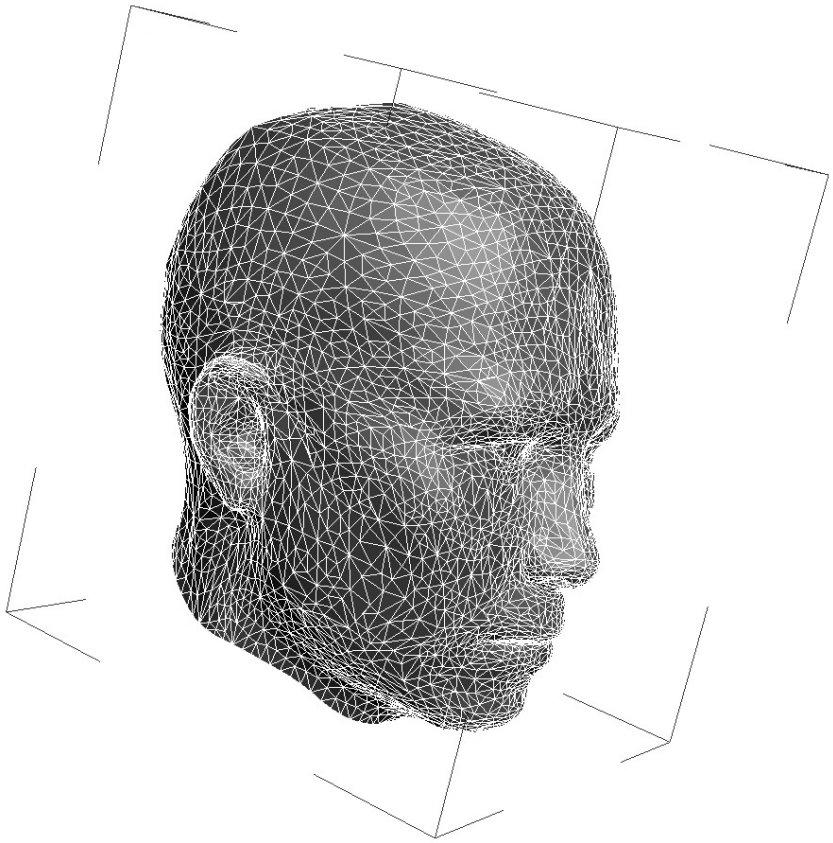
ANIMETRICS

WHITE PAPER

# NEXT GENERATION FACE RECOGNITION

*Driving the Convergence of Surveillance and Access Control*



## INTRODUCTION

Many face recognition vendors are in search of the Holy Grail to solve one of video's toughest challenges – accurately identifying faces in access control and surveillance applications where people or backgrounds cannot be controlled. Why? Perhaps due to the fact that the video surveillance market is already a $5 billion market and is expected to grow to $13 billion by 2010 according to J.P. Freeman Co. More cameras, more video footage, equate to more faces to find and identify. In fact, in the United States alone, there are an estimated 26 million video cameras generating more than 4 billion hours of video footage per week. Solving the problem of dynamically identifying faces from live streaming or stored video will enable an integrated security solution for bullet-proof security. A few companies will succeed in video-based face recognition but most cannot due to the "after-the-fact" approach.

Animetrics® offers a seamless transition between access control and surveillance video. No other face recognition system can make this claim.

Airports, borders, ports, energy plants, historical buildings, monuments, manufacturing plants, retail establishments, and businesses require access control and surveillance video solutions that will prevent destruction and capture those individuals whose intent is to cause harm. The intelligent video surveillance (IVS) software market, including video analysis, is experiencing significant growth in light of this need. Presently, most systems do not incorporate face recognition biometrics as the problem still remains that face recognition does not work well on video surveillance footage. Key factors contributing to the problem include low resolution of CCTV cameras, poor lighting, the subject's position, facial hair, ornaments such as eyeglasses and jewelry, and background noise.

