EasyChair Preprint

№ 3562

Optimization Algorithms in Visual Cryptography

Bukurie Ibrahimi, Zamir Dika and Artan Luma

June 7, 2020

Optimization algorithms in visual cryptography

Bukurie Ibrahimi[1], Zamir Dika[1], Artan Luma[1]

Faculty of Contemporary Sciences and Technologies, South East European University
Tetovo, Macedonia

bukurieshabani@hotmail.com, z.dika@seeu.edu.mk, a.luma@seeu.edu.mk

Abstract - Visual Cryptography is a cryptographic technique which intends to hide a secret within images. These images are encrypted into n shares and decrypted without computer calculations. In this work, we briefly describe a new proposed (*n*,*n*) Secret Sharing Scheme for grayscale/color images. We will approach the problem by two main algorithms: the algorithm of Cheng et al. and the deterministic (*n*, *n*) algorithm of Wang et al. We will modify them such that new obtained secret sharing scheme becomes more efficient and more secure. The scheme uses XOR operation sharing images, algebraic function for creating a secret image for authentication, while the size of the original image and shadows are the same. In the paper, we will make use of Cantor function, which makes possible the generation of respective codes for each participant.

Keywords*: Visual Cryptography, Secret Image Sharing, XOR operation, Cantor function*

1. Introduction

The rapid development of technology has made possible to transmit and store easily a large number of digital data. However, the transmission of data over the internet or their storage in computers can be easily intercepted by "attackers", if such data are not secure enough. Therefore, information security, especially in the world of Big Data and new Cloud “paradigm”, represent a very emergent issue.
One of the proposed schemes for information security is Visual Cryptography. It was firstly presented by Naor, Shamir [1]. Visual Cryptography (VC) is a new type of cryptography that intends to hide a secret within images. These images are encrypted into n shares and decrypted without computer calculations.

Some of the practical applications could be in medical images where the patient information is sensitive and needs to be protected during storage and transmission, especially in the cloud [15,19]; the internet voting system [16,17]; biometry privacy [20,21], etc. References [13], [14] provide very useful information about the most recent important trends in Visual Cryptography.

Research in Cryptography, in general, and in Visual Cryptography, in particular, is developed and expanded in multiple directions. Various schemes were improved. There were newly presented schemes, algorithms get advanced, etc.

In the following, we will describe some of the trends and directions of scientific research in the field of Visual Cryptography.

It is worth mentioning that Visual Cryptography schemes mainly concerned with black and white images. It was Verheul and Van Tilborg [2], who for the first time propose Visual Secret Sharing Scheme
for color images, which presently is known as color scheme of k out of n.

Because Visual Cryptography in color images allows the use of natural color images to store information, it has become a very important field of study.

More advanced schemes based on Visual Cryptography are presented in [4, 5, 6]. In those schemes colored image is hidden in many meaningful covered images. Chang [4] in 2000 has introduced a new secret colored sharing scheme in which the ordinary collection of sub-pixels and rows are modified [5]. This new technique does not require the collection of transparent and as such is suitable for real-time applications, however, this scheme, to restore the image without losses, requires the use and storage of a Color Index Table (CIT). The disadvantages of this method are: it

requires large space for storage of information, a long time during searching in the CIT as well as a loss of image resolution in the case of an increase of colors in the image secret.

Chang and Yu [6] presented an advanced scheme to hide color images into numerous images that do not require CIT. This technique achieves a restoring of the secret image without loss; however, created divisions (covered images) contain redundant noise. They use meaningful shares to hide the secret image, and each pixel is transformed into 9 subpixels. The scheme needs only the XOR operation. The advantage of this scheme is that it can share complex images.

Youmaran, Adler and Miri [3] proposed an improved algorithm based on Chang and Yu's scheme in order to enhance the quality of covered images. Through this method, one achieves the restoring of data without loss and also there is noise reduction in images without changing at all the complexity of the calculations.

The purpose of the research [18] by Askari and Heyse is EVC (Extended Visual Cryptography) security scheme, which requires no more pixels during sharing and recovering images than the secret original image, and it still retains the image of good quality during the process. They used two methods, one for processing the secret image, and the other one for balancing the image after processing the secret image. This proposed scheme realizes high-security scheme based on EVC [19].

In [7] Wang, are proposed two methods without pixel expansion: probabilistic $(2,n)$ scheme for binary images, and deterministic (n,n) scheme for grayscale and color images. Both of these methods are based on Boolean operations and both provide high security.

The deterministic (n,n) algorithm of Wang et al. [7] is an algorithm that uses a random grid to generate share images. It requires no codebook. It's based on Xor operation and the size of secret images is the same as share images.

