Efficient Colour Visual Encryption or 'Shared Colors of Benetton'

Vincent Rijmen* Bart Preneel†

Katholieke Universiteit Leuven, Dept. Electrical Engineering-ESAT,
Kardinaal Mercierlaan 94, B–3001 Heverlee, Belgium,
{vincent.rijmen,bart.preneel}@esat.kuleuven.ac.be

1 Introduction

Since its introduction by M. Naor and A. Shamir at Eurocrypt'94 the paradigm of visual cryptography has attracted wide attention. Naor and Shamir describe in [2] a simple system to split a black-and-white picture in several shares. This idea can be applied to both visual secret sharing and visual encryption. Various extensions to this scheme have been proposed. In this abstract we present a new and efficient way to add colour support to visual cryptography.

2 Related work

In [3] Verheul and van Tilborg describe a method to encrypt coloured images. We summarize their method. To simplify the discussion, we only describe the case of a two out of two secret sharing scheme, which corresponds to a one-time pad for encryption. For a c-colour scheme every pixel is divided into c subpixels. Subpixels are divided into c colour regions, one fixed region for each colour. In every subpixel exactly one colour region will have the associated colour c_1, the other colour regions are left black. We say this subpixel has colour c_1. By defining subpixels in this way we see that the stacking (generalized "OR") of two subpixels is a black subpixel, except when both subpixels are of the same colour. The set of subpixels corresponding to one pixel contains exactly one subpixel with every colour. The order of the subpixels is random. To encrypt a pixel of colour c_1, we ensure that the subpixels with colour c_1 have the same position on both shares, and that this holds for no other colour.

*N.F.W.O. research assistant, sponsored by the National Fund for Scientific Research (Belgium).
†N.F.W.O. postdoctoral researcher, sponsored by the National Fund for Scientific Research (Belgium).

An important disadvantage of this scheme is the reduction in resolution: if we want to encrypt an image with c colours, we get a resolution reduction with a factor c^2.

Another scheme for encryption of coloured images is shown in [1]. Naccache observes that every colour is characterized by its wavelength λ. It is possible to construct filters that let only pass light with a wavelength in certain intervals. The scheme uses two filters, chosen such that the combination of the two filters absorbs all wavelengths, except for the wavelength of the colour of the original picture.

In the two out of two case every filter of this scheme reveals one bit of information per pixel.

3 A more efficient colour scheme

In the colour scheme of [3] two different situations can occur when we stack coloured regions: either one of the regions is black, and then the result is black, or both regions have the same colour, and then the result has the same colour. In our approach we use a different solution: by stacking two different colours we get a third colour, e.g. red on blue gives a hue of purple.

In the basic version of our scheme each pixel is divided into four subpixels, with the colours red, green, blue, and white. These subpixels can appear in any order. Taking symmetries into account, we get 24 different possibilities for the combination of two pixels. If the subpixels are small enough, the human visual system will average out the different possible combinations to 24 different colours. To encrypt a pixel of the coloured image we "round" the colour to the nearest representable colour, select a random order for the subpixels on the first share, and select the ordering on the second share such that the combination produces the required color.

The advantage of our scheme is that we can represent 24 colours with a resolution reduction of four, instead of 24^2. The disadvantage is that the 24 colours are fixed once the basic set of subpixel colours is fixed.

This result can be extended to an arbitrary number of colours by adding more subpixels (and more colours) to the basic set.

Readers who want to try this at home may want to have a look at `http://www.esat.kuleuven.ac.be/~rijmen/vc`.

References

[1] D. Naccache, "Colorful Cryptography — a purely physical secret-sharing scheme based on chromatic filters —," *Coding and Information Integrity*, French-Israeli workshop, December 1994.

[2] M. Naor, A. Shamir, "Visual Cryptography," *Advances in Cryptology, Proceedings Eurocrypt'94, LNCS 950*, A. De Santis, Ed., Springer-Verlag, 1995, pp. 1–12.

[3] E.R. Verheul, H.C.A. van Tilborg, "Constructions and Properties of k out of n visual secret sharing schemes," *submitted to DC&C.*