These problems must be solved in order to make effective use of existing video recordings and to embark upon "action oriented" preventative analytics that will provide next generation security methods. This paper examines 1) how Animetrics face recognition software significantly contributes to the value of access control and intelligent video surveillance and 2) why Animetrics' approach enables an easy transition from the access control environment to the surveillance video environment.

## TRENDS IN FACE RECOGNITION AND VIDEO SURVEILLANCE

To understand what is driving the popularity of face recognition and video surveillance, it's important to understand the market dynamics and trends.

***Face recognition's non-intrusive nature will put it to the forefront as the biometric of choice.*** ICAO (International Civil Aviation Organization) has embraced face recognition as its biometric standard. Acuity Market Intelligence, Inc., in its 2005 Market Report, projects face recognition to surpass fingerprint by 2009. This may be due to its non-invasive nature.

***"By 2007, network cameras will make up more than half of the overall security camera market. " (Frost&Sullivan)*** These network (IP) cameras are expected to have better lenses and better resolution than CCTV cameras. This will aid significantly to improve face recognition accuracy. Along with network cameras is the increased use of Network Video Recorders (NVRs). The NVRs store motion JPEGs making it easier and faster for face recognition software to identify faces.

***Integrated video, access control and IT happening now.*** Forrester predicts that 40% of businesses will want integrated security. The proof is already in the pudding. GE Security, Honeywell, Tyco and IBM are just a few of the big names that have already ventured into this space. These three technologies are pulling each other along in the security industry. The access control market is expected to reach nearly $4 billion in 2007 (RNCOS 2005).

***The IP network backbone makes it easy to integrate network cameras, access control systems and IT together***. These three technologies work synchronously together to provide a powerful security application. Imagine the ability to have a single report automatically generated telling you when a suspicious individual came through the door, which hallways and rooms they were in, and when they logged in to their computer.

***"Smart Buildings" will include integrated security.*** Honeywell, TAC (division of Schneider) and Siemens are examples of big players in the building automation industry. These markets will integrate utility controls with security. For example, when a person goes by the RFID reader and camera for entry to a building, the lights and air conditioning will turn on. This industry, currently a $20 billion business is already looking at integrated security as an added value.

## ANIMETRICS TECHNOLOGIES PRIMED FOR SURVEILLANCE

The surveillance environment has posed a great challenge for face recognition technology. Face recognition today works well in “controlled settings” where people are cooperative, illumination is sufficient and even, and background views are simple and uncluttered. The “uncontrolled” surveillance environment introduces uncooperative subjects where facial pose may vary dramatically, lighting may be poor or uneven, and background views include multiple objects. Animetrics software was designed from inception to account for these challenges by facilitating the simultaneous ability to address the controlled “checkpoint” access application as well as the “uncontrolled” surveillance video application.

### *SEAMLESS FROM ACCESS TO SURVEILLANCE*

Animetrics patent pending 2D-to-3D technology is the core foundation enabling the seamless transition between the controlled checkpoint environment and the uncontrolled surveillance environment.
High performing 3D systems require interfaces to a secondary 2D-3D technology (such as Animetrics) when operated in the "surveillance at a distance" mode since 3D imaging devices cannot project into a distance uncontrolled volume. This is why 3D technology will be limited to applications requiring subjects and settings to be highly controlled. Pure 2D-to-2D technology is also limited to the controlled environment as NIST FRVT 2002 proved the need for utilizing 3D technology to handle the confounding variables – pose, lighting, and expressions.

Animetrics 2D-to-3D technology provides the unique solution for simultaneous high performance in the image at a physical access checkpoint “controlled” scenario, as well as the "image at a distance" surveillance scenario. It is the core 3D data structure Animetrics generates from a 2D image that is responsible for the impressive accuracy achieved by its face recognition system (Figure 1). Animetrics examines the data structure for information about the image including pose, lighting, artifacts and background. It analyzes these variables and corrects the information necessary to boost face recognition accuracy and performance. The Animetrics data structure serves both controlled and uncontrolled environments enabling access control and surveillance applications the ability to invoke a single face recognition technology in a converged building security solution.