Wu and Chen [23] were the first who have encrypted two secret images into two meaningful images, say A and B, where the first image was obtained as a result of merging A and B, and the other one as a result of first the opposite clockwise rotation of A for 90° and then merging it with the image B. Extensions and modifications to the above method are given in papers [24-26].

Chen and Wu [27] have proposed an effective method for a multi-secret sharing scheme based on Boolean operators. The advantage of this scheme stands in the fact that the scheme is expanded to encode n images comparing to one image as it was previously.

Latter, Reddy and Prasad [28] proposed a new scheme based on [27]. It uses meaningful shares for multiple secret sharing and also for covering images. It also uses Boolean operations and lossless recovers multiple secrets.

Independently from the security issues in VC, many researchers have experimented with the idea of cheating the system. The methods for cheating the basic schemes on VC and EVC as well as their techniques have been presented in [13].

Yang and Laih [29] have proposed a method for cheating prevention. In this method, one requires a Trusted Authority (online) to verify the sharing of participants.

Another method for cheating prevention is described by Horg [30]. In this case, the cheater needs to have exact information about the distribution of black and white subpixels of sharings of "honest" participants.

Hu and Tzeng [31] proposed improvements in the method of Yang and Laih from [29]. According to them, the scheme for cheating prevention needs no support from direct Trusted Authority. Instead, it is needed the verification of images for each participant to be different and to be known only for participants.

Recently, there were research studies linking VC and graph theory. In [33] it is considered a new visual cryptography scheme that allows for sharing of multiple secret images on graphs. More precisely, given an arbitrary graph (V,E)

where every node and every edge are assigned an arbitrary image. Images on the vertices are “public” and images on the edges are “secret”.

In [34] is considered a visual cryptography scheme characterization of all connected graphs G with the minimum value of the pixel expansion 4 and the clique number of graph G being 5. For more details see [34] and references therein.

The remainder of this paper is organized as follows: in Section 2 we briefly review related work and 2.1 explain the proposed scheme. Section 3 describes our structure-aware VC algorithm in detail. Section 4 presents results and compares them to those obtained by previous methods. The conclusions are drawn in Section 5.

The deterministic (n,n) algorithm of Wang et al. [7] is an algorithm that uses a random grid to generate share images. It requires no codebook. It's based on Xor operation and the size of secret images is the same as share images.

2. Proposed scheme

In this paper, we propose an algorithm (n,n) -Visual Secret Sharing (VSS) as a result of modification of algorithms of Chang and Yu [6] and Wang [7].
More precisely, we will combine algorithms from [6] and [7], to obtain a new scheme, through which we aim to increase the level of security. Firstly, we use the Cantor function together with a random image to create a secret image. Then through the algorithm in [6], we will create share images in the form of a tree, as explained in the scheme in figure 1. We consider dividing the image into sub-image shares in order to enlarge the cases of combinations between sharing images and to make it very hard to be decrypted. Those images, by applying the algorithm presented in [7], will be used to make covered images and thus to share the secret image.

Therefore, through this approach, we aim to increase the level of security.

2.1. The Algorithm

This scheme is divided into three phases. In the first stage, we are dealing with the creation of a pin code for each participant. We will accomplish this by using the generalized Cantor function. In this way, we will get an additional security element. In the second phase, the encryption of the secret image will be carried out, i.e. the image will be camouflaged for each participant. We will do this by sharing the secret image in *n* - meaningless shared images. Our approach will be based on algorithms [6] and [7]. And naturally, in the third stage, we have the process of decryption, first of the pin code and then of the secret image. In the first case we use the modular arithmetic and in the second the Boolean algebra of the XOR operator.

2.1.1. Generation of value B

1) We assume there are n - participants and the secret dealer gives each of them an m -digit number. The algorithm generates a natural number b ,that meets the following conditions:

i. Number $b = b_1 b_2 ... b_{m \cdot n}$ is of length $m \cdot n$ (contains $m \cdot n$ digits).[1]

[1] The length of number *b* can be easily adopted in situations when one requires a number of longer lengths, and even in situations when we want to share to participants values with different number of digits.

ii. Digits b_i satisfy the relation $b_{m\cdot i+1} < b_{m\cdot(i+1)+1}$, for $i = 0,1,...,n-2$.

Note. 'The first digit ' (as well as other digits) not necessarily should be binary digits (from 0 to 9). The first digit, for example, can be 491 ($b_1 = 491$), the second digit can be 27 ($b_2 = 27$), the third digit can be 1001 ($b_3 = 1001$),and so on. In such cases, to avoid confusion, values b_i ($i = 1,2,...,n$) are separated by a comma. In the above example $b_1 b_2 b_3$ which corresponds to the sequence 491271001, will be written as 491,27,1001.

