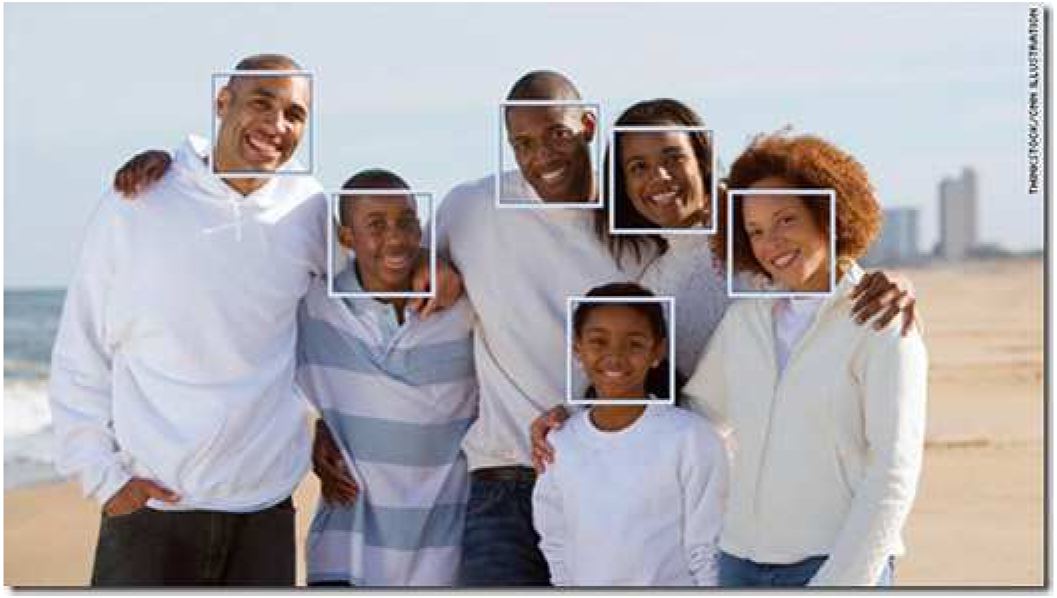
How to Hide from Machines

The perilous glamour of life under surveillance.



CV Dazzle is a response. It is a form of expressive interference that combines highly stylized makeup and hair styling with face-detection thwarting designs. CV, or computer vision, Dazzle is an updated version of the original dazzle camouflage from WWI, which was used to protect warships from submarine attacks. Like the original dazzle war paint, CV Dazzle is an unobvious style of camouflage because its eye-catching patterns and colors draw attention instead of hiding from it. As decoration, CV Dazzle can be boldly applied as hair styling or makeup, or together in combination with accessories. As camouflage, this facial markup works to protect against automated face detection and recognition systems by altering the contrast and spatial relationship of key facial features. The variations are limitless.

When disrupting face-detection it is advisable to avoid wearing makeup that enhances facial features. For example, emphasizing the darkness around the eyes with eye shadow or eyeliner would make your face more visible to face detection algorithms. Ideally, your face would become the anti-face, or inverse. In the animal kingdom, this inverse effect is known as countershading. A similar effect can be achieved by creating a partial inverse that targets key areas of the face. For example, darkening or obscuring areas that normally appear light, such as the nosebridege area or the upper cheek. Areas that vary widely, such where facial hair grows, are lower priority. Since eyeglasses are commonly worn by many people, they are not typically considered obfuscations. Results will vary. The CV Dazzle protocols were developed to thwart face detection by OpenCV, which uses the Viola Jones method. The looks shown here were also tested and validated against Facebook's PhotoTagger, Google's Picasa, and eblearn.

These videos visualize the detection process of OpenCV's face detector. The algorithm uses the Viola Jones method of calculating the integral image and then performing some calculations on all the areas defined by the black and white rectangles to analyze the differences between the dark and light regions of a face. The sub-window (in red) is scanned across the image at various scales to detect if there is a potential face within the window. If not, it continues scanning. If it passes all stages in the cascade file, it is marked with a red rectangle. But this does not yet confirm a face. In the post-processing stage all the potential faces are checked for overlaps. Typically, 2 or 3 overlapping rectangles are required to confirm a face. Loner rectangles are rejected as false-positives.

Here are several guidelines to follow when creating your own looks:

1. Avoid enhancers

They amplify key facial features.

2. Partially obscure the nosebridge area

The region where the nose, eyes, and forehead intersect is a key facial feature.

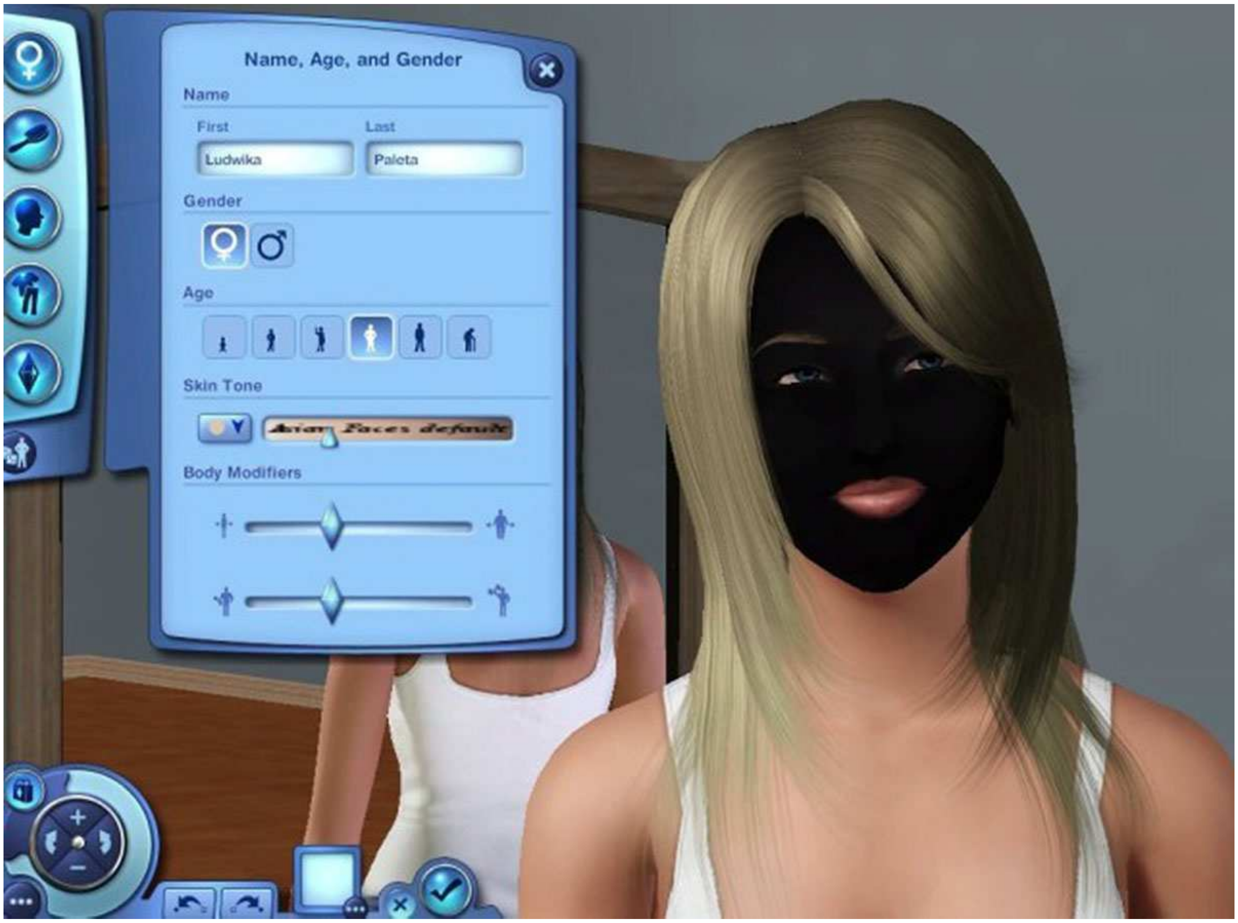
3. Partially obscure the ocular region

The position and darkness of eyes is a key facial feature.

4. Remain inconspicuous

For camouflage to function, it must not be perceived as a mask or disguise.

NB: Wearing masks or disguises can be illegal in some cities, including here in NYC.



