FULL-LENGTH PREPRINT – differs from the original in layout but not in contents. Accepted for print as:
Orłowski A., Chmielewski L.J. Generalized Visual Cryptography Scheme with Completely Random Shares.
In: *2nd International Conference on Applications of Intelligent Systems (APPIS 2019), January 7-9, 2019, Las Palmas de Gran Canaria, Spain,*
ACM, New York, NY, USA, 6 pages
The original publication will be available at doi:10.1145/3309772.3309805
© 2019 Copyright held by the owner/author(s). Publication rights licensed to ACM.
Recompiled last time on February 9, 2019.

Generalized Visual Cryptography Scheme with Completely Random Shares

Arkadiusz Orłowski
Department of Informatics
Warsaw University of Life Sciences – SGGW
Warsaw, Poland
arkadiusz_orlowski@sggw.pl

Leszek J. Chmielewski
Department of Informatics
Warsaw University of Life Sciences – SGGW
Warsaw, Poland
leszek_chmielewski@sggw.pl

ABSTRACT

A modification of the standard Naor-Shamir scheme for visual cryptography and visual secret sharing is proposed. Better statistical properties of shares are obtained at the cost of the slightly worse quality of reconstructed images. Advantages and disadvantages of such an approach are discussed.

CCS CONCEPTS

• **Security and privacy → Cryptanalysis and other attacks**; **Mathematical foundations of cryptography**; *Key management*;

KEYWORDS

visual cryptography, non-classic tiles, random shares, information leak

ACM Reference Format:
Arkadiusz Orłowski and Leszek J. Chmielewski. 2019. Generalized Visual Cryptography Scheme with Completely Random Shares. In *2nd International Conference on Applications of Intelligent Systems (APPIS 2019), January 7–9, 2019, Las Palmas de Gran Canaria, Spain.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3309772.3309805

1 INTRODUCTION

The standard Naor-Shamir visual cryptography scheme, serving also as a visual secret sharing protocol, was invented more than two decades ago [4, 5]. Since then many more or less successful generalizations have been proposed, including multi-level secret sharing arrangements and color visual cryptography (see [2, 3] and references therein). The original invention is provably secure – in fact it is equivalent to the one-time pad (Vernam cipher [6]). There is no information leak from the shares as each of them treated separately remains completely uncorrelated to the encoded image. We show that, despite looking random, the shares are not random in the statistical sense, due to the requirement (or rather a consequence of the design) of the locally equal number of black and white pixels in each share.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
APPIS 2019, January 7–9, 2019, Las Palmas de Gran Canaria, Spain
© 2019 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-6085-2/19/01…$15.00
https://doi.org/10.1145/3309772.3309805

In this paper we generalize the standard black-and-white visual cryptography in a way that makes both shares not only looking random but also being random – shares treated as a distribution of black and white pixels do pass statistical tests for randomness. We have checked that this advantageous property comes with a price – the reconstructed image is slightly deteriorated. We believe however that taking into account that full randomness of shares is achieved and the corresponding deterioration level of reconstruction is less than moderate, this price is worth to pay.

We consider the simplest (2, 2) visual cryptography scheme, in which there are two shares and both of them are necessary to reveal the secret.

The remaining part of this paper is organized as follows. In the next Section the general methodology used in visual cryptography is briefly presented and the motivation for changes is outlined. In Section 3 the proposed generalization is introduced. In Section 4 some changes in this generalization which could reduce its drawbacks are presented and criticized. Simple statistical analysis of the proposed methods is presented in Section 5. In Section 6 the errors made in the presented coding methods are discussed. In Section 7 the paper is concluded.

