SESSION ID: FLE-W01

Fakes Aren't Funny: Why Business Needs to Address Image Manipulation Now

Dr. Thomas P. Keenan, FCIPS, I.S.P., ITCP
Professor, School of Architecture, Landscape and Planning and Department of Computer Science
University of Calgary
Calgary, Alberta, Canada
@drfuture
We are all Image Fakers
The Reality...and How Facial Images are Under Scrutiny

www.betafaceapi.com/demo.html
Advertisers and Editors Have Done it For Years

What’s Wrong with This Picture?!?

The picture on the left was taken from the cover of a brochure. The picture on the right was the next photo in the series directly from the photographer. There seems to be a subtle difference in the background.

It could have been Photoshop – which was created in 1987!
A counterfactual conditional “photograph”: If Groucho and Rambo had been at Yalta. Paul Higdon/NYT Pictures.
Not the “National Geographic Photo of the Year”
We Have Put Amazing, Easy to Use, High Quality Image Faking Tools into the Hands of the General Public

- I once asked the photo editor of the *New York Times* if he could detect a fake
  - “I used to be able to see razor blade marks where negatives were cut”
  - “Once it’s been through a computer, there’s no way”

- Adobe Photoshop, InDesign, Gimp, Fotor, Pixlr, Inkscape...

- Photos are increasingly important in a social media world
  - Entire platforms like Instagram and Pintrest are largely image-oriented
  - Tweets with images are 34% more likely to be retweeted
Sometimes Faking is as Simple as Camera Angle
People Line Up for that Rock
Sometimes Fakery is Totally Innocent
Other times it’s not!

Investigators say parents were editing their kids' heads onto stock photos of athletes to help get them into elite colleges.
Fakery Used in Anger: High School Senior Emma Gonzalez
We Are Becoming Photo and Video Skeptics
Videos are Not Immune to Fakery
Jordan Peele as the “Voice of Barack Obama”
Videofakery weaponized for political purposes

REAL VIDEO

DISTORTING REALITY

RUDY GIULIANI PEDDLES DOCTORED VIDEO OF PELOSI

FAKE VIDEO

CNN

4:29 AM PT
White House shares fake video to support punishment of CNN's Jim Acosta

Washington: White House press secretary Sarah Sanders on Wednesday night shared a video of CNN reporter Jim Acosta that appeared to have been edited to make his actions at a news conference look more aggressive than they were.

The edited video looks authentic: Acosta appeared to swiftly chop down on the arm of a White House aide as he held onto a microphone while questioning US President Donald Trump. However in the original video, Acosta's arm appears to move only as a response to a tussle for the microphone. His statement, "Pardon me, ma'am," is not included in the video Sanders shared.
Sarah Sanders has shared a doctored video of CNN reporter Jim Acosta that appears to make his actions at a news conference look more aggressive than they were. This video posted on Twitter @aymanndotcom shows the discrepancies.
Why This is a Critical Business Issue

- We still rely on paper for many business processes
  - Perhaps we scan it, but there’s still a paper stage
  - Small businesses like cheques - they have smaller fees than credit or debit cards, and the business owner can retain and control the records
- Canada had a recent dispute with China over “forged veterinary certificates” for pigs which resulted in export ban
- When we “go paperless” the risks for tampering are even greater
- Most people are honest, but some aren’t, and frontline staff are usually not trained to detect fakes
- Sites that help people cheat have sprung up
Want a Free Drink on the Plane? (Don’t Try This!)
Boarding Pass Paper Stock Used to Be Special!
Oh, You “Lost” that Meal Receipt? No Problem.
I Bought a Guy an $11 Beer at a Conference Recently

Real

JASPER PARK LODGE
1 OLD LODGE ROAD
JASPER AB

CARD 9934
CARD TYPE VISA
DATE 2019/05/27
TIME 4462 18:39:01
RECEIPT NUMBER H85046233-001-137-003-0

PURCHASE

TOTAL

$22.00

FAKE

Jasper Park Lodge
1 Old Lodge Road

05/27/2019 06:39 PM
TAB 9 HOST STEVEN
VISA 9934

QTY 1

AMT $22.00
SUBTOTAL $20.95
CGST $1.05
BALANCE $22.00
Fake Paper Coupons are a Real Problem

7 On Your Side: Fake $50 Lowe's coupons circulating online as part of scam

WASHINGTON (ABC7) — So what are you getting your mom for Mother's Day? If you think Lowe's and Facebook just came to the rescue with a free $50 coupon... guess again. 7 On Your Side reports the coupon caught on fire over on Facebook. A free $50 Mother's Day coupon sounds like a sweet deal!!!
My Own Encounter With Lowes

**CRAFTSMAN 25cc/17 2-Cycle CS+ Gas Trimmer**

**Branding:** CRAFTSMAN 25cc/17 2-Cycle CS+ Gas Trimmer

Lowe's Item #: 829271  
SKU: 13735093 Model: 41AD25CC593

<table>
<thead>
<tr>
<th>Shipping</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>$189.00</td>
<td></td>
</tr>
</tbody>
</table>

**Shipping Details:**
Most orders ready in 2 hours, some orders may take up to 24 Hours. You will receive an email when your order is ready for pick-up.
Photos Play a Big Role in Fraudulent Insurance Claims

Alleged fraudster undone by old photos

Insurance fraud cases 'included photo tricks'

Exaggerated gym injuries and road accidents were among the rising number of fraudulent insurance claims made in the UK, an industry group has said.

