Analysis of the paper: A new *k* out of *n* secret image sharing scheme in visual cryptography

Guillem Barta & Oriol Juan

***Abstract*—Visual Cryptography is the technique of sharing an encoded secret image by dividing it up into many shares and distributing them among various participants. It is essential to amass all the shares in order to decrypt the original image.**

A *k out of n* scheme represents a big leap forward in Visual Cryptography, providing versatility and security to older methods. By applying certain conditions and executing XOR operators it is possible to divide the secret image into n shares, while being able to recover the image by superposing an arbitrary subset k of those transparencies.
In this paper we explore Shakar and Swaran's (k,n) technique. Structural and security flaws of the proposed methodology are discussed. In addition, an alternate hypothetical method using Shamir's 1979 paper [1] is discussed.

I. Introduction

THIS paper explores the mathematical *k out of n* method (first proposed by Shamir [1] in 1979) applied to visual cryptography. On the one hand, Shamir's *k out of n* scheme goes as follows; A *share* of the secret is provided to each of the *n* users, so that any of the *k* shares superposed can reveal the secret, but less than k shares should not give any information about the original message. On the other hand, visual cryptography is a powerful but simple technique used to encrypt a picture into transparencies. This way, the stacked shares reveal the original image. This method was first introduced by Naor and Shamir [2] in 1994.

We intended to extend Shamir's [1] secret sharing concept to visual cryptography. To do so, we followed Shakar's and Eswaran's [8] *k out of n* scheme for color images. Being able to send encrypted color images represents a significant improvement over the original binary images proposed in Naor and Shamir's [2] paper, Visual Cryptography. Nevertheless, while reproducing Shakar's and Eswaran's [8] paper we found inconcluences in the author's methodology which prevented us from getting the expected result.

II. Related works

To better understand the topic we are dealing with, we have to take a look at the most relevant previous works:

- **How to Share a Secret [1]:** In 1979 Adi Shamir published the paper that would revolutionize the way a secret could be shared; how to divide data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of k-1 pieces would reveal absolutely no information about D. This technique enables the construction of robust key management schemes.
- **Visual Cryptography [2]**: In 1994 Naor and Shamir proposed an innovative method to share encoded images without the need for any cryptographic computations. A brand new cryptography topic was created, Visual Cryptography.
  First, the authors proposed a basic scheme, where the user could decode the secret by overlapping a pair of transparencies.
  Although it introduced a new and powerful tool to share secret binary images, it did not discuss the possibility to share gray-scale or color images. The authors then extended this method to a *k out of n secret* sharing problem.
- **Sharing multiple secrets in visual cryptography [7]**: In 2007 Jian Shyu's team discussed a new application to the visual cryptography problem, sharing multiple secrets at once.
  Using two circle shares and stacking them together the user can decode the messages by rotating multiple times the second share an angle x.
  This was the first paper that discussed the ability to share up to any number of multiple secrets in two circle shares.
- **Visual cryptography for color images [4]**: In 2003 Young-Chang Hou published three new methods for visual cryptography of gray-level and color images, based on past studies on the halftone technology [5] and the color decomposition method [6]. They also can be incorporated into the *k out of n* model.
  This methods retained the advantages of black-and-white visual cryptography, but can also be applied to a gray-level or color image.

III. A New k out of n Secret Image Sharing Scheme in Visual Cryptography

The aim of this technique is to protect a secret image by encrypting the data and dividing it into *n* transparencies or shares, while being able to decode it if *k* shares are stacked together, being *k* and *n* arbitrary numbers following the condition $k \leq n$.

Assume the USA army wants the nuclear bomb codes to be encrypted for an unauthorized person, but available at any time for those who have been granted the access.

For security reasons, the secret is split into 4 (*n*) image shares, given to each of the president's trusted team members along with a *key* which will help them decrypt the secret once

the shares are amassed. This way a person with only one share and the key can not decode the codes by himself.

A war is unpredictable and there might be the need for a quick response and to join all four may be a difficult task (one of the members could be captured by the enemy). This scheme allows the users to recover the code not with four but just 2 (k) transparencies and the key.

This way, the secret can be secured from an individual intentions, since it will need the consensus of at least two persons, but can be decoded without the need to gather all the shares.