2 GENERAL METHODOLOGY

Let us recall the basic notions. The binary image to be encoded is called the *secret*. It is encoded in two images called the *shares*. Any one of them contains no information on the secret, but when overlaid on one another they reveal it to the human eye. This is called the *decoding*. In general, each pixel of the secret corresponds to a square of $n \times n$ pixels, called the *tile*, in each share, and in our case $n = 2$. In the coding process one share called the *basic share* is generated according to some rules independently of the secret, and the other share called the *coding share* is the function of the first share and the secret. We shall call the tile in the basic share the *basic tile*, and the one in the coding share the *coding tile*. All possible 2×2 tiles are shown in Fig. 1.

Said in the simplest way, the *encoding* process consists in that a coding tile is set to equal to the respective basic tile if the corresponding pixel in the secret is white, and it is set to the negative of the basic tile if the corresponding pixel in the secret is black.

The Naor-Shamir coding, called here the *classic* coding, consists in that the basic share is formed of tiles which have two black and two white pixels each: tiles 4, 6, 7, 10, 11, and 13, drawn at random. Thanks to that, each black pixel of the secret is decoded as a black tile, like tile 1, and each white pixel as a half-white tile, like one of the tiles just listed.

Figure 1: All possible 2×2 tiles and their indexes.

We shall illustrate the considerations with an example image shown in Fig. 2. There is a large graphical motif, with large black and white fields, some lines of varying width, and a chequered pattern, which should be an example of a difficult pattern to decode.[1] Numbers of black and white pixels are not equal.

Image of Fig. 2 decoded from the classic coding is shown in Fig. 3a. The secret is visible with half of its original contrast. No single share contains any information on the secret, as the tiles are drawn randomly. The basic share from the classic coding is shown in Fig. 4a; the coding share has exactly the same appearance.

It is easy to check whether the classic shares are random images in a sense that their pixels form a random series of zeros and ones. The answer is negative, due to that neighboring pixels are constrained by the restricted choice of tiles; specific results will be shown in Section 5. Because the shares are specific to the coding process, in classic visual cryptography the information which leaks is the information that the coding itself is performed. A proposition will be made to avoid this leak.

3 RANDOM VERSION

Our proposition is to draw the tiles in the basic share at random from all the possible tiles (Fig. 1). The coding is done in the way described above. The basic and coding shares will now be completely random; specific results will be shown in Section 5. The basic share of the *random coding* is shown in Fig. 4b. Let us add that in random coding, as it was in the case of classic coding, the appearance of the basic and coding shares for the human eye is exactly the same.

The decoded image is shown in Fig. 3b. In this coding, the decoding errors appear. They comprise, above all, tiles which should contain white pixels but there are not enough white pixels in the basic tile. In the classic coding scheme there are always two white pixels in a tile, so let us take this case as a reference. Therefore, errors appear when one or two white pixels are missing in the basic tile. The most severe error is when there are no white pixels in the basic tile, so a white pixel in the secret has to be decoded as black, contrary to the half-white decoding of the classic scheme. Let us call this a −2 pix error. One white pixel missing, called −1 pix error, is not so severe. There are also errors in plus, when there are three or four white pixels in the basic tile, so in the decoded image there is a tile in which more than two white pixels appear. These are the +1 pix and +2 pix errors. These errors are not important, as they do not hinder the visibility of the secret in the decoded image. Obviously, no errors are possible in black pixels of the secret. The errors of various types will be shown in Section 6.

[1]Some images are shown in this paper in large scale, which can seem excessive. However, by making the images large we have tried to make it possible for the reader to examine them by eye and to see the described phenomena, as much as possible irrespective of the quality of the medium with which the publication is viewed.

4 NEAR-RANDOM VERSION

Modifications which could make the decoding result closer to that of the classic coding could potentially improve the visibility of the secret in the decoded image. One might be tempted by two possibilities of excluding the −2 pix and the −1 pix errors, by resigning of using some of the tiles. The −2 pix errors would be eliminated by not using the tile denoted as 1 in Fig. 1. The −1 pix errors can be eliminated by not using tiles denoted as 2, 3, 5, and 9, but this case will not be investigated in this paper. Both types of errors can be independently dealt with according to the following possibilities.

