This is a pre-print of a contribution to Proc. PP-RAI 2022. The final version is available online at https://wydawnictwo.umg.edu.pl/pp-rai2022/.
Full citation:
L. J. Chmielewski, M. Nieniewski and A. Orłowski. Truly random color visual cryptography without surplus color spikes. In: P. Jędrzejowicz and I. Czarnowski, editors. *Proc. 3rd Polish Conference on Artificial Intelligence PP-RAI'2022*, pages 53-56, Gdynia, Poland, 25-27 Apr 2022. Publishing House of Gdynia Maritime University.
Last compiled on November 7, 2022.

Truly Random Color Visual Cryptography without Surplus Color Spikes

Leszek J. Chmielewski[1], Mariusz Nieniewski[2], and Arkadiusz Orłowski[1]

[1] Warsaw University of Life Sciences – SGGW
Institute of Information Technology, Warsaw, Poland
{leszek_chmielewski,arkadiusz_orlowski}@sggw.edu.pl
[2] University of Lodz
Faculty of Mathematics and Informatics, Łódź, Poland
mariusz.nieniewski@wmii.uni.lodz.pl

Abstract. Color visual cryptography with truly random shares is attractive because transferring pure noise conceals the very fact that actually the information is transferred. The previously proposed method exhibits two types of errors, which lead to representing color with loss of brightness and to the presence of spikes with excessive brightness. The method without this second type of error is proposed. The randomness of shares as well as the potential for parallel processing is maintained.

Keywords: Visual cryptography · Color · No spikes · Random shares · True randomness.

1 Introduction

Since the pioneer work of Naor and Shamir [6] new publications in the domain of visual cryptography emerge continually (with [5] as a good example). The subject of randomness in the cryptographic methods is crucial; however, it seems that it is usually studied regarding the random nature of only the coding process (see e.g. [4]). The randomness of the *shares* has also been considered to some extent, for example in [8], where the autocorrelation was used as the measure of randomness. However, the randomness of the substrate in which the coding takes place treated as the means of masking the very process of information transfer has gained little or no interest in the literature so far. Using truly random shares makes it necessary to sacrifice the accuracy of the transferred message to a limited extent, but in the case of image information this is admissible thanks to the capability of our visual system to properly understand the slightly corrupt information. Therefore, in [7] we have proposed the coding of black-and-white images with truly random shares, with their randomness finally confirmed in [3] with the set of NIST randomness tests [1]. Further, this proposition was extended to color images in a series of publications, and finally the actual randomness of the shares for color cryptography was confirmed in [2] with the same tests.

The algorithm of color visual cryptography presented in [2] generates two types of errors in the decoded image. In this paper we propose an algorithm in which only one of these errors can appear.

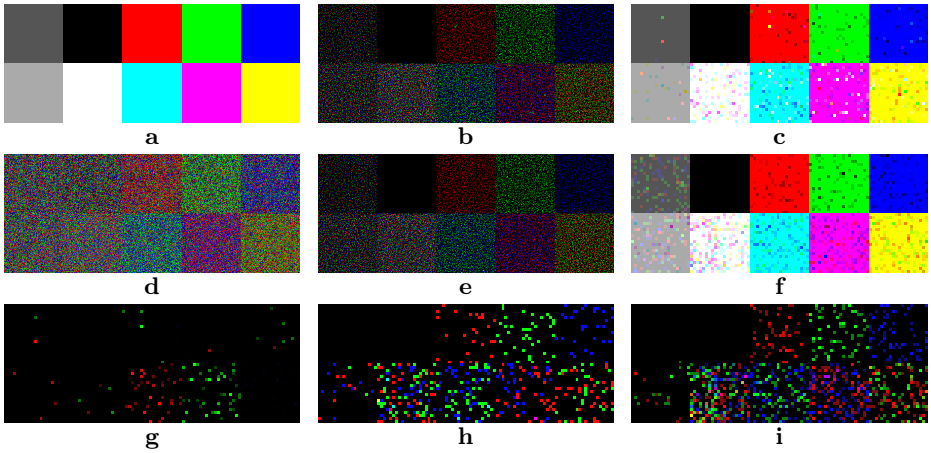

Fig. 1. Decoding, restoration and errors for a test image. (**a**) Secret, 100×40 [3]. (**b, e**) Image **a** decoded 600×240, and (**c, f**) restored 100×40, (**b, c**) with the *classic* method [2], and (**e, f**) with the *no hiding error* method. (**g, h**) Decoding errors 100×40 from *classic* method: (**g**) *hiding failure* error, (**h**) *missing color* error; (**i**) only *missing color* error from *no hiding error* method. Brightest spots in **g**, **h**, **i**: 3 errors per pixel. (**d**) Share from the *switching shares* method, strong information leak visible.

