Facial Recognition Countermeasures and The Future of the CIA

By Lance Winslow - 2002

Presently Universities and Private Enterprise are working to build more robust "Facial Recognition Technologies" due to the Homeland Security Funding for such research this field continues to grow. Anti-Terrorist efforts are a worldwide goal, so we are sharing this technologies with allies for use in their countries. These new technologies will also end up in the hands of our enemies or perhaps future enemies. Such hostile nations towards the US with such recognition software may prevent our clandestine spy efforts abroad. Getting our assets and spies in country can be difficult and history has shown that it takes much secrecy and effort to get in, get information and get out without detection.

Hostile nations will consider our spy efforts in those countries as International Terrorists, much the same way as we see their spies who come to our country if and when they are caught. Such Facial Recognition and software equipment will therefore be readily deployed to detect our infiltration efforts and exploitation of their systems. Since we have now invented this technology we need to find a way to beat it when, it is used against us by our enemy.

The United States allows citizens from other countries to attend our Universities, which do intensive research in these areas "human recognition" and that information is being duplicated in their countries of origin. We will explain the most common types of human recognition in this report. Currently Facial Recognition Technologies are not used very often since they are far from perfect and are probably not the best identification device, however the technology is rapidly becoming very viable. Soon such recognition software will be more than adequate for identifying those people we wish to catch and keep out of our sensitive areas.

The CIA has a terrible leak problem with information, the FBI not much better. The FBI has lost some 2000 computer laptops, is now sharing information and data bases with other law enforcement and we all remember the Spy Sex Scandals recently. The CIA also cannot keep a secret, nor can those in Washington who are in the know, as we recently found out with the wife of a Senator being written about in a major newspaper.

Then of course there are sleeper sells, deep cover operatives and hackers all waiting in the shadows and gathering information. Once a database of operatives has been exploited or a cover of a clandestine agent is discovered their face will be put into data bases of foreign countries to catch them using such facial recognition and other human recognition software and equipment. Today the problem is not wide spread but the technological advances of mankind are not exclusive to the US alone. So what exactly is Facial Recognition Software and how does it work?

http://people.howstuffworks.com/facial-recognition.htm

So far the companies promoting their technologies in the Facial Recognition Software and Equipment sector have found killer applications. After 9-11 there has been much money flow for projects, which can help identify International Terrorists. The technology was further spurred on by such big screen movies as "Minority Report" as security professionals decided, wow, now if we had that technology we could prevent an International Terrorist act. Of course free rights advocates cringed and thought of it as a wake up call to what big brother might be thinking about next. Link Discussing Thoughts on "Minority Report" – Movie:

http://artificialintelligence.ai-depot.com/Future/568.html

The TSA has approved Facial Recognition Systems and technologies for several Airport Terminals on a trail basis.

Overview of Progress of the TSA Security Screening:

http://www.tsa.gov/public/display?theme=44...9000519800cf9c8

Large Stadiums have also used Facial Recognition Systems to scan individual faces as they walk into the events such as Baseball, Football, Air shows, Shuttle Launch Spectator Areas and even at NASCAR races. As this technology continues to achieve a higher percentage of positive recognition it will be more widely used. We know this will be the natural progression of facial recognition systems because we have watched the growth and refining of other types of recognition software, which are now widely used and considered common practice. Technologies like those used in document scanning, OCR, and those used in Speech Recognition. These are now commonplace business tools used worldwide. Security Professionals are now taking these to the next step and finding ways to use these technologies in Homeland Security, Intelligence and law enforcement. Facial Recognition will also follow this type of growth curb in the next 4-5 years.

Geo Spatial technologies have also gotten better with aerial satellite recognition, able to quickly point out a new building, missile silo, change in landscape from an Earth Event or a truck convoy anomaly in an area where it rarely occurs. These technologies are also used in national security within our borders and law enforcement to a large degree, when prior they were used for only war planning, intelligence gathering and watching mother earth.

