non-examples".*

Professor Ivan Tyukin expanded. *"From a mathematical point of view, when you pose a question or pose a problem for machine learning it is presented in a particular way. Here is the data, we know that the data is real and that the data can be classified into faces and non-faces. At this point the probability distribution, in fact the information about how the data is distributed, is assumed to be unknown.*

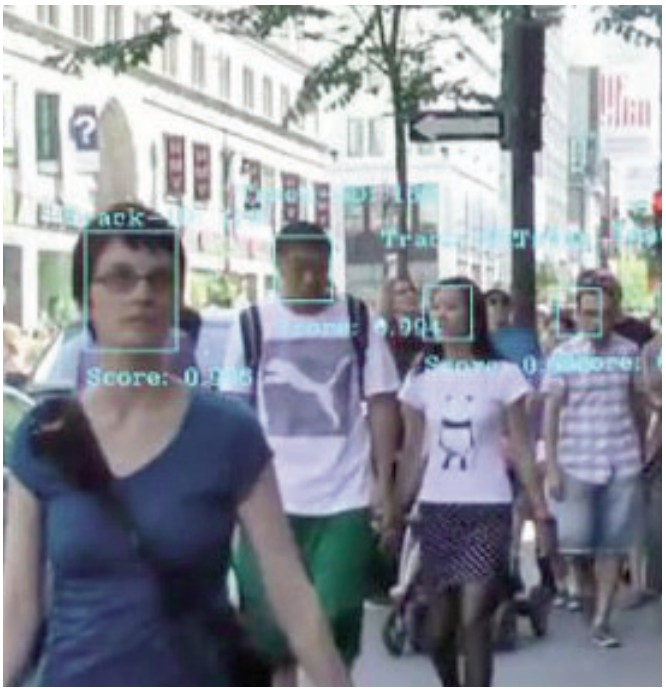
So, what is real is presented, one-way or another by an expert who labels the data. Now it can be wearing a mask and it can be without a mask and in this particular case, it's the ability of the expert to label the data which gives the quality that determines the algorithm.

So, at that point we accept that there is an expert but we don't require or ask for any model from that expert, we just assume that there is one and we use the information from the expert, the real data and the split of the labels that the expert provided to confirm the details in the data that are specific to the case that we are interested in. And the machine does this very well".

What to look for in a facial recognition system?

- *Real Time Facial Detection*
- *High Speed Facial Data Processing*
- *High Performance Matching Engine*
- *Machine Learning Capability*
- *Client Specified Matching Criteria*
- *Digital Tagging*
- *Ease of Use*

Real Time Facial Detection Reduces Image Processing



Advanced Imaging - Facial detection algorithms result in vastly reduced processing of video data. In most systems the entire field of view from the video stream is processed frame by frame.

By utilising the Artificial Intelligence based facial detection algorithms, only the data from the detected areas are processed i.e. faces, substantially increasing detection and recognition speeds, allowing high speed computation and hence increased accuracy.

Next Generation Facial Data Processing

High Speed Facial Data Processing – Unlike other systems the latest solutions do not use the five or six points of reference nor the geometric model, which have been historically used in biometric systems. You don't want the face to be the thing that is being manipulated, so actually doing direct comparisons of one face against another is not what you should be looking for.

The preferred system should turn the face into a code, the codes are the things that get compared so we no longer need the face once we have made the code. These codes cannot be reverse engineered to re-create the facial image.

The new generation of solutions utilise the Histogram of Oriented Gradients (HOG) method. The solution generates metadata directly from the facial data via a Convolutional Neural Network (CNN), producing a data-string not unlike a DNA signature.

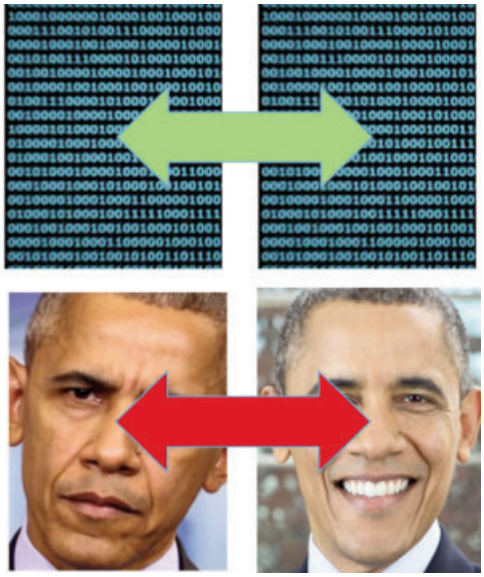
These signatures are far more easily processed and matched.