2 The Method

In this short paper we shall only outline the algorithms, and the details can be found in [2,3]. Assume a color R, G, B pixel in the secret image is represented by a 6×6 segment in a share, consisting of randomly displaced R, G, B and black (K) pixels, with equal probabilities. There are two shares. Overlaying one on the other reveals color pixels if colors in a given position are the same (*uncovered*), or black ones, if colors are different (*covered*, ideally narrow-band color filters are assumed). Obtaining a fully bright color (for example, all 36 pixels red and uncovered) in a segment is statistically improbable, so having for example six pixels uncovered in each non-black color is considered as white (brightness loss is unavoidable). Let us call these pixels *open*; numbers of open pixels is established by dithering the secret in a palette of $\{0, \ldots, 6\}$ pixels in each color per segment.

Classic method [2] Initially the shares are equal, so all the pixels are *uncovered*. We attempt to cover all the pixels except the *open* ones by swapping the pixels, by pairs, in share 2 within a segment. If, at random, there are less R pixels than the required number of *open* R pixels in a segment, then the *missing color* error occurs. If some non-*open* pixels cannot be *covered* due to lack of pixels in a covering color in share 2, then the *hiding failure* error occurs.

This is illustrated in Fig. 1b (and c showing the restored image [2]), where for example in a G field some dark pixels appear – *missing color* error, and in a R field some G pixels emerge giving yellow – *hiding failure* error.

No hiding error method (strictly, *no hiding failure error* method) It is proposed to start from shares with all pixels covered: for each pixel in share 1, in share 2

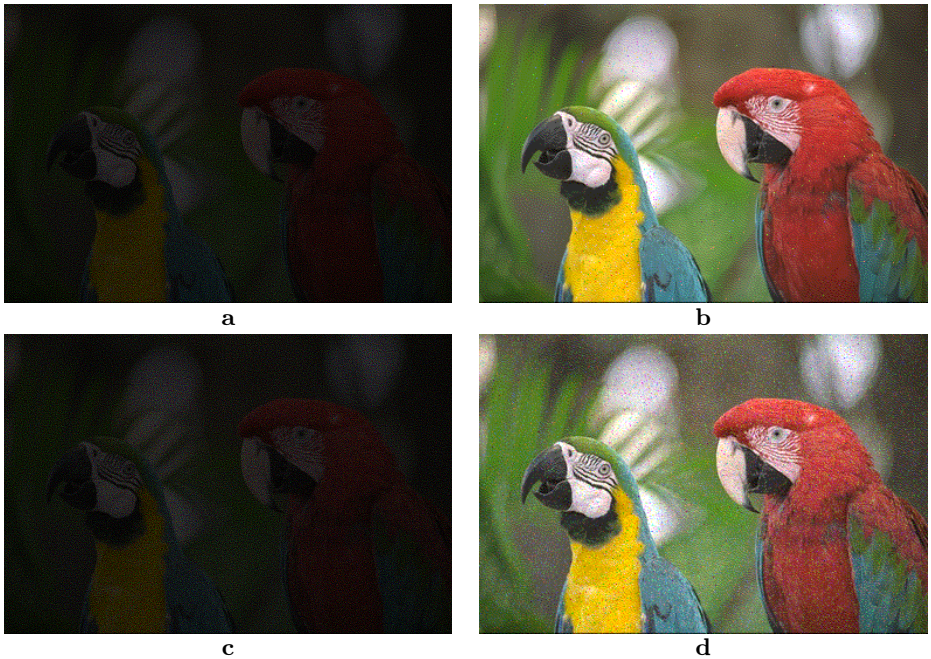

Fig. 2. Results for a natural image `parrots`, 384×256. (**a, c**) Decoded, 2304×1536; (**b, d**) restored, 384×256. (**a, b**) *classic* method [2]; (**c, d**) *no hiding error* method.

a pixel with any color different from that of share 1 is set at random. We attempt to *uncover* the *open* pixels by swapping the pixels, by pairs, in share 2 within a segment, while avoiding *uncovering* any not-*open* pixel. The *hiding failure* error cannot appear, but the *missing color* errors can be statistically more frequent, as there should be enough pixels in a color not in one, but in two different shares. This is illustrated in Fig. 1e, f, where some pixels are too dark – *missing color* error. Unbalanced missing color errors can give rise to changes of hue.