2) After obtaining the number b satisfying above conditions, the dealer gives to each n-participants m-digit number

$b_{m\cdot i+1} b_{m\cdot i+2} ... b_{m\cdot i+m}, i = 0,1,2,...,n-1$ $b_{mi+1} b_{mi+2} \ldots b_{mi+m}, i = 0, 1, 2, \ldots, n-1,$

and then the value of b will be erased.

3) By using generalized Cantor function [32], by combining values of each participant x_i, $i = 1,2,...,n$ we obtain a unique natural number B given by

$$B = \langle x_1,...,x_n \rangle = \sum_{h=1}^{n} \left\{ \frac{1}{h!} \prod_{j=0}^{h-1} \left[\left(\sum_{i=1}^{h} x_i \right) + j \right] \right\}, \forall (x_1,...,x_n) \in \mathbb{N}^n . \quad (1)$$

2.1.2 Proces of encrypting the image

1) We first take an image I (face, fingerprints, retina, etc.,), to which we associate a matrix of order $m \times n$.

2) Each pixel a_{ij} of the above image is associated with a new number B obtained by the function given in (1). As a result, we obtain a new pixel s_{ij} of the secret image. The secret image is given through the following function (and should be done for each RGB pixel alone):

$$s_{ij} = (a_{ij} + B + a_{ij} \cdot B) \bmod 257 \quad (2)$$

where $i \in \{1,2,...,m\}$, $j \in \{1,2,...,n\}$.

From this relation are determined and saved (for each a_{ij}) values of $\overline{k}_{ij}$:

Secret image S, based on the given algorithm in[6] is divided into n sharing images $G_1, G_2, ..., G_n$, of the same dimension as the secret image S. By applying again the above-mentioned algorithm from [6],each sharing image $G_i, i \in \{1,2,...,n-1\}$ gets divided into two other sharing sub-images which we denote by $G_{i,i-1}, G_{i,i}$, while image G_n maps into itself. Again, all sharing sub-images have the same dimension as a secret image S.

Using the algorithm given in [7], from matrices that represent sharing sub-images $G_{i,i-1}, G_{i,i}$ are formed matrices $S_j, j \in \{1,2,...,n\}$ that are obtained as follows:

In the case when we have two shares, i.e. when $k = 2$, we have

$S_1 = G_{10}$

$S_2 = G_{11} \oplus G_2$

In the case of three shares, so when $k = 3$ we have

$S_1 = G_{10}$

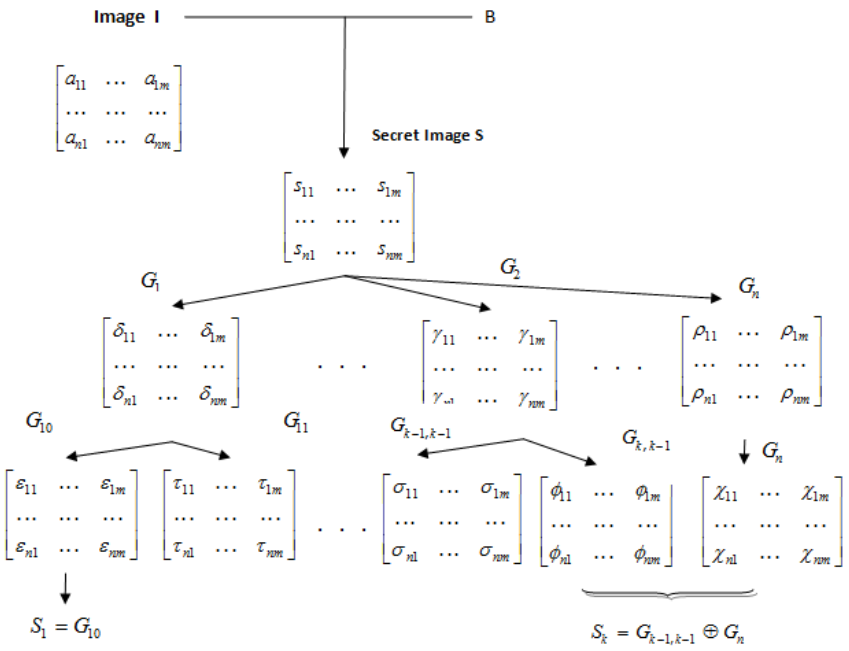
$S_2 = G_{11} \oplus G_{21}$

$S_3 = G_{22} \oplus G_3$

In general for $k = n$ one has

$$S = \begin{cases} G_{10,} & for \quad k = 1 \\ G_{k-1,k-1} \oplus G_{k,k-1}, & for \quad k = 2,3,...,n-1 \\ G_{k-1,k-1} \oplus G_k, & for \quad k = n \end{cases} .$$

