Asasec Advisory System Against Sexual Exploitation of Children

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission - Directorate-General Justice, Freedom and Security

How to find an image despite it has been modified.

Authors

Diego García Ordás – ULE
Laura Fernández Robles – ULE
María Teresa García Ordás – ULE
Óscar García-Olalla – ULE
Enrique Alegre Gutiérrez – ULE

Abstract

Image manipulation is a common and simple technique that can be carried out by the vast majority of people. It can be useful in many situations: to correct image imperfections, to improve its appearance or just to create art, but it can also be used with malicious purposes. For this reason, image manipulation, whether it is voluntary (face obfuscation, frame adding or watermarking) or involuntary (format and compression changes), has become a problem when we need to search or identify images in big datasets. To fight against this problem, a technique called *similarity search* is used. This technique is based on perceptual hashing, but unfortunately perceptual hashing methods are not robust against all kind of possible manipulations. University of León (ULE), within the framework of the ASASEC European project, is working to provide a perceptual hashing solution that outperforms current techniques.

Content

It is said that a picture is worth a thousand words and that is the reason why we are interested in manipulating images at our will with different purposes. Image manipulation is a powerful process that was born almost at the same time than photography and it has been used all along history in numerous contexts, sometimes with cosmetic purposes (Figure 1) and sometimes with politic purposes (Figure 2). Nowadays, this process is open to everyone since the easy access to image manipulation software means that singular skills are no longer required. One proof of this is that lots of teenagers with basic computer knowledge touch up images when sharing them in their social networks.

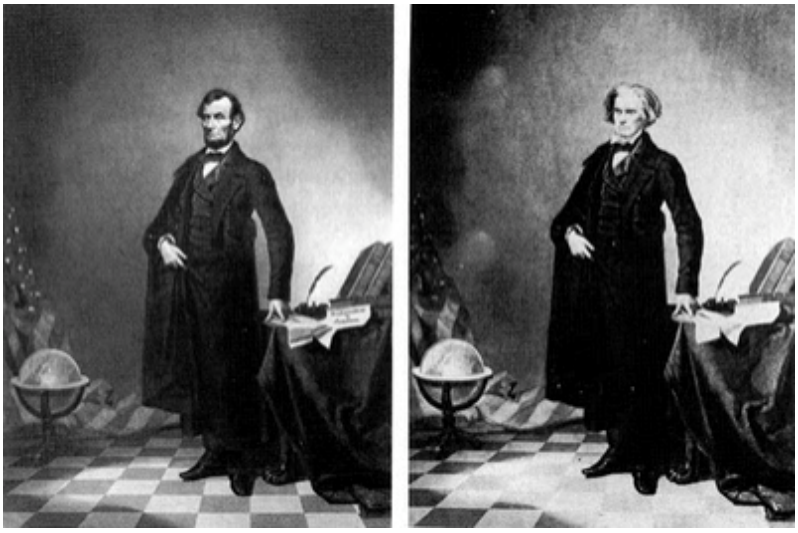

Figure 1: Abraham Lincoln's head on John Calhoun's body (1860).

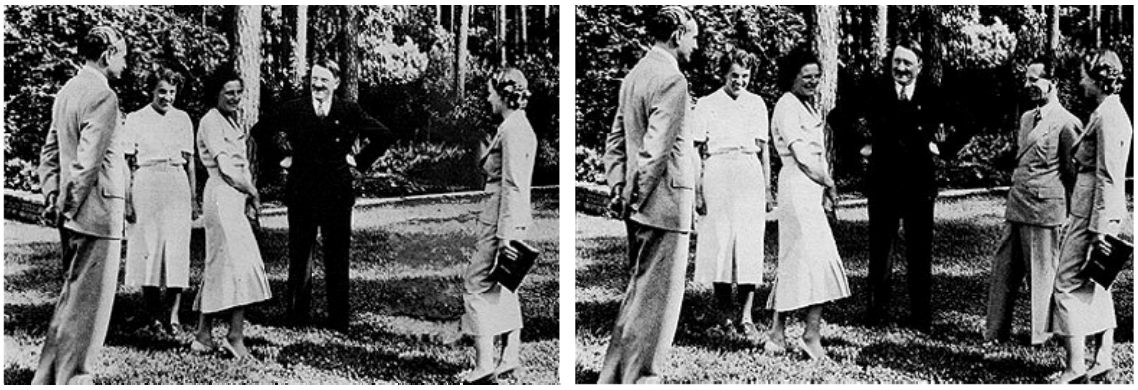

Figure 2: Nazi propaganda minister removed from the picture.