(1) The listed tiles can be eliminated from the coding image.
(2) The listed tiles can be sampled only in the black regions of the secret image.

The basic share prepared according to the possibility 1 is shown in Fig. 4c. It has no black tiles, so its appearance is less uneven than the random basic share of Fig. 4b. This makes the decoded image shown in Fig. 3c look also less uneven than that decoded with random coding, Fig. 3b. Let us call this process the *near-random 1* coding. Indeed, as it will be shown in Section 6, the number of coding errors is smaller than in the random version.

However, both possibilities just proposed have important drawbacks. Possibility 1 implies the leakage of information that coding is performed (see Section 5). It is easy to check the fractions of the tile types used and to see that some of them are missing (see Fig. 6c).

Possibility 2 should be immediately excluded as it implies the leak of information on regions which are black in the secret image, which is even more severe. There is a visual information leak in the coding share shown in Fig. 5, where a shade of the secret can be noticed quite easily. This is caused by using the black tiles (tile 1 of Fig. 1) only where there are black pixels in the secret and the basic tiles are white. This effect can be easily removed by using the basic share without not only black, but also without white tiles, which we shall call the *near-random 2* coding. Indeed, with this coding, the coding share does not reveal the secret, and its appearance is like that of the basic share shown in Fig. 4d. However, as we shall see in Section 5, either in this case the shares do not have fully random properties.

5 RANDOMNESS OF SHARES

In classic coding, the tiles in the basic share are sampled at random from the tiles with exactly two white pixels. Evidently, this implies that the individual pixels are not sampled at random, which can clearly be seen by comparing a classic share, like this in Fig. 4a, and a share form random coding in Fig. 4b, which is random at pixel level. This observation can be confirmed by tests for randomness, for example the test based on the number of runs of consecutive values, 0 or 1. The results for both basic and coding shares in the classic, random and both types of near-random coding are shown in Tab. 1. For the tests, the values of pixels are sequenced, by rows or by columns. The p-values are slightly different for ordering the pixels

Figure 2: Example image to be coded: a 500×200 binary image.

Table 1: Results of randomness tests for shares in codings. The null hypothesis is that the values come in random order. Results equal for significance levels 5% and 1%. p-value given for ordering the pixels by rows and by columns. Only the shares from random coding can be considered fully random.

Coding	Share	Hyp. rejected	p, rows	p, columns
Classic	basic	true	$0.0{\cdot}10^{0}$	$0.0{\cdot}10^{0}$
	coding	true	$0.0{\cdot}10^{0}$	$0.0{\cdot}10^{0}$
Random	basic	false	$5.1{\cdot}10^{-1}$	$5.3{\cdot}10^{-1}$
	coding	false	$1.9{\cdot}10^{-1}$	$8.7{\cdot}10^{-1}$
N.-rand. 1	basic	true	$4.9{\cdot}10^{-109}$	$2.6{\cdot}10^{-104}$
	coding	true	$7.7{\cdot}10^{-87}$	$1.5{\cdot}10^{-87}$
N.-rand. 2	basic	true	$0.0{\cdot}10^{0}$	$0.0{\cdot}10^{0}$
	coding	true	$0.0{\cdot}10^{0}$	$0.0{\cdot}10^{0}$

by rows and by columns. What is the most apparent in this table is that the only coding for which the shares can be considered as truly random is the random coding. Only in this coding the fact that the coding is performed is fully hidden, as well as the secret itself. This is done at the cost of some loss of quality of reconstruction of the secret. It can be seen in the reconstructions in Fig. 3 and in the visualization of decoding errors in Fig. 7 in Section 6 that this cost is within the acceptable range, provided that the level of detail in the secret image is moderate.

A simple measure of randomness is the fraction of tiles of various types in the shares. Fractions of tiles in shares for various codings, for the example image of Fig. 2, are shown, respectively: classic in Fig. 6a, random in Fig. 6b, near-random 1 in Fig. 6c and near-random 2 in Fig. 6d.

