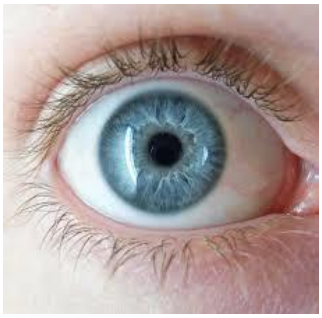
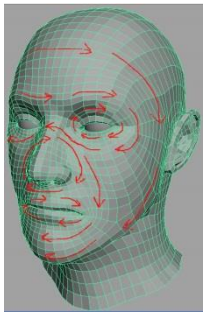
White Paper

The Necessity of MultiModal Biometric Systems for Large Scale Deployments



Iris Recognition

Fingerprint



Face Recognition

The Rapid Global Growth of Biometric Identification Management Systems

10 years ago, if you asked most identity management experts whether they thought the use of biometrics for individual identification management would become mainstream globally, most would have agreed with the idea that it would be used in some capacity, but few could have predicted the enormous scale and scope of some larger deployments developing around the world. The application of biometric technology has grown for a number of reasons, perhaps the most important being the need to help fill the "[i]identity gap" suffered by many developing nations that inhibits an ordinary citizen's ability to effectively interact with the state – or with private entities – for access to basic rights and services, including: education, employment, financial services, voting, social entitlement programs, healthcare, and more.

Biometrics offers distinct advantages because it relies on identifying someone by "what they are" compared to other identification methods that rely on "what you know" (e.g. – a password) or "what you have" (e.g. – a credential or token), which can be subject to fraud or simply forgotten or lost by an individual. Biometric authentication measures the unique physiological and/or behavioral characteristics of individuals in order to verify their identity and is considered to be much more convenient and secure than traditional systems since there is no password to forget or identification document to be lost or shared. Furthermore, biometric enrollment profiles must be provided in person to eliminate borrowing or swapping identities and to reduce fraud.

Many will argue that in a world where fraud, waste, and crime are largely precipitated by the ability to exploit traditional forms of identification, biometrics has emerged as one of the only feasible technologies to protect individual identity.

An Introduction to Multimodal Biometrics for Large-Scale Deployments

Despite their clear superiority over other more traditional forms of identification, unimodal (biometric deployments using only one modality) biometric systems are not without accuracy limitations when deployed in certain environments, depending on a number of factors, including:

- **Noisy sensor data**: "Noise," or factors affecting the quality of the image produce by the biometric device, can be present in the acquired biometric data mainly due to defects or environmental conditions.

- **Non-universality:** If every individual in the target population is able to present the biometric trait for recognition, the trait is said to be universal; however, not all biometric traits are truly universal (e.g. - people with hand related disabilities, manual workers with low skin integrity caused by cuts and bruises on their fingertips, and people with very oily or dry fingers). The National Institute of Standards & Technology reported that 2% of the world's population can't enroll in biometric fingerprint systems[ii] because of skin integrity issues.

- **Lack of individuality:** Features extracted from biometric characteristics of different individuals can be very similar (e.g. - a small proportion of the population can have nearly identical facial appearances due to genetic factors).

- **Intra-class variations**: The biometric data acquired from a user during verification will not be identical to the data used for generating the user's template during initial enrollment.

- **Spoofing:** Although it is extremely difficult to steal someone's biometric traits, it is possible with some biometric devices for an impostor to circumvent a biometric system using spoofed traits (behavioral traits like voice and signature are more susceptible to these types of attacks than those based on physiological traits).

Despite the ability of unimodal biometric systems to achieve very high levels of accuracy for smaller population sizes, they continue to be based on performance recognition that relies on a single source of biometric information. This can compromise the integrity of the matching system since unimodal biometric systems rely on a single physiological characteristic, which can be significant in very sensitive or high-security environments.

Therefore, the ability of a unimodal biometric system to accurately and consistently identify 100% of a population is limited. In addition, because of the rapid growth of large-scale deployments, a unimodal system can be considered undesirable unless combined with a second biometric modality.

The Rise of Multimodal Biometric Systems

Considering the limitations of unimodal systems, more biometric deployments that encompass large-scale population databases are turning to multimodal systems. Multimodal biometric systems are defined as those that are capable of using more than one physiological trait for authentication to help overcome the limitations of unimodal systems. Multimodal biometric systems combine biometric identifiers to obtain a more accurate decision on an end user's identity claim based on multiple sources of evidence.

