Demo: Blockchain-grade privacy protection in surveillance systems

Andrea Zanotto
DISI, University of Trento
andrea.zanotto@studenti.unitn.it

Nicola Conci
DISI, University of Trento
nicola.conci@unitn.it

Alberto Montresor
DISI, University of Trento
alberto.montresor@unitn.it

ABSTRACT

We propose a solution to increase the privacy of people recorded with security cameras without decreasing the details stored in the videos. We strongly believe that CCTV recordings are a necessary and precious source of information to be analyzed when a crime or other unfortunate events happen; for this reason, we would like to have powerful surveillance systems that are able to hide the identity of the recorded people while allowing subsequent recovery of the data.

We use face morphing algorithms in order to transform the faces in such a way that the protected video keeps the original likeness but does not leak sensitive face information. We store the transformed information in a decentralized way and we adopt smart contracts on permissioned blockchains to guarantee that in order to retrieve the data, a collection of trusted authorities must give their consent.

KEYWORDS

Surveillance system; privacy protection; face morphing; Hyperledger Fabric blockchain.

INTRODUCTION

In the past, the resolution and the frame rate of surveillance videos were not high enough to allow precise identification of subjects, so privacy issues were limited. However, technology breakthroughs and the need for sharp details led to high-resolution images from which it is possible to extract a lot of data, both for legitimate and less legitimate purposes. For this reason, we think that it is useful to build a system that is able to protect privacy by design and that does not allow anyone to extract identification features, unless a group of trusted authorities decide otherwise.

LOSSY PROTECTION

In order to protect privacy, we first analyzed solutions that remove sensitive features. They can be powerful at protecting identities, but they lack a way to recover the erased information. Examples of these techniques can be: pixelization, blurring, masking or downscaling. Using such techniques, however, makes not possible to recover the lost details afterward. Other techniques that can provide both secrecy and recovery are based on encryption; the problem, however, is just moved one step way to the holder of the decryption key. Furthermore, the decryption is "all or nothing": you cannot unlock the video just to have an overview of the situation; when you do that, all details are available. An intermediate solution could be to only encrypt some areas of the video, such as the face of the people, but then the image becomes fragile as the change in one pixel could completely destroy the encrypted information.

LOSSLESS APPROACH

We wanted a solution that protects sensitive features while allowing their recovery, and a reversible face transformation was the right compromise. The idea is a system that detects the faces in images and applies to them a reversible transformation that hides the sensitive features. To revert the function, we need a set of parameters that will be the key to unlock the images. The transformation is a face morphing that hides the original face into a target one. The result will be a combination of the two, where it is not possible to extract the original data without the secret parameters. This approach allows to keep the imagery likeness, because the mask applied is still a face, but it is a completely new one. The parameters and the target face, together, become the morphing key and this information must be kept secret because it is used to unlock the imagery.

In our design, the faces in videos must be morphed so that it is not possible to identify the people in the video [1]. Then the parameters needed to unlock the video must be kept secret until there is the legit need to recognize some identities (probably because of a crime or other critical events). The decision to retrieve private information must be validated by a group of trusted authorities before being approved.

We want to guarantee secrecy, integrity, availability and access control in a decentralized fashion. By decentralizing the resources and the decision making we force more authorities to reach an agreement on how to deal with the data and disallow any of them to have full control. All these requirements can be achieved with a permissioned blockchain, and we choose to use the Hyperledger Fabric blockchain framework implementation [2]. The real-world authorities can be mapped on Hyperledger organizations that are a managed logical group of entities and resources in which there is usually a degree of mutual trust between them. As an example, an organization can be a local police department or the regional court with all the respective servers and employees.

For this demo, we assume that hiding the facial feature is enough to protect the privacy, and we work with frontal still images. However, this is only a possibility and it can be extended in order to use other protections.

We use face detection algorithms that are able to detect faces by recognizing a number of facial points that will be used to perform the morphing.

As soon as a new image is ready, we need to compose the key that will be used to hide the original face. The first thing to choose is the target face, that is the face behind which we will hide the original one. It can be chosen randomly from a big and secret set or it can be generated on-the-fly, in order to increase the security. The second group of parameters are the *interpolation strength* and the *intensity strength*. The first control how much the resulted-face points will depend on the original or the target face, the latter control the dependency of the resulted colors taken from the two images. They range from 0 to 1, where 0 means completely dependent on the original one, 1 completely dependent on the target. A safe range that guarantees both privacy and good recovery is between 0.6 and 0.9 for both interpolation and intensity values [1].