It is apparent that for the near-random 1 coding, Fig. 6c, in the basic image the fractions of tiles are nearly equal to $\frac{1}{15}$ (not precisely, due to the randomness of the sampling process), except the absent tile no. 1, and in the coding image the tile no. 1 is present, due to the process of making some tiles number 16 negative.

The variability of the fractions of tiles can be simply expressed by the variance of these fractions in each share, for each coding. This is shown in Table 2. The variance is the lowest in the random coding. In both random and classic coding the values of variance in

Table 2: Variance of tile fractions for shares in codings.

Coding	Share	Variance
Classic	basic	$6.9{\cdot}10^{-3}$
	coding	$6.9{\cdot}10^{-3}$
Random	basic	$1.6{\cdot}10^{-6}$
	coding	$1.3{\cdot}10^{-6}$
Near-random 1	basic	$2.8{\cdot}10^{-4}$
	coding	$1.3{\cdot}10^{-4}$
Near-random 2	basic	$6.0{\cdot}10^{-4}$
	coding	$6.0{\cdot}10^{-4}$

the two shares are close to each other. In the near-random 1 coding the variances are relatively small, but the difference between the variances in the shares is more than two-fold.

The fraction of tiles of subsequent types in the basic share can be set arbitrarily, while in the coding share it is the function of the basic share and the coded secret. The reduction of the number of tiles can be seen as a gradual, but stepwise transition form the random coding, with all 16 tiles, to the classic coding, with only 6 tiles. We have made the first step by resigning of the black tile 1 in the basic share. This step appeared to have negative results, as already said. It led to the loss of symmetry in the fractions of tiles and, most of all, to the leakage of information about the secret.

Simple tests of fractions of tile types in both shares reveal the fact that the coding process was performed, for all codings except the random coding. In the case of the near-random 1 coding the information which share is which can be easily revealed.

6 VISUALIZATION OF DECODING ERRORS

In the modified coding schemes the decoding errors are made only in the white regions of the secret. The errors are visualized in such a way that the white pixels of the secret which were decoded in a way different from that of the classic coding are displayed in colors. The −2 pix, −1 pix, +1 pix and +2 pix decoding errors are displayed with a color palette adapted from the color-blind safe, printer friendly, 5-class diverging palette, generated with the `www.ColorBrewer.org` web service [1]. In this palette, denoted BrBG, the negative errors are represented by shades of brown and

Figure 3: Example image of Fig. 2 decoded from three codings: (a) classic, (b) random, (c) near-random 1.

the positive ones by shades of turquoise. The adaptation made here consists in replacing brown with dark red, for better perspicuity of the most severe −2 pix error, and in replacing the middle greyish color of the original palette by pure white. The images of decoding errors are shown in Fig. 7.

No errors are made in the classical coding. In random coding, all types of errors appear, and the most severe −2 pix errors can be found in around $\frac{1}{16}$ of white pixels of the secret. In the near-random 1 an 2 codings only ±1 pix errors appear. However, the near-random 1 coding is not worth further analyzing due to its important drawbacks.

The errors deteriorate the decoded image to a largest extent in its most minute details, like the thinnest lines. The chequered pattern with 1-pixel wide squares seems to be the element which is the least suited for visual cryptography and it clearly sets the limit for the reconstruction accuracy, as after decoding in place of a regular pattern such artefacts as blobs and lines appear, which is seen in Fig. 7 as well as in Fig. 3.