A man who cut his thumb in the gym presented a photo of a more serious injury, downloaded from the internet, to try to get a bigger payout.

In another case, 30 bus passengers made whiplash claims in a staged accident.

The Association of British Insurers (ABI) said that fraudulent claims last year were up 5% on 2010.

It said that insurers had detected 139,000 bogus or exaggerated claims in 2011.

'Footing the bill'

Home insurance frauds were the most common, the ABI said, with 71,000 dishonest claims having been detected, valued at £106m.

Pro tip: If you’re going to commit insurance fraud, make sure you don’t post photos that disprove your claim on social media.

That concept was apparently too difficult for a Utah man who was charged with insurance fraud for allegedly filing a false claim, according to local news affiliate ABC 4.

Jason Doyle Cook, 44, filed a claim with American Family Insurance in June 2018, saying that his truck had been damaged when he collided with a wooden post and a semi tire in the middle of the freeway. Cook reported that the crash caused damage to the bed of the truck and the rear brakes. He also claimed that he was towing a trailer, which he said was damaged so severely it was no longer operable.
Check the Metadata

INSURANCE FRAUD? CHECK THE METADATA IN PHOTOS.

Check out the metadata using your favorite picture viewer or IrfanView. Metadata in photos has allowed us to demonstrate that some photos of stolen goods were taken AFTER the theft was reported to an insurance company. Interesting situation! After the receipt of our report it is not unusual to get a call from law enforcement in the beginning of their fraud investigation.

Metadata is important when we do forensic investigations of computers and phones. Often it can detect attempts to alter documents and spreadsheets to fake contents. Judges are very unhappy when this sort of evidence alteration is discovered.

But, metadata can be faked too!
## Integrity Solutions – Starting With the Simplest – File Size

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
<th>Type</th>
<th>Size</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captures</td>
<td>2019-02-20 12:17 AM</td>
<td>File folder</td>
<td></td>
<td></td>
</tr>
<tr>
<td>obama_deep_fake</td>
<td>2018-12-31 11:43 AM</td>
<td>MP4 File</td>
<td>2.843 KB</td>
<td>00:01:12</td>
</tr>
<tr>
<td>obama_deepFake_with_cc</td>
<td>2018-12-31 11:43 AM</td>
<td>MP4 File</td>
<td>2.843 KB</td>
<td>00:01:12</td>
</tr>
</tbody>
</table>
Moving Up to Checksums

A checksum = check + sum = a sum that is used to check the original number. What do we mean by ‘sum’? Simple, you add the numbers like this:

\[ 3 + 8 + 9 + 2 = 22 \implies 2 + 2 \implies 4. \]

This ‘4’ is the checksum. Now, instead of sending 3892, you send 38924. It adds only one digit to the message, instead of four (if you’re sending it twice). When your counterpart receives it, he or she will perform the same ‘sum’, and get ‘4’.

The two of you have already agreed beforehand that the last digit in the message will be the checksum. When your counterpart adds your message to get 4, and sees the checksum is also 4, he or she knows the message is correct.
Checksums Have Limitations

- Offsetting errors
- More than one video can legitimately yield the same checksum (that’s quite unlikely)
- Someone who knows algorithm can defeat it by reverse engineering “bit twiddling”
What Do the Hollywood Pros Use?

The two most widely used algorithms in checksum software are:

- MD5
- SHA-1

Both these algorithms aren’t secure enough for high-security data, but great for error checking and correction. They are also freely available and widely supported on all platforms – Macs, Windows and Linux.

So, how does this work with video? Every time the data is copied to another drive or system, you use the verification software to ensure the data is the exact same. You can also use this to check if any metadata has been changed, and so on. This ensures that every backup is the exact replica of the original camera data.

Social Media is Implementing an “Out of Band” Validation Infrastructure for Businesses
New Technology Fights Child Porn by Tracking Its "PhotoDNA"

December 15, 2009 |

REDMOND, Wash. — Dec. 15, 2009 — Most people will never be exposed to photos of children being sexually abused by predators. But images of that abuse can be found in dark corners of the online world, where networks of child abusers and child-pornography consumers produce and propagate photos of children being victimized.

This week, Microsoft is donating a new technology to the National Center for Missing & Exploited Children (NCMEC) that has the potential to make a drastic difference in the fight against the spread of child pornography online.