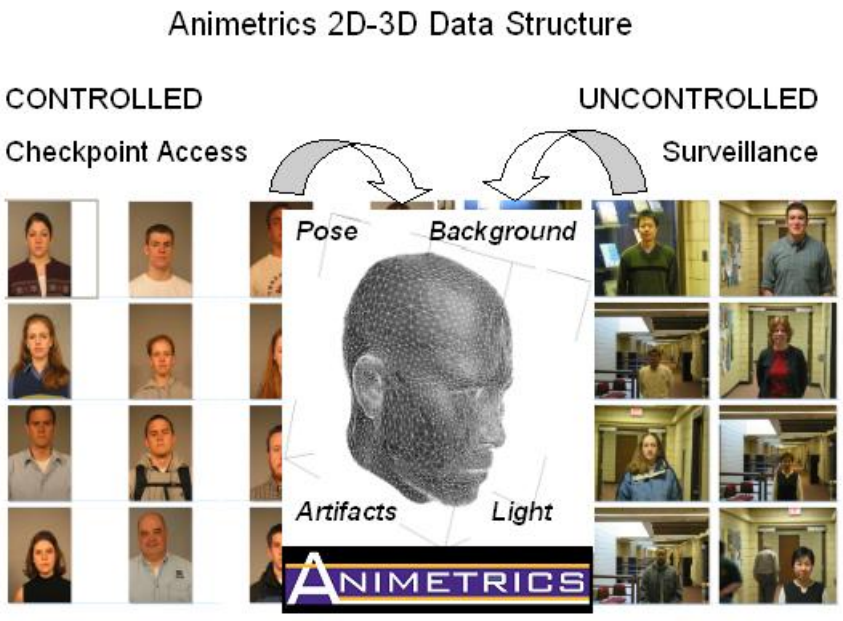



*Figure 1: Animetrics Data Structure*

## *BREAKTHROUGH FACE RECOGNITION TECHNOLOGY*

Animetrics breakthrough technology is the vehicle that will propagate the convergence of access control and surveillance because it will solve the problem of "face recognition from random video". For every facial image, Animetrics provides a coherent 3D representation based on data collected from access control and surveillance imagery. Such a 3D representation unifies all motion artifacts associated with the position of the face and the random location and uncalibrated configuration of the cameras used in these applications. Simultaneously, this 3D provides the technological vehicle for representing photometric information (such as shadowing) and the confounding effects of lighting. So whether an individual is being observed in the highly controlled configuration of the "checkpoint access control camera" or the dynamic and highly variable uncontrolled configuration of the "surveillance camera", an identical methodology is used to determine the axis coordinates of the individual being tracked in the photograph. This 3D information tightly integrated with Animetrics powerful matching algorithm is

the cornerstone that will propel the convergence of access control and surveillance.

Animetrics face recognition system architecture is based on a modular framework, facilitating the interoperability with other state-of-the-art applications and technologies. The combination of Animetrics breakthrough technology and modular architecture allows the ID system software to work directly with IP based video acquisition (or CCTV). Animetrics face recognition system works with any 2D camera (i.e. still camera, IP surveillance, CCTV surveillance) leveraging its ability to convert images into 3D data structures. This approach significantly differentiates Animetrics from those vendors requiring expensive 3D cameras. Components of Animetrics face recognition system include detectors, a search engine, pose processing, and light processing.

## Detectors with Bull's Eye Accuracy

All identification and video analytic systems that will utilize face recognition require the ability to detect a person's head in the photograph. "Detectors" sit at the front-end of a face recognition system so in order for face recognition to work effectively, it is critical to have detectors with bulls-eye accuracy. A face recognition system is only as good as its detectors. If you cannot find the face and the location of the facial coordinates, then important data is lost and the face matching algorithm will fail. Animetrics face recognition algorithm uses this technology on the front end. Customers have also experienced great success in utlilizing this technology in conjunction with a matching algorithm to tackle face recognition on challenging images such as those from CCTV cameras.