7 CONCLUSIONS AND PERSPECTIVE

In classic visual cryptography the information which leaks is the information that coding itself is performed. This leak can be avoided. A modification of the classic Naor-Shamir scheme for visual cryptography consisting in using fully random shares was proposed. Statistically testing the shares reveals their random character, while the coding itself is safe. The quality of the decoded image is slightly

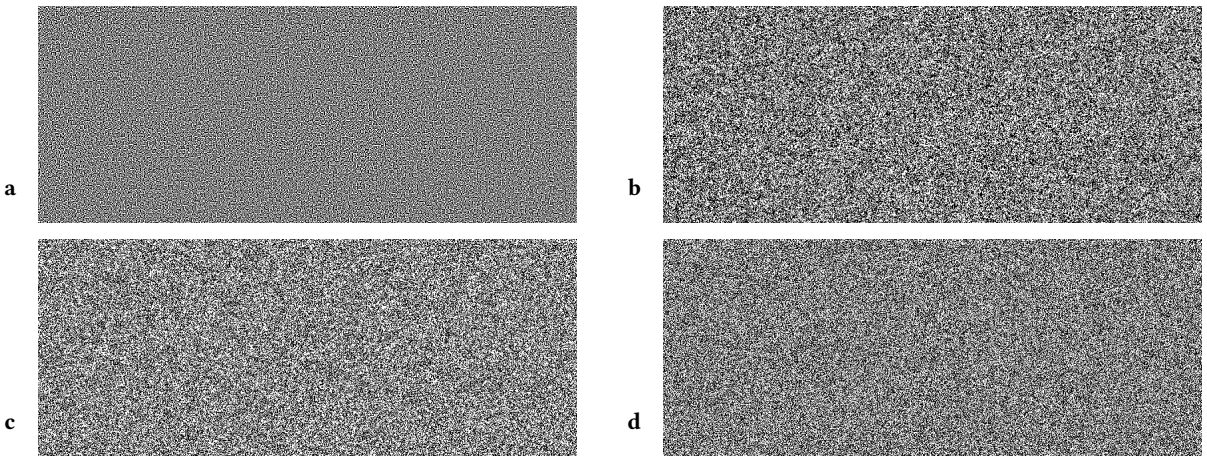

Figure 4: Basic shares (upper left quarters) from codings: (a) classic, (b) random, (c) near-random 1, (d) near-random 2.

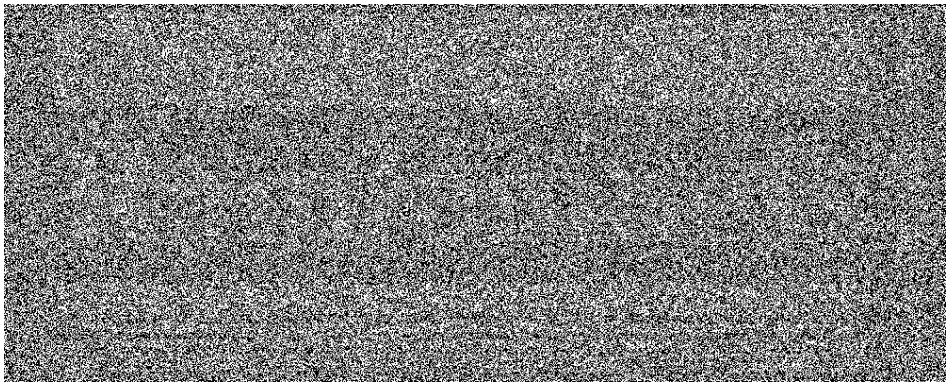

Figure 5: Coding share from the near-random 1 coding: a shadow of the secret can be seen.