Once we have determined the key parameters, we need to store them in order to guarantee secrecy. To avoid having a single organization that controls the data, we split each of them into $\boldsymbol{n}$ pieces and we require at least $\boldsymbol{k}$ parts to rebuild the information. These values are completely customizable under the constraint that $\boldsymbol{k} \leq \boldsymbol{n}$. By splitting the data, at least $\boldsymbol{k}$ organizations must reach an agreement before the original data can be reconstructed. To achieve this, we use a Javascript implementation of the Shamir's secret sharing [3] together with a Hyperledger fabric smart contract (chaincode).

The Hyperledger private data feature allows private information exchange between the organizations. Every organization has the same chaincode source code, but a different definition of the private data. In particular, every organization specifies itself as the only entity that can access the data exchanged through its chaincode.

When an image has been elaborated and it is ready, the client camera splits the secret data into $\boldsymbol{n}$ parts, equals to the number of the organizations, and then uses the $\boldsymbol{n}$ corresponding chaincodes to send one piece to every organization. For the recovery part, an authorized client uses the same chaincodes to ask the retrieval of some particular record. The chaincodes that manage the data exchange can be coded with an arbitrary complex and flexible algorithm that states who can request the data and which requisites it needs to satisfy before its request can be approved. The power of having the data split into multiple pieces is that to compromise the system, at least $\boldsymbol{k}$ organizations must be under control of an attacker before having access to the secret data. Once all the pieces have been collected, the client combines them together and reconstruct the secret parameters. These parameters are the used in de-morphing algorithms that are able to invert the function and recover the original hidden face.

REFERENCES

[1] P. Korshunov and T. Ebrahimi. Using face morphing to protect privacy. In 2013 10th IEEE International Conference on Advanced Video and Signal Based Surveillance, pages 208–213, Aug 2013.

[2] Hyperledger fabric. https://www.hyperledger.org/projects/fabric/.

[3] Adi Shamir. How to share a secret. Commun. ACM, 22(11):612–613, November 1979.

[4] Actress Anna Unterberger. https://commons.wikimedia.org/wiki/File:Actress Anna Unterberger-2.jpg, 2012.

[5] Governor Tim Pawlenty. https://commons.wikimedia.org/wiki/File:Tim Pawlenty official photo.jpg, 2009.

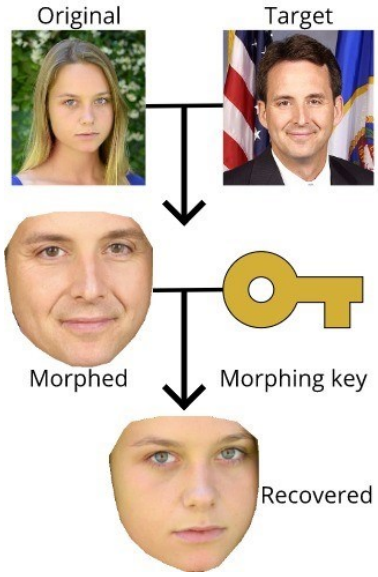

Figure 1: Example of morphed and demorphed faces

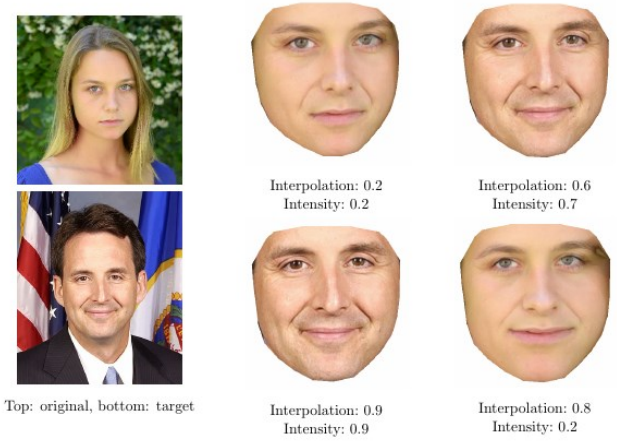

Figure 2: Example of morphing with different parameters. People in the photo: [4][5]

Icon taken from https://material.io/tools/icons/