DOI: 10.20396/revpibic2720191762

Visual Cryptography and Steganography in High Quality Digital Images and Audio Files

Leandro H. Ribeiro*, Hélio Pedrini

Abstract
Visual cryptography is a technique that consists in dividing an image into other *n* images (denominated *shares*), so that only with a superposition of $k \leq n$ of them the input image can be reconstructed. In the method proposed by Naor and Shamir [1], this superposition can be digitally made, through software, or physically, printing the shares in transparencies and then stacking them. However, it is limited to operating with binary images. In this work, a technique of visual cryptography specific for the digital context is developed, with the advantage of operating in monochromatic and colored images, given that little modifications would be necessary to functioning in deeper images and even audio files. The similarities between the original and reconstructed images from the shares were superior to 97% in all the experiments conducted. In addition, techniques of steganography are employed so that the shares have visual meaning, differently from what happens with the method proposed by Naor and Shamir [1], in which they are visually random. Both approaches were compared and the proposed method demonstrated to be robust to digital applications.

Key words:
Cryptography, Steganography, Images.

Introduction

Cryptography is the study of the principles and techniques used to protect the exchange confidential information. To make it simple, cryptographic methods transform a determined message (text, image, audio, video) into an unintelligible code, in a way that only authorized people can restore the original information, that is, the secret. One of these techniques is the visual cryptography, developed initially by Naor and Shamir [1], in 1994. The principle used is the following: given a binary image, it is divided into other *n* images, also binary, denominated *shares.* In order to obtain the original message, it is necessary to superpose $k \leq n$ shares. With $k - 1$ shares, no information of the secret is revealed. The method works both on real images (printing the shares in transparencies and stacking them, to show the secret) and on digital images, but it is limited to binary images. In this work, a visual cryptography technique to operate both on monochromatic and colored images, with little loss of quality in the recovered images, is developed and evaluated. The method makes use of steganography since the information of the original image is hidden by two other images. Thus, the shares are not simply random images that hide the secret, but visual representations, with meaning. It is worthwhile to mention that it also operates on audio files. In contrast, the method is only applicable to digital files since the superposition of shares is done through computer operations. Moreover, it was idealized to work with only two shares.

Results and Discussion

The idea behing the developed algorithm is to combine visual cryptography and steganography to generate two shares that hide the secret image and have visual meaning. From the point of view of the *recovered* image, the loss of quality is very low, because it is guaranteed that each pixel can only differ in one unit in comparison to that of the original image. Although the *shares* are not random images, their quality it is not high, being similar to binary images. Next, we have the two shares generated and the secret image, which can be recovered from them. It is important to mention that not even a single pixel can be retrieved with only one of the shares.

Image 1. The shares (both on the left) generated by the algorithm operating on RGB images. Despite their appearance, they are RGB images. It is only possible to recover the secret image (the cat, in this case) from both.

Conclusions

The method proposed by Naor and Shamir [1] perform a very important function, since the shares can be digital or printed in transparencies. However, the secrets limit themselves to binary images and there is a great loss of quality of the recovered image. In this context, the approach proposed in this work allows a visual cryptography in high quality digital images and in a way to minimize loss of quality of the secret. In addition, it can operate on monochromatic images, on colored ones and even on audio files. It is worth mentioning that the algorithm is less generic, idealized to generate only two shares that must be digital images, since computational operations are necessary to superpose them. Moreover, the shares are not visually random images, since the usage of steganography allows that they are covered by binary images. These two factors are fundamental to allow the utilization of visual cryptography in several digital applications.

---

[1] M. Naor A. Shamir. Visual Cryptography. In: De Santis A. (eds) Advances in Cryptology - EUROCRYPT 1994. Lecture Notes in Computer Science, vol 950. Springer, Berlin, Heidelberg, 1994.