Name, Age, and Gender

Name

First: Ludwika

Last: Paleta

Gender

Age

Skin Tone: Asian Faces default

Body Modifiers

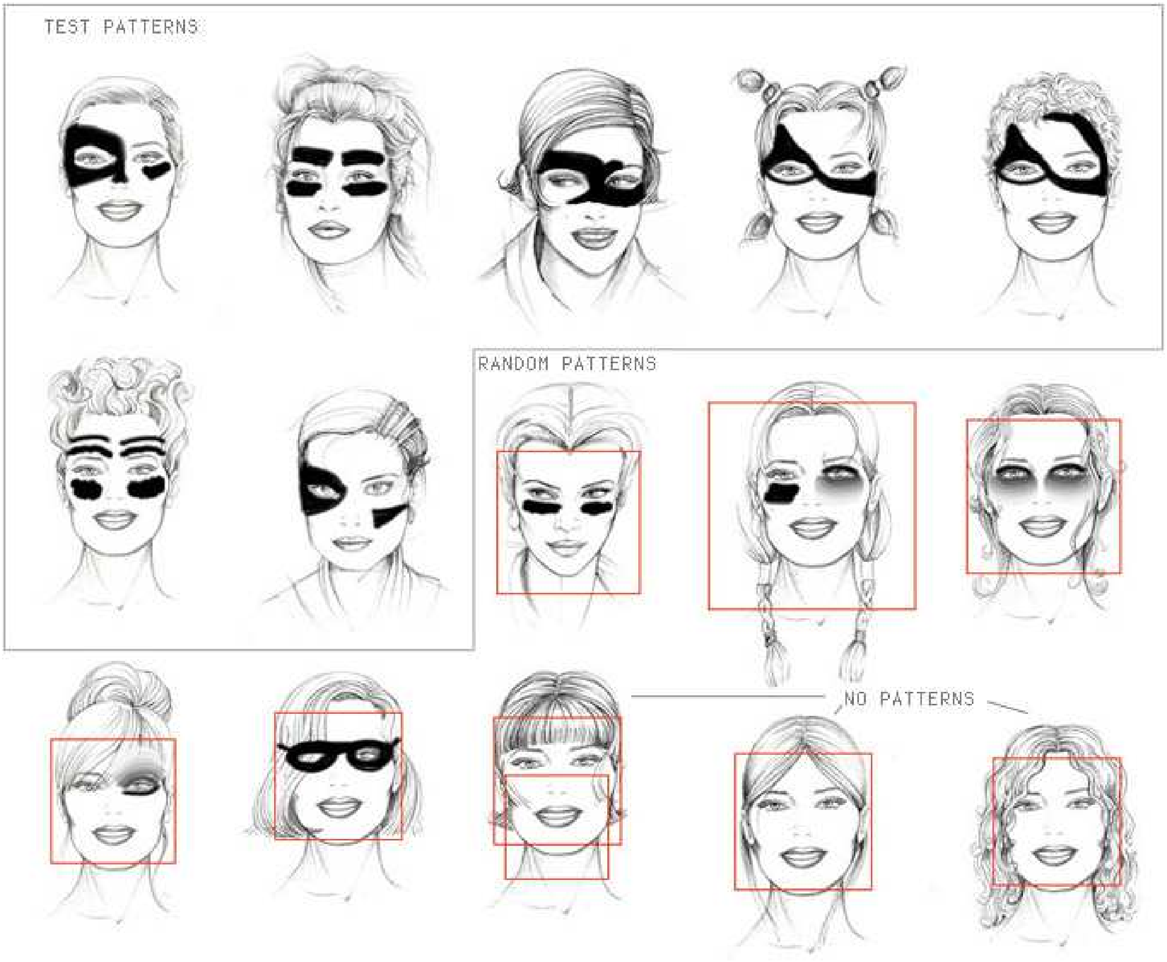
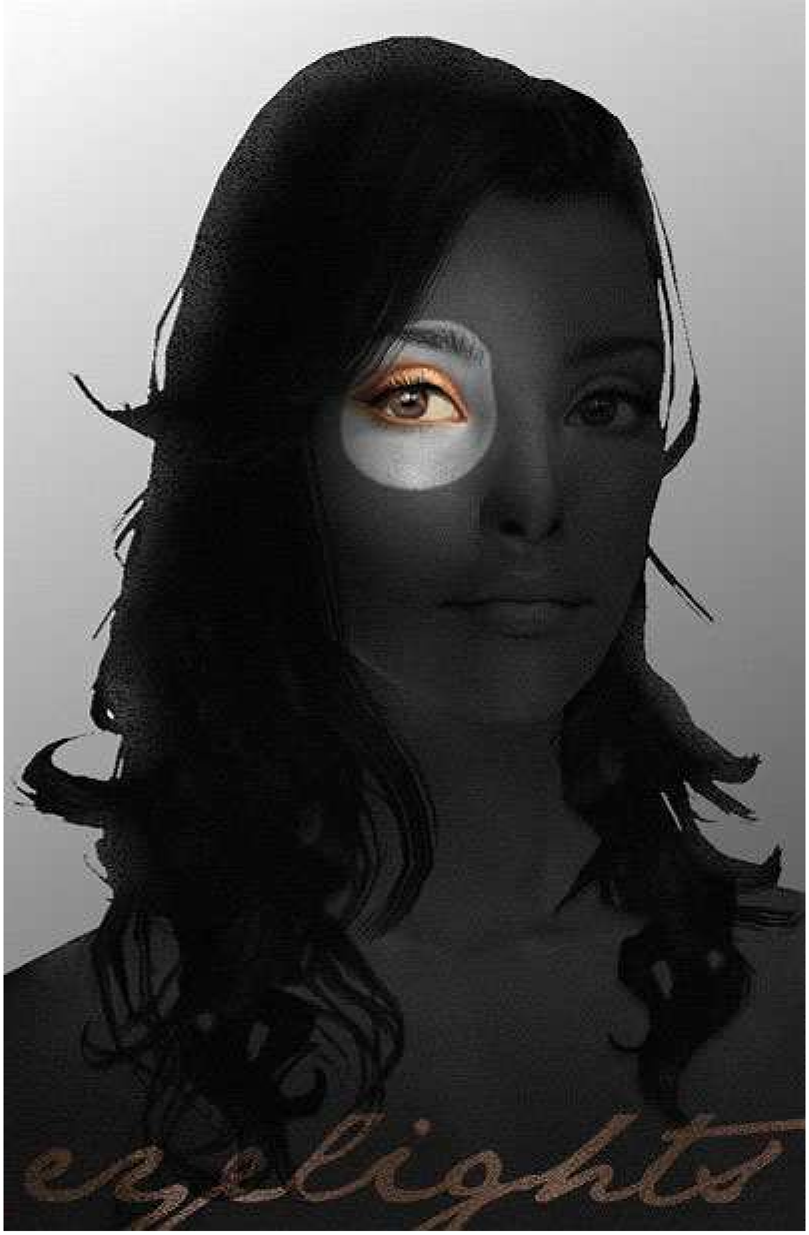
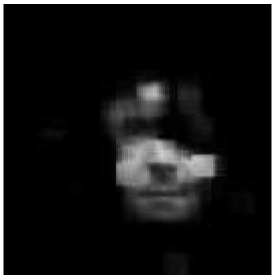
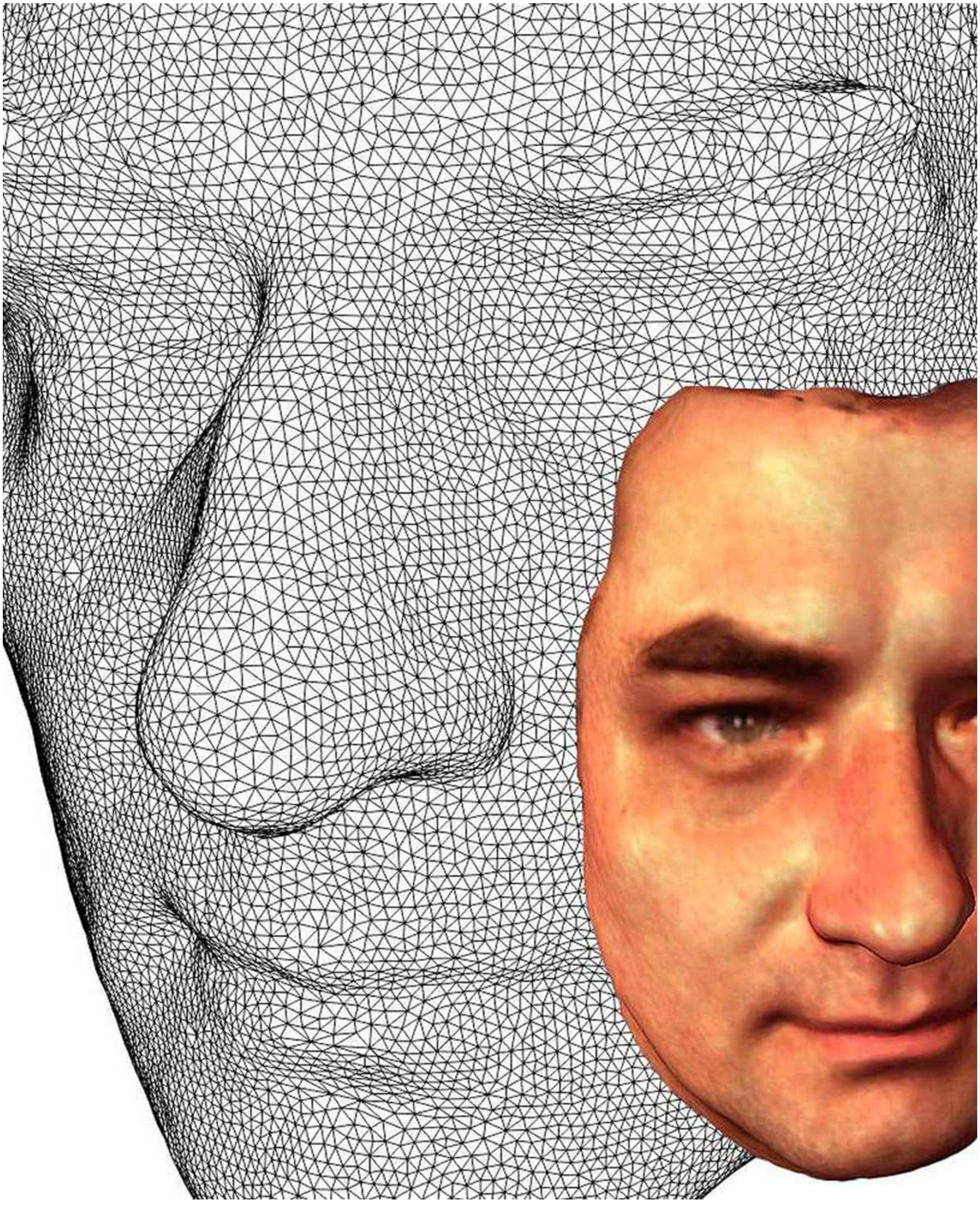


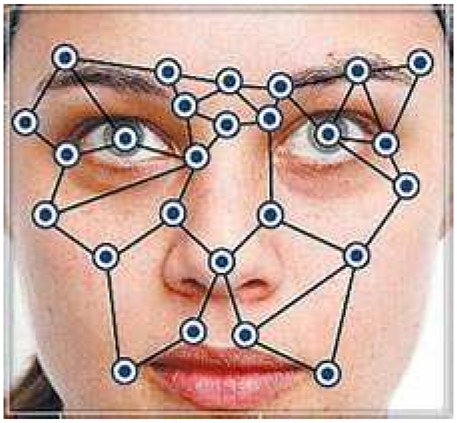
Figure Drawing for Fashion Design by Pepin Press

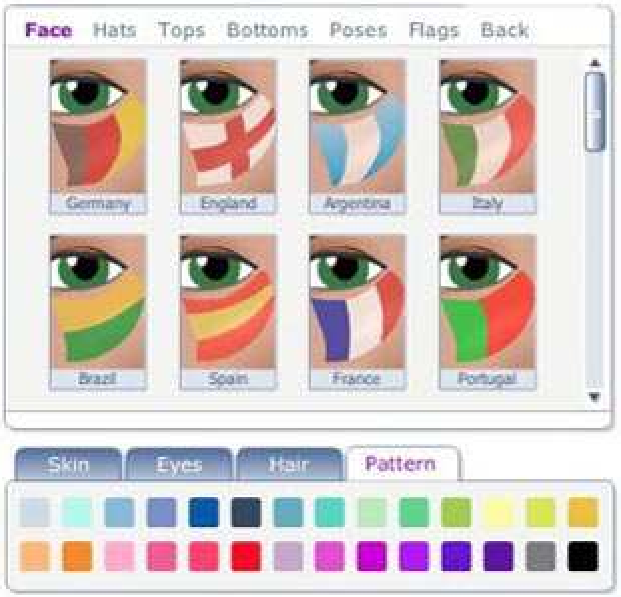

eyelights

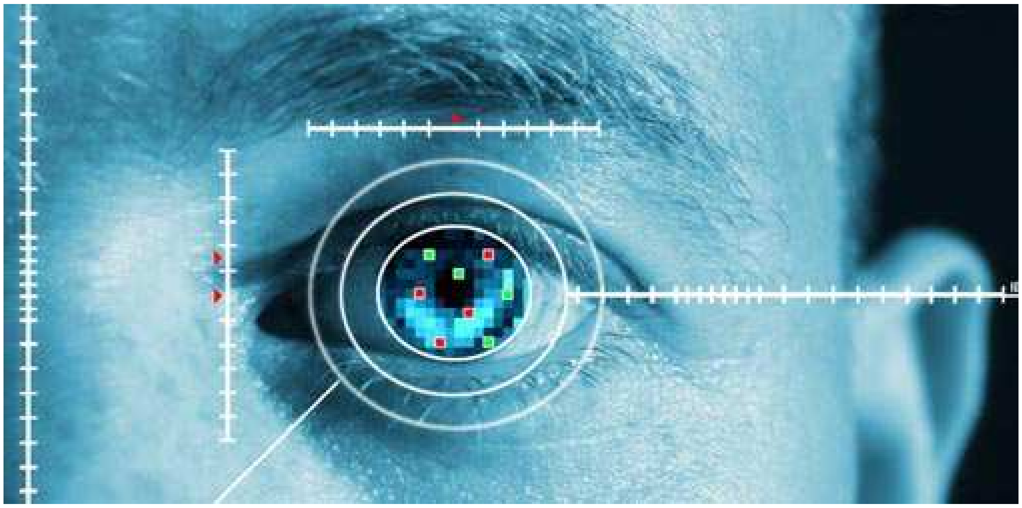
© GOFF

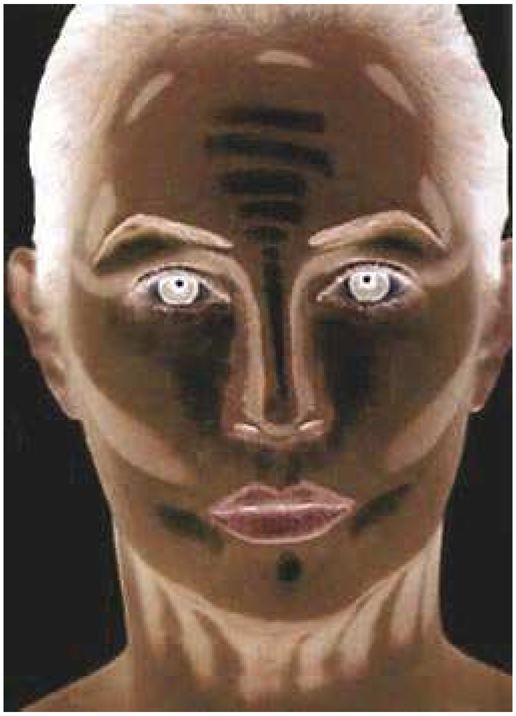







Face
Hats
Tops
Bottoms
Poses
Flags
Back
Germany
England
Argentina
Italy
Brazil
Spain
France
Portugal
Skin
Eyes
Hair
Pattern





Anti-Surveillance and CV Dazzle Concept and Text Adam Harvey

Photography Marco Roso
and Adam Harvey
Web Production Nick Scholl
Hair Pia Vivas
Makeup Lauren Devine
Featuring Maria Verdú Bertomeu, Irina Cocimarov, Jude MC, Michael Vontsolos, and Jen

Special thanks to Obinna Izeogu for introducing us to CV Dazzle and his help in facilitating this collaboration.

Clothing by A.F. Vandevorst, Issey Miyake, Final Home

How to use camouflage to thwart facial recognition

By Tom Cheshire 04 January 12

Face recognition is ubiquitous and "freaks most people out", says Adam Harvey. So the New York-based designer created CV Dazzle, a camouflage that prevents computers recognising faces.