It stands to reason then that as similar technologies in recognition get better and better that human recognition technologies such as "human gait recognition" and "human eye recognition" will also become more reliable. Facial Recognition is within this class of rapidly coming of age human recognition technologies. Our Intelligence Communities including the clandestine departments of the CIA will need to figure out how to protect their agents and fool these systems long enough to get in safely, collect human intelligence and get out undetected.

In prior periods CIA clandestine operations use an array of various methods to conceal identity of agents, operatives and assets. They often used movie industry tricks like make-up, eyeglasses, fake mustaches, and wigs. They put rocks in their shoes to cause a walk which stood out and which caused observers after the fact to remember the limp rather than the face or tell tale features, which might easily get them caught. (Rule Number One: "Don't Get Caught"). Unfortunately these techniques in the Spy Book Manuals may not work, as human recognition software gets better.

The human facial recognition software measures distances between features and comes up with percentages of identical matches to these numbers. So even if half your face is covered the other half of your face might give you away. Artificial mustaches, fake wigs or mustaches will not work, because they do not change the distances between points on the face, nor are they thick enough to change to stop the scanning if any sort of frequency bounce is being used in conjunction with the system. Any attempt to thicken these fake cover objects will show anomalies in one's heat signature, thus as systems get smarter and start incorporating combined human recognition technologies such as "human gait", "heat scanning" and "human eye-recognition" with advanced Facial Recognition Technologies it will be extremely difficult to fool them.

The fact that systems are unlikely to be fooled is a deterrent which most likely will cause those who are known to be problematic or have been discovered as International Terrorists to look elsewhere for targets and the participants of large events will be that much safer. To fool such systems one will need extremely sophisticated technologies or even complete plastic surgery makeovers or face lifts. This will cause the facial recognition software to further innovate and some young scientists, researcher or entrepreneur will figure out a way to teach these facial recognition systems to look for anomalies in scar tissue.

Scar tissue is easy to spot, expect in the cases of the world's best plastic surgeons. So unless one is using the world's best dermatologist along with a top notched plastic surgeons they will not be able to fool the future facial recognition systems. This will limit the number of recruits to the nameless clandestine CIA spy rosters, because those entering will not only have to ditch their identity like the do in the CIA or French Foreign Legion, but also have to kiss their face good bye, because any photo ever taken in their life with their name next too it can get them caught and killed and all they will have to show for it is another star on the wall. Perhaps ugly people might want free facial makeovers and this might entice them to join the CIA's clandestine Spy division?

Is there any easy solution to this dilemma for our CIA or Intelligence Community? Is there a cheaper way around this? Well the answer is yes and no. Long term, the answer is no, because these technologies will be coming of age and become better and more sophisticated. Short term the answer is yes, there are ways to fool the system now with the present technology, if you understand how the facial recognition software works. As each system is fooled those behind their technologies will work through ways to close holes in the systems. We can see this type of evolution in IT Networks as hackers exploit holes in the computer systems. IT Professionals attempt to create patchware to close those security-breached areas in their systems to prevent further attacks and then the hackers find new holes and exploit those. This analogy works well because it is quite similar, only difference is one is the real world and one is the virtual world. Both worlds matter and they are inherently interconnected. In the future it will be quite obvious just how closely connected they really are.

The movie the "Matrix" might be worth viewing as it seems to help us visualize the world of one's and zero's and the real world we see everyday. As infiltrators try to sneak into facilities, transportation hubs and airports, security professionals will use all technologies available to stop them. Human Recognition and specifically human facial recognition will follow similar paths of evolution, so eventually the systems will not be able to be fooled. Those who count out facial recognition now in it's infancy will eat crow later, just like the nay sayers of previous recognition technologies are looking rather silly today.

One way to close holes that presently exist as these technologies move towards reaching their full potential yet leave us somewhat underwhelmed is to have combined technologies to screen using many different types of human recognition systems, each looking to find anomalies. You may be able to fool some of the technologies, but you would have to get pretty creative to fool them all. This is part of the strategy at the TSA for airport passenger screening. If any anomalies come up such as metal detector goes off, your ID is suspect, you look or act guilty, you have previously traveled to many states which are known to be problematic, etc then you are taken to another level of scrutiny.

