Physical Security in a Networked World:

Video Analytics, Video Surveillance, and You.

Joshua Marpet

Jmarpet@datadevastation.com

Video Analytics is a component of many advanced video surveillance systems. It includes such well known features as License Plate Recognition and Facial Recognition. Does it actually work? How well does it work? How can you hack it? How can you access it?

Video surveillance is becoming more and more prevalent in our world, with some estimates showing that walking down Bourbon Street in New Orleans gets you photographed or videoed 3 times for every step you take. Are these systems legal? Who can see that video, or publish it? Is there a way to take advantage of the huge amount of video cameras?

You'll find out.

Video Surveillance

Every time you walk down the street these days, the likelihood is strong that you are being recorded. Not because you are a movie star, or even that pretty[1], but simply because cameras are so prevalent in today's society. ATM's, gas station, Stop-N-Rob's, they all have cameras in them, that capture video of customers, products, and probably the sidewalk outside, and you walking along.

Is it legal? Short answer is yes.[2] Video surveillance is legal in most instances, so long as no one is using a zoom lens on your bedroom window. Specifically zooming in, using a telephoto lens, or aiming solely at your bedroom window, is prohibited under peeping tom laws, and commons sense. However, if my house faces another house, and I put a camera on the front of my house to capture

[1] Regardless of what your mother says.

[2] Please note that this is VIDEO only. Audio surveillance is a whole other topic. The laws there are radically different, since they are based on the old wiretapping laws. Again, Video only.

anyone coming up the sidewalk, it will probably capture images of your house. And that's acceptable, since it wasn't put there to specifically capture your bedroom window, or invade your privacy.

Does it invade your privacy, in ways you might not have thought of? Absolutely. It records everyone coming in and out of your house, for starters. But only your neighbors have access to that video. Wrong. Any idiot (lawyer) with a subpoena can get a copy of the video, assuming your neighbors store it.

So video can be taken of you at any time, at almost any place, so long as you are outside. Can this help you? Assuming you need an alibi for the police, yes. Your lawyer can subpoena the footage to help you. But do it fast. Most home or small business systems only store video for 3 days. Some store for 15, and a few store it for 30. The difference is in the storage space vs. Resolution and frame rate.

Simple way to figure out storage:

Frame rate baseline: 30fps
Compression Scheme: Mpeg-4
Resolution: 4 cif

At baseline, one camera with a reasonable amount of motion will be sending 4-6 megabytes of data per second down the wire to be stored.

There are multiple different compression schemas. The primary 3 are MJPEG, Mpeg-4, and H.264. H.264 is the most efficient for video Surveillance, and it is also the newest. It is being adopted now by many manufacturers, and I actually spent the last few months replacing MPEG-4 encoders with H.264 encoders at a large metropolitan police department's surveillance site.

Most smaller locations will not have the storage for more than a few days.

Video Surveillance Seizure Lessons:

Lesson 1: When involved in an incident likely to go to court, get out there with a lawyer within 3 days to collect video to support your side of the lawsuit.

Check:

Storefronts

Gas Stations

Police stations (for cameras scattered around town)

Businesses

Office Buildings

Houses

Taxi companies – Most taxis nowadays have dash cams, and a driver can manually trigger them.[3]

Any witnesses with cellphones

Any witnesses with digital cameras/camcorders

Traffic cams

Red light cams

Lesson 2:

Get a court order/subpeona for the footage. This gives a business or person legal liability mitigation.

[3] Admittedly, this would only work if one drove by, and the driver was nice enough to trigger it. But it never hurts to check.

Lesson 3:

Take a picture of the clock on the video system, with a clock that is atomic synchronized.[4]

This allows the timing of the video to be determined, i.e. if the video system is 5 minutes off, then your version of the accident might be suspect without that picture.

Lesson 4:

Make sure you get a copy of the player program. Most video systems have proprietary player programs, or can export to AVI. That's fine, but the proprietary player can often watermark, or "prove" to the court that it hasn't been tampered with.[5] It looks better in court, essentially.

Lesson 5:

The CSI Effect is real. The CSI Science is not, mostly.