Ignore accessories

That fedora isn't going to fool anyone. Face-recognition algorithms typically focus on a small triangular area starting above the eyes and down to the chin, widest at the eyes. "That's where most of the information is -- ears don't affect it too much, nor does wearing a hat," says Harvey.

Go monochrome

"A lot of face-detection algorithms convert photos into black and white," says Harvey. "When you're applying make-up, it's really about the white and the black, the contrast." He recommends off-the-shelf black-and-white make-up which doesn't crack when it dries. Apply light foundation.

Avoid enhancers

Enhancers such as eye shadow and lipstick amplify key features. "They make your eyes darker and lips more pronounced. You want to do the opposite," Harvey says. The old adage with make-up is less is more. "You don't want to look ridiculous. Camouflage must not be thought of as a mask."

Mask the T-zone

The region where eyes, nose and forehead intersect is "probably the most focused-on area in facial recognition". But there are a few effective ways to fool computer vision. Bring hair down across the eyeline. If you have dark skin, bring down light hair, and vice versa. Or use eye shadow to disguise contours.

Does face recognition represent an improved benefit, or an erosion of privacy? I suggest it has the potential to be both. It is everybody's responsibility to ensure the benefit is worth the price paid. I believe we must have both the proponents of this technology and the advocators of privacy; we all have a role to play to decide how face recognition will be applied over time.

Imagine for a moment that a loved one of yours has come to harm. The authorities can use face recognition to aide in their recovery, and / or to ensure that justice is done. Are you concerned with privacy?

Allevate

Jan 4th 2012

ObscuraCam: Secure Smart Camera

We are developing a secure camera application named ObscuraCam in partnership with Witness.org, the leading human rights video advocacy and training organization. This collaboration grew out of an open hackday at the 2010 Open Video Conference.

This is an open-source project and you can track our progress here: https://github.com/guardianproject/SecureSmartCam.

March 2012 Update: ObscuraCam v2 Alpha with Video:

- *blog update: https://guardianproject.info/2012/03/02/obscuracam-v2-now-with-video-demo-screens/*
- *Alpha v2 download: https://github.com/guardianproject/SecureSmartCam/ObscuraCam-2.0-Alpha-2.apk/qr_code*

How To Get The Latest Release

*We've recently **pushed out** our V1 release for testing that supports a limited set of features for face detection and obscuring in still photos. You can find the app in the **Android Market** or scan the QR code below, which will take you in that direction.*

For those without access to the Android Market, you can get the ObscuraCam.APK file from our public builds folder. The official signed release binary is also available here. For these options, be sure to check back for updates, because the app will not auto-update itself.

Available on the
Android Market

Download ObscuraCamV1 Today (via link or scan the qr code above!)

User Stories

Here are some of the user stories we aim to support, along with links where to track our progress and find out more:

1) An activist group records a video interview of a spokesperson at a protest and wants to protect the identify of the people in the background of the shot.

Development of video filtering and processing is underway:
https://github.com/guardianproject/SSCVideoProto

2) A rights defender uses their smartphone to take many pictures of abuses in a village. On their way back to their hotel, they are detained by local authorities and their phone is confiscated.

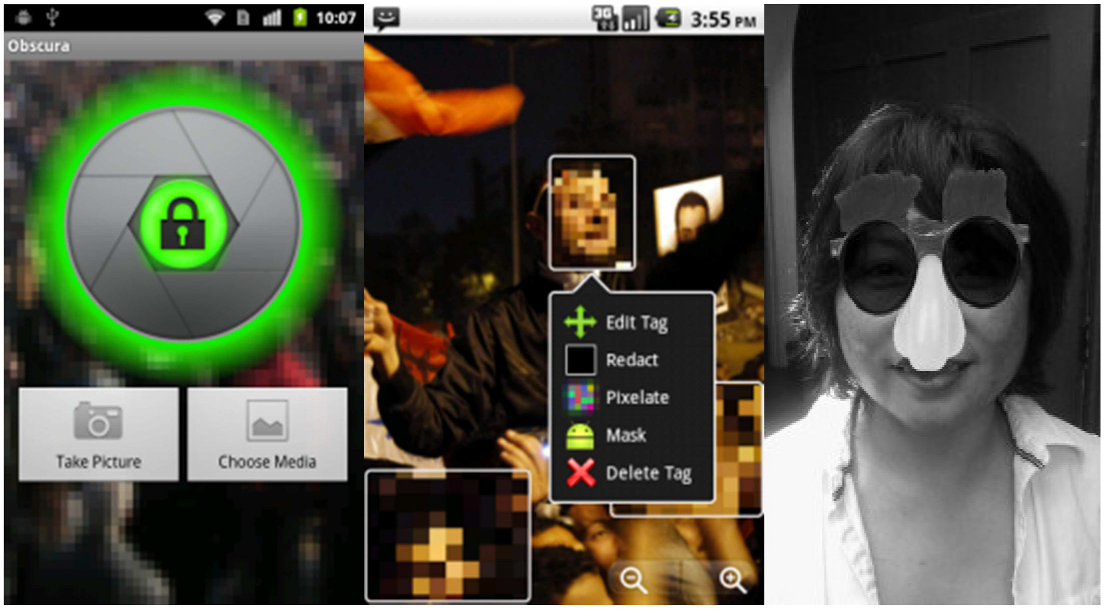
Learn more about our encrypted database library SQLCipher: https://guardianproject.info/code/sqlcipher/ and our Cryptographic features planning: https://github.com/guardianproject/SecureSmartCam/wiki/Cryptographic-features

3) The internet and mobile network are shutdown. Images taken at a protest of human rights abuses need to be delivered out of the country. (tor/proxies/bluetooth/wifi mesh)

Xfer is our video upload and download app that works over the Tor network: https://github.com/guardianproject/sscxfer

4) My phone could be compromised. I have already delivered what I need to. I want to remove all traces of any images captured.

InTheClear is our panic/data-wipe app: https://github.com/guardianproject/InTheClear

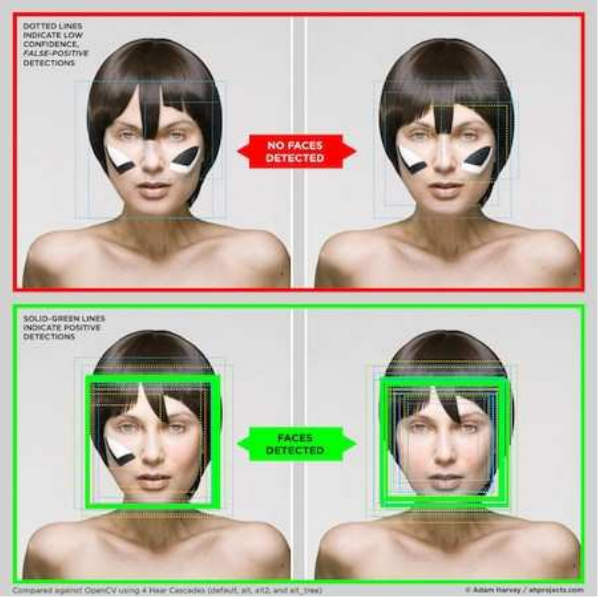


I-R.A.S.C.
The device developed by U.R.A. / FILOART offers the public reliable protection against governmental security measures (and those of other surveillance agencies). The I-R.A.S.C. offers security against security, and in so doing reveals the discrepancy in power between the state and the individual. The I-R.A.S.C. not only demonstrates systems of interaction, developed specifically for surveillance purposes between humans and machines, but also between machines themselves. This absurd accumulation of technology is symptomatic, for although the security measures are supposedly for the good of the people, the individual is considered less and less in current security concepts.

The I-R.A.S.C. is an infrared device, which protects against infrared surveillance cameras. It can be made by anybody; no special skills are required. The device radiates infrared light disrupting the reception of infrared surveillance cameras. A sphere of light covers the face of the person under surveillance and as the interaction is invisible to the human eye (at a frequency between 780nm and 1mm), the individual is unaware of what is going on i.e. they don't see the infrared rays emitted by either the surveillance camera or the I-R.A.S.C.

During the exhibition the device can be tested and video material with live footage viewed. Further video and printed material provide information on the panel discussion "Protection against Protection - Surveillance and Disciplinary Measures in the Public Space", which was part of the I-R.A.S.C. Project at the Kunsthaus Tacheles in Berlin.

This exhibition is presented in conjunction with the Warm up of the Stuttgarter Filmwinter and in collaboration with wand 5 e.V.


DOTTED LINES INDICATE LOW CONFIDENCE, *FALSE-POSITIVE* DETECTIONS
NO FACES DETECTED
SOLID-GREEN LINES INDICATE POSITIVE DETECTIONS
FACES DETECTED
Compared against OpenCV using 4 Haar Cascades (default, alt, alt2, and alt_tree)
© Adam Harvey / ahprojects.com

Not interested in having yourself automatically identified in photos across the internet? Then you might want to take a cue from Adam Ant (or *Blade Runner's* Pris, if you prefer), as Adam Harvey, a student in NYU's Interactive Telecommunication Program, has discovered that some over the top face makeup applied in just the right way can thwart most facial recognition software. Dubbed CV Dazzle (after the Dazzle camouflage used in World War I), the makeup works simply by enhancing areas of the face that you otherwise wouldn't ordinarily enhance -- so instead of applying the makeup around your eyes, you'd apply some on your cheeks and effectively "invert" that area. According to Harvey, that method is effective at blocking the face recognition used by Facebook, Picasa and Flickr -- and it doesn't simply cause some mild confusion, it actually prevents the software from detecting any face at all. Head on past the break for a quick video.

Computer Vision Dazzle Makeup

March 31st, 2010

Adam Harvey is currently writing his thesis at the ITP and his topic is Computer Vision Dazzle. He's researching and developing privacy enhancing counter technology, to protect individual privacy for everyone. So here you can find some makeup patterns which make it impossible for the OpenCV library and it's Haar cascade files, to detect a face. Fun times ahead!

About this image:

Images with a red square tested positive, a face was found
Images without a red square tested negative, no face was found
Images under the section "TEST PATTERNS" are made according to results of the Haar deconstruction
Images under "RANDOM PATTERNS" are random doodles made without the anti-face detection patterns in mind
Images underneath the "NO PATTERNS" heading are left untouched to show that the face detection works well on simple line drawings