High Performance Matching Engine

Let a computer do what it does best – the matching process should be optimised by utilising the comparison of meta data, not image against image.

Computational power when applied to the comparison of a string of digits is both faster and more accurate than image v image comparisons.

The processing power required to process two images is both slow and inefficient. The benefit of this type of solution is superior speed.



Machine Learning Capability

Machine learning increases confidence levels – The issue of false positives has plagued traditional facial recognition systems. Frame by Frame the solution should interrogate the facial data to achieve a maximised DNA signature to optimise matching. Utilising machine learning techniques, the solution should retain/replace (client specified) facial data to provide the most appropriate signature for matching purposes.

Several signatures may be then linked to the subject of interest to increase accurate matching.

Client Specified Matching Criteria

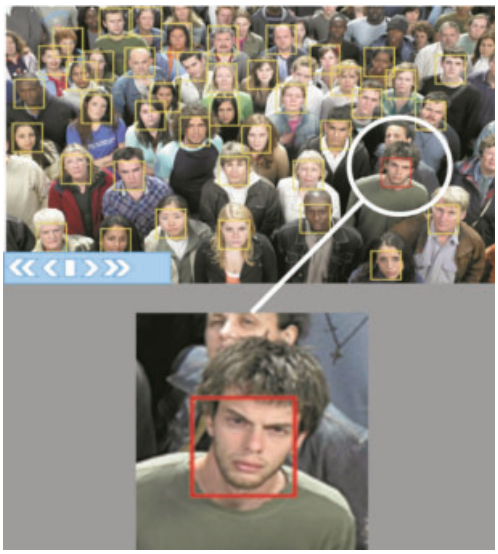
Fit-for-Purpose Solution - The application of facial recognition technology and the environments within which it's utilised vary significantly - from a closed, well illuminated environment in an airport, through a flood lit stadium, with multiple subjects and busy, fast-moving subjects in a poorly lit high street.

The solution should provide the user or operator with the option to control the thresholds of the confidence levels, generated by the system when raising alerts.

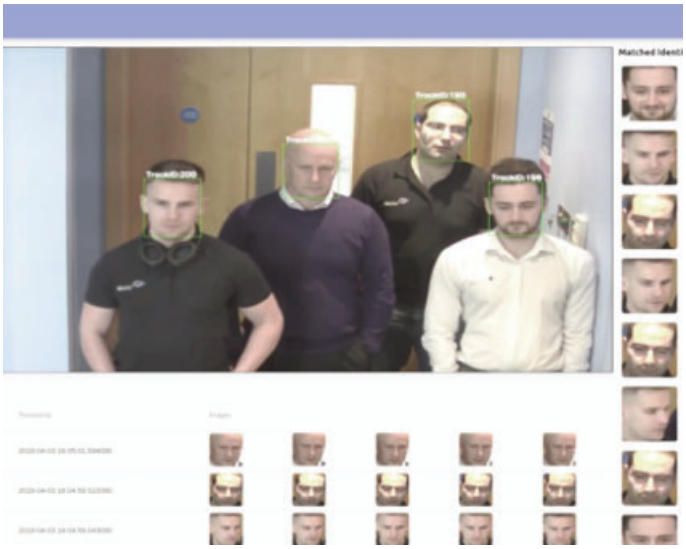
Digital Tagging

Digital tags linked to Surveillance Video – Digital tags should be linked with retained surveillance video, such that the matched subject of interest can be identified within the surveillance video stream.

This surveillance video footage can then be shared or further analysed by the operator or end-user, subject to the approved policies and protocols. This footage can then be communicated to colleagues in the field via various technologies.



Ease-of-Use



Consider the Operator – Following years of experience in the development of video management systems and PSIM solutions, the importance of the user interface has been identified as a crucial element within the overall solution.

The combination of ease-of-use and an appropriate GUI (Graphical User Interface) enhances the operator experience and increases the effectiveness of the overall solution.

False positives and how to combat them

"False Positive – noun - a test result which wrongly indicates that a particular condition or attribute is present."

