MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Holographic Encryption – Part 2

Author: Nicolas Pavillon

March 2017

Introduction

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.

Challenge (1/2)

Decrypt the three given phase-shifted holograms "challenge_holo0.tif", "challenge_holo1.tif" and "challenge_holo2.tif".
The result will be the original field represented by two images (such as "challenge_plain0.tif" and "challenge_plain1.tif"), which has been encrypted with a double phase Fourier encryption. You are also given three known images and their holograms, which were encrypted with the same phase masks.

The solution consists of the family name of the author of the encrypted picture and of the shown codeword (both indicated in the picture). Please enter the solution in capital letters with a space between the two words, e.g. NAME CODEWORD.

Challenge (2/2)

Hints:

1. The three known plaintexts have a very particular structure.
2. It is in principle possible to solve this challenge with the known plaintexts, but a much simpler attack is to use them for a chosen-plaintext attack.

References

In the document "mtc3_holocrypto_description.pdf" the cipher is explained in detail. You can find it within the additional zip file.

An implementation of the encryption procedure is provided in "holoCryptoFourier.c", which can be employed to test the putative phase masks. During encryption, the program takes two 8-bit images [0, 255] as input (i.e. "input0.tif" and "input1.tif"), which represent the input field, with respectively the amplitude and phase of the field $o = Oe^{i\varphi}$, and the 2 phase masks encoded as 8-bit images ("mask1.tif" and "mask2.tif"). The output is given by 3 phase-shifted holograms encoded as 16-bit images [0, 65535] (i.e. "holo0.tif", "holo1.tif" and "holo2.tif"). During decryption, the inputs and outputs are reversed. You can find the implementation also within the additional zip file.

Additional Files

The additional zip archive contains the following files:

- mtc3_holocrypto_description.pdf
  ➥ detailed explanation of holographic encryption
- challenge_holo0.tif, challenge_holo1.tif, challenge_holo2.tif
  ➥ the phase-shifted holograms of the encrypted image
- plain10.tif, plain11.tif, plain20.tif, plain21.tif, plain30.tif, plain31.tif
  ➥ the three known images
- holo10.tif, holo11.tif, holo12.tif, holo20.tif, holo21.tif, holo22.tif, holo30.tif, holo31.tif, holo32.tif
  ➥ the phase-shifted holograms of the three known images
- holoCryptoFourier.zip
  ➥ C source code and test files for holoCryptoFourier
- All tif files are also available as csv files.