The CSI Effect - "Enhance, Enhance, Magnify, Enhance"

People believe what they see on TV. The amount of effort placed into TV cases would raise your taxes about 1000% if it were done for every case in real life. There have been cases where a person brought a fiber in, and demanded to know whose credit card was used to buy it.

The CSI Effect in web cartoons

CSI Science – Images can be magnified. They can not be magnified past the limits of the information the image contains. On film, it goes grainy. In digital video, it goes pixelated. Interpolation, edge sharpening, noise reduction, etc only goes so far.

[4] Many wristwatches are atomic synchronized these days. This should be a trivial requirement.

[5] It's actually fairly trivial to tamper with the footage, but that will be addressed in the Video Analytics section.

Video Analytics

What is Video Analytics?

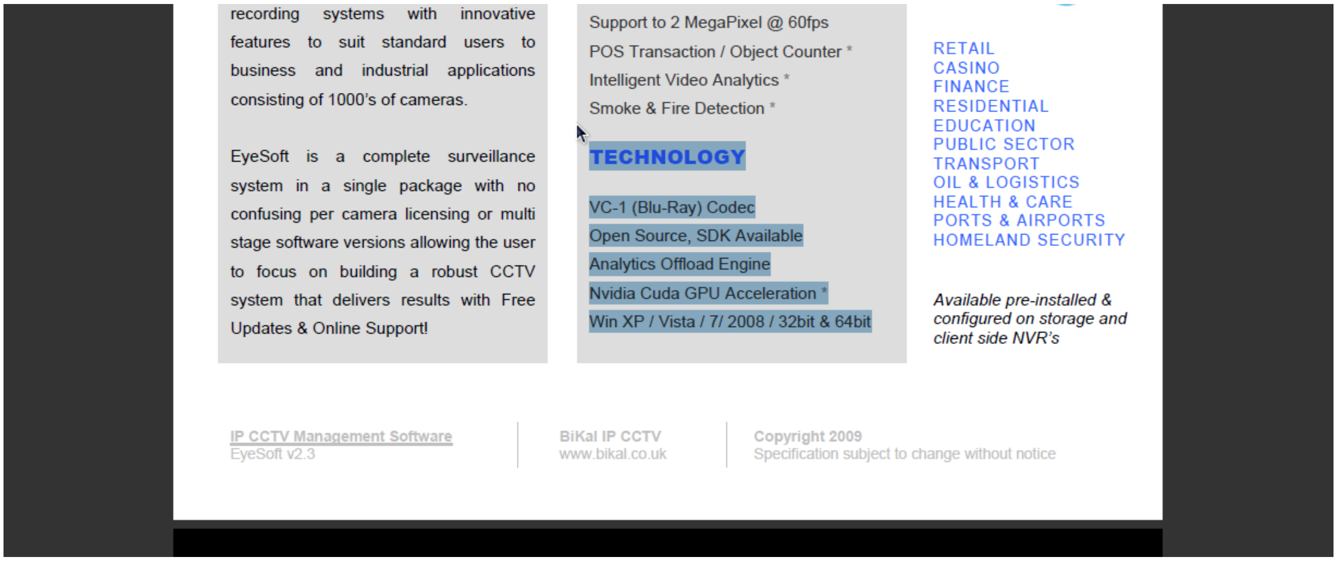
Interpretation of a video stream, done either in real time, or performed on a recorded stream.

There are different types of Video Analytics, including:

- Motion Detection
- Facial Recognition
- License Plate Recognition
- Package Leave Behind
- Line Crossing (“Trip-Wire Detection”)
- People Counting
- Incident Alerting
- Motion/Trajectory Tracking
- Currency Checking
- Smoke and Fire Alerting

There are open source video analytics programs, including:

Kinovea - http://www.kinovea.org/en/ - While primarily used for sports, this software is useful for watching how people or vehicles move (trajectory or Motion Tracking). Being able to magnify scenes, and synchronize multiple video scenes are also great features.



recording systems with innovative features to suit standard users to business and industrial applications consisting of 1000's of cameras.

EyeSoft is a complete surveillance system in a single package with no confusing per camera licensing or multi stage software versions allowing the user to focus on building a robust CCTV system that delivers results with Free Updates & Online Support!

