Human Encryptable Visual Cryptography

Andrea Hawksley[1] and Andrew Lutomirski[2]

[1]Hillsborough, CA; andrea@andreahawksley.com
[2]Hillsborough, CA; andy@luto.us

Abstract

We present a system to enable easy human encryption of visual cryptographic messages, consisting of pre-cut templates for use with a one-time pad. This allows for quick, manual creation of secret messages in the field. We describe a workshop that introduces students to the concept of visual encryption, then continues to allow students to generate their own secret messages.

Introduction

Visual cryptography is a method of hiding messages or images in a two-dimensional image that, by itself, is indistinguishable from random noise such that the message is decryptable visually by overlaying a key. The basic method was introduced by Naor and Shamir in 1994 [1]. This cryptographic method is generally easy for a human to decrypt, but is tedious, if not impossible, to encrypt without using a computer. Many more complex variations have since been explored, but all have a strong dependence on computers to easily create the encrypted message. Efforts have been made to increase the ease of decryption of complicated visual cryptography messages involving many sheets [4], but the initial encryption method remains dependent on computers and printers.

We introduce a system that enables rapid human encryption of visual cryptographic messages. In the field, this system would be used to quickly encrypt a message, after which the encryption tools and original message could be destroyed. The encrypted message could then be decrypted using a one-time pad already in the possession of its recipient.

We then incorporate this system into a workshop that introduces students to the math and theory behind visual encryption, then allows them to generate their own secret messages by hand.

Encryption Method

The basic encryption remains the same as that originally described by Naor and Shamir [1]. The original image is a black-and-white $m \times n$ grid of pixels. The encrypted message and the key are each a $2m \times 2n$ black-and-white image. They consist of 2×2 blocks, and each block has one diagonal black and one diagonal white, as in Figure 1. In the key, each block is chosen independently at random. For each original white pixel, the encrypted image contains the same block as the key. For each original black pixel, the encrypted image consists of the opposite block as the key. At least one of the key and the encrypted image is printed on a transparent sheet. When the sheets are overlaid, original black pixels look like a 2×2 black block, original white pixels are a half-white, half-black 2×2 block, and the secret image is visible.

This is, in effect, just a one-time pad [3]. By itself, each block of the key is just a left-diagonal or a right-diagonal, independently at random. Similarly, by itself, the key has exactly the same property – each block has an equal chance of being a left-diagonal or a right-diagonal, regardless of what the secret message contains.

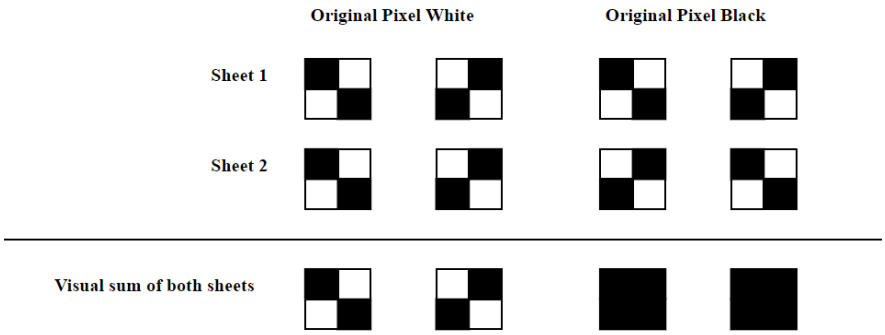

Figure 1: *Each pixel in the original image is divided into four subpixels spread across two images*

Figure 2: *The left two black and white images combine to reveal the message in the last image*

Encrypting by hand is very tedious. To encrypt an $m \times n$ image, one could flip a coin mn times and, depending on the outcome of the coin flip, carefully color in one of the two diagonals on each block of the key and the secret message, for a total of $4mn$ black squares colored in.

We propose an alternative, and significantly more fun, way to encrypt a message.

Setup and Materials

To prepare, we use a Python script to generate a $2m \times 2n$ key of four-subpixel blocks, each randomly chosen as a left-diagonal or a right-diagonal. We also generate a laser-cutter template that cuts a hole for each black key subpixel and a separate laser cutter pattern that cuts a hole for each white key subpixel. The Python code and a set of sample templates and keys are available online at https://github.com/amluto/visual_crypto. We print the key on an ordinary piece of paper and we cut each template on a separate sheet. The templates work best cut out of thin plastic.