As the size and scale of biometric identification deployments grow, it becomes imperative that they combine the data obtained from different modalities using an effective fusion scheme to significantly improve the overall accuracy of the system. In addition, a multimodal biometric system can reduce the Failure To Enroll (FTE) and Failure To Capture Rates (FTC), and provide more resistance against spoofing because it is difficult to simultaneously spoof multiple biometric sources.

It may come as no surprise then that the use of a multimodal approach to biometric identification requires a higher allocation of resources and time, especially during the initial enrollment and data collection phase, but in deployments where security and accuracy are paramount, multimodal systems have become ubiquitous. It therefore follows that customers who seek to maximize the accuracy of biometric identification systems are investing in multimodal biometric systems. By moving beyond unimodal deployments, adding additional modalities also accelerates the de-duplication process and is

more accurate. This is especially true as you add users to an existing database where the de-duplication process compares the newly enrolled person against the total existing biometric database.

The Most Popular Forms of Biometrics for Large Scale Identity Management

Although biometrics as an industry could be accurately considered in the early growth stages of the product lifecycle, there are legacy biometric modalities that have become staples for many deployments and others that are making headway as viable options. Which modalities are the most and least used across the globe for large-scale identification management and what are the potential risks to relying on a unimodal versus a multimodal approach?

Fingerprint

Fingerprint recognition is a widely accepted technology in both the government and private sector, and for over a century it has been used by civil, forensic research, and law enforcement agencies in many countries. Its existence and subsequent use in Automated Fingerprint Identification Systems (AFIS) in many countries makes it the popular biometric modality by choice. Fingerprint is the most developed biometric modality, with more history, research, and hardware designs than any other.

Here is a list of positive characteristics that define fingerprint biometrics as a viable modality for individual identification:

- **Utility:** Most countries have existing fingerprint databases for forensic use, even those which don't have an AFIS system. The commonality of fingerprints along with their widespread use for other purposes renders them a very familiar and effective modality for identifying individuals.
- **Storage Capacity:** Fingerprint biometric templates require small storage space compared to other modalities, which reduces the size of the database, lowers hardware costs, and facilitates fast data transfer speeds.
- **Accuracy:** Fingerprint recognition systems have low false rejection rates (FRR) or false acceptance rates (FAR) in populations with a low incidence of outliers (groups varied by age or gender).
- **Variety:** A wide variety of enrollment devices are available for multiple fingers (i.e. 10 fingers, 2 fingers, single fingers).

Fingerprint is not without its limitations, however. Here are a few to consider when evaluating fingerprint biometrics for deployment:

- **Comparative Accuracy:** Fingerprints are not as accurate as some forms of biometrics, such as iris and retinal scanning.
- **Skin Integrity:** Fingerprints may be obscured, damaged or changed due to an individual's occupation, physical condition or disability, which may require multiple enrollments for some

people over the course of their lives or even the inability to identify someone who may be rightfully registered in the system.

- **Spoofing:** Despite recent technological advancements by fingerprint sensor manufacturers to combat the issue of spoofing, fingerprinting still remains one of the easiest biometric modalities to spoof. Recent evidence on the ability to spoof biometric fingerprint systems surfaced through Apple's TouchID fingerprint sensor[iii], and in Brazil where an employee used silicone fingers to spoof a fingerprint based biometric time clock.[iv]

Major factors that affect fingerprint system accuracy:

- Live scan quality
- Enrollment scan quality
- Scan device usability
- User skin condition
- User fingerprint expression
- Closed vs. open biometric system
- Liveness detection

Example of unimodal fingerprint recognition in a large scale biometric identification management deployment:

The Netherlands began issuing unimodal biometric passports in 2005 to their citizens that contain a single fingerprint image embedded on a sensor within the document.

Iris

Iris Recognition is another method of biometric identification where mathematical pattern-recognition techniques are used to identify individuals. Digital templates encoded from iris patterns by mathematical and statistical algorithms allow the identification of an individual or someone pretending to be that individual.

Here is a list of positive characteristics that define iris recognition biometrics as a viable modality for individual identification:

- **Accuracy**: Every individual's eyes are different than others (even in fraternal or identical twins). Moreover, an individual's left and right irises are also different. This is the reason that the FAR (False Acceptance Rate) is extremely low (1 in 1.2 million) in iris recognition. One iris template contains more data than a biometric template that combines a finger, face, and hand data. This is another reason that iris recognition is capable of providing more accurate data than other recognition systems.

