Holographic encryption

Nicolas Pavillon

January 2017

Holography has the ability of recording the full information of an electromagnetic wave. Its most popular feature is the possibility of rendering 3D images by projecting fields through the propagation of waves along with their phase information.
As it also has properties of information encoding and data compression, it has been proposed to employ holography to encrypt images, especially as it can record the encrypted information directly on the storage medium.

1 Introduction

Holography encodes the field information by recording the interference between the image to encode and a known reference field (* is the complex conjugate) as

$$\begin{aligned} I &= |o + r|^2 , \\ &= |o|^2 + |r|^2 + or^* + o^* r. \end{aligned} \tag{1}$$

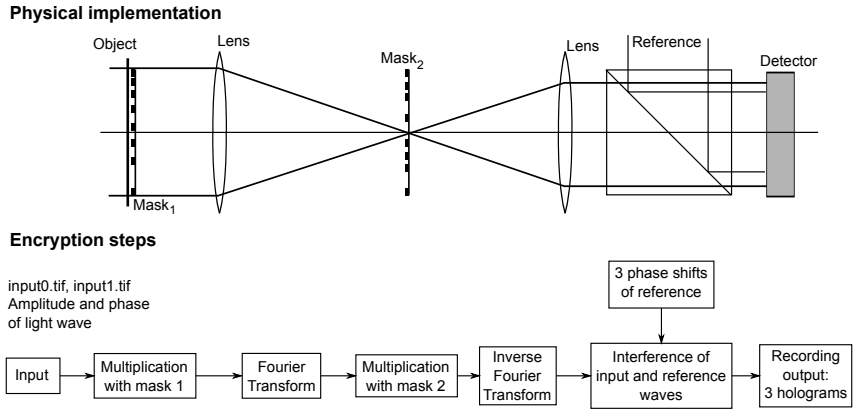
A hologram is therefore an image which contains both the intensity of the object (as a standard image), and the field information o as amplitude and phase. This method can be applied with a physical recording medium or a digital recording device for computer processing [1].

There are various methods in order to recover the field o from the hologram. The method employed here is phase-shifting [2], where several holograms are recorded with reference waves having difference phase shifts, i.e. $\varphi_r = \varphi_0 + n\Delta\varphi,\ n = 0, 1, 2, ...$ The object field can then be recovered through linear combinations of the holograms. The method employed here is 3-step phase-shifting, with $\Delta\varphi = \pi/3$, $\varphi_0 = 0$ and $n \in [0, 2]$. If the object field is defined by its amplitude O and phase φ_o as $o = Oe^{\mathrm{i}\varphi_o}$, it can be showed that the field can be recovered from the three holograms I_1, I_2, and I_3 as

$$\begin{aligned} a &= 2I_1 - 3I_2 + I_3, \\ b &= \sqrt{3}(I_2 - I_3), \\ O &= \sqrt{a^2 + b^2}, \\ \varphi_o &= \tan^{-1}(a/b). \end{aligned} \tag{2}$$

2 Holographic encryption

The encryption in holography can be performed by employing phase masks which alter the field before propagation. This makes the image unrecognizable when recorded. As the physical change of the field propagation is reversible, the image can be recovered by applying the mask back when back-propagating the recorded pattern. The masks can therefore be employed as encryption keys; in case of a digital setup, the phase values can be chosen arbitrarily at each pixel. To ensure fixed values, the masks are encoded as integer values between 0 and N. The actual phase values can then be distributed throughout $[0, 2\pi[$ by coding them as $\theta = x/N \cdot 2\pi$, where x is the mask value.



The encryption scheme employed here is a Fourier encryption scheme, where the Fourier transform is optically performed at the focal plane of a lens (see schematics). The encryption is based on two phase masks, where one is placed right after the object, and the second is located at the Fourier plane of the lens [3]. The beam then interferes with the reference, where the hologram is recorded by the detector. In that settings, the encryption process of an image P is given by

$$C = \mathscr{F}^{-1}\{y \cdot \mathscr{F}[x \cdot P]\}, \tag{3}$$

where x, y are the two phase masks, and $\mathscr{F}$ is the Fourier transform operator.

This method can lead to very large keys, as an image of 64×64 pixels with one pure binary mask already implies a key space of 2^{4096} possibilities. However, the encryption scheme suffers from several weaknesses, in particular in regards to its linearity.

3 References

1. T. Kreis, "Handbook of Holographic Interferometry: Optical and Digital Methods", (2004), ISBN: 978-3-527-40546-6.

2. I. Yamaguchi, and T. Zhang, "Phase-shifting digital holography", *Opt. Lett.* **22**, pp. 1268–1270 (1997).

3. B. Javidi, and T. Nomura, "Securing information by use of digital holography", *Opt. Lett.* **25**, pp. 28–30 (2000).