The supplies required to encrypt a message are the two laser-cut templates, a piece of grid paper with one cell per 2×2 block of subpixels, a sheet of transparent film, and two different colored markers that can write on the film. Choosing one lighter and one darker color marker will make the encryption process easier. Choosing the darker color to not be black will make the decryption process easier, as the correctly aligned transparency and key will be black and white outside of the image and black and colored inside of the image, leading to higher contrast. The message's recipient needs the printed key.

Procedure

To encrypt a message, draw and color in a design to be encrypted on the grid paper. Each grid of the grid paper is one pixel and must be either all colored or all white. Use the lighter marker to make the next step easier. Additionally, since the image is highly pixellated, and the extracted image will have a noisy, grey

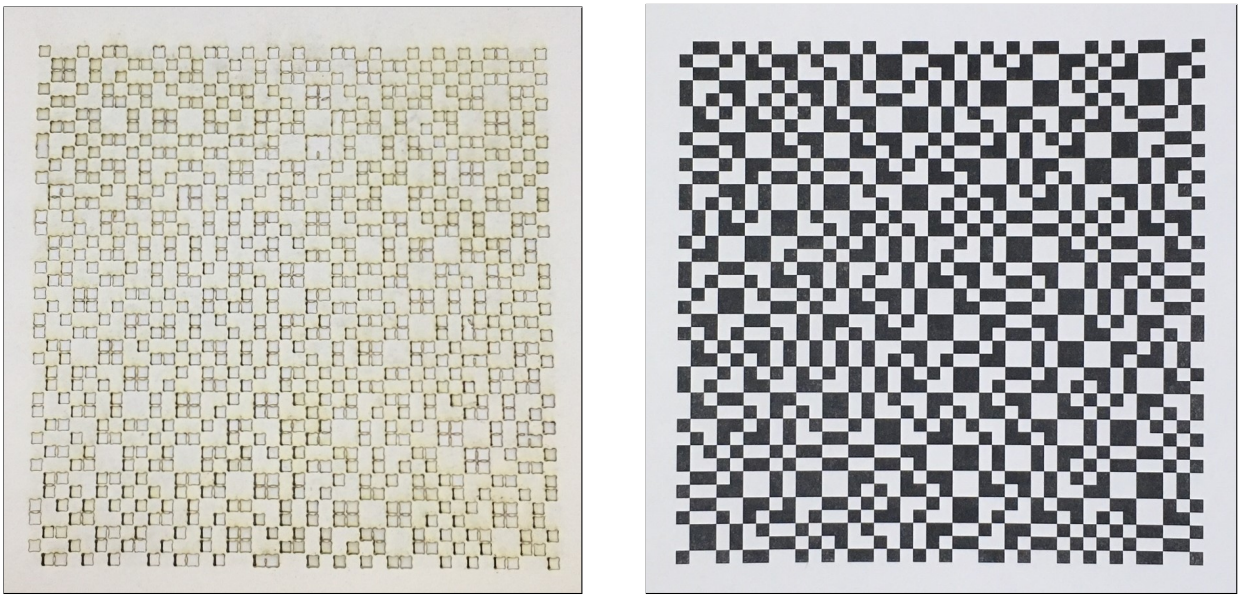

Figure 3: *A laser cut template and a printed key.*

background, it will work best with simple, high-contrast designs. In general, this means avoiding lines of only one pixel in width. Figure 4 gives examples of "good" and "bad" designs.