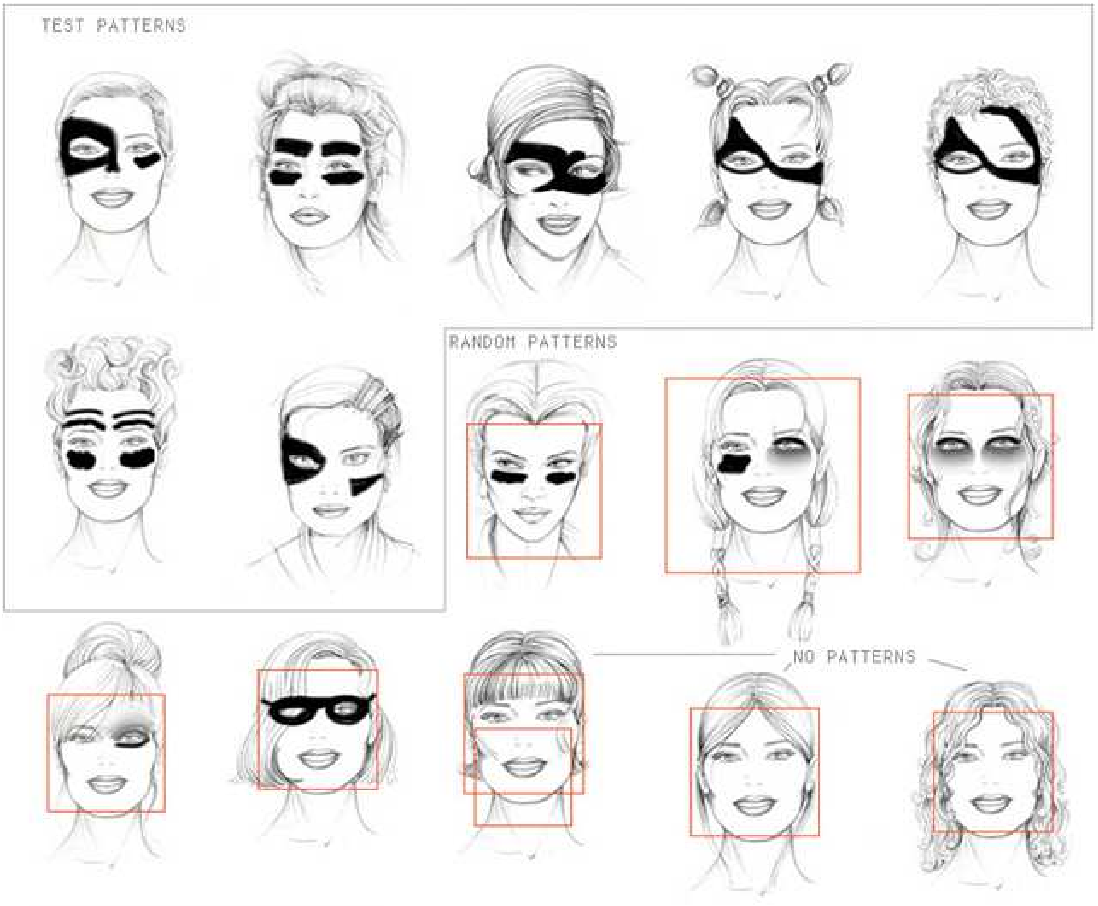
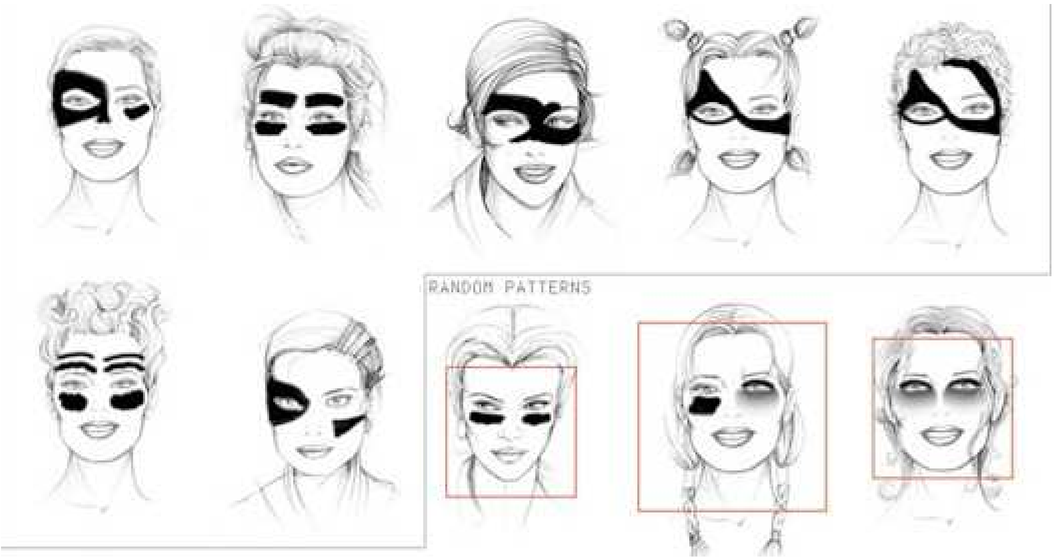


Figure Drawing for Fashion Design by Pepin Press

Abstract, Cyber Warrior Makeup May Hide Your Face From Surveillance

by Leila Brillson on March 31, 2010 at 01:06 PM



Well, it appears the cyber punk movies of the early eighties ('Liquid Sky,' 'Jubilee,' even 'Blade Runner') got it right: in order to defend against our Big Brother overlords, we are going to need to stylistically paint our faces in bizarre and senseless ways. For his graduate's thesis at New York University's Interactive Telecommunications Program (or ITP), Brooklyn-based Adam Harvey is trying to create, as he says, "privacy enhancing counter technology" in a world abundant with face detection software. He posits that since the average individual won't want to be watched, personal style, adornment and accessorizing will change accordingly.

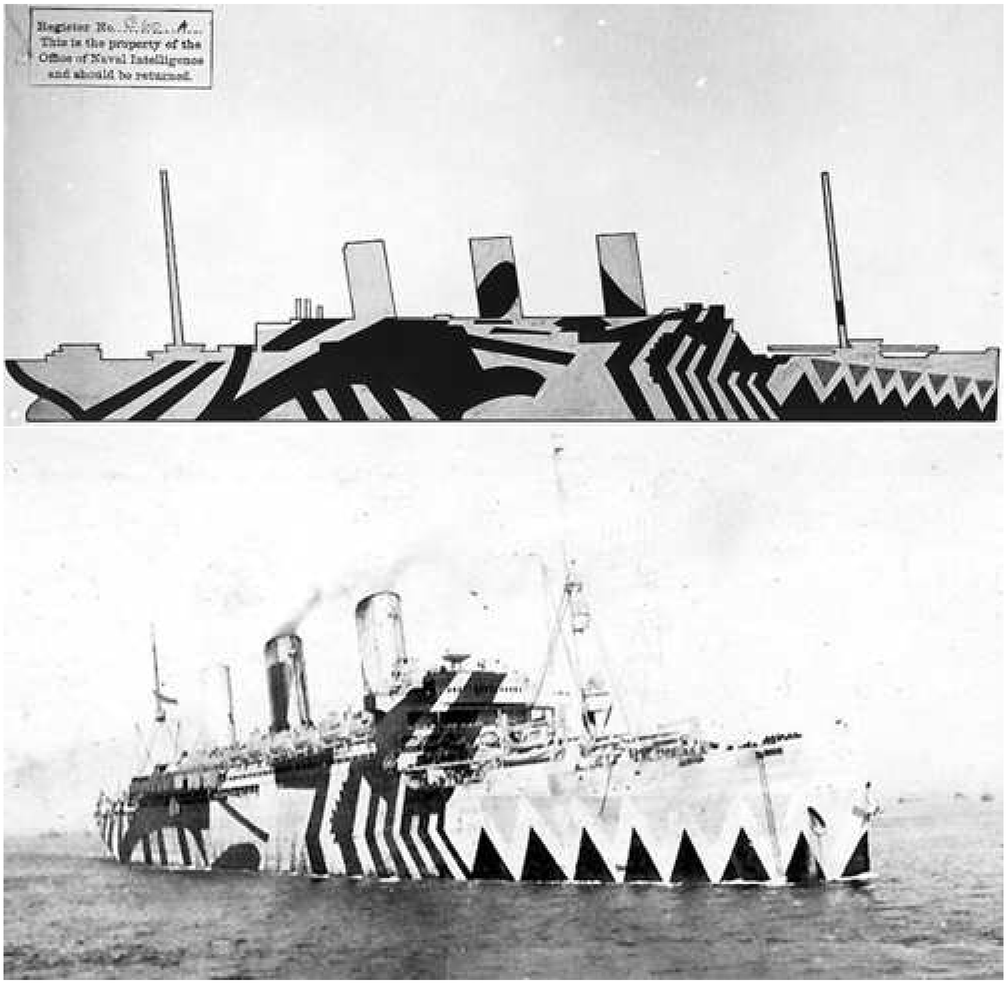
Gathering info from a variety of different face-tracking programs (all based on the rudimentary, yet effective Viola-Jones Method, Harvey alters and experiments with images to make them undetectable. His most recent run used women's faces from "Figure Drawing for Fashion Design" and smeared each visage with, erm, Lady Gaga-esque weirdness. As one may suspect, the stranger, more asymmetrical designs evade the detecting software more readily. Identifying 'Haar-like features' for identification -- or the pixels that cameras detect as belonging to face -- Harvey attempted to confuse and contort the software, by confusing and contorting the face.

That unfortunate facial tattoo the guy on the train has may keep him safe from prying cyber eyes. If tattoos aren't your thing, you can always gussy up using some day-glo paint and magic markers. Oh, and mohawk is optional. [From: AH Projects]

Face-Off

What do you dress for? Seriously, think about it. Remove the preconditioned notion that it's socially unacceptable to walk around sans clothes. There are a number of reasons, some functional and some frivolous: protection, attraction, deflection, association, decoration, tradition, I could go on. The consensus on our last blog post is that good design solves a problem. Adam Harvey, a fellow Brooklynite, technologist, designer and friend of ours is in the biz of solving modern problems caused by technology with technology. He is currently tackling the problem of personal privacy. Adam's the man behind the ***Anti-Paparazzi Clutch*** *that Sheena flashed at Ars Electronica back in September. Since then, he's been busy with his latest project on how to artfully dodge surveillance cameras, in style.*

He calls it CV Dazzle, an assortment of makeup and hairstyles that camouflage your face from computer vision (CV). Camouflage in fashion was originally purely functional dress for protection that turned into a trend. You're probably thinking, "camo is so '98," but there are many patterns beyond jungle green and desert storm. Like Dazzle, which looks as snazzy as it sounds. Dazzle was a camouflage paint scheme used on ships during World War I. At first glance Dazzle seems like the anti camouflage, because it stands out rather than blends in. But its purpose is confusion rather than concealment. It makes it hard for an observer to distinguish the stern from the bow of a ship and whether it's moving towards or away from them. (Same logic applies to zebra print.) Dazzle camo is also not specific to environmental lighting conditions, ie. it works rain, shine or online. ***(via wikipedia)***

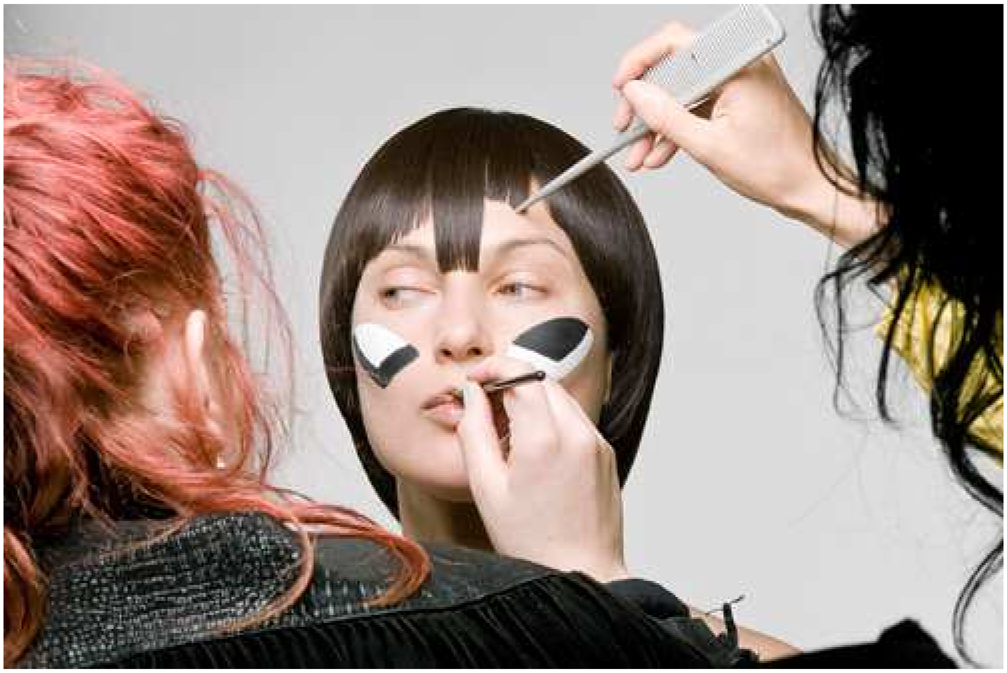

Register No. [illegible] A
This is the property of the
Office of Naval Intelligence
and should be returned.