- **Stability:** There are a variety of conditions such as climate and skin integrity that can sometimes prevent other types of biometric hardware from reliably enrolling and identifying a person. Extensive testing and analysis of iris recognition by NIST determined that no consistent change occurs in the distinguishing texture of irises for at least a decade, rendering the modality a strong biometric because of its stability and uniqueness. [v]

- **Speed**: Iris technology is fast because it is designed to deliver one-to-many (1:N) searching of large databases in real time. Iris biometrics is widely considered by many in the industry to be the fastest and one of the most accurate biometric modalities.

- **Scalable:** Iris data templates require very small storage per iris compared to other biometric modalities. Without affecting performance accuracy, very large databases can be managed and quickly searched with iris technology.

- **Non-Invasive:** During the imaging and iris authentication process, no bright lights or lasers are used. Contact lenses or sunglasses don't create any impact during the identification process and no physical contact is required from the end user.

Major factors that affect iris recognition accuracy:

- **Spoofing:** Javier Galbally revealed that it's possible to spoof a biometric iris scanning system[vi] using synthetic images derived from real irises. The tests were carried out against a commercial system and the synthetic images were produced using a genetic algorithm.

- **Alcohol -** Alcohol consumption causes recognition degradation as the pupil dilates/constricts, causing deformation in the iris pattern.

- **Form Factor -** Some iris cameras do not have a mechanism to automatically locate a subject's face, and can therefore be cumbersome for multiple people of different heights to use in succession.

- **Price** – As the technology has continued to evolve, iris camera pricing has lowered significantly. However, overhead iris-based authentication systems and self-contained kiosks designed for in-motion identification can be quite expensive.

Example of iris recognition in a large-scale biometric identification management deployment:

Cairo Amman Bank (CAB), has deployed over 500 iris cameras and enrolled more than 100,000 retail banking customers.

Facial Recognition

Facial recognition uses the inherent physiological features of the human face for identity recognition. These biometric systems first recognize that a human face has been detected and then utilize algorithms to extract unique feature data from the facial image. These algorithms can measure certain focal points, such as the distance between the eyes and the width of the nose, from a two or three dimensional perspective. Three dimensional systems are considered to be more accurate but require specialized cameras to capture the face image and can be slower in processing time.

Here is a list of positive characteristics that define facial recognition biometrics as a viable modality for individual identification:

- **Accuracy:** Under ideal conditions, facial recognition can achieve accuracy rates of up to 99%[vii]. However, identifying individuals in uncontrolled environments still presents a challenge for facial recognition reliability.
- **Non-invasive:** During the imaging, enrollment, and identification process, a high resolution digital photograph is all that is needed rendering this modality hygienic and non-invasive.
- **Usability:** Unlike fingerprint biometrics, facial recognition does not rely on quality skin integrity for use.
- **Acceptability:** The photograph (facial image) is generally accepted in most cultures.
- **Universality:** Many countries have a legacy database of facial images captured as part of the digitized production of passport photographs or driving license which can be encoded into facial templates and verified against for identity comparison purposes.
- **Familiarity:** Human verification from facial recognition against a photograph/person is relatively simple and a familiar process for border control authorities.

Major factors that affect iris recognition accuracy:

- **Privacy:** Facial recognition technology can provide benefits for consumers, if they are willing to sacrifice some privacy.
- **Reliability:** In certain cases such as uncontrolled environments and differentiating between twins, facial recognition might not be a suitable choice.
- **Vulnerability:** Facial recognition technology is perhaps the most vulnerable modality to identity theft as most of our photos are publicly available throughout the internet on social or professional networks, such as Facebook, Twitter or LinkedIn.

- **Feasibility:** Facial Recognition systems often acquire poor facial images in real-world environments such as airports or anywhere with low or diffused light.

Example of facial recognition in a large scale biometric identification management deployment:

Several UK airports use facial recognition systems to compare a traveler's face to the photograph recorded on the 'chip' in their epassport.