In that way, image manipulation has become an obstruction in some domains like the fight against child pornography, which is the object of our study. One of the main clues followed by police when investigating this kind of crimes is the detection of illegal images. At the beginning of the child pornography prosecution, a suspect image was contrasted against a dataset compound of previously marked as illegal images, and if there was a positive match, that new image was also marked as illegal. However at the moment, confiscated images can be exactly no equal but just visually similar, because they have suffered any kind of manipulation (compression, size changes, brightness and contrast changes, face obfuscation, etc.). This becomes a serious obstacle because that new image will not be categorized as illegal and criminals could take advantage of this deficiency. To avoid this phenomenon, we can use a process called *similarity search* that allows us to find not only identical images but also images that are similar to a given one. One of the most commonly used methods of *similarity search* is *robust or perceptual hashing,* which will be discussed later.

ASASEC (Advisory System Against Sexual Exploitation of Children) is a European research project whose goal is to provide a technological solution to help the fight against child pornography. A consortium of public and private entities expert in innovative technology is developing this project; they are INTECO (Communication Technologies National Institute), University of León, Official Association of University Graduates in Computer Science, Technological Investigation Brigade of the Spanish National Police and Polytechnic University of Madrid.

University of León is developing and testing one of the most innovative tasks of ASASEC project, the use of artificial vision techniques to analyse evidences in child pornography databases.

In particular, University of León is working on several artificial vision methods, among them:

- **Entity detection:** Illegal images usually contain entities or clues that the police, given their experience, can recognize from past crime scenes. Therefore, scenarios and evidences can be manually tracked and analysed. University of León is creating an automatic system for clue detection. Using this system, the police, will be able to perform this task in an automatized way.
- **Scene categorization and tampering detection using perceptual hashes:** As we previously said, it is common to manipulate illegal images (face obfuscation, watermarking, etc.) making difficult their categorization using the current cryptographic hash methods. University of León is creating a perceptual hashing method, robust against all of these modifications to substitute present systems.

Finding images using perceptual hashing

A hash is a unique identifier associated to a file, some kind of summary of the file based on its content. Broadly speaking, generating a hash from a file is similar to convert that file in a piece of representative “text”.

Perceptual hashing is a subset of hashing usually applied to images. It consists of extracting a simple representation of the image, in such a way that small changes over the image from the point of view of human perceptual systems imply small changes on its perceptual hash, and similarly, large changes over the image imply large variations of its perceptual hash (Figure 3).

Figure 3: Left: original image, right: modified image due to color changes. MD5 cryptographic hash extracted from the original image: *"bb4f0a96c77e8737d02755457c2e49c8``*, MD5 cryptographic hash extracted from manipulated image: *"6d4d51dfc23becf3edb0019448f78c8c``*. Perceptual Hash (pHash dct) extracted from original image: *"4e1e4967f518cec2"*, Perceptual Hash (pHash dct) extracted from manipulated image: *"4e1e5d47b518cec0".'*

As we can see in these pictures, both are very similar from the point of view of human visual systems, however, a cryptographic hash (MD5 is shown in the figure) is not able to reflect this similarity. We can use cryptographic hashing to verify the integrity of a

picture, but this kind of hash does not offer information about the picture's visual structure. As we can observe, the cryptographic hashes of both images show no similarity at all, however, perceptual hashes do. When images are similar, distance between their perceptual hashes is very low, and in the same way, if both images are slightly different, their perceptual hashes will be very far away in distance terms. Perceptual hashes reflect the relationship between the similarity of two images and the distances between their hashes.

If the perceptual hash of the images in a dataset is known, it is easy to perform searches and image categorization. If we have a dataset with millions of images and we want to look for a specific image, an automatic exhaustive search will take too long: Images should be checked one by one to determine if there is a match. Besides, if our image has suffered some kind of modification (compression, format and size changes, brightness and contrast changes…), a match will probably not be found, because there is no image in our dataset that provides a perfect match with the current one. This problem can be solved using perceptual hashes. Hence, each image would be associated to a fixed-size hash (usually lower or equal than 512 bits, depending on the used method), which is faster than when comparing complete images and also robust against several types of modifications.

Current systems use cryptographic hashes for confiscated images and video indexing. Cryptographic hash does rely on the image binary structure - the binary code used to store that image in a computer - rather than on human perceptual system over an image. For this reason, the change of one single bit, almost imperceptible for human eye, would result in the generation of a completely different cryptographic hash that will not allow us to discern if both images are the same from human perception point of view. As mentioned before, it is very common to manipulate images: colour correction, watermarking, rotations, scales, compressions, etc. For that reason, University of León proposes the use of perceptual hashes, robust against all kind of manipulations within the frame of the ASASEC project.