USS Leviathan's starboard side "dazzle" camouflage pattern (U.S. Naval Historical Center Photograph)

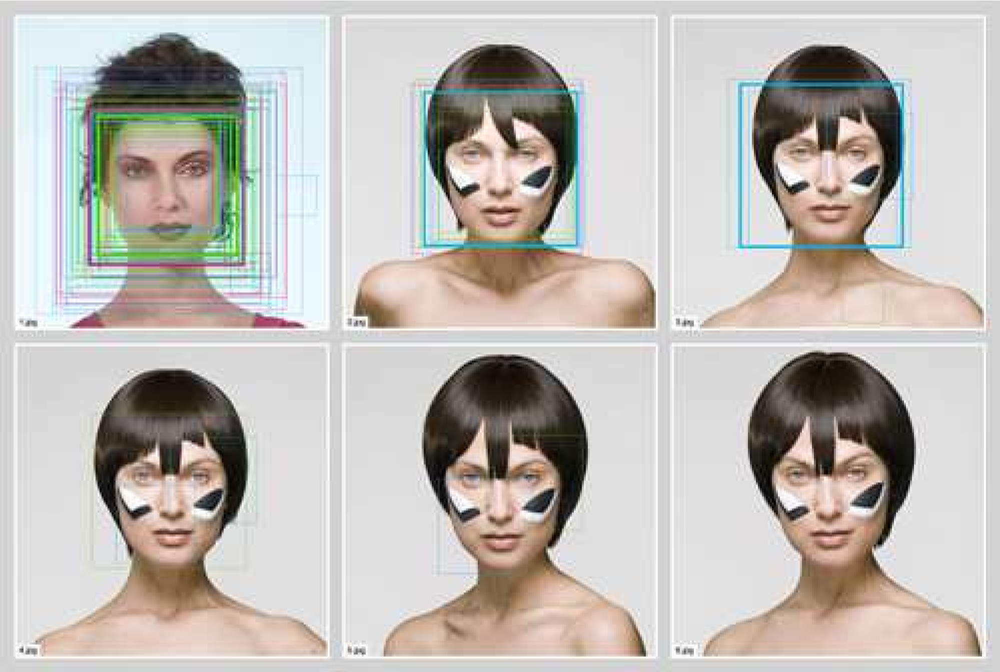
Adam applied the principles of Dazzle to face concealment. First, he figured out what features make a "face" recognizable to a computer; its contours and shadows. Then he inverted the light areas with the dark to essentially create an anti-face. It looks like an extreme glam rock makeover, but actually it's the opposite. Regular makeup enhances your facial features, making your face easier to recognize. CV Dazzle breaks up the gestalt. People can still see a "face," but computers can't. He's now working on a SPF-CV scale from 0-50 (yes, like sunscreen) that takes lighting conditions and face angles into account and works for online applications, so you don't have to worry about your computer stalking you at night.

Adam not only advocates privacy, he's also for purposeful style; to deflect the wrong kind of attention and attract the right kind. His work proves that fashion *and function aren't mutually exclusive. In his own words "It doesn't work if people don't want to wear it." So, next time you reach for your compact, decide if you want to put your face on, or take it off.*

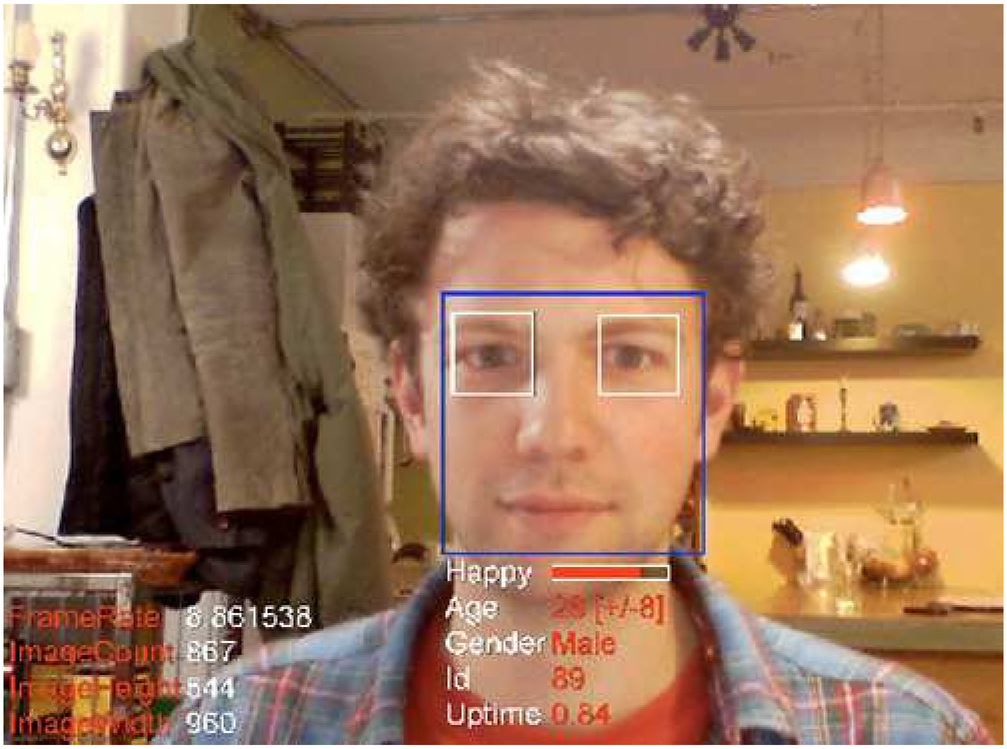
x. wasabipear
'Take a bite.'



Model: Jen Jaffe, Photographer: Adam Harvey, Makeup: Leigh Brown, Hair: Pia Vivas



The dotted lines represent everything the computer things might be a face. The solid lines indicate a positive face detection. Each of the four colors—cyan, magenta, yellow, and green—represent each of the four face profiles. Images without any solid lines have beaten the face detector.



```
FrameRate   8.861538
ImageCount  867
ImageHeight 544
ImageWidth  960
```

```
Age     28 [+/-8]
Gender  Male
Id      89
Uptime  0.84
```

Adam Harvey’s face recognized. Image from ***SHORE*** *(you can download a demo and DIY).*

Sheena flashing the 'Anti-Paparazzi Purse' presented at the Wearables Symposium at ARS Electronica 2009.

How to Camouflage Yourself From Facial Recognition Technology

Published: July 2, 2010

The day when you'll be able to hold up your phone and identify a stranger through a viewfinder is getting closer.

Google's Goggles, a mobile app for visual search,?has a facial recognition version unreleased to the public, while Israeli startup Face.com's technology can tag people's faces in Facebook photos. Facebook even released a basic version of face detection last night, although it doesn't have recognition.

So in a world where technology chips away at our ability to remain anonymous, how does one reclaim some semblance of control?

It turns out there's actually a pretty simple way around the facial recognition technology available in the market today, according to Adam Harvey, a graduate student at NYU's ITP (the same program that produced Foursquare chief executive Dennis Crowley and that Twitter's location guru Raffi Krikorian taught at).

If you change the contrast in certain parts of your face — either through a watermark or by wearing a strategically-placed sticker or facepaint, recognition technology can't identify that your face is a human face.

"It?breaks apart the gestalt of the face," he said. "That's what original camouflage was supposed to do."

Harvey said he got his idea from studying camouflage methods use during World War I and World War II. His project, CV Dazzle, is based on the original dazzle camouflage used by the military to hide ships in the 1940s.

While the flashy geometric patterns don’t seem like they would be able obscure a thing, they thwarted the enemy’s ability to tell the make or size of the ship. Similarly, zebra camouflage does little to blend the animal into the background of the savannah. But when zebras are in herds, predators like lions have difficulty picking out animals from the herd. (Dazzle camouflage was eventually phased out by the military as aviation technology and rangefinders improved.)

Harvey says there a couple of projects that could stem from idea. He could either build a basic watermarking technology that could render faces unidentifiable to these programs while still being recognizable to humans. Or he could work with make-up artists and designers to create interesting real-world looks that prevent facial recognition.

“Putting paint on your face isn’t always practical,” he said. “This is?just the way that I wanted to test this. But if you wanted to be covert, you could try wearing different styles of make-up or accessories. You could position?a Band-aid on the right spot on your face. The power of this idea is that people can interpret it in their own way.”

You can see face-detection evading makeup below. The examples that have red squares around them were identified. But the ones that don’t have squares passed facial recognition software undetected.

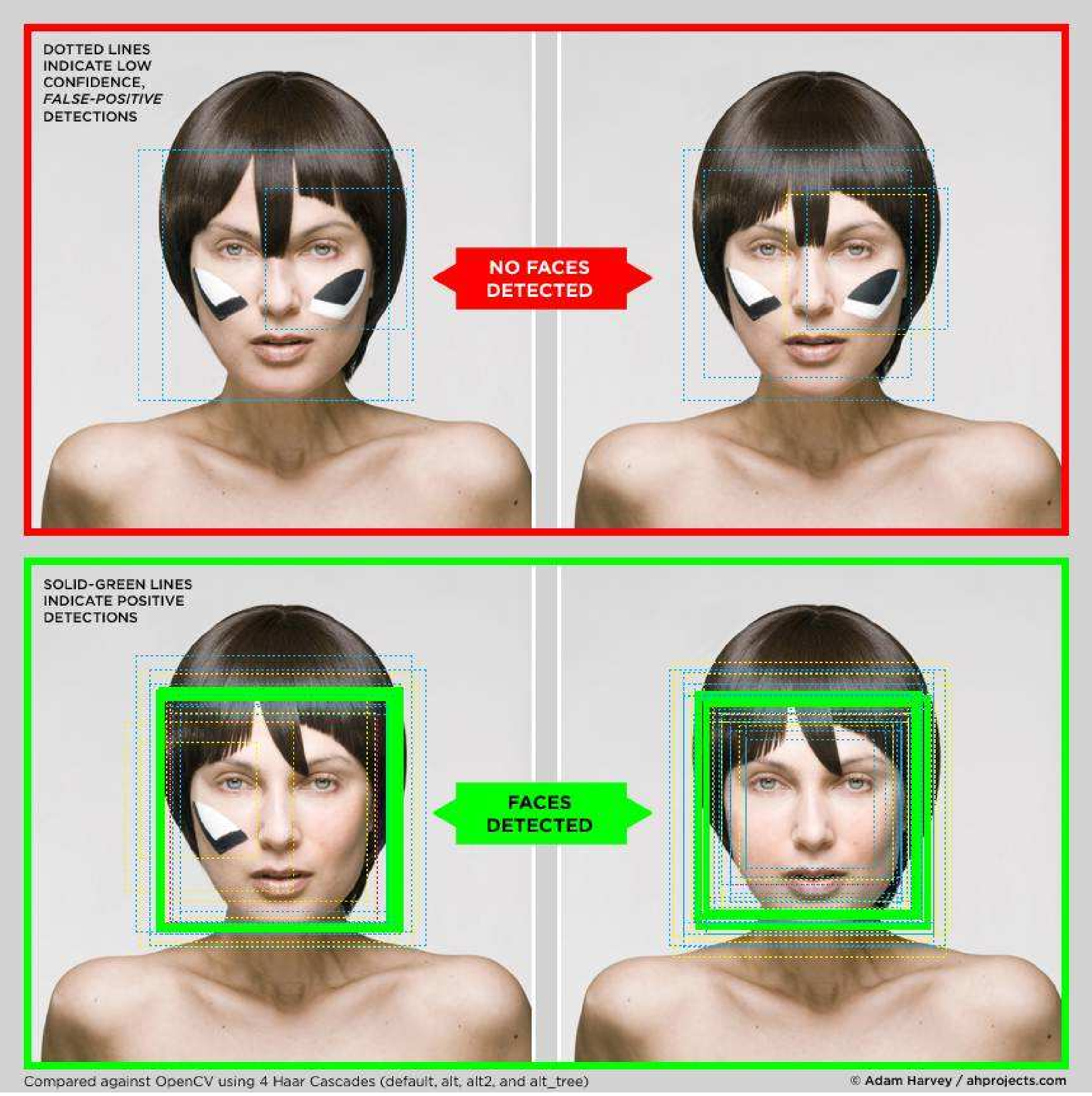
It seems like a pretty far-off idea given that if Facebook ever did release full-fledged facial recognition, it would never be completely automated. Humans would most likely have final say to tag or untag themselves. It’s also unclear how Google could ever release a facial recognition Google Goggles, given the privacy concerns it is already facing from European governments and consumers alike.

But if an augmented reality app that automatically identified people from your phone ever emerged, perhaps we could see a fad of facial camouflage.