Despite the potential upsides of using any of these biometric modalities for individual identification, there are also inherent risks to relying on a unimodal approach. For example:

- **Spoofing:** Unimodal biometric systems raise the potential risk of spoofing or forgery.
- **Environment:** Since the effectiveness and accuracy of biometric systems are directly related to the ability to capture clean enrollment templates and subsequent scans, deployments that rely on a single biometric modality run the risk of receiving data that cannot be understood or interpreted correctly, perhaps due to environmental conditions. For example, the ability to capture a quality fingerprint image is often directly related to the quality of the environment in which is it captured or to user demographics.
- **Non-universality:** Biometric deployments that rely on a single modality run the risk that the captured biometric characteristic will not be applicable to an entire population. For example, low skin integrity and the subsequent inability to enroll or be accurately identified are often cited as a major drawback of fingerprint biometrics.

Examples of Existing Multimodal Biometric Identification Management Deployments

One of the primary benefits of using multimodal biometric systems is that by using multiple forms of biometrics, a system can retain a high threshold recognition setting and the system administrator can decide the level of security needed. For high security deployments, the use of up to three biometric identifiers may be needed and for lower security environments, only two modalities may be needed. In addition, the use of two or more biometric modalities significantly reduces the risk of admitting an impostor.

Unimodal biometric systems such as fingerprint, facial recognition, and voice biometrics are especially susceptible to problems like noisy data, non-universality, and spoofing, leading to high FARs and FRRs, limited discrimination capability, and a lack of permanence. Multimodal biometric systems have proven to be more reliable due to the fact that deployments which use two or more independent biometrics that meet high performance requirements can counteract many of the problems of unimodal systems described above. Multimodal biometric systems are also a serious deterrent to spoofing because it is

next to impossible to spoof multiple biometric traits and a system can be set up to request an individual to present random traits that can only be executed by a live person.

Multimodal biometric deployments are often driven by various factors such as: risk and viability of spoofing, universal enrollment requirements, accuracy/integrity requirements, suitability for the environment, and transaction time flexibility.

The utility of multimodal biometric systems has never been more readily apparent than in actual deployments that we can examine to gauge its effectiveness:

- **India's UID Program:** Launched in 2010, India's unique ID program (UIDAI) marks the largest and most ambitious biometric identification management project in history as they attempt to capture the fingerprints, iris, facial images, and demographic data of India's 1.2 billion citizens. The biometric modalities were chosen to make sure that there was no doubt that each citizen would be seen as unique though their biometric signature. Since both fingerprints and irises are being captured in India, high levels of accuracy are being achieved in enrolling residents demonstrated by a reported False Negative Identification Rate (FNIR) of the UIDAI system to be as low as 0.035%. This implies that 99.965% of all duplicates submitted to the biometric de-duplication system are correctly caught by the system as duplicates. As of the end of January, 2014 the Indian government has completed issuing 560 million unique ID numbers through the UID program.[viii]

- **United States Military:** The U.S. military has used multimodal biometrics including finger, face and iris to identify enemy combatants so there are no mistakes in identification. Considering the importance of positively identifying and capturing terrorists, the use of a multimodal biometric identification system is a clear investment to maximize accuracy for the sake of international security.

- **Mexico's RENAPO:** The country of Mexico's Registro Nacional de Població (RENAPO) government agency uses fingerprint, iris, and facial capture project to identify 110,000,000 citizens for the Mexican government population registry.

In each of these deployment scenarios, the purposeful use of multimodal biometric systems are helping to achieve record levels of identification accuracy and are a bulwark against potential identity spoofing or forgery. They are also instilling faith and confidence in system performance.

While these are only three examples of multimodal biometric identification systems, there are many other cases where governments want to be sure of a person's identity since entitlement and subsidy programs such as food rations, voting, driver's licenses, border control, prisoner management, etc. are all tied to making sure that the right person is accurately identified. Another example of multimodal biometric systems used in the field is that of the US Customs and Border Protection Organization, which had previously only used two fingerprints to identify individuals coming into the US, but are now using 10 fingerprints, a photo, and are currently implementing pilot programs to add the iris biometric data to their IDENT database.

Selecting Biometric Modalities for Multimodal Deployments

The importance of incorporating multimodal biometric identification systems for large-scale deployments cannot be overstated for its ability to identify duplicates, ensure the highest level of identity accuracy, and guard against spoofing or forgery. Congruent with the reality that multimodal biometric identification systems are almost mandatory in modern deployments is the importance of selecting the appropriate biometric modalities that will be used within the system. With the proliferation of biometric modality choices on the market, which ones are most suitable and should be used in combination for individual identification? The answer is: it depends on the unique needs of the end user, budget, internal and external support infrastructure, and public perception/acceptance of biometric technology.

