13. Optical encryption by computational ghost imaging

Enrique Tajahuerce and Jesús Lancis

Universitat Jaume I

Status

Computational imaging uses digital sensors, optics, and computation, together with microstructured illumination or coded apertures, to develop novel imaging applications. It operates by optical coding followed by computational decoding, as do many optical security and encryption techniques. In fact, the well-known double-random phase encryption procedure can be understood as a secure coded-aperture imaging technique [1]. Likewise, digital holographic encryption techniques require computation to decode encrypted images from interferometric information [127]. In this section we focus on the application of computational ghost imaging (CGI) to encryption.

Computational imaging with single-pixel detectors enables spatial information to be obtained of an object by sampling the scene with a set of microstructured light patterns [128]. A simple bucked detector records the signal associated with each pattern and the image is reconstructed by mathematical algorithms. In the case of ghost imaging, the information is encoded in the correlation of the intensity fluctuations of two light signals [129]. The first, the reference signal, measures the intensity distribution of the light illuminating the object, while the second, the object signal, collects the total amount of light interacting with the object. The computational version, CGI, emulates numerically the optical propagation through the reference arm, enabling imaging the object by just a bucket detector [130].

Image encryption with CGI is a cryptography technique with a modified symmetric key [63]. The idea is outlined in figure 19(a). The coherent light beam illuminates a phase-only spatial light modulator (LCoS) codifying a set of N different random phase distributions sequentially. Propagation of the light beam generates a corresponding set of N speckle patterns onto the object (O) which can be evaluated numerically. By measuring the total intensity, the bucked detector (BD) provides the projections of the object onto the patterns. The object is recovered by correlating the speckle patterns and the measured projections. Only with the proper set of speckle patterns, the key, is it possible to recover the image of the object. The bottom pictures in figure 19 show an example of encryption. Figure 19(b) is the image to be encrypted, (c) the decrypted image, and (c) an attempt of decryption with the wrong key. An outline of the optical encryption methods is depicted in figure 20. Several encryption techniques based on this idea have recently been reported [131, 132]. A similar approach for information authentication can be seen in section 14.

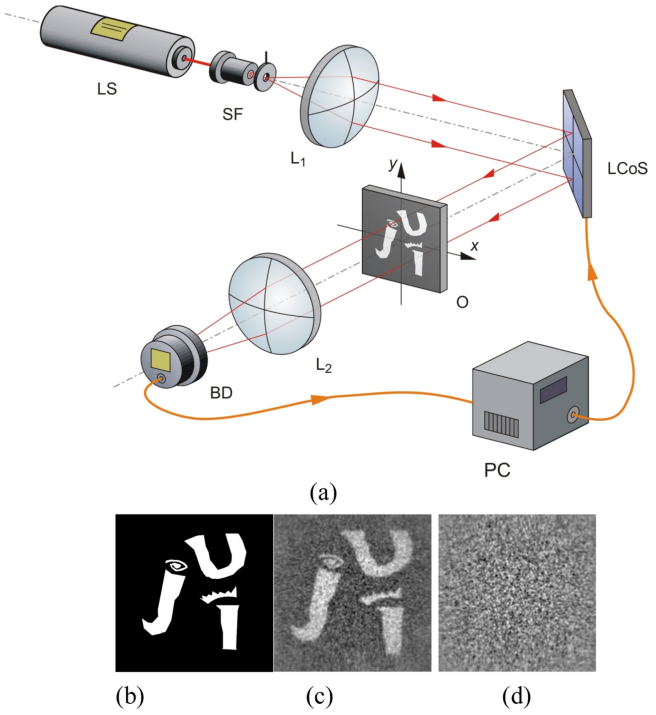

Figure 19. Optical encryption by using computational ghost imaging. Reproduced with permission from [63].

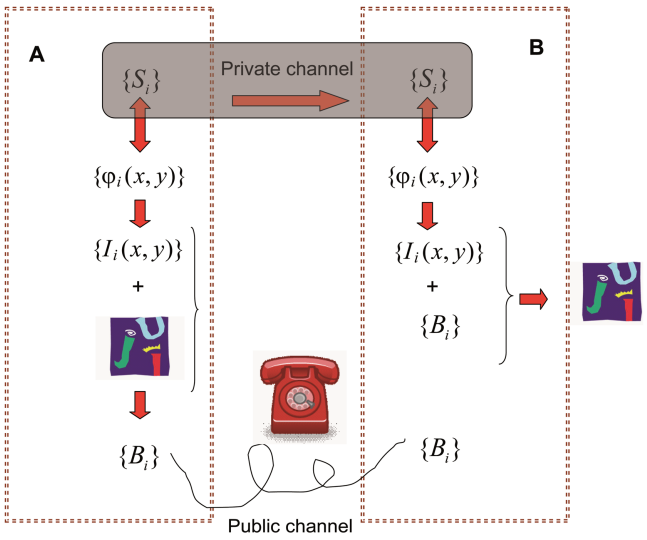

Figure 20. Outline of the optical encryption system [63]. The transmitter (A) and the receiver (B) share a secret key {Si} generating the phase distributions $\phi_i(x, y)$ in the SLM (LCoS) in figure 19. The information is encrypted on a vector containing the intensity values {Bi} detected by the single-pixel detector (BD) in figure 19.