Face recognition is only as good as the front-end detectors.
And Animetrics delivers the best.

## Orbital Classifier Algorithm Matching Fingerprint Performance

There are a number of methods used to process faces in face recognition algorithms. The main methods used today include eigenfaces (Principal Component Analysis), local feature analysis, and neural networks. Animetrics has developed a technique based on "orbital classifiers" that enable FACEngine ID, its face recognition system, to accurately identify faces in photos where the environment is uncontrolled. In fact FACEngine ID has

achieved peformance equal to that of fingerprint. That is, a 99.9% False Accept Rate (FAR) and a .1% False Reject Rate (FAR). This means VERY accurate.

Facengine ID equals fingerprint accuracy making it the biometric of choice in access control.

## Pose Invariance Making Surveillance ID a Reality

Conventional high performing 2D systems degrade dramatically from an environment such as the controlled physical access checkpoint setting to the surveillance setting. In the surveillance setting most faces are captured with some degree of pose, or non-frontal view of the face. Animetrics has mastered the ability to correct for severe off-pose positions. Today, Animetrics can detect faces that are turned up to a +/- 40 degree yaw (Y-axis). Then Animetrics' 3D technology will automatically rotate these faces to a front facing position (ie: 0 degrees pose). This process is most beneficial for enhancing the face matching algorithm.

The graph in Figure 2 demonstrates the amazing boost in face recognition performance Animetrics achieves when attempting to recognize face images at forty (40) degrees of pose or greater compared to that of leading face recognition vendors. The green curve shows a 94% verification rate at the false accept rate of 0.1%. This means that 94% of the time the system was able

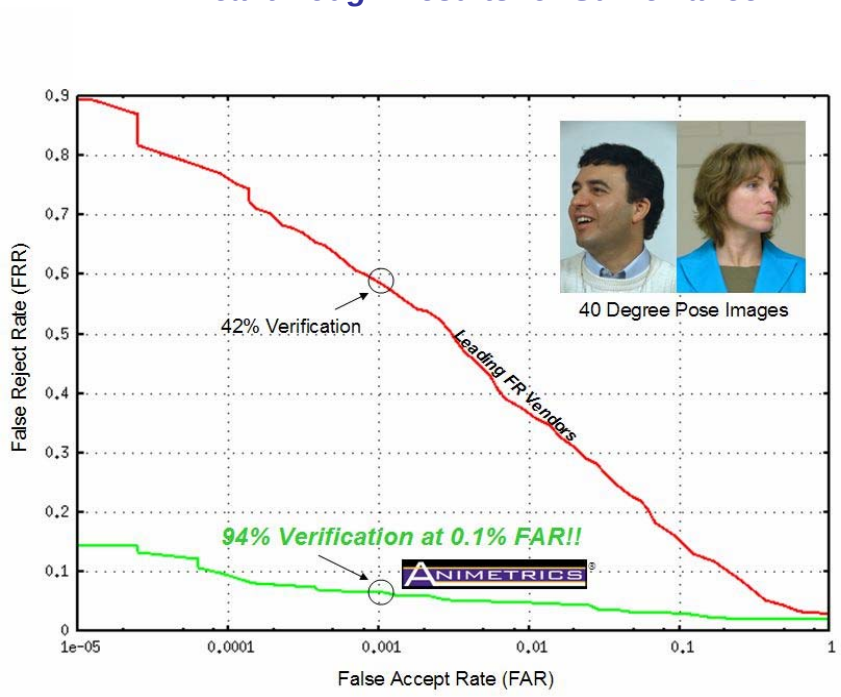



*Figure 2: Animetrics Face Recognition Performance*

to recognize and verify that the person is who he says he is. At the same time, the system only accepted people incorrectly 1 out of 1,000 times ( ie the FAR). If the FAR is contrained to approximately 1 out of 100, or 1% false accepts, then it follows that the verification rate goes up.