The system is not full proof, but it seems to work pretty well, although currently does often impede on personal rights issues. It often judges incorrectly due to programmed red flag anomaly scenarios, case in point would be Teddy Kennedy ending up on a "no fly" watch list. Anyone who has been pulled aside for a further scrutiny or strip search who is merely just a traveling individual can vouch for this. The systems at airports seem to be working well so far and as these new human recognition technologies are added only well financed and equipped people will slip through provided they have some sort of inside connection. Once computer systems are made more robust, human error will be the biggest problem.

It is for this reason that if we truly wish to protect ourselves we must more carefully scrutinize those on the inside at all levels. For instance security guards, police officers, facility maintenance employees, etc. A human recognition system cannot protect you if the infiltrator is merely directed around it. You may recall the shooting where a politician allowed his guest to circumvent the metal detector at a government building?

Now then generally the answer is 'no' there is not a cheap way around all these technologies, but there are inexpensive ways around a few of them. However until these combined technologies, sensors, screening and recognition devices reach their full potential and used together to prevent exploitation of the weaknesses in any one of them, they can be fooled. Many of those inside security audits have shown that one could sneak on a device of some type onto an aircraft or one could get through a border check point. Soon as the systems close the holes, become more robust and are used in combination, it will be hard pressed to beat them.

Currently our clandestine spies can infiltrate the facial recognition systems by using under skin simple devices or strategies, so short term (next 4-5 years) the answer maybe "Yes". For instance plastic Halloween Dracula Teeth, type teeth covers will cause protruding of the facial region surrounding the mouth, simple, inexpensive and it will cause the numeric distance between facial features off.

Chewing Tobacco is another simple easily deployed strategy to fool facial recognition systems since it will cause lower jaw distance to be slightly off the measurements. If you have ever noticed someone was chewing tobacco, you might have thought something was not right, but did not know what it is until they spit.

Someone going into a baseball game while chewing tobacco would not be an unnatural event. It would not be out of place at any sporting event, truck weight station, border crossing, rodeo, outdoor celebration, etc. Chewing Tobacco however would be questionable at an airport and create an anomaly. With practice, those who often chew tobacco in small amounts can talk and chew without detection although even chewing tobacco does have an odor.

So a combined recognition systems for detection could be "human plume technologies" to prevent this from not being detected, thus could red flag that anomaly and help you catch the infiltrator. Since the facial recognition software measures all portions of the face for eyebrows and eye regions, small "Botox" injections can radically change the distances between features in that region of the face.

Nose plugs used by used by some emergency first responders in a slightly smaller form will cause the nose to look different to a computer and throw off the readings of facial recognition software for that central region of the face. These of course are cheap and inexpensive ways to slip in and out of choke points, which have facial recognition software and systems deployed. Eventually the innovators of such technology will close the gaps on such clandestine disguise tactics and methods and prevent the easy fooling of these systems. In the United States we have the homeland security dollars already deployed and entrepreneurs across the land have taken up the challenge to build a foolproof system, they have come a long way, but still have a ways to go.

Since International Terrorism is a worldwide problem these technologies will be exported to other nations, which also have similar nuisances or threats with International Terrorism. Rogue nations may also deploy these technologies along with regimes, which wish to control the freedom of their subjects and promote their own Dictatorship Style Leadership. We will be faced with infiltrating these countries and their borders to gain access to information, human intelligence, future hostile intentions and enforcement of international crime, drug shipments, human sex trafficking and military WMD build up.

Our CIA Clandestine units need to have simple ways to fool the newest infant human recognition technologies and commit to a 4-5 year plan to upgrade tactics, ideas and technologies through intensive research to stay ahead of the rapidly increasing use of surveillance robotics, imaging, recognition software and early detection security technologies. Exploitation methods and strategies should be incorporated into our own security technologies on key infrastructure facilities to prevent these systems from being infiltrated.