IV. Adaptations of the proposed scheme to Python

A basic idea of the algorithm is as follows: The secret image is divided into three gray-level images (R, G, B). By projecting (multiplicating) each gray-level matrix with the corresponding Dirichlet matrix created using numpy.random.dirichlet (detailed in section IV) we are able to generate multiple matrices that satisfy step 5 and 6 [8]. Operating between matrices as explained in step 7 [8] and applying XOR operations with the keys, results in the creation of n shares. The reconstruction consists on reapplying the XOR operation and stacking at least two shares together.

The proposed scheme was implemented in Spyder 5.2.2, using Python 3.9 . It only employs *skimage.data*, *numpy* and *matplotlib.pyplot* libraries.

In the first steps of the project, the code was poorly optimized. The execution of the code took on average 53 seconds. We concluded the reason was an excessive use of iterations.

In order to adapt this paper's *k out of n* method, we have implemented many specific Python functions, which helped in compacting and optimizing the code, taking the average execution time from 53 seconds to just 2.25 seconds, resulting in a 95.75 % time improvement.

A. Relevant functions

- **Dirichlet Distribution** A key method in this paper's algorithm is the numpy.random.dirichlet function, used to adapt step 5 [8] to Python. This function generates a set of random numbers (following Dirichlet's distribution) that always sum up to one, which is convenient for this step's purpose. It was also optimal for the need of 3-channel images, by creating 4 dimension arrays, which eliminated the need for any iterations.

- **Bitwise XOR** The first code drafts used numpy's function *numpy.logical_xor*, it only computed the truth value element-wise. The final project utilizes *numpy.bitwise_xor*, which computes the bit-wise XOR of two arrays, element-wise.
  This enables the user to share gray-level or color images, instead of just binary images.

V. Results

We could successfully reproduce Shankar and Eswaran's [8] paper. We can see the expected result in Fig 1, and the image generated by our code in Fig 2.

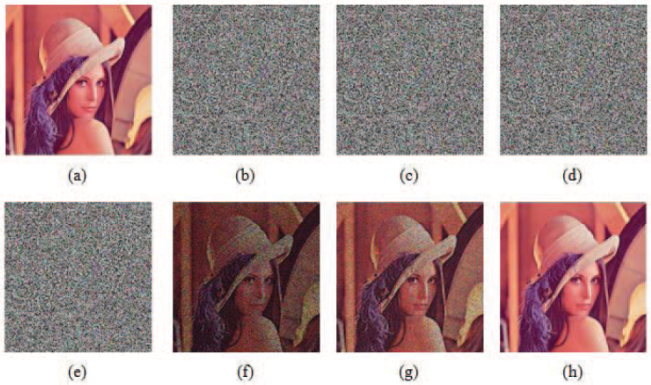

Fig. 1. Results of Lena in Shankar and Eswaran's paper. (a) Secret image (b-e) Shares (f-g) Reconstructed images with 2 and 3 shares, respectively (h) Final Image with four images stacked

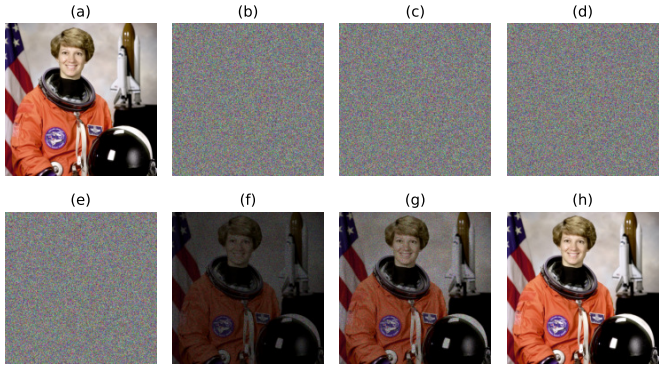

Fig. 2. Results of Astronaut in our project. (a) Secret image (b-e) Shares (f-g) Reconstructed images with 2 and 3 shares, respectively (h) Final Image with four shares stacked

VI. Conclusion and flaws of the methodology

Due to the data type used when processing the image (*uint8*), some of the pixel values had to be truncated, therefore we can see less contrast in the recovered image in comparison to the original one. We cannot state for sure if the authors had this problem, since it is not addressed in the original paper [8]

Even though we obtained a similar result, we came across some structural flaws concerning the security of the method, which we list below:

- **Structural flaw:** The original paper [8] claims this method to be a (k, n) secret sharing scheme. This means that the shares contain all the information to decipher the secret. However, an **additional key matrix** is used to encrypt them with an XOR operation. It implies that

every participant needs access to such key, defeating the purpose of the paper itself, which is to have the shares, and only the shares, reveal the image.