When we compare the Animetrics green curve to the red curve which represents other face recognition vendors systems performance we see a dramatic argument for the use of face recognition in surveillance or uncontrolled, uncooperative subject application

### Illumination Invariance Shedding Light on Image Enhancement

There are several types of lighting conditions that make it difficult to verify or identify a person from a visual perspective or from computer based recognition. The conditions that cause these issues include 1) uneven lighting where one side of the face may be darker than the other, 2) flash lighting that causes a "washed out" look and then 3) dim lighting where facial features may not be entirely clear. Animetrics lighting normalization attempts to normalize such conditions making visual and computer based recognition easier for identification purposes. Animetrics generates a 3D map of light intensities whereas conventional methods use a discrete set of light sources that are based on a "guess" as to where the sources originate. By looking at the infinite vector space, Animetrics' algorithm can not only "normalize" but also adjust lighting conditions.

## THE SOLUTION FOR INTEGRATED SURVEILLANCE AND ACCESS CONTROL

One of the significant trends identified by the analysts (Forrester Research and RNCOS) is "integrated security". The security systems of the future will integrate surveillance, physical access to buildings, and logical access to computers. Industry drivers for this trend include 1) "smart buildings" where security systems, HVAC, power and lighting are integrated for the purpose of conserving energy and lowering tenant or owner costs and 2) the emergence of IP network cameras. Devices and computers supporting surveillance video and physical and logical access will soon be running off an IP network backbone. For the customer, this makes managing security a much easier task. Animetrics face recognition

software makes this vision possible serving as the foundation for the highest standard in integrated building security.

## Animetrics face recognition - the foundation for integrated building security.

Legacy building security systems mean separate network protocols, separate monitoring software, and separate security reports for the three key areas of building security (surveillance, physical access, logical access). All of this is converging so that security personnel for government, businesses or the like can run a single report that tells them when an individual came in the door, when they were spotted in certain rooms or hallways and when they logged on to their computers. Animetrics FACEengine ID face recognition software ties into surveillance video, access control (and eventually logical access). Animetrics offers end customers and integrators "one-stop" shopping for face recognition with seamless technology between controlled and uncontrolled photographic imagery (Figure 3).

*Figure 3: Animetrics Enabling Integrated Security*

## *ANIMETRICS A PERFECT FIT FOR NEXT GENERATION ACCESS CONTROL*

Face recognition technology will be prevalent in access control "checkpoints" and in general surveillance monitoring within buildings as depicted in Figure 3. Face recognition is the biometric of choice enabling non-intrusive verification or identification of a person. A "checkpoint" is a dedicated area of a building where people must slow down or stop and be verified or identified before a door, turnstile or gate is triggered to open. Checkpoints will normally require a person to use an electronic card such as an RFID card, smart card, or magnetic strip. Then that person would be verified by the face recognition system before the door is triggered to open. There are actually two configurations for the checkpoint access scenario involving face recognition.

**Controlled Checkpoints.** This is where the person passing through must actually come to a stop at the checkpoint. In this case the person attempting access must be in close proximity to the card reader and camera. The person stops at the checkpoint, runs the card through or by the reader, looks into the camera, and the picture is taken via a still or video camera. The face recognition software is configured in a one-to-one matching configuration where it matches the live picture to the stored template on the card. Assuming the person is verified (it is indeed that person), the door opens or unlocks.