No single biometric modality can meet the requirements of all applications; therefore no biometric modality is optimal under all circumstances all the time.[ix] The optimal choice of which biometric modality is the most appropriate for a particular deployment is often defined by the suitability and practicality of the modality to accurately identify an individual based on external environments. For example, in identification systems where the biometric sample input has to be compared against a large number of identities in a database, biometric systems based on physiological characteristics such as a fingerprint or iris could be more relevant than behavioral traits such as a gait or signature. In addition, ease of acquisition plays an important role to determine whether biometric samples can be acquired under different operational, environmental, and geographical conditions with sufficient quality and adequate quantities.

Flexible, Customized Multimodal Biometric Identification Systems from M2SYS Technology

One of the core missions at M2SYS Technology is to provide our end users with innovative, customized tools to effectively and efficiently manage biometric identification deployments. We have comprehensive global experience to help our customers determine not only if the use of multimodal biometrics is relevant to their own unique situation, but to also help identify which combination of biometric modalities are the most effective to ensure the highest accuracy and security of the deployments.

We provide all of the instruments to ensure the success of multimodal deployments through the innovative and progressive products and support that we offer. Here is a list of the software and hardware tools that help to differentiate our commitment to ensuring the success of your multimodal biometric identification system:

Software Tools

- **Hybrid Biometric Platform™:** Through this multimodal biometrics system, we are positioned to offer our customers any combination of fingerprint, finger vein, palm vein, iris, facial or other

forms of biometric recognition. The concept of Hybrid Biometric Platform™ is to offer the flexibility of choosing one or more biometric modalities to ensure 100% identification accuracy and the highest security possible.

- **Automated Biometric Identification System (ABIS):** M2-ABIS™ is a scalable and customizable software package that allows you to perform a wide variety of tasks for processing, editing, searching, retrieving and storing biometric templates and subject records. This system leverages our multi-modal platform capability to combine fingerprint identification with an iris or facial recognition modality.

Hardware Tools

- **M2-FuseID™:** This is a fused biometric device that simultaneously captures both fingerprint and finger vein images with the single touch of a finger. M2SYS incorporated state-of-the-art technology to combine two sensors into a single unit, creating this innovative hybrid biometric scanner. The M2-FuseID™ is the only biometric fused device that can perform 1:N server-side matching for both fingerprint and finger vein templates and is designed to read 100% of end users, eliminating limitations of relying on either modality alone.
- **M2-S™, M2-EasyScan™, M2-TenPrint™, M2-TwoPrint™, M2-B™ Fingerprint Readers:** We offer a wide variety of durable, ergonomic, and affordable fingerprint readers designed for use in high-throughput settings and built to last. Each fingerprint reader comes with a unique set of features and benefits specifically tailored to meet the needs of your deployment environment.
- **M2-PalmVein™ Reader:** Using near-infrared light to create a "vein map" of an end users' palm, this vascular biometric reader works well in 1:1 verification or 1:Few identification projects. In environments where skin integrity may inhibit the use of fingerprints, palm vein biometric readers can serve as a viable alternative.
- **M2-FingerVein™ Reader:** This vascular biometric reader also uses near infrared light to map vein patterns in the finger for individual identification. Finger vein authentication is extremely robust, demonstrating a unique ability to easily cope with fingerprint limitations such as sweaty, dry, or aged fingers.
- **M2-DualEye™ Iris Camera:** Ideal for environments that require the utmost accuracy, a high-level of security, fast authentication, and a contactless experience, this iris camera quickly processes dual eye image acquisition, and encoding of high-quality eye images.
- **RapidCheck™:** A multimodal mobile biometric device capable of capturing FBI quality 10-print patterns, dual iris scans, ICAO standard facial images and data from contact and contactless smart cards. This device wirelessly tethers to smartphones/tablets and is ideal for use in law-enforcement, military, border control, Navy, Coast Guard, and counter-terrorism units to identify and verify subject identities in the field.

Conclusion

The importance of implementing multimodal biometric systems for large-scale deployments cannot be understated in the context of achieving the highest level of accuracy and security. When relying on a unimodal system:

- There is an increased risk that a deployment environment could be subject to imperfect biometric acquisition conditions.
- Individuals may not be able to provide a particular biometric trait.
- Diminished FAR and FRR rates can affect system accuracy.
- The risk of spoofing is increased, especially in the case of behavioral biometric characteristics such as voice or signature.

