# Privacy

### 20 Feb 2020

#### We are working with a different problem than standard cryptography

In the privacy world, we have to deal with multimedia (or even objects) that can be “faked” and the authenticity, ownership, origin, tracing, of the multimedia/object needs to be able to be verified. There are a couple of situations where this would be different from standard crypto:

1. Situation where we have an image that we want to find if it has been reposted on the internet. Standard cryptographic hashes are sensitive to even the slightest bit change, which would make it impossible to solve the issue of finding images, since any additional noise would cause the hash to register as a new hashed value.

2. Physical objects cannot be traditionally protected in the same way

#### We work with digital watermarking and robust hashing (fingerprinting)

#### Digital Watermarking is the active method of data hiding

In the world of privacy we care about the metadata (who what when where etc) as well as the actual media (content). Digital watermarking is the act of digital data hiding. We are embedding some data (where is a secret) into the media in order to allow us to verify its authenticity, integrity, or some sort of ownership/tracking information.

It is important to note that quality is a major factor, since the goal is not to deteriorate the quality.

In DDH, the assumption is that before distribution, some sort of active method is employed.

#### Fingerprinting is the passive method of evaluating hashes

This allows us flexibility because we’re able to determine that two images could be the same if the hamming distance of their hashes don’t differ by too much. This allows us to have a method of comparison that doesn’t rely on an active method before distribution. However, of course this would not allow us to solve the problem of ownership necessarily.

### 27 Feb 2020

#### We separate the topics into 3 sub categories

1. Robust Data Hiding

2. Steganography

3. Tamper proofing

Here, the differences lie in the objective of the attackers, and the knowledge of the scheme.

In robust data hiding, the attacker knows that the copyright info exists. The attacker’s goal is thus to remove the watermark.

In secret comm (steganography), the attacker does not know if there is a message in the image. The goal is to detect the presence of a hidden message (done via machine learning, having lots of images with messages with different keys, and clean images in order to classify) Note that the detection of presence does not imply knowing what the message is. The detection itself is plenty hard already.

In tamper proofing, the attacker’s goal is to modify the content such that it is undetectable by the defender.

This is all based on the same technology (overarching)

#### Distance as a concept in hashing

In digital fingerprinting, we talk about a function and a key that generates a binary representation (hash) that has the property that if the distance between x and y images are not far, then the binary rep (hash) distance (hamming) should not be that far off either. This is where the difference is between digital fingerprinting (robust hash) and cryptographic hashes.

Note that in machine learning, there is a process called Autoencoders, that trains a set of encoder decoder architecture that allows you to represent the image in a hash, as well as then take the hash and reconstruct the image. Note that this opens up a challenge in privacy, since we might not want the image to be reconstructed (think fingerprint data: we wish to store the hash and do comparisons to allow biometrics, but we probably dont want the fingerprint itself to be reconstructed because then privacy is compromised. The solution is to add some noise to the binary rep so that reconstruction is not possible even with the ML architecture, there are some slava papers on this)

#### Binary Symmetric Channel

akin to the noisy channel? we have channel where there is a possibility of bit flip. capacity is the measure of bits reliably communicable by the system.

### 05 Mar 2020

#### Standard cryptography can’t solve all issues of security

One of the emphasized points is thinking about the situations where standard cryptography cannot resolve the issue of security in the context that we need. For instance, standard encryption doesn’t really care about the input format (word, image, etc) but we definitely care about the format in relation to security as the end-user, for instance, when we transfer images we are prone to small afflictions and packet loss, which could cause corruption of encryption. Additionally, time-sensitive/efficiency-sensitive activities would cause issues (such as a streaming service). And even if we assumed that we never had data corruption, once the encryption is decrypted, it does not solve the security issue of that information then being spread. This concept is known as the unprotected hole, or a variation of the situation where copyright in images is harder to detect when the image is print to analogue (newspaper for instance) called the analogue hole. The idea here is that in certain contexts security really needs to be “built in” or constant, but standard crypto might not be robust enough to solve these issues.

### 12 Mar 2020

#### Watermarking is a detection problem (yes/no)

While data hiding could deal with hidden data and potential extraction of said data. The slight nuance in definition here. We can consider and think about data-hiding as a communication through an unreliable channel. We have to address capacity.

#### Watermarking and DH can be prone to security leakages

For instance, there are cases where we can accidentally leak information about the key from the watermark itself, and that is a security consideration that we have to keep in mind.

#### Stochastics and Perceptual invisibility

Seen from the stego notes, we can skip in favor of the paper notes

#### The tradeoffs of security, robustness, and visibility within watermarking, steganography, and data hiding is at the core of the discussion.

This is considered an exam question. Explain the tradeoffs, and what each specification of the field is looking for and giving up in order to achieve their goals.

We consider:

- Content related/unrelated messages

- message existence known/unknown

The applications here on robust watermarking, IP guarantees, authentication, tracking, fragile watermarks, tamperproofing, content recovery, overt embedded communications, media tracking, control of access, etc...

In a watermarking scheme, we can consider that each transaction will be re-watermarked specifically tailored to that transaction, to state the rights and usage agreements. And we expect that watermark to survive even after attempts at removing it.