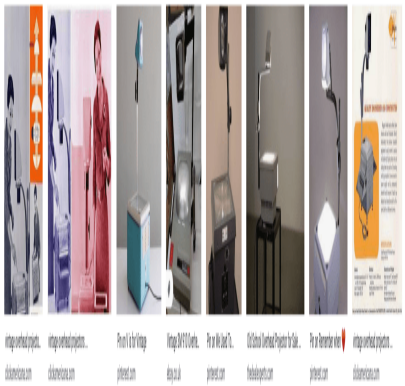


Secrets of the overhead projector

Description

All transmission of data across digital networks now involves encryption. Itâ??s interesting to read articles from the 1990s in which cryptography was applied usually to messages only requiring high levels of security. A seminal 1995 article by Moni Naor and Adi Shamir began

> â??In this paper we consider the problem of encrypting written material (printed text, handwritten notes, pictures, etc.) in a perfectly secure way which can be decoded directly by the human visual system.â?• (1)

The challenge was to transmit short, singular messages, a bit like instructions between HQ and submarines in WWII, and of the kind intercepted by the Bletchley Park code breakers.

Visual encryption

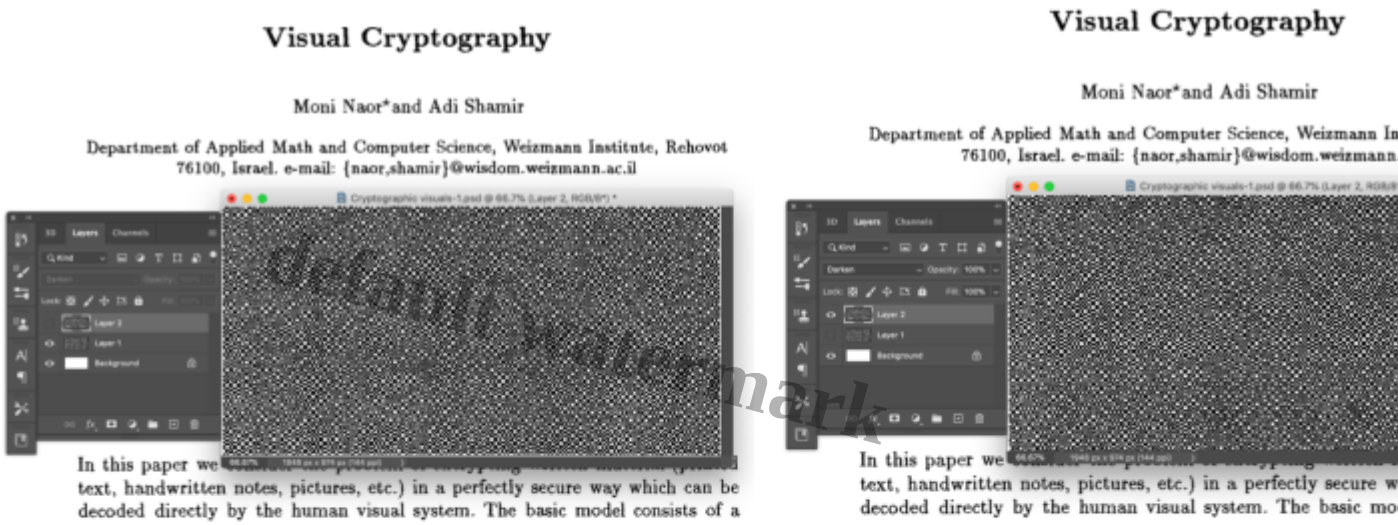
The second remarkable proposition in this article was that even though computers might be required to generate an encrypted message, its decryption could be accomplished by purely visual means, such as laying images photocopied onto transparent sheets of acetate.

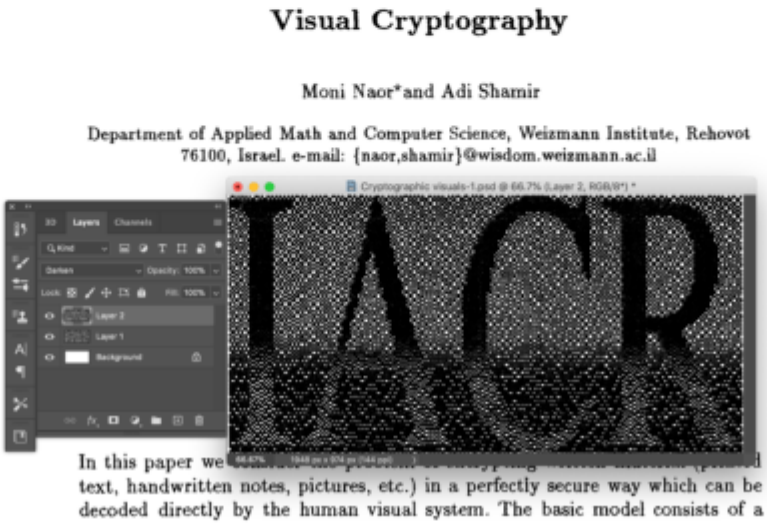
> â??The basic model consists of a printed page of ciphertext (which can be sent by mail or faxed) and a printed transparency (which serves as a secret key). The original cleartext is revealed by placing the transparency with the key over the page with the ciphertext, even though each one of them is indistinguishable from random noise. The system is similar to a one time pad in the sense that each page of ciphertext is decrypted with a different transparency. Due to its simplicity, the system can be used by anyone without any knowledge of cryptography and without performing any cryptographic computations.â?• (1)

To illustrate the method Naor and Shamir provided two images:

> â??two random looking dot patterns. To decrypt the secret message, the reader should photocopy each pattern on a separate transparency, align them carefully, and project the result with an overhead projector.â?• (1)

I donâ??t have access to a photocopier, acetate or an overhead projector, but I have Photoshop (PS). Here are the two noisy images in the article as PS layers. Overlaying with the PS â??Darkenâ?• transparency filter reveals the hidden text, â??IACR.â?• (These are the initials of The International Association for Cryptologic Research.)





This 1995 article has over 3,000 citations, and itâ??s still being referenced in 2021. So thereâ??s some substance to the concepts. As an example, a 2017 article by Petrauskiene and Saunoriene discusses how secret messages can be hidden and revealed by shaking things up:

> â??secret information is encoded into a single stochastic moirÃ© grating, which is fixed onto the surface of the vibrating structure. It is shown, that the secret can be visually decoded if

the cover image oscillates according to a chaotic law.â?•

Secret messages may be hidden within moirÃ© patterns, 3d magic eye and other innocuous imagery. See posts tagged steganography.

Bibliography

- Desmedt, Yvo, Shuang Hou, and Jean-Jacques Quisquater. 1998. Audio and Optical Cryptography. In K Ohta, and D Pei (eds.), *ASIACRYPTâ??98, LNCS 1514*: 392-404. Berlin: Springer-Verlag.
- Naor, M., and A. Shamir. 1995. Visual cryptography. *Workshop on the Theory and Application of Cryptographic Techniques*, (950)1-12.
- Petrauskiene, Vilma, and Loreta Saunoriene. 2017. Application of dynamic visual cryptography for optical control of chaotic oscillations. *JVE INTERNATIONAL LTD. VIBROENGINEERING PROCEDIA*, (15)81-87.

Category

1. Media

Date Created
July 4, 2021
Author
rcoyne99