The technology, called PhotoDNA, was initially created by Microsoft Research. It was further developed by Hany Farid, a leading digital-imaging expert and professor of computer science at Dartmouth College, to help NCMEC in its efforts to find hidden copies of the worst images of child sexual exploitation known today.
Flexible, highly scalable photo forensics tool

Hidden in the pixel data and the file structure of an image is a wealth of information that could help you gauge its authenticity. Insight, powered by Truepic, exposes this rich set of information, addressing the 2+ billion unverified photos that are captured & uploaded to the internet every day.

Uncovering modern paint forgeries by radiocarbon dating

Laura Hendriks, Irka Hajdas, Ester S. B. Ferreira, Nadim C. Scherrer, Stefan Zumbühl, Gregory D. Smith, Caroline Welte, Lukas Wacker, Hans-Arno Synal, and Detlef Gunther

PNAS first published June 3, 2019 https://doi.org/10.1073/pnas.1901540116

Edited by Katherine Faber, California Institute of Technology, Pasadena, CA, and accepted by Editorial Board Member Tobin J. Marks April 30, 2019 (received for review January 29, 2019)

Significance

Can radiocarbon (¹⁴C) dating uncover modern forgeries? Radiocarbon dating has the potential to answer the question of when an artwork was created, by providing a time frame of the material used. In this study we show that with two microsamples (<500 μg), from both the canvas and the paint layer itself, a modern forgery could be identified. The canvas dating is consistent with the purported attribution to the 19th century; however, the ¹⁴C age gained on the paint contradicts this as it offers clear evidence for a post-1950 creation. Thus the additional dating of the paint reveals the forger's scheme where the repainting of an appropriately aged canvas was used to convey the illusion of authenticity.
There *are* Often Authoritative Sources
My Proposed System Combines Checksum à la PhotoDNA (or similar) and Blockchain

- Trusted source (whitehouse.gov?) sends official image video along with computed checksum
- Link to video and checksum are put on a blockchain, probably a private (permissioned) one
- Consensus mechanism prevents re-entering same video file ID, just as Bitcoin is protected from double spend
- Tampering can be easily detected and earliest version is automatically determined
How Could a Business (Organization, Government, etc.) Actually Do This?

- We need a reliable blockchain infrastructure that will allow us to store a unique video id and a hash
- Best not to make your own blockchain infrastructure
  - Labor intensive
  - Easy to do it wrong
  - 51% attack
- Instead, piggyback onto an existing blockchain infrastructure like Bitcoin or Ethereum Classic and insert data into a comment field in a way that is stored on the chain
Without getting too technical - this is how you could do it in Bitcoin, by transferring 1 Satoshi (ignoring overheads)

1 Satoshi = USD $0.0001113480

*Click the Satoshi value or USD value to change it*

Jul 5, 2019 06:23:00 UTC

Input Scripts

ScriptSig: PUSHDATA(71)
[304402204d9be1defe05e7629e90f57ff7541666d530af39c1d9d8aad0fe402200582f12e9450bc6e6980025c08f53c43c50bc472706e3e9e71fa5724a4bc4d01]
PUSHDATA(33)[0365330363a7e9db476e9d3697eb9d573aa76944b0aadbc347593a793797b689]

Output Scripts

DUP HASH160 PUSHDATA(20)[3c9b62c3ad29f08d13e82b156ebe7057e9bc1b43] EQUALVERIFY CHECKSIG

DUP HASH160 PUSHDATA(20)[c6a3b9d15d3f6915c4b5100c106f2ad1e90c] EQUALVERIFY CHECKSIG

RETURN PUSHDATA(11)[e8b6e6c6b207757f726c64]
(decoded) hello world

DUP HASH160 PUSHDATA(20)[e62287a5ee8b15c7ccc9f9cb7e6692810845] EQUALVERIFY CHECKSIG
I Hope I Have Convinced You That

- Image fakery actually is fun!
- But not if you are the victim of fraud
- The tools to do it are in the hands of everyone who wants them
- You are quite probably being scammed right now
- You can fight back with better technical measures
- You should “pick your battles” and maybe not worry about the free in-flight drink
Ways to Apply this Knowledge Right Away

- Conduct an inventory of points in your company’s business processes that could be vulnerable to image/video manipulation
- Determine the magnitude of the exposure (a free drink or a $200K insurance fraud?)
- Start monitoring fraud trends in your industry with Google keywords etc.
- Please *don’t* fake your RSA expense claim, even if you now can – your employer knows that you were here today!
Three Months from Now You Should be Able to:

- Speak authoritatively about image and document fakery risks in your business and how you are managing them
- Tell great stories about how people in your industry have been victimized by image and video fakery
- Have an ongoing awareness program on fakery
Six Months from Now, and Forever, You Should

- Address the high value risks with better business processes such as bar codes that are harder to tamper with
- Have an ongoing surveillance program around emerging risks
- Have a formal step in all new projects that evaluates fakery risks, quantifies, and attempts to mitigate them
Thank you!

- Dr. Thomas P. Keenan, FCIPS, I.S.P., ITCP
- keenan@ucalgary.ca
- www.technocreep.com
- @drfuture