Investing in multimodal biometric identification systems lowers these risks significantly by utilizing more than one information source to provide a greater level of assurance for enrollment and identifications. As multimodal biometric systems use more than one biometric trait, each of those traits can offer additional evidence about the authenticity of any identity claim. For example, the fingerprints of two persons of the same family (or coincidentally of two different persons) can be similar. In this scenario, a unimodal biometric system based only on fingerprint pattern analysis may result in false recognition. If the same biometric system also includes iris biometrics, recognition rates would significantly increase.

Biometric systems use scores (also called weights) to express the similarity between biometric templates. The higher the score, the higher the similarity is between them. An identity is confirmed only if the score is higher than a certain threshold. In theory, authorized user scores (scores of patterns from persons known by the system) should always be higher than the scores of impostors. If this was true, a single threshold, that separates the two groups of scores, could be used to differ between clients and impostors. This unfortunately is not the reality for real world biometric systems. In some cases, impostor patterns can generate scores that are higher than the threshold. For this reason when the classification threshold is chosen, some classification errors may occur. For example, you may configure the threshold with a high setting, which will result in a higher FAR. On the other hand, the authorized user patterns with scores lower than the threshold are also falsely rejected, so the tradeoff is a higher FRR. The opposite scenario would be to configure a low threshold that ensures no client patterns are falsely rejected. However, this would then allow a certain percentage of impostor patterns to be falsely accepted. If you choose the threshold somewhere between those two points, both false rejections and rejections false acceptances occur. This creates an environment which is obviously not ideal for high-security installations.

The key to multimodal biometrics is the fusion of various biometric modality data at the feature extraction, matching score, or decision levels.[x] Consider some of the fusion testing statistics reported by NIST to show how significantly accuracy improves in a multimodal biometrics system comparing fingerprinting as a standalone modality and then fingerprint combined with iris:

"Two different multimodal fusion systems are tested on this dataset each with a different Fingerprint feature extractor (detailed above) and same Iris feature extractor. The raw results from both are compared with the corresponding raw individual unimodal scores. This comparison is done to illustrate the fact that the proposed system provides improved results as compared to the results from the individual constituting unimodal system. Table provides the results for this experiment. The results show a marked improvement in the accuracy as well as a considerable decrease in the Equal Error Rate."[xi]

	Correct Match	False Accept	False Reject	Incorrect Match
System 1 with Chain code based Minutiae Extractor				
Fingerprint	60	15	15	10
Iris	65	13	13	9
Fused	72	9	9	10
System 2 with Binarization based Minutiae Extractor				
Fingerprint	64	13	13	10
Iris	65	13	13	9
Fused	75	8	8	9

By using more than one means of biometric identification, the multimodal biometric identifier can minimize FAR or FRR rates. The system administrator can then decide the level of security they require. For a high-security site, they might require multiple biometric identifiers to recognize the person or for a lower security site, only one. With a multimodal methodology, system accuracy and user enrollment rates are significantly higher than a unimodal approach.

End Notes

[i] Alan Gelb and Julia Clark, *Identification for Development: The Biometrics Revolution,* The Center for Global Economic Development http://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf (January 28, 2013).

[ii] ID Newswire, Trends in Personal Identification and Biometrics, *Biometric Enrollment Errors A Problem, But Not Fatal,* National Institute of Standards & Technology (July 9, 2003).
[iii] Adam Vrankulj, *Chaos Computer Club claims Touch ID fake fingerprint spoof,* BiometricUpdate.com (September 23, 2013).
[iv] Lee Hutchinson, *Brazilian docs fool biometric scanners with bag full of fake fingers*, Ars Technica, (March 13, 2013).
[v] National Institute of Standards and Technology, *NIST Study Advances Use of Iris Images as a Long-Term Form of Identification,* (August 20, 2013).
[vi] Blackhat USA 2012, *From the IrisCode to the Iris: A New Vulberability of Iris Recognition Systems,* (July 25, 2012).
[vii] PBS, *The Limits of Facial Recognition,* NovaNext (April 26, 2013).
[viii] Medha Basu, *India's National ID Project Nears 600 Million Target,* Asia Pacific Futuregov (January 28, 2014).
[ix] IEEE Biometrics, *Module 2: Biometric Modalities,* The IEEE Biometrics Council, (2012).
[x] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, (2003).

[xi] Robert Snelick, Umut Uludag, Alan Mink, Michael Indovina and Anil Jain, *Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems,* (March 2005).