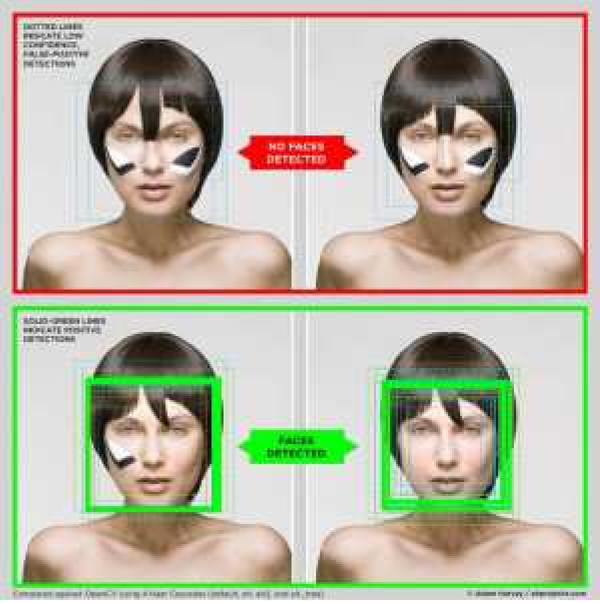
Interview: Adam Harvey and The Anti-Face

By corey armpriester

April 18, 2011 · 2 Comments


DOTTED LINES INDICATE LOW CONFIDENCE, *FALSE-POSITIVE* DETECTIONS
NO FACES DETECTED
SOLID-GREEN LINES INDICATE POSITIVE DETECTIONS
FACES DETECTED
Compared against OpenCV using 4 Haar Cascades (default, alt, alt2, and alt_tree)
© Adam Harvey / ahprojects.com

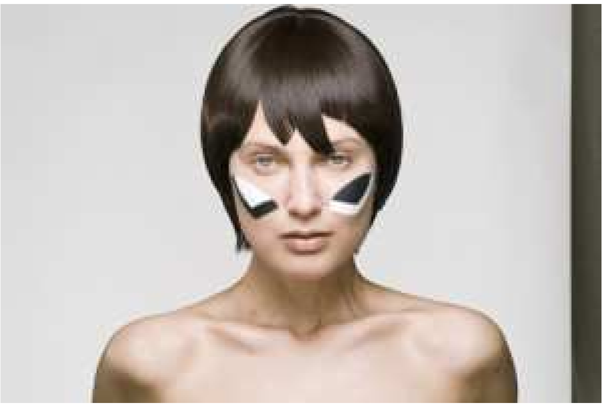
Surveillance will find you, and artist Adam Harvey's CV Dazzle is the antidote, providing a kind of camouflage with makeup and hair–makeup and hair specifically used to protect against automated face detection and recognition systems. The term Dazzle refers to the type of camouflage paint design used on military ships during War World I, created by British artist Norman Wilkinson who coined the term "dazzle painting"; CV refers to computer vision (the eye). Look! It's a bird; it's a plane, no- it's a satellite archiving the bone structure of your face. Never fear- CV Dazzle is here to save the day, seriously. Borrowed identities once reserved for the underground fringe now has a place in your life. This is the ticket into the invisible class–men, women and children deleting themselves from the digital eye. In our telephone conversation Adam Harvey said he has been working on this project for a little over a year; CV Dazzle is a work in progress and you can view the CV Dazzle effect on his website.


DOTTED LINES INDICATE LOW CONFIDENCE, FALSE-POSITIVE DETECTIONS
NO FACES DETECTED
SOLID GREEN LINES INDICATE POSITIVE DETECTIONS
FACES DETECTED

The top look foils face recognition software. the bottom, not.

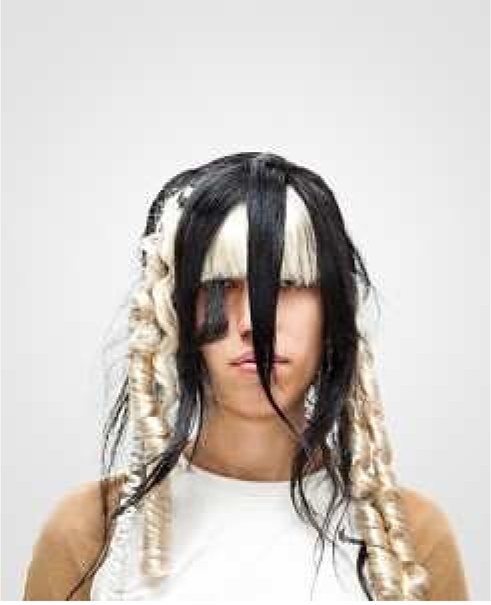
CA- Why did you become an artist? What were the influences in your life that lead you to this?

AH- That's kind of a hard question. Sometimes it may be art and sometimes it may be an experimental project. I am doing projects that are supposed to be art projects but some of them fail to do that but others do succeed and in the end, it's up to the audience to look at it and judge it to their criteria. I've always been interested in photography and that's been a big influence on the work that I do.



Adam Harvey. This CV Dazzle look also works.

CA- Why did you move to New York City?
AH- I can remember a turning point one year when we were taking a family vacation and I bought a magazine and the magazine was full of pop culture and that was something I had never seen before and I can remember that as a decisive moment when I was a kid. I realized that there was this whole world out there that I hadn't seen growing up in the country [i.e. the Poconos] and I was really curious about it. Ever since I was a kid I wanted to live here in New York.



One of the successful CVDazzle looks.

CA- Is CV Dazzle a personal protest?
AH- You can think of it like that, I actually staged other activist events against

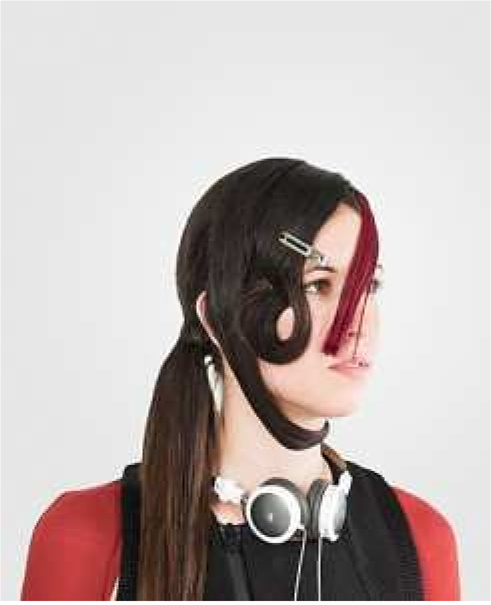
surveillance; I was always interested in protesting the state of surveillance, I would consider this a type of protest but when you put it that way, I think it turns a lot of people off.

CA- Are surveillance cameras being used for reasons other than what we are being told?
AH- There have been a few accounts where people have abused the system; police officers have used it for voyeuristic activities that I've read about. I not sure anyone knows exactly where all the footage goes.

In another tactic, Camoflash, a reflective surface foils paparazzi. Harvey has an interest in blocking any surveillance.

CA- When is it appropriate to CV Dazzle oneself?
AH- A lot of people take photos at night at parties and they end up on line. My question was is there any way to avoid having these party photos from being picked up on search engines, for example, Google's image search has face detection face recognition systems.

CA- Have any government agencies shown interest in your CV Dazzle project?
AH- I've been contacted by a few companies that do face detection or face recognition. I haven't been contact by any legal authorities yet, I think because it's somewhere between an art project and a full-fledged research project.



Adam Harvey, CV Glitter sample including a hair clip

CA-What is the biggest misconception about your work?
AH- People seem to understand it pretty well.

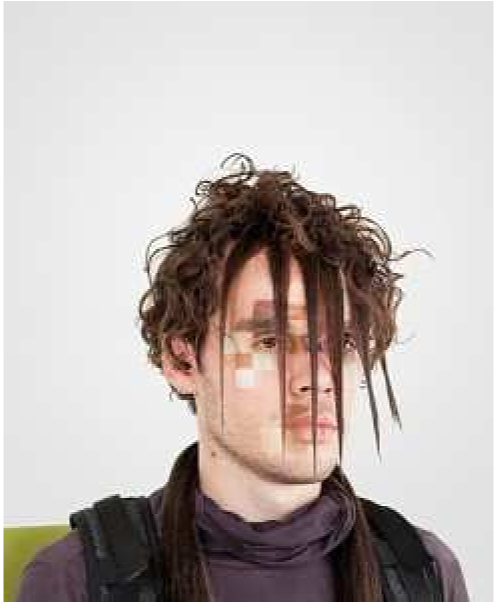
CA- Have you been accused of being anti-American?
AH- No, actually all of the feed back has been very positive. There’s a real interest by security people to better understand how individuals are avoiding face detection.

More CV Glitter

CA-Is that in direct conflict with what you are doing?
AH- That's interesting because how can you prevent a collection of looks that people can use without those looks being picked up by those that want to make face detection stronger? It's a big dilemma. What I would like to do with this project is to make it more accessible so that people can make their own looks. In designing your own look you can feed it into the system [a future interactive online feature] and if your look is strong then it can help create an algorithm that helps generate looks for other people.

CA- Have you studied cosmetology?
AH- I work with a makeup artist and hair stylist.

CA- Do you oversee what they do?
AH- It has to be guided in a certain way to counteract basic shadow patterns on the face. What you are trying to do is create an invert of your face, the anti-face. It doesn't have to be makeup, you could use stickers or removable items that you can put on the face. If you're going through a surveillance area, you could essentially turn it [the CV Dazzle effect] on by moving things [stickers, hair or a shirt collar, for example] in a certain way and then later turn it off.



Adam Harvey, a subtle CV Glitter look. Even bandaids, properly applied, could create shadow confusion.

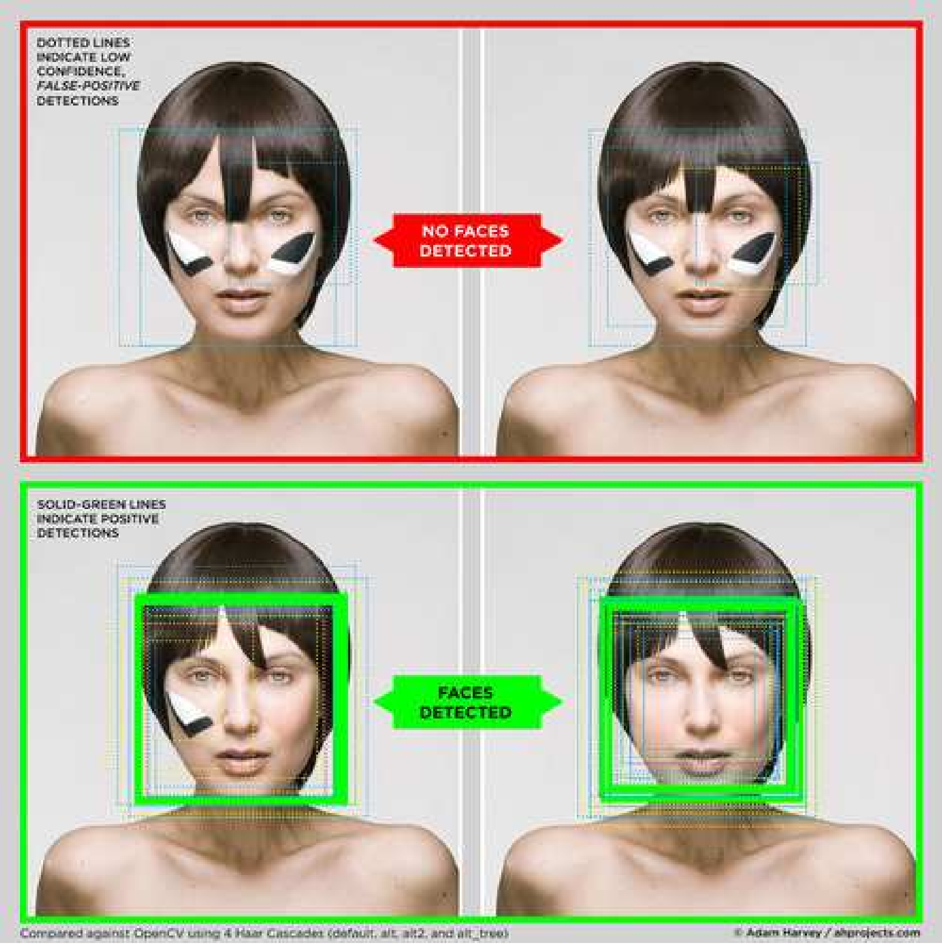
CA-The Patriot Act is…
AH- A defining moment in our changing relationship to surveillance.

CA-Have you taken Bill Brown's "Video Surveillance Tour of Manhattan?"
AH-No, but I would like to.

CA- How have you come to terms with being a photographer and creating anti-photography projects?
AH- Photography is about communication. If you're designing something that is anti photography, as long as it's communicating I think it's still interesting.

The studios of Brower Propulsion Laboratory and Adam Harvey Projects are hosting an interactive public event that will allow guests to engage in open intellectual intercourse and manipulation of custom made devices in various stages of completion, Saturday, April 23, 2011. 2:00pm-8:00pm, 63 Flushing Ave. Building 280, Suite 521, Brooklyn, NY, Phone 347-223-8877

6 questions with...Adam Harvey


DOTTED LINES INDICATE LOW CONFIDENCE, *FALSE-POSITIVE* DETECTIONS
NO FACES DETECTED
SOLID-GREEN LINES INDICATE POSITIVE DETECTIONS
FACES DETECTED
Compared against OpenCV using 4 Haar Cascades (default, alt, alt2, and alt_tree)
© Adam Harvey / ahprojects.com

PopTech's new series, ***6 questions with…*** *gives us a chance to get into the heads of social innovators, technologists, artists, designers, and scientists to see what makes them tick.*

We're kicking off the series with Adam Harvey, a designer whose work focuses on computational design, human-computer interactions and dreaming up new ways to utilize technology. Harvey went through NYU's ITP program where his thesis project, CV Dazzle, "a camouflage from computer vision," uncovers ways to design make-up and style hair to defeat facial recognition software. Named after a type of camouflage used in WWI, CV Dazzle can interfere with technologies on Facebook, Flickr, and Google's Picassa that may compromise one's privacy – while simultaneously providing an outlet to experiment with some fantastical hair and make-up styles.