Support to 2 MegaPixel @ 60fps
POS Transaction / Object Counter *
Intelligent Video Analytics *
Smoke & Fire Detection *

TECHNOLOGY

VC-1 (Blu-Ray) Codec
Open Source, SDK Available
Analytics Offload Engine
Nvidia Cuda GPU Acceleration *
Win XP / Vista / 7/ 2008 / 32bit & 64bit

RETAIL
CASINO
FINANCE
RESIDENTIAL
EDUCATION
PUBLIC SECTOR
TRANSPORT
OIL & LOGISTICS
HEALTH & CARE
PORTS & AIRPORTS
HOMELAND SECURITY

Available pre-installed & configured on storage and client side NVR's

IP CCTV Management Software
EyeSoft v2.3

BiKal IP CCTV
www.bikal.co.uk

Copyright 2009
Specification subject to change without notice

Bikal claims in their brochure to be Open Source, even though there is no place on their website to download the source. They have been emailed to ask for the source code.

OpenCV is a group of programming routines designed to be used to with images. There are currently projects now doing iris recognition, as well as facial recognition.

http://opencv.willowgarage.com/wiki/

The Truth behind the Image

A cute section title not withstanding, there is a lot of truth about Video analytics, and a lot of horror shows.

Video Analytics works. If you take the time to set the customer expectations, budget for the time to perform proper calibration and end user training, and test it appropriately, according to the Statement of Work, Deliverable Schedule, or whatever it is called at your company.

If you don't, it will fail. That simple.

As for metrics, the problem is that most systems are proprietary, making it very hard to determine an industry wide metric to see if it works.

Anecdotally, facial recognition works about 60% of the time. It has huge amounts of false positives, and requires endless amounts of human time to check the errors.

Package Leave Behind is worthless without properly trained systems, and frankly, it's easier to have humans checking. Although the systems are getting better, this is so difficult to train, that it's not worth putting in production right now, outside of very controlled circumstances.

Trajectory tracking works very well, right out of the box. That's because, as stated earlier, simple motion detection works well already. This just adds a tracking component to the motion detection. Essentially, the machine is thinking it's playing Pong. It follows the ball, or car, or boat, in this case.

Line Crossing and People Counting does work, but don't count on it as a gospel count. Its great for approximate counts, but not exact. Hugging, swaying, walking a child over the line, among other events, will all mess with the count.

Currency Checking, being similar to License Plate Recognition (looking at a specific size picture, for specific features, in a specific and exact alignment), works rather well. It is starting to be used at casinos, and some hotels.

Incident Alerting is a new one, where the system determines if a more than usual amount of people are moving in an unexpected direction. Then the human can check and see what is going on. It works, but it has been known to be triggered by a jackpot in a casino, where everyone rushed over to see. It is also triggered by a celebrity walking by, or a pretty waitress dropping a glass.

If the common theme here is that video analytics is appropriate in certain controlled circumstances, which are carefully calibrated, monitored, and watched, then the right idea has been transmitted. Outside those controlled environments, the only video analytic products ready for the real world are License Plate Recognition, and simple motion detection.

Implementation

Video Analytics is fairly new in widespread implementation, and there are no tried and true formulas to getting it working, mostly because every piece of video analytics is totally different than any other piece. 100% successful implementation is extremely rare, for several reasons.

- Customers expect it to be a magic bullet, capable of spotting criminals and terrorists in a single bound. It's not.
- Integrators don't realize how much time and effort it takes to train the system.
- Total screwup of implementations is common.
- It's fairly sensitive technology, able to be avoided with a few simple steps.
- The consequences of adding Video Analytics to the corporate network are not foreseen.
- The consequences of adding Video Analytics to the corporate storage San are not foreseen.

The only really effective and simple Video Analytics technologies are simple motion detection, and license plate recognition. Other than those two, implementation of a successful video analytics system depends on two things, namely time and money. Simple motion detection is very useful, and widely used. It is essentially “commoditized”, and is in almost every video surveillance system. License Plate Recognition is so widely used that tow trucks now have LPR cameras on them, to find vehicles to repossess.