Current and future challenges

Optical systems employed in encryption by CGI are simple, robust, and secure. In contrast to other optical security techniques, the encrypted version of the object is not a complex-valued matrix but just an intensity vector, which reduces the number of bits to be sent. Moreover, by avoiding sensor arrays it is possible to add new degrees of freedom to the sensing process. However there are still some limitations and

challenges to face related with security, acquisition time and detection schemes.

Some recent research in encryption by CGI has focused on increasing the security of the method against eavesdropping attacks. In one approach the sensing pattern is not reproduced in the computer but measured by a digital camera, and security is increased by manipulating the correlation position of the reference and object beams [133]. One challenge in this direction could be to explore the use of non-thermal sources such as those used for quantum ghost imaging for ghost encryption.

Because of the sequential nature of the projection method, it will be crucial to decrease the acquisition time to improve the performance of this encryption technique. One approach is by using recent advances in compressive sensing techniques (see section 7). In fact, computational imaging with single-pixel techniques is very well adapted to apply compressive sensing strategies. This will improve the reconstruction quality by using the same, or even less, number of realizations. The first schemes have already been proposed both in CGI and optical encryption by CGI [134]. Another approach to reduce the acquisition time is by employing faster spatial light modulators (SLMs) operating at high frequencies. To this end, it could be necessary to find new ways to codify phase distributions. Finally, an interesting method in this direction may be to use adaptive techniques that reduce the number of sensing patterns by iterative approaches.

The single-pixel detection scheme characteristic of ghost imaging techniques should allow systems to be developed with very sensitive light sensors, to explore unusual spectral bands for imaging, or to use exotic photodetectors such as spectropolarimeters. These ideas, which have been developed already in other single-pixel imaging techniques, could improve encryption operations by CGI.

Advances in science and technology to meet challenges

As happens with other optical encryption techniques, the main advance to increase security in encryption by CGI will arise by developing non symmetric keys (see sections 4 and 6). In this way it will be possible to use public keys for encryption and private keys for decryption, avoiding transmission of the key by secure channels. We also believe that encryption by CGI will benefit from general advances in quantum imaging [129]. Most likely, the advantages of using quantum properties of light will enhance security in ghost imaging devices.

Regarding time acquisition issues, on the one hand, the development of new compressive sensing strategies will be fundamental for practical applications of encryption by CGI. Some research in this field tries to find appropriate combinations of the base of functions to generate the sensing patterns and the base of functions used to apply the compression algorithms. Also, development of encryption techniques using deterministic patterns for sampling, instead of random ones, can be the key to develop new efficient applications. On the other hand, optical encryption by CGI, as for any other single-pixel imaging technique, will benefit from the development of faster SLMs. Currently, the fastest 2D devices are ferroelectric liquid crystal SLMs, able to work at frequencies of the order of kHz, and digital micromirror devices (DMDs), which modulate patterns at frequencies of the order of tenths of kHz. A promising technique for very fast modulation is that of microelectromechanical system (MEMS) based diffractive SLMs, which are able to work at hundreds of kHz but in linear array configurations.

Advances in light detectors will have a significant impact in the development of optical encryption by CGI. The development of sensors with high sensitivity, high dynamic range and low noise will allow using fast SLMs even with low light levels. Besides, by using multidimensional detectors, able to measure different optical parameters such as polarization, phase, or spectral content, it will be possible to consider more keys, and the technique will improve into a more versatile and secure encryption method.

Concluding remarks

Encryption by CGI is a promising optical security method with several advantages over other optical approaches. The optical system is simple and robust providing a high level of security. The simplicity of the light sensor device makes it a good approach to encrypt multidimensional information. However several challenges still remain, such as the need of a symmetric key and the time required for sequential operation. Recent advances in SLM technology and light detectors will allow these encryption systems to operate at high speed. Besides, the fact that CGI comes from the evolution of quantum imaging, and therefore both techniques are closely related, could be further explored in the near future giving rise perhaps to more secure optical encrypting methods.

Acknowledgments

We acknowledge financial support from MINECO (grant FIS2013-40666-P), Generalitat Valenciana (grants PROMETEO2012-021 and ISIC 2012/013), and Universitat Jaume I (P1-1B2012-55).