The densities of errors per pixel are larger in general in the *no hiding error* method than in the *classic* method. The total density of two types of errors together from the *classic* method versus the density for one type of error from the *no hiding error* method are: 0.141 vs. 0.191 for the `test100` image, and 0.031 vs. 0.039 for the `parrots` image (Fig. 2). These densities clearly depend on the image brightness, see Fig. 1g-i.

Both above methods need the search for pixels to be swapped which now is performed at random, to keep unchanged the originally random properties of the shares. Speeding up this search is possible, but was not attempted. The processing of each segment is independent and can be performed in parallel.

Switching shares method A method was tried in which the pixel for the share 2 was chosen from share 2 of the *classic* method if the pixel in a segment should be *open*, and from the share 2 of the *no hiding error* method otherwise. The idea would rely on selecting pixels from two random distributions, which should give another random distribution. The catch is that in this case the selection is not

random, but it depends on the secret. The share 2 generated in this way, shown in Fig. 1d, reveals a strong leak of the secret. Therefore, this method, although extremely quick, is totally unsuccessful and will be postponed.

In an example of a natural image (Fig. 2), in spite of that the density of errors is smaller with the *no hiding error* method, the image quality seems to be better with the *classic* method. The *hiding failure* errors which produce surplus color spikes are not harmful in images a, b, while the density of *missing color* errors in the brighter and more colorful regions of images c, d is conspicuous.

The results of randomness tests [1] performed for 100 realizations of coding the images with the new method are similar to those from the *classic* method presented in [2], so in this short paper we shall omit showing the large graphs.

3 Conclusion

A new variant of the color visual cryptography method has been proposed. Only the *missing color* errors appears in it, as compared to the previously used method in which also the *hiding failure* errors are present. The secret images decoded in the proposed method have no surplus bright color spikes, although the color can be more uneven in bright regions. Both the new and the previous method have the same virtue of true randomness of the shares. More research is necessary to speed up the processing, besides that each algorithm can be parallelized.

References

1. Bassham, L.E., Rukhin, A.L. et al.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. (2010), NIST Rep. 800-22 Rev 1a. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762
2. Chmielewski, L.J., Nieniewski, M., Orłowski, A.: Can color visual cryptography be truly random? In: Proc. Int. Conf. CORES. LNNS vol. 255, pp. 72–86 (2021). https://doi.org/10.1007/978-3-030-81523-3_7
3. Chmielewski, L.J., Nieniewski, M., Orłowski, A.: Testing the randomness of shares in color visual cryptography. Pattern Analysis & Applications **24**(4), 1475–1487 (2021). https://doi.org/10.1007/s10044-021-00999-5
4. De Bonis, A., De Santis, A.: Randomness in secret sharing and visual cryptography schemes. Theor. Comput. Sci. **314**(3), 351–374 (2004). https://doi.org/10.1016/j.tcs.2003.12.018
5. Liu, Z., Zhu, G. et al.: Contrast-enhanced color visual cryptography for (k, n) threshold schemes. ACM Trans. Multimedia Comput. Commun. Appl. (2022). https://doi.org/10.1145/3508394, accepted Feb 18, 2022
6. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT'94. LNCS vol. 950, pp. 1–12 (1995). https://doi.org/10.1007/BFb0053419
7. Orłowski, A., Chmielewski, L.J.: Generalized visual cryptography scheme with completely random shares. In: Proc. 2nd Int. Conf. Applications of Intelligent Systems APPIS 2019. pp. 33:1–33:6. ACM (2019). https://doi.org/10.1145/3309772.3309805
8. Ulutas, M., Yazici, R. et al.: (2,2)-secret sharing scheme with improved share randomness. In: Proc. 23rd Int. Symp. Computer and Information Sciences ISCIS 2008. pp. 1–5. IEEE (2008). https://doi.org/10.1109/ISCIS.2008.4717857