- **Security flaws:** Supposing there was no key matrix, therefore not applying an XOR encryption step, the shares we are left with contain most of the original image information, as we can see in Fig. 3. This means that the method, as it is explained in *'A new k out of n secret image sharing scheme in visual cryptography'* [8], does little to no encryption before the application of an XOR operation.

  This is a major flaw, since there is no way to apply this scheme to real life situations. Also, the authors give little to no explanation about how their method should be used.

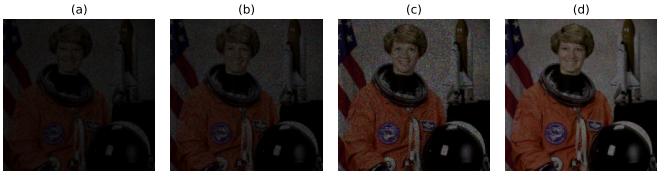

Fig. 3. The four shares previous to the XOR operation. The secret image is still visible.

VII. Hypothetical Proposed Solution

Given that the explored scheme was unsuccessful, we propose a solution that combines Shamir's [1] mathematical method with XOR image encryption; Our idea is to generate a random key matrix with a unique seed. Knowing this seed the user will be able to duplicate the key at any time.

First, using Shamir's mathematical *k out of n* scheme, it is possible to hide the seed by generating *n* shares (which represent the x and f(x) values of the polynomial). If k of this duplets are combined, the secret can be revealed. Secondly, encrypt the original image with the key matrix, applying an XOR operation. This will code the secret image and make it unreadable unless the user reapplies the operation.

Then, we need to generate the image transparencies. A transparency will be constituted by the encrypted image, but with a little twist; The first two pixel values of any transparency will be replaced with the coordinates x and f(x).

A transparency will be allocated to each of the members. In order to reconstruct the secret image, it will be necessary to gather k of the duplets hidden in the transparencies. Once the user knows all the necessary information, the *k out of n* method will allow him to know the secret seed, thus it will be possible to reconstruct the key matrix and reapply the XOR operation, decoding the secret image.

References

[1] Adi Shamir. 1979. How to share a secret. Commun. ACM 22, 11 (Nov. 1979), 612–613. https://doi.org/10.1145/359168.359176

[2] Naor, M., Shamir, A. (1995). Visual cryptography. In: De Santis, A. (eds) Advances in Cryptology — EUROCRYPT'94. EUROCRYPT 1994. Lecture Notes in Computer Science, vol 950. Springer, Berlin, Heidelberg.

[3] Abdelsatir, El-Tigani Alhesseen, Sahar Ali, Hyam Hashim, Afra. (2014). A Novel (K,N) Secret Sharing Scheme from Quadratic Residues for Grayscale Images. International Journal of Network Security Its Applications. 10.5121/ijnsa.2014.6406.

[4] Young-Chang Hou,Visual cryptography for color images,Pattern Recognition,Volume 36, Issue 7, 2003, Pages 1619-1629, ISSN 0031-3203, https://doi.org/10.1016/S0031-3203(02)00258-3.

[5] Y.C. Hou, F.Lin, C.Y. Chang, A new approach on 256 color secret image sharing technique, MIS Review, No.9, December 1999, pp.89-105.

[6] Y.C. Hou, C.Y. Chang, F.Lin, Visual Cryptography for color images based on color descomposition, Proceedings of the Fifth Conference on Information management, Taipei, November 1999, pp. 584-591

[7] Shyong Jian Shyu, Shih-Yu Huang, Yeuan-Kuen Lee, Ran-Zan Wang, Kun Chen, Sharing multiple secrets in visual cryptography, Pattern Recognition, Volume 40, Issue 12, 2007, Pages 3633-3651, ISSN 0031-3203, https://doi.org/10.1016/j.patcog.2007.03.012.

[8] K. Shankar and P. Eswaran, "A new k out of n secret image sharing scheme in visual cryptography" 2016 10th International Conference on Intelligent Systems and Control (ISCO), 2016, pp. 1-6, doi: 10.1109/ISCO.2016.7726969.