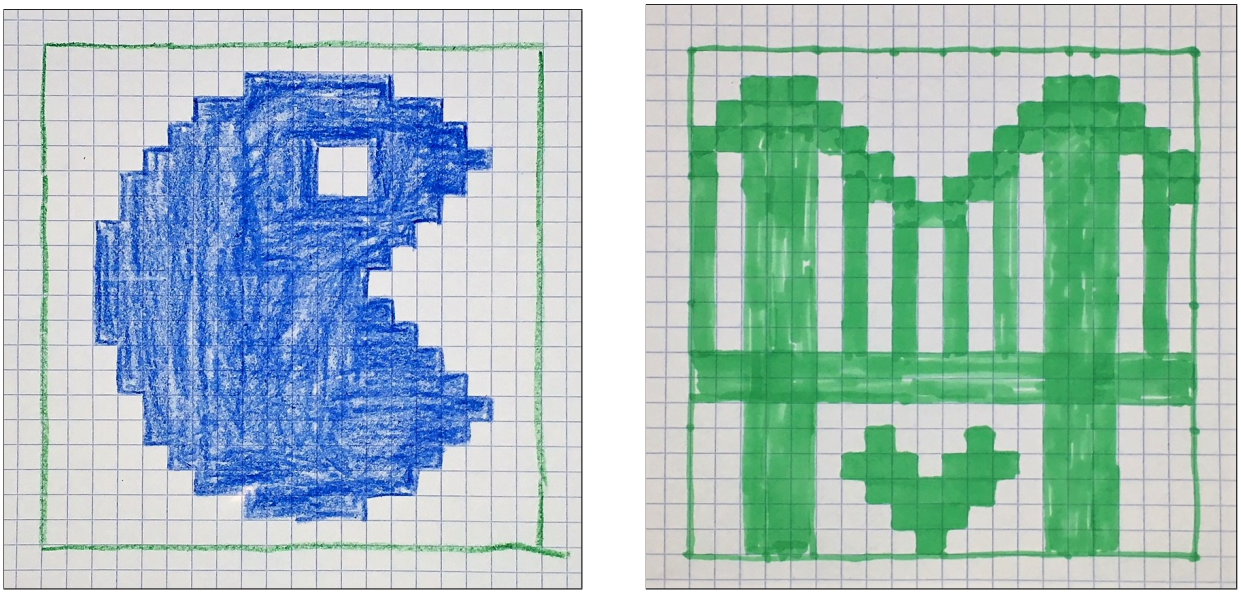

Figure 4: *The design on the left has an appropriate level of detail. The design on the right is more complicated than is ideal, making it difficult to recognize the decoded image.*

Next, tape the transparent film on top of the grid paper. The tape helps keep the sheet aligned. Then tape one of the templates on top of the film such that it correctly aligns with the grid and the design, as in Figure 5 (left).

Using the darker-colored marker, color in each square of the template that overlays a colored grid square,

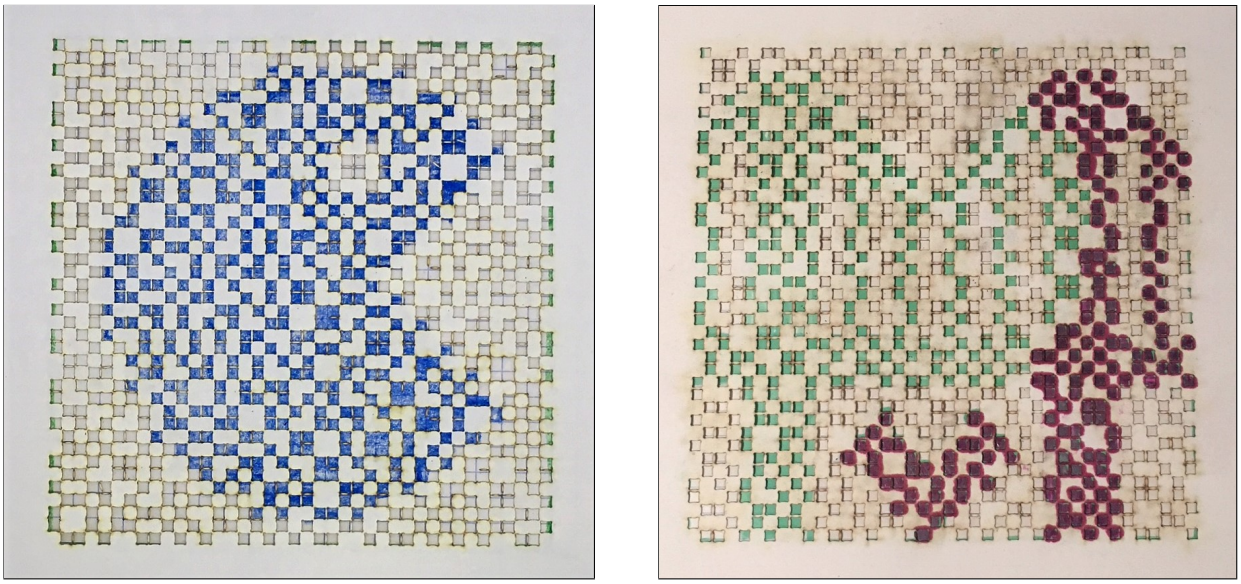

Figure 5: *A template correctly overlaid on the gridded design. The image on the right shows a partially colored state.*

as in Figure 5 (right), and remove the template. It should look something like Figure 6 (left).