In the context of this piece we are considering false positives occurring during the various phases of the facial detection and identification process.

The first opportunity for false positives to appear within the system is the facial detection phase. This is where an area of an image or part of a video stream is detected as a face when it isn't. Some graphical elements, architecture, cloud formations and "tricks of-the-light" may be presented as facial data, causing unnecessary processing and inaccurate results.

The second area where false positives may occur is in the matching (identification) phase, where two images are compared, flagged as a match when in fact they are not. In this case the data which is being compared may not be fit-for-purpose, i.e. out of date, of poor quality or in some way obscured.

A fit-for-purpose solution will take these exceptions into account, ensuring that, firstly the quality of the video stream is of an acceptable level, that the detection algorithms take into account external conditions and have the ability to learn providing greater accuracy, extracting only the true facial data from the scene for subsequent processing.

The processing and matching engines should also be robust enough to cope with high volumes of data maintaining matching integrity. By pre-processing of the facial data, it should be possible to determine which provided images offer the greatest confidence levels during a comparison. Clearly a pre-processed image with a confidence level of less than 50% should be discarded and flagged as inappropriate.

In summary; to avoid "False Positives" when utilising a Facial Detection and Identification system it is essential that the video stream is of acceptable quality and that the solution can identify "what is a face", with a high level of certainty. The system should also process the live data and client data in a fast, efficient and accurate manner and when appropriate, alert the operator as the final decision maker, providing such additional information to assist in that decision (for example; matching confidence data and tagged video footage).

GDPR and Facial Recognition

Where does face recognition fall under GDPR?

The GDPR data privacy and security legislation is the biggest overhaul since 1995, giving users more power than they've ever had. Given the pace at which technology is evolving, it has also left companies guessing how to catch up.

As Face Recognition Technology (FRT) collects information of a person's facial features, it's classed under biometric data, which is labelled as "sensitive personal data." The verbatim definition of biometric data in GDPR is… *'Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'.*

Clearly, the GDPR breaks biometric information into two categories…

- Physical characteristics: facial features, fingerprints, iris characteristics, weight etc.
- Behavioural characteristics, habits, actions, personality traits, quirks, addictions, etc.

The rule set also gives member states further powers to add restrictions on sensitive data as they see fit.

Anonymise and/or pseudonymise the data

One method to protect FRT data is to anonymise it altogether, making it impossible to determine who the information points to outside its utility. You can consider removing names from data sets before they are logged into a database.

In situations where anonymising won't prove practical, pseudonymised data can be used. Pseudonimising data is covered in GDPR where it is defined as processing personal data in a way that makes it impossible to attribute it to its source without the aid of additional information which can be kept in a secure environment.

An Appropriate and Secure Solution

As pointed out in this paper, the system discussed utilises the Histogram of Oriented Gradients Method to creates true anonymous data which has no relationship to the original, (which is discarded) providing an additional layer of security. Plus, data is also pseudonymised with the introduction of a unique identifier at the time of processing – This data cannot be reverse engineered to produce the original facial data and is stored in a secure environment.

Introducing TITAN AI - Advanced Imaging

TITAN AI is a range of Advanced Imaging products based around the latest patented* Artificial Intelligence, Neural Network and Analytical Techniques. Each TITAN AI product is individually tailored to the client's specific requirements and environments, providing both state-of-the-art and fit-for-purpose Detection, Recognition and Identification solutions.

Utilising the unique Award Winning TITAN AIM Advanced Imaging Technology, TITAN AI high performance systems offer both flexible and scalable solutions.

TITAN AI has been created by a team of artificial intelligence (AI) specialists to provide state-of-the-art advanced image processing technologies for use in a wide range of applications across several vertical market sectors.

TITANAi™

Operating at the forefront of cutting-edge video, behavioural analytics and image processing technology, Visual Management Systems Ltd. has developed the TITAN AI software and hardware solutions for the growing security, health and safety and physical analysis markets.

The unique Advanced Imaging Module (AIM) architecture, algorithms and machine learning capability, provide a combination of high speed and accuracy, offering a level of performance and capabilities that eclipses any existing solution.

*Patent Pending

COUNTER TERROR AWARDS 2019 COMMENDED

Who will benefit from accurate multi-subject facial recognition?