If I'd been a fly on the wall of your office/studio yesterday, what would I have seen you doing?

Hopefully this fly on the wall is not spying on me because counter-surveillance is one of my areas of research. Though, for the past few months I've been working on a non-related project. It's a stethoscope paired with sound recognition, kind of like Shazaam for your heart. If you were here, you probably would have seen me coding Java and drinking Bustello at my studio in the Navy Yard.

What's the mark you're hoping to leave on the world? Why is your work relevant at this point in time?

One of my major influences is Susan Sontag's book, *On Photography*. I own three copies. Not on purpose though. Two of them were gifts. In her work she dissects our relationship with photography and cameras. It's an interesting topic that becomes more relevant with every camera sold. Photography has changed a lot since she wrote the book in 1977. Now, over 85% of millennials (age 18-29) own at least one digital camera. I own 14. London has over 500,000 within their ring of steel. As these numbers climb, we will need to learn how to adapt and understand this phenomenon. I like to think of my work as a continuation of what she started several decades ago, an emerging critical discourse about photography and cameras.

What do you wish you had known when you began working on this project?

It would have been easier to work on this project had I known more about machine learning and face detection algorithms. That's a topic I hope to spend more time researching this year.

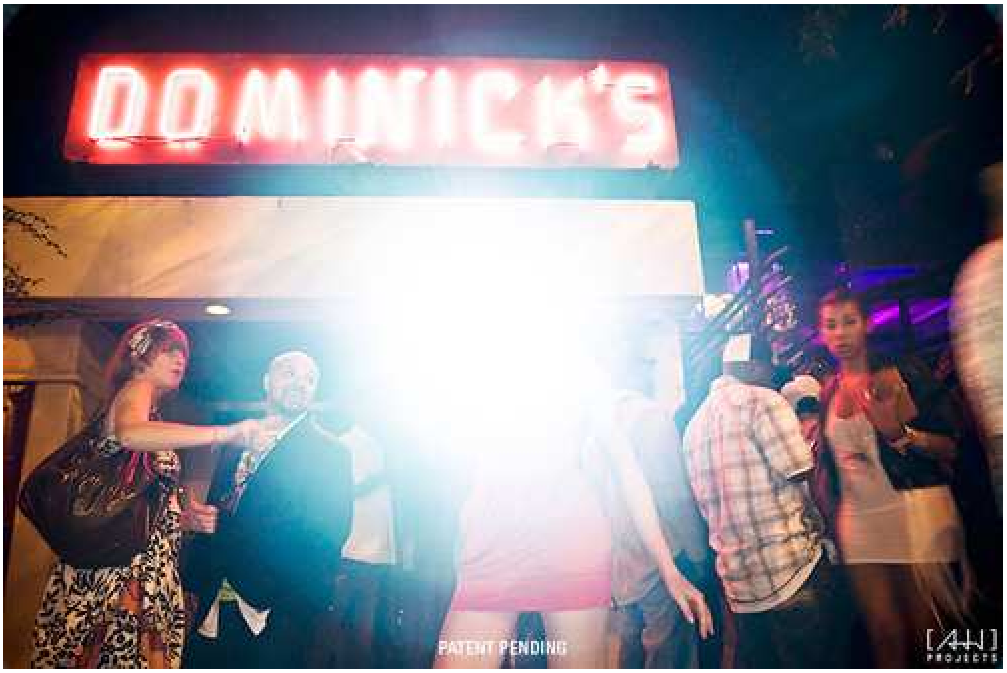
What was the pathway that brought you to this work?

There were two things that inspired me to work on this. One of them was my friend's Halloween costume from the Uniform Project, which was deceiving to humans but not machines. And the other was a drawing of a face that was deceiving to machines, but not humans. I have always been critical and uncomfortable with surveillance in public and seeing these two forms of deception led me to the idea of creating something that was deceiving to machines but not to humans. I was also really inspired by the Boombox party scene in London and friends who wear lot of makeup. Camouflage has to look good otherwise no one is going to wear it.

Who or what has most influenced your life and work?

When I first moved to New York City in 2004, I began looking for work as a photographer. I tried photo assisting but found it unrewarding. To supplement my income I started creating websites. And to hone my skills as a photographer I would shoot parties at night, mostly for free. Developing websites taught me programming and shooting parties taught me a lot of about social behavior around cameras. Out of all this, I decided I was more interested in the culture of photography than in trying to sell my photos. This is the decision that has influenced most of my work in the past few years.

One of my takeaways from party photography was that the photographer always had the upper hand. This led to one of my first photo-centric projects at ITP, Camoflash: The Anti-Paparazzi Clutch. It's a device that gives the subject the power to say "no, thanks" with a blinding pulse of light that overexposes the photo. In a similar vein, *CV Dazzle* is about opting out of the paparazzi in the sky, surveillance.



What book is on your nightstand right now?
I'm reading: *Spycraft: The Secret History of the CIA's Spytechs* and *Functional Aesthetics*.

Reverse-engineering artist busts face detection tech

-

Hacking Big Brother with help from Revlon

By **Dan Goodin** • **Get more from this author**

Concerned about the proliferation of face recognition systems in public places, a grad student in New York is developing privacy-enhancing hacks designed to thwart the futuristic surveillance technology.

Using off-the-shelf makeup and accessories such as glasses, veils, and artificial hair, Adam Harvey's master's thesis combines hipster fashion aesthetics with hardcore reverse engineering of face detection software. The goal: to give individuals a low-cost and visually stimulating means to prevent their likenesses from being detected and cataloged by face-recognition monitors.

"The number of sensors that are going into the public spaces has been increasing," said Harvey, a student in New York University's interactive telecommunications program. "There's a lot of work to be done to catch up to where cameras are going because there have been so many advances in the last few years."

Although still in its adolescence, face recognition technology is quickly being adopted by governments and corporations to identify individuals whose images are captured by surveillance cameras. At the 2001 Super Bowl, for instance, officials digitized the faces of everyone entering Raymond James Stadium in Tampa, Florida and compared the results against photographic lists of known malefactors.

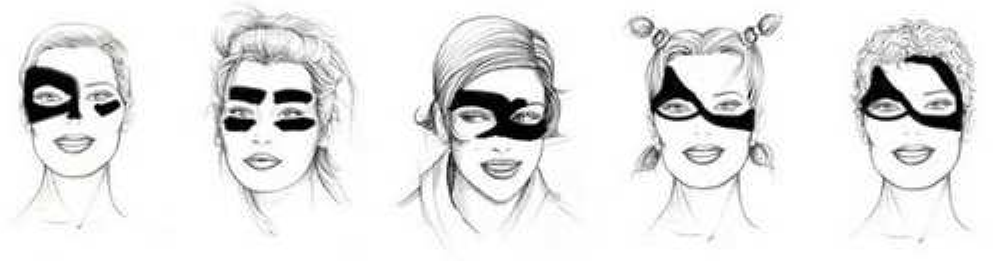
In another example, the city of Chicago two years ago made much fanfare of "Operation Virtual Shield," which was to use IBM software to analyze in real time thousands of hours of video being recorded on more than 1,000 continuously running cameras.

As a starting point, Harvey's research involves the reverse engineering of OpenCV, which its creators describe as an open-source "library of programming functions for real-time computer vision." From that work, he developed an understanding of the algorithm used to tell if an image captured by a camera is, say, a car, a building or a human face.

Based on the so-called Viola-Jones method (pdf), the algorithm examines the spatial relationships of an object captured in an image and looks for features commonly found in faces. Most faces have a dark region just above the eyes, while the cheek bones and nose bridge will appear lighter. When the algorithm detects enough such attributes, it guesses the object is a face. The method is generally regarded as effective. Errors are in favor of false positives, making it hard for unobstructed faces to escape notice when they aren't captured at an angle.

Once a face is detected, other technologies, such as face recognition, can be used to compare the face against a database in an attempt to identify the person it belongs to.

But Harvey has discovered that face detection can often be thrown off by using makeup to alter the contrasts the technology looks for. For example, dark patterns applied around eyes and cheek bones, as in the image below, are one such possibility.



These faces aren't detected by Viola-Jones algorithms

"There's a lot of trial and error," Harvey said. "The common thread is throwing off the symmetry" the algorithm looks for. "It's a lot more difficult than applying a bunch of makeup and hoping it works or putting on your 3D glasses left over from *Avatar*."

Technology that detects or recognizes faces still hasn't gone mainstream, said Ralph Gross, an expert in the field and a scientist at Hyperactive Technologies. For now, it's mostly limited to specialized applications, such as the Super Bowl outings or Las Vegas casinos, but he said he expects that to change.

"The technology is getting better all the time," he said. "Along with computing power being greater, it becomes more of an option. I think we're heading to the point where we as a society need to think about what we are comfortable with."

At the same time, Gross said a pair of dark sunglasses or a simple veil would probably prove just as effective at thwarting face detection as anything Harvey is recommending.

But Harvey, said the point of his project from the beginning has been to create disguises that do more than simply hide a person's face.

"The combination of hair, makeup and accessories gives you the potential to do an infinite number of creative new looks that have some futuristic value to them with anti-face-detection functionality," he said. "Maybe you could go to a privacy hair stylist in the future." ®

CV Dazzle vs PhotoTagger from Adam Harv on Vimeo.

Everywhere you look this week the Winsor Report on police pay and conditions and the Hutton Report on pensions, not suprisingly, have been dominating the policing agenda. So, I thought now might be a good time to provide a short attention break from all of that, and shift the focus to recent tech related issues that have potential implications for policing.

I'm going to kick off with a startup outfit called Broadcastr.

Broadcastr allows you, or anyone else for that matter, to record and upload audio clips and have them organised by geographic location. What this means is that people can listen to an audio clip that is tagged to a specific location. They can also choose to listen to a specific category of story. The highest rated stories are played first and people can share stories they like with their social networks or follow the person who submitted it.

For me this potentially provides yet another great opportunity for policing to move into an additional engagement channel. I have blogged before about how forces, and neighbourhood teams in particular, could take advantage of geo location services such as Gowalla and Foursquare to allow people to 'check in' with their neighbourhood policing teams and 'earn' badges and rewards by greater levels of engagement (Communication to Cooperation to Collaboration). Broadcastr opens an additional channel. Neighbourhood policing teams could for instance, record 'about your neighbourhood team' audio clips, or 'team updates' or 'you said, we did' updates, or crime appeals or or or! Public order commanders could have safety messages uploaded that were appropriate to the event and location and change them easily as the event progressed. Roads policing might use it to publicise an enforcement campaign in a specific area.

The site is in beta right now (and a bit on the slow side), but you can already listen to people talking about holiday visits to various parts of the UK. Check it out here.

Next up an interesting article that's quite timely given the possible scale of protest in the near future, anti-surveillance camouflage, CV Dazzle (or how to hide from facial recognition software).

At the moment CV Dazzle is a New York University thesis project, but the website describes the concept as 'camouflage from computer vision (CV)'

The site goes on 'It is a form of expressive interference that combines makeup and hair styling (or other modifications) with face-detection thwarting designs. The name is derived from a type of camouflage used during WWI, called Dazzle, which was used to break apart the image of warships, making it hard to discern their directionality, size, and orientation. Likewise, the goal of CV Dazzle™ is to break apart the understanding of a face, or object, and make it undetectable to computer vision algorithms, in particular face detection.

And because face detection is the first step in automated facial recognition, CV Dazzle™ can be used in any environment where automated face recognition systems are in use, such as FaceBook, Google's Picasa, or Flickr'

It may only be a thesis project at the moment, but next time you're working a public order event and you see people wearing highly stylised make up designs, it just might be a Dazzle disguise. Find the site here

Staying on the unmasking disguises theme, Fast Company magazine reports that

'Researchers at Concordia University have discovered a way to mathematically uncover the unique (and often sub-conscious) writing style, or "write print," of each individual. The most immediate application will help law enforcement identify the author of anonymous emails from a line of suspects. As of now, the program is roughly 85% accurate and confined to email sniffing, but it's conceivable that the technology could eventually unearth the identities of spammers, trolls, or even terrorists.