Next, tape the other template on and align it with the grid. When correctly aligned, there should be none of the darker color visible through the template. Again using the darker marker, color in each square that overlays a white grid square, and remove the template. The result should look like Figure 6 (right). At this point, optionally coloring in small gaps between adjacent squares will increase clarity of the extracted image.

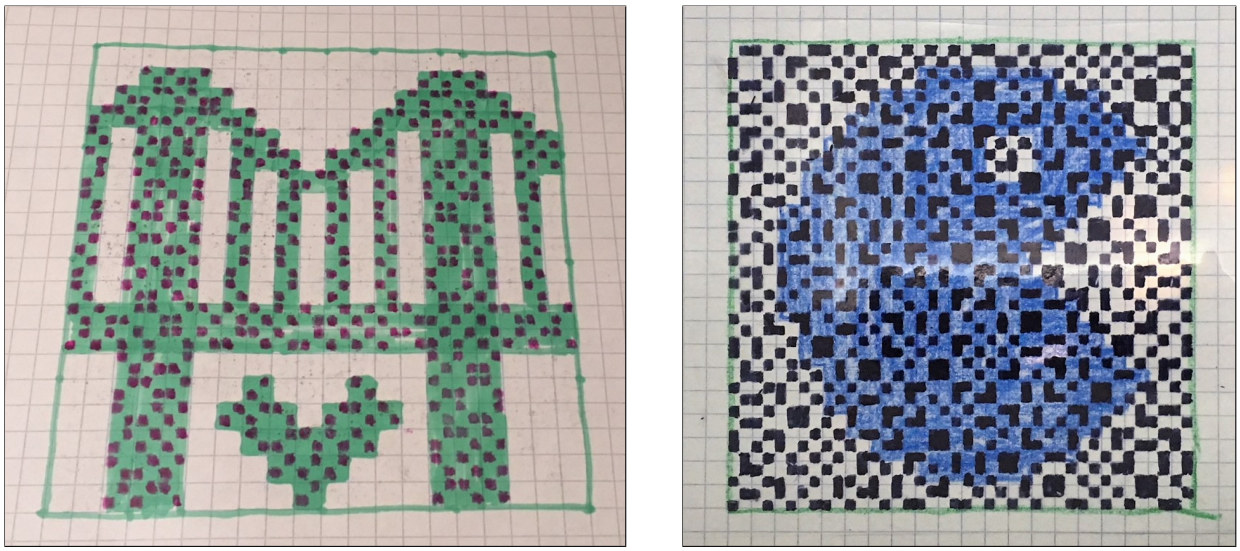

Figure 6: *As the first (left) and second (right) templates are removed, the grid should be overlaid with black squares over first the colored area (left), then the whole image (right).*

Finally, send the transparent film to the recipient, who can place it on top of the key to reveal the message.