The reason that LPR works is that the camera is looking at a rectangle (license plate) which must be in roughly similar locations, and has very large, machine readable type on it, which by law, must be lit up at night. If the typeface was allowed to be up to the driver, it wouldn't work at all. Zapf Dingbats would take over the roads, and police wouldn't be able to find stolen cars.

Other than LPR, Video Analytics takes a staggering amount of time to calibrate, as every scene must be manually calibrated. For example, you must tell the program that the tree is an acceptable part of the scene, and then that anything else that gets left there for more than 60 seconds motionless is a left behind package, and to alert on it. Then the light changes, and the shadows change, and the system starts alerting for no visible reason. End result? Video Analytics gets turned off. Money and time wasted.

Also, all testing must be done rigorously. If testing, and that bag does not result in an alarm, that is a false negative. The bag must not be moved to accommodate the alarm system. That is not testing. That should properly be part of the calibration process.

Implementation is a huge problem with Video Analytics. If the proper time and intelligence is not used to plan this out, spectacular failure is sure to occur.

The best recommendations possible are these.

1. Have a manufacturer's representative go over the requirements with you, and sign off on them, that the Video Analytics system will perform them.
2. Use the manufacturer's rep to help with calibration and installation.
3. Have clearly defined goals for the system.
4. Use a manufacturer's demo system to show the client how the system works, and what it cannot do.
5. Train at least one person at the client how to maintain and calibrate the system, so you don't get called out to do it many many many times.
6. Demonstrate to the client, and have them sign off on the system, after that have tested it with their own people.

Video Analytic Hacking

Non-Tech Hacks

Abandoned Bag Video Analytics

Color Matching - If the bag matches the colors of the sidewalk/walk/ground, it won't get picked up. If the shadows have moved since calibration time, the bag will not get picked up. If the camera is knocked even a few degrees off its calibrated field of view, it will not alert, or alert continuously, until manually checked, and turned off.

Bad field of view – If the camera has a deep field of view, so a bag left at the back of the field of view will have people walking in front of the bag, it will not alert on the bag.

Motion Detection

Sloooow motion is possible, although the movie “Sneakers” was not a good way to train for this. Motion detection, even using a PIR, has a lower motion limit. Move slow enough, you don't get picked up.

Facial Recognition

Balloons – A photo of the person, taped to a balloon, can oftentimes get past a facial recognition system.

Disguises - Facial Recognition is not great if you cover its data points.

Line Crossing (Trip Wire)

Line crossing software has problems if you sway on the line itself, but you need to know where the specific line is.

Holding hands or hugging will also confuse the software immensely.

People Counting

Hugging works here too. It is fairly simple to simply look like one fat person, rather than 2 people, to a computer. It doesn't count legs, just blobs crossing an imaginary line.

Techie Hacks

“Loop the Video!”

It actually works. See Defcon Demo Darkreading Article

Axis - Older Axis camera models do motion detection at the camera. Remove the camera, no motion detection alarms will go off.

IP Cameras - Many IP camera models are the same as the Axis, where motion detection is present on the camera. Remove or deface the camera, destroy the motion detection capability of the system.

Hack the Gibson!

Most Video Surveillance systems are windows based. Some of them are Windows 98. Many of them are unpatched, never maintained, and would make a novice CTF player very very happy. But they are airgapped, and totally secure. In a perfect world.

Unplug an IP camera, and plug it into your laptop. Kiss your server goodbye.

But Video Analytics systems are either add-on modules to the Video Surveillance system, or Appliance based. Username and password on a web based front end? Perhaps not the best idea.

Conclusion

Video Analytics is an exciting field, with the real possibility to move many companies from closed source proprietary systems to a more open source world. Unfortunately, the mindset in video surveillance is "Sell it, walk away". With that mindset, the idea of service costs is not normal, so they must keep their code as a trade secret.

Video Analytics works, but needs to be a managed process, not simply a salable item. With a managed process that includes service, support, and training, on a long term basis, video analytics has the potential to change the entire mindset of the physical security industry. Also, considering the server space, storage, and power it requires, the IT Security Industry is already getting interested in getting some control of this monster. With that prospect, the physical security industry is becoming more and more like the IT security world.

In the near future, more and more Video Analytics applications will make it into the wild. Right now, most of them are not ready for prime time.