Current Proposals

Nowadays thanks to perceptual hashing, we can detect almost any manipulated picture that allows the police to detect illegal images. Let us do an overview to some of the methods used to generate perceptual hashes. Yuenan Li et al [4] obtain a hash robust against rotations using a modification of Gabor filter, achieving a good balance between robustness and discriminability. Longjiang Yu et al.[9] propose a method robust against compressions and scales using Cosine Discrete Transform to extract the hash taking into account the low frequencies of the image, that contains the perceptual basic structure of the image. Another works such as Jinglong Zuo [10], Monga Vishal [6] or Chen Brenden [2] present robust methods against compressions, scales and rotations. There are also methods capable of detecting malicious manipulations, Ahmed Fawad [1], Sujoy Roy [7] and Han-ling Zhang [5], that can be used for tampering detection. In this research line, Farid [3] proposes a method to analyse compression changes over images to detect artefacts that unveil the presence of spliced regions. There are also some approaches that solve specific problems for example Senel Kamil [8] applies perceptual hashing for face recognition for biometric authentication, extracting robust hashes from face images.

As we can observe, there is not a perceptual hash capable of solving all types of modifications that an image can suffer. Some hashes are good against some types of attacks like changes in scale and compressions and other hashes are good against rotations or other kind of modifications.

ASASEC project needs a solution robust against all kind of attacks that images of child pornography usually suffer. University of León is working in this challenging task, trying to combine and improve existing methods in order to diminish their deficiencies and adapt them to our needs.

Conclusions

Cryptographic hashing methods commonly used are not very adequate for *similarity search*, required in child pornography datasets. For that reason, University of León proposes the use of perceptual hashes. This type of hashes is generated based on the content of the perceptual structure of the image from a human observer point of view, instead of being generated based on the binary structure of the image. However, there are many techniques we can use to generate perceptual hashes, each of one with their advantages and limitations, so it is necessary to develop new useful solutions for our specific problem. University of León is actively working in the search of this solution in the frame of the ASASEC European project, collaborating with several public and private entities.

Once this general purpose hashing techniques are released, their use will not be limited to the exclusive needs of this project. On the contrary, they can also be used in different contexts, for example authorship protection in video sites like YouTube or the search of images by content on image management systems.

References

[1] F. Ahmed and M.Y. Siyal. A secure and robust hashing scheme for image authentication. In Information, Communications and Signal Processing, 2005 Fifth International Conference on, pages 705 –709, 0-0 2005.

[2] B. Chen and V. Chandran. Robust image hashing using higher order spectral features. In Digital Image Computing: Techniques and Applications (DICTA), 2010 International Conference on, pages 100 –104, dec. 2010.

H. Farid. Exposing digital forgeries from jpeg ghosts. Information Forensics and Security, IEEE Transactions on, 4(1):154 –160, march 2009.

[4] Yuenan Li, Zheming Lu, Ce Zhu, and Xi- amu Niu. Robust image hashing based on random gabor filtering and dithered lattice vector quantization. Image Processing, IEEE Transactions on, 21(4):1963 –1980, april 2012.

[5] Han ling Zhang, Cai qiong Xiong, and Guang zhi Geng. Content based image hashing robust to geometric transformations. In Electronic Commerce and Security, 2009. ISECS '09. Second International Symposium on, volume 2, pages 105 –108, may 2009.

[6] V. Monga and M.K. Mhcak. Robust and secure image hashing via non-negative matrix factorizations. Information Forensics and Security, IEEE Transactions on, 2(3):376 –390, sept. 2007.

[7] Sujoy Roy and Qibin Sun. Robust hash for detecting and localizing image tampering. In Image Processing, 2007. ICIP 2007. IEEE International Conference on, volume 6, pages VI –117 –VI –120, 16 2007-oct. 19 2007.

[8] K. Senel, M.K. Mihç andak, and V. Monga. A learning framework for robust hashing of face images. In Image Processing (ICIP), 2010 17th IEEE International Conference

on, pages 197 –200, sept. 2010.

[9] Longjiang Yu and Shenghe Sun. Image robust hashing based on dct sign. In Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH-MSP '06. International Conference on, pages 131 –134, dec. 2006.

[10] Jinglong Zuo and Delong Cui. Retrieval oriented robust image hashing. In Industrial Mechatronics and Automation, 2009. ICIMA 2009. International Conference on, pages 379 –381, may 2009.