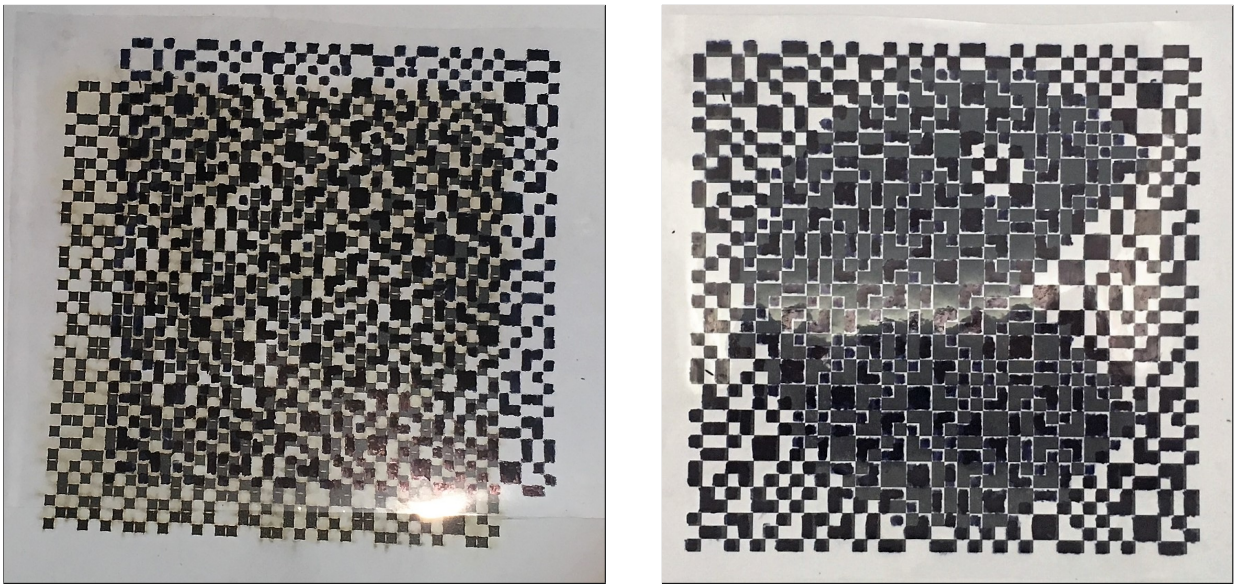

Figure 7: *The secret message is revealed only when the completed transparency is correctly overlaid with the one-time pad (right).*

Security

If done perfectly, this scheme is a secure one-time pad. Since it is done by humans with pens, there are several caveats. For example, all of the encrypted subpixels corresponding to black pixels are filled in before the encrypted subpixels corresponding to white pixels. If the marker dries out a little or otherwise behaves at all differently over time, a careful adversary may be able to guess which pixels are white and which are black. Similarly, if the two templates are not aligned exactly the same, then the black and white subpixels will be slightly offset, again revealing the secret message. Additionally, if the templates are re-used, an adversary who recovers two messages encrypted with the same templates can overlay them to learn the exclusive-or of the two messages, which can reveal a considerable amount of information about both of them.

Workshop Description

The workshop begins by introducing an example of an image encrypted by visual cryptography. We then pass out the templates, one-time pads, and grid paper to participants and describe the procedure to generate such an image.

At this point, we ask participants to examine their materials and discuss what they observe about them. Observations may include that the templates appear to be half solid and half holes, that the two templates are exact opposites of each other, and that one of them matches the key exactly. Participants will find that the encrypted images look like random noise until they are overlaid on the key and aligned correctly.

We then discuss how one-time pads work, and how the visual encryption process is mathematically identical to a standard one-time pad.

Finally, we pass out markers and tape to the participants and have them create their own secret messages using the method described.

Conclusions

We describe a method for creating visual cryptographic messages by hand. This method is a fun way to introduce cryptographic concepts like one-time pads in the classroom. Since visual cryptography messages are often small pictures, having students create the designs is a nice way to incorporate art into a STEM topic. A good classroom unit incorporating both art and math/engineering might start by exploring pixel art from an artistic and historical standpoint. Students would then create their own designs in this artistic context, then explore how to encode those designs as numbers and communicate them to classmates. Finally they might try to communicate them secretly via encryption.

A major downside of this strategy for classroom use is the difficulty in cutting the templates. Most people do not have easy access to cutting machines, so it would be nice to be able to sell templates and matching one-time pads inexpensively for classroom use. This could be done through a laser-cutting service, such as Ponoko [2], but for any kind of larger-scale classroom use it would be preferable to die-cut the templates.

The current methodology works for black and white images. It would be interesting to develop a strategy for using transparency overlays to manually encrypt colored messages.

References

[1] M. Naor and A. Shamir. "Visual Cryptography." *Workshop on the Theory and Application of Cryptographic Techniques*, Springer, 1994, pp. 1–12.

[2] Ponoko. Online Laser-Cutting and Engraving. https://www.ponoko.com/.

[3] B. Schneier. "One-time Pads." *Applied Cryptography*. 2nd ed. Wiley, 1996, pp. 15–17.

[4] W. Q. Yan and D. Jin and M. S. Kankanhalli. "Visual Cryptography for Print and Scan Applications." *Proceedings of the 2004 International Symposium on Circuits and Systems.*, IEEE, vol. 5, 2004.