The proving ground for the team's sleuth algorithm was 200,000 real-life emails from 150 Enron employees. From a small sample of 10 subjects and 100 emails, the technique correctly identified between 80 to 90% of subjects. Thus, it's not accurate enough for a court of law (because 20% of subjects would be falsely accused), but it is enormously beneficial to resource-strapped detectives'.

Just to add to the detectives joy, it was reported last week that a team led by an Indian scientist has developed new software that can, allegedly, automatically match hand-drawn facial sketches to mug shots stored in police databases.

The research is published in the journal IEEE Transactions on Pattern Analysis and Machine Intelligence. Good luck getting hold of that.

And finally, when they say that 'a little bird told me' they may just be telling the truth. Researchers have developed an unmaned aerial drone in the shape and form of a hummingbird.

With a 6.5-inch wing span, the remote-controlled bird weighs less than a AA battery and can fly at speeds of up to 11 mph, propelled only by the flapping of its two wings. A tiny video camera sits in its belly.

The bird can climb and descend vertically, fly sideways, forward and backward. It can rotate clockwise and counterclockwise. Most of all it can hover and perch on a window ledge while it gathers intelligence,

Just to really scare you, the researchers are apparently working on new drones that look like insects and the helicopter-like maple leaf seed.

Finally, don't forget that only blog items are emailed to you. Check out the 'interesting things' category on the www.openeyecommunications.com web site for snippets that don't make it to the blog email and the 'agency reports' section for the latest reports and publications from across the various agencies and government ministries.

Makeup to Fool Face Recognition Software

An NYU student has been reverse-engineering facial recognition algorithms to devise makeup patterns to confuse face recognition software.

Comments

Of course, wearing such camouflage to confuse face recognition would probably just attract the attention of actual people.

Looks a lot like military camouflage makeup patterns -- which are designed to confuse our face recognition brainware.

Don't agree. Depends on the fashion of the time. People might begin wearing more makeup as a resistence to surveillance.

Remember Johnathan crossing the border in Gotcha? Using another guys passport and photo his friends painted him so glam that the guard didn't bother to authenticate further.

If it could defeat camera imaging celebrities would start wearing it tomorrow and then everyone else would follow suit.

I may be mistaken, but I believe his make-up patterns only fool a system which is trying to determine if the image contains a face, not whose face it is.

They're also designed to work with a specific class of algorithms using "Haar Faces." Of course many face recognition algorithms operate completely differently.

Some are even designed to account for things like make-up and camouflage. I acted as a test-subject for an effort to collect data for just such testing many years back.

There's already a great way to escape face detection software if you don't mind standing out on the street corner: just put on a mask or a veil or something similar. That doesn't rely on knowing in advance what algorithm the system uses.

What if I rock an eye patch to get on a plane, perhaps some gauze wrapped around one side of my face covering one cheek/eye/eyebrow. What if I use a Halloween prosthetic and sun glasses, I really don't think this is going to attract much attention: http://www.frightcatalog.com/i/360x360/...

The makeup patterns provided are not actually all that eye-catching... in the world of avant-garde fashion makeup. I am actually planning a shoot this summer that will have a model wearing high fashion makeup (not specifically designed to defeat this algorithm, granted! ;-)) parading down a city street. And frankly, aside of a few curious glances, I don't expect it to attract all that much attention. Hiding in plain view...? :-)

Back in World War One they did the same thing but to hide ships it was known as "Dazzle camouflage" and it worked on the "optical illusion confusion" principle.

That is it caused an operator using an optical range finder (using the split image coincidence effect) to be sufficiently unsure of what they where looking at. Thus unable to take an accurate range by aligning the image.

Dazzel was invented in 1916 by the artist Norman Wilkinson. It was still in use during the second world war on the arctic convoys where it helped hid a vessal in amongst ice fields etc.

http://en.wikipedia.org/wiki/Dazzle_camouflage

So in conclusion to beat it, you need to change the way your face looks.

First we're dealing with a work in progress. Pilots and prototypes are meant to be rough.

Second if an attack works then it gets refined and generalized. Maybe the paints don't have to be visible to human eyes etc.
If it can defeat facial detection would a system even get to recognition? Doesn't the system have to be able to detect the face first? If they reported negative detects we'd have an infinite number of "No one" "No one" "No One" "No One" "Still No One" "No One" "No One". I realize this depends on the algorithm used.

Finally the attack targets an _automated_ systems. Where have they suggested deploying these? On Urban street and transit camera systems, sporting events, large gatherings of people. NOT One detector flanked by two human guards.

Why? So it can deal with the amount of data those cameras that ARE working produce. So if you can defeat the machine you never have to deal with the humans. Other people may look at you funny and during a football game or in NYC?, as GrinMouse points out, not even that.

I snicker at the thought of makeup and other forms of recreational costume being outlawed.

If methods for defeating the FR systems became common knowledge, what if anything could law enforcement do to stop people from employing them?

Virginia has rules about what you can not do in the way of makeup and wigs when getting a driver's license. UK has similar for people in hats and hoodies in certain public places. Could US police legally do the same when you are in public?

Of course the question is as you note if this works at making the system not detect a face let alone recognise who it is,

How little make up is required to foil recognition.

Which is as you may remember a question I was asking a little while ago about the (supposed) Mossad "hit people" in Dubai.

I wonder if "facial putty" etc could do the same job but less obviously to humans.

Lets be honest if I had a nose that looked like Ron Moody's "Fagin" or a chin that looked like Jimmy Hill's, people would (I hope) not say anything to my face out of social necesity.

As I understand it most FC systems work not on "direct measurment" but "releative measurment".

So although I might not be able to change the real measurment between my eyes I might will be able to change other relative measurments to say my cheak bones and chin or teeth so that relativly my eyws look closer or further apart, and thus have a different ratio that is not mine in the DB.

For those in the US you can think Jimmy Durante and Jay Leno for local cultural milage.

@Clive "might not be able to change the real measurment between my eyes I might will be able to change other relative measurments "

Which gives the advantage to the confuser if they could become more in the middle of the normal distribution curve and generate more type II errors.

For those interested in facial recognition systems there is sadly not much info out there (yes I know it's available in Apple's iLife software and some online photo DB's).

There are one or two (out of date) articles one of which is,

http://electronics.howstuffworks.com/gadgets/...

However since 9/11 FRsystems have gone underground and it has been suggested that this is deliberate to get "funding" from various UK and US three letter agencies.

What is known that most systems that have been tested on CCTV systems have been far from a success.

Apparently Boston Airport (Logan) tried two full face systems but got little better than 61% correct recognition and a system that has been running in the London Borough of Newham has not spotted on criminal on the streets even thought there are quite a few "known offenders" living in the borough who are in the database.

Also the Australian SmartGate software using bio-metric passports appears no where as good as people are led to belive.

Second if an attack works then it gets refined and generalized. Maybe the paints don't have to be visible to human eyes etc.

If the camera are working with visible light (and they do; IR is unreliable for biometrics) then there isn't much you can do with "invisible paint."

Finally the attack targets an _automated_ systems. Where have they suggested deploying these? On Urban street and transit camera systems, sporting events, large gatherings of people.

But there are other ways to determine if there is a person in an image like that. People move in a distinctive way, so even with this you're going to look like a person strolling along the street who maybe doesn't have a face.

If it can defeat facial detection would a system even get to recognition? Doesn't the system have to be able to detect the face first?

Yes, but see above. There are other ways to determine if you should run the recognition program. AFAIK This particular one is only effective if the face is in front of the camera, facing it head-on.

The most important part is that this scheme counters ONLY Haar-face based detection algorithms. That's just like only defending against bombs-in-shoes but not bombs generally, and it has the same drawbacks. Bruce has covered the futility of countering a specific technique at length.

i've been wondering for a couple of years whether dazzle patterns could disrupt face recognition software. i am glad someone has investigated it for me.

"Looks like it fools face detection not recognition."

This is true, but consider how face recognition software is likely to be used. It takes a lot of time viewing videotapes from the various feeds these days. In order to save money (wages paid to investigators) a smart thing to do would be to run video feeds through a routine which acts like a sieve, sorting out frames that contain faces from frames that do not. Then the frames can be passed through an algorithm to determine which of those frames might be the person you're looking for in them.

If you break the first part of that sequence then the computer may never recognize that a face (your face) is in a frame in order to process it. The technique may confuse the facial recognition part as well and that just hadn't been experimented with yet by the researcher.

Based on this early research I guess we will not be seeing Facial Recognition Systems doing security at a star trek convention any time soon.

"The most important part is that this scheme counters ONLY Haar-face based detection algorithms. That's just like only defending against bombs-in-shoes but not bombs generally, and it has the same drawbacks."

You are arguing that it "counters only Haar...", when it has "only been tested against Haar...".

The two are not the same thus you cannot say it does not work against other "face detecting" systems untill either it has been tested against them or you can show good grounds for your reasoning. Nor can you argue that it does not work against "face recognition" systems for the same reasons.

Further there are two distinct uses for FR systems,

1, Is this face a match for the credential presented.

2, Does this face match any in the "rouges gallary" DB.

In the first you should actually be looking to "disprove" the match (ie pick up on differences)

In the second you should initialy be looking for similarities (data base reducing searches are "and" not "or").

In the general case "Face detecting" is only going to be used for the latter system.

It would appear that untill 9/11 FDsystems where not investigated that much, and most of the improvments in FR (not FD) where by automaticaly adjusting for "off full face" 2D presentation and other "real time" issues.

And few people have publicaly looked into the various forms of "deception" that might work against either FR or FD systems.

But we do know some FR systems designers have given up on 2D presentation and are now using 3D presentation.

However 3D presentation has distinct limitations in that it works only when the test subject is within a relativly short distance of the stereo camera. And this causes a much increased system cost.

Normaly as a system designer you would not opt to make a "fundementaly limiting" design choice unless there where good reasons to do so. Likewise you would normaly chose the least costly system that works.

So some of the designers of FR systems are certainly aware of 2D presentation short commings and thus may well be aware of the issues of "deception" as they have opted to go for a fundementaly different and considerably more expensive way of building FR systems.

As for your comment,

"... and they do; IR is unreliable for biometrics..."

I for one would be interested to know what you base that on. There are a number of biometric systems that do use "near visable" IR just more effectivly for scanning objects (including faces) for two reasons,

1, Because the human eye is insensitive to it and it does not cause the iris to change.

2, The sensors and optics actualy work better at those wavelengths.

I wonder if instead of fancy colored makeup, a person could apply IR absorbing and IR reflecting makeup instead? Perhaps you'd look normal to creatures with limited eyesight, but enough to screw up machines that don't differentiate between colors.

I recall something (quite recently) about some software which was ment to ensure that a video camera tracked someone's face. So long as someone's skin wasn't "too dark".
So you might not even require something that radical to fool machines...

I believe there are already some limitations (not sure about the legal grounds, but certainly practical) on where you can go with makeup on. For example, I was a clown in San Diego quite a while ago (cue the jokes), and the head clown warned us about not going into banks while in makeup--makes the guards very nervous.

If it works with makeup, might it work with bandages? Much as we'd all like to see Lady Gaga apprehended on suspicion of terrorism, there will surely be less obviously voluntary ways of getting around this.

Everyone seems to be imagining crazy makeup that looks unnatural. Why not paint someone to look like they have a port-wine stain (vascular birthmark)? Or vitiligo? Would that fool the facial detection algorithm?

Did you see the new Iphone app for facial recognition to be used by the police ?
http://www.popsci.com/technology/article/2010-06/...

Wonder if we have to walk around with make-up and when that gets forbidden.

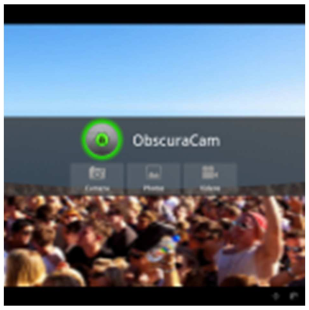
ObscuraCam v2 ALPHA (with video!)

We’ve been making exciting progress with our work on ObscuraCam, part of the SecureSmartCam project with our partner WITNESS. The biggest jump forward is the addition of video support, including automated face detection, pixelization and redaction.

Screenshots below, and soon a video below (also at:
http://youtu.be/9hi4c_DCrkw)

Source code branch is here:
https://github.com/guardianproject/securesmartcam/tree/obscurav2

Latest ALPHA test build at:
https://github.com/guardianproject/SecureSmartCam/ObscuraCam-2.0-Alpha-2.apk/qr_code


ObscuraCam
Camera
Photos
Videos