**Semi-uncontrolled Checkpoints.** In this configuration, a video camera is used to capture photographs of the person at the checkpoint. In this case, the person may be at a distance greater than three feet from the camera and may not come to a full stop. However, since this is still a checkpoint, the person attempting access will carry an RFID card. The video camera will record and capture the best photo of that person via frames or motion JPEGs. However, the photo captured may or may not serve as the trigger to actually open the door. The card may be used for that while the captured image may be used instead for monitoring for later viewing. Or, it could be used to discreetly alert a security person if a one-to-many identification does not match up. The information collected from the access control application can be combined with the video data collected from the surveillance monitoring

system described below. The combination of the two systems form a smart security system.

### *ANIMETRICS, A PERFECT FIT FOR INTELLIGENT SURVEILLANCE*

**Surveillance Monitoring – Active or Passive**. In the "general monitoring" scenario, cameras may be located at entrances, hallways, conference rooms, utility rooms, offices, computer rooms, manufacturing floors or anywhere critical assets reside. In this scenario, people passing through these areas can be identified via a "one-to-many" face recognition configuration. The identification can be done actively (near real time) just after the video frames are collected. Or, it can be done at a later time such as after the video for a 24 hour period has been recorded.

**Video Analytics**. Face recognition is the technology driving the value of surveillance video analytics. In video analysis, face recognition can be used to 1) identify a face, 2) find and identify a face in a group and 3) correlate a new face (probe) with that face in other photographs via a process called meta-tagging. Figure 4 below illustrates the significance of face recognition as it applies to video analytics. For example, face analytics can answer "who is that person?" "where have we seen her before?".

Video Analytics

*Face Meta-Tagging and Photo Correlation*

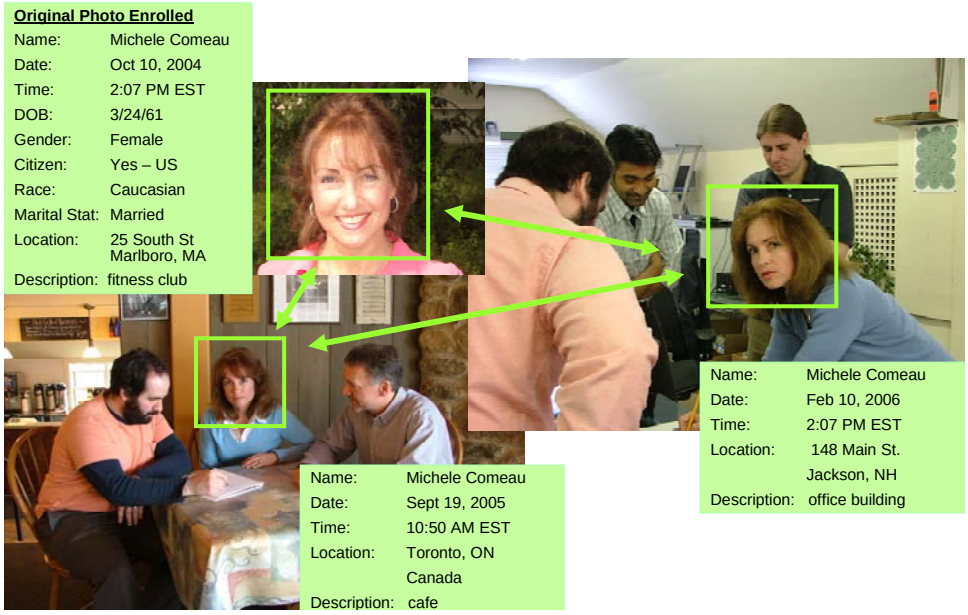


*Figure 4: Finding Faces, Face Tagging & Correlation*

## CONCLUSION

Animetrics' leading edge face recognition solution has tackled the existing face recognition problems found in access control and surveillance video. It has achieved performance and reliability comparable to fingerprint biometrics making it a natural fit for next generation touch-free access control. At the same time, the Animetrics ID system can deal with the challenging problems of detecting a face and matching it to a watchlist for surveillance. Now there is a single face recognition software application that can accommodate both access control and surveillance video.

Animetrics is driving the convergence of video surveillance and access control.