- Law Enforcement
- Retail, Warehousing and Logistics
- Hospitality and Events
- Entertainment Venues
- Sports Stadia
- Transportation
- Ports and Airports
- Border Control
- Public Spaces
- Defence and Military
- Education and Health Care

TITAN AI - A Practical and Proven Solution

TITAN AI™

The flagship products provide tried and tested solutions for a range of vertical markets and applications:

- **TITAN AI Detect** - Facial Detection, and Recognition solution
- **TITAN AI Identify** - Facial Recognition, Analysis and Identification solution
- **TITAN AI Queue** - Customer Queue Management System

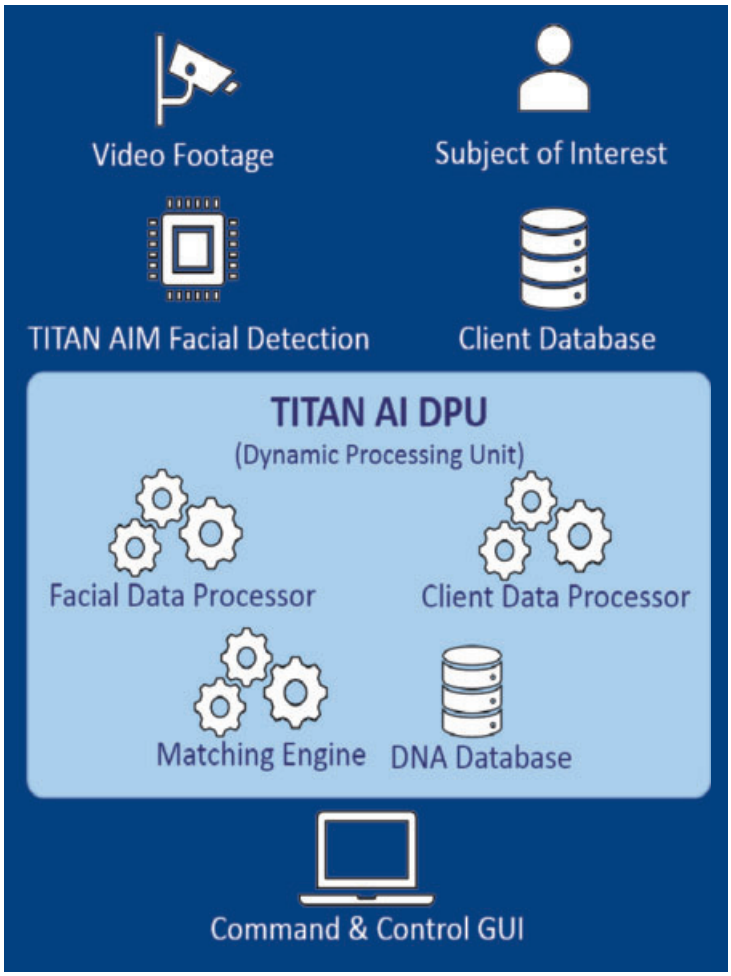
IP Video Surveillance Camera provides a video stream of the scene – video footage to security management and recording system is unaffected.

The AIM (Advanced Imaging Module) detects the facial data using Artificial Intelligence and a sophisticated extraction algorithm transferring the facial data and other meta data to the Facial Data Processor. Video data is unaffected by this process and continues to the monitoring system.

The Facial Data Processor analyses the facial data and converts it into a data string not unlike a DNA signature. This function is also performed using Artificial Intelligence and Convolutional Neural Network (CNN) technologies – This unit can handle more than 200 individual data streams. Image data is no longer required.

Finally, the Matching Engine, compares the facial DNA signature with the client's pre-processed database of images to identify the subject of interest. Utilising the confidence rating allows the operator to determine the level of accuracy and Image/video data is presented via an easy to use Graphic User Interface (GUI).

The operator reacts to system alerts presented via Command and Control Console GUI. Reviewing associated Video footage for verification, reacting in accordance with client procedures and protocols and distributes data as required.



Further Details: www.titan-vision.com/AI
Call: +44 141 643 3070

VMS

TITAN™

Visual Management Systems Limited
15 Cambuslang Road, Cambuslang Investment Park.
Glasgow G32 8NB. United Kingdom
Tel. +44 141 643 3070 | Fax +44 141 643 3079
Email info@titan-vision.com | www.titan-vision.com

© Copyright Visual Management Systems Ltd. 2019 All rights reserved