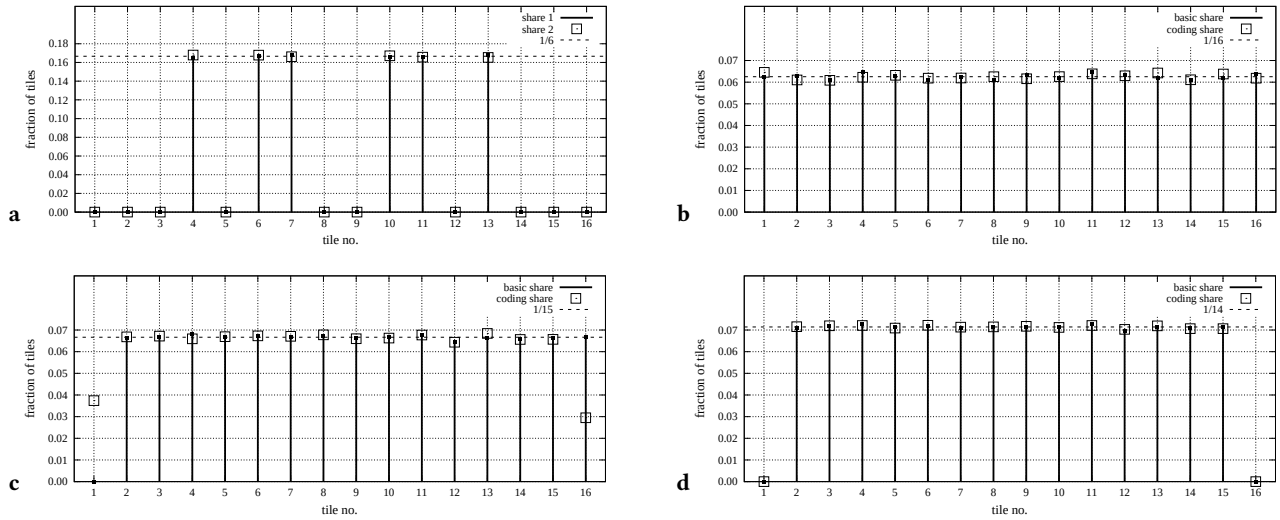

Figure 6: Fractions of tiles in the codings: (a) classic, (b) random, (c) near-random 1, (d) near-random 2.

Figure 7: Decoding errors for decoded images of Fig. 3, decoded from three codings: (a) random, (b) near-random 1, (c) near-random 2. Meaning of colors: dark red (■): −2 pix error; beige (■): −1 pix error; turquoise (■): +1 pix error; teal (■): +2 pix error. In (a) all types of errors appear. In (b) there are no −2 pix errors. In (c) there are neither −2 pix nor +2 pix errors. (See also text.)

worse than in the classic coding, however for secret images with a moderate level of detail it is acceptable. There is a range of coding methods, with the shares ranging from fully random to those of the classic coding. From these, in all but the fully random scheme a leak of information that the coding was done can be found. Nevertheless, it would be interesting to investigate the other visual coding schemes, trying to optimize the decoding quality versus the secrecy of the process of transmitting information ratio.

REFERENCES

[1] C. A. Brewer. 2018. www.ColorBrewer.org. Retrieved November 2, 2018 from http://www.ColorBrewer.org

[2] S. Cimato and C.-N. Yang. 2011. *Visual Cryptography and Secret Image Sharing (Digital Imaging and Computer Vision).* CRC Press, Inc., Boca Raton, FL, USA. https://www.crcpress.com/Visual-Cryptography-and-Secret-Image-Sharing/Cimato-Yang/9781439837214

[3] F. Liu and Wei Qi Y. 2014. *Visual Cryptography for Image Processing and Security: Theory, Methods, and Applications.* Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-09644-5

[4] M. Naor and A. Shamir. 1995. Visual Cryptography. In *Proc. Advances in Cryptology — EUROCRYPT'94*, A. De Santis (Ed.). Springer, Berlin, Heidelberg, 1–12. https://doi.org/10.1007/BFb0053419

[5] M. Naor and A. Shamir. 1997. Visual Cryptography II: Improving the Contrast via the Cover Base. In *Security Protocols*, M. Lomas (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 197–202. https://doi.org/10.1007/3-540-62494-5_18

[6] G. S. Vernam. 1926. Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications. *Transactions of the American Institute of Electrical Engineers* XLV (Jan. 1926), 295–301. https://doi.org/10.1109/T-AIEE.1926.5061224