More specifically, for the encryption process, we will use the first Chang et al. algorithm. This algorithm will be used to create share images $G_{10}, G_{11}, ..., G_n$ from the original secret image S. These images will be covered through the Wang deterministic algorithm, denoted by $S_1, S_2, ..., S_n$, where during this process number of arbitrary input images for coverage will be much smaller compared with two algorithms. Then these covered images will be used to share the secret image. In the following it is given the schematic description:



2.1.3. Decryption process

During the decryption process, in the first stage is done the verification of $m \cdot n$ digits pin-code. Each of n participants put its pin-code with $m \cdot n$ digits, in any order. According to the description, sorting algorithm based on increasing order of first digits, through (1), verifies the pin-code.

Verification for a_{ij} is done based on the following formula:

$$a_{ij} = \left(\overline{k}_{ij} \cdot 257 + S - B\right) \cdot (1+B)^{-1} \mod 257 \qquad (3)$$

where $(1+B)^{-1}$ is the inverse element of $(1+B) \bmod 257$.

For retrieving the secret image S we should collect all the n sharing images with XOR operator to revile the secret image. Any $n-1$ or fewer shares cannot retrieve any information about the secret. Therefore, the reconstructed secret image is:

$S = S_1 \oplus S_2 \oplus S_3 \oplus ... \oplus S_n$.

Verification for a_{ij} is done from the following formula:

$a_{ij} = \left(\overline{k}_{ij} \cdot 257 + s_{ij} - b\right) \cdot (1+b)^{-1}$,

where $(1+b)^{-1}$ is invers element of $(1+b)$ modulo 257.

2.2. Performance comparisons

In Table 1 we compare our proposed scheme with those of Wang [7] and Chang [6]. The reason for implementing the Chang and Yu [6] scheme is that it can share complex images, while its disadvantages are such as pixel expansion. Also, insecurity will be eliminated in our scheme. The Wang algorithm [7] uses $n-1$ random images as well as a secret image to create shared images, while the proposed scheme only by using the secret image creates shared images. Since it is considered a safe scheme, through this scheme we aim to increase the level of security compared to that of Wang.

Table 1.

Features	**Chang and Yu scheme [6]**	**Wang et al.[7]**	**The proposed scheme**
Pixel expansion	Yes	No	No
Sharing capacity	1/*n*	1/*n*	1/*n*
Image format	Binary gray-level-color	Binary gray-level-color	Binary gray-level-color
Type of algorithm	(*n*, *n*)	(*n*, *n*)	(*n*, *n*)
Security enhancement	NO	Yes	Yes
Sharing shapes	Rectangular	Rectangular	Rectangular
Significance of shared images	Meaningful	Meaningless	Meaningless

3. Discussion

From the described process we understand that in our proposed scheme we involve two levels of security and in both of them, the encryption process is 'easy' while decryption is very difficult. In the first level, one easily generates numbers b_i and B, while conversely to obtain B one needs all values x_i (to obtain Cantor function one needs to know all the values of participants x_i). It is important to mention that this process is used only once in the beginning of the encryption and thus does not take too many resources. Similarly, in the second level, it is easy to determine shares S_i from the secret image S, while for generating secret image S one needs all shares S_i (in order to reconstruct the secret image). Therefore the reconstruction of the secret image is very hard to be decrypted since it is obtained as a combination of all values x_i, coefficients k_{ij} and shares S_i.

As explained previously, our algorithm modifies algorithms in [6] and [7]. Now, we get to the main point on why we decided to modify these two important algorithms.

From the literature we reviewed, we found that the algorithm given in [6] is very appropriate for dividing the image into sub-images and since we did not use the same approach of pixel expansion, we have chosen to modify the algorithm in [7] to cover those sub-images. It is worth mentioning that dividing the image into sub-images that we carried in section 2, increases a number of combinations when one considers attacking the system, by making the scheme very secure.

4. Conclusions

From the extended literature review, one can understand that we have to do with a new, interesting, and important field of study. Visual Cryptography appeared as a result of daily necessities to hide information and then recovering them in the cases when it is not possible or necessary to carry out computer calculations.

We also understand that in the field of Visual Cryptography, one can orient in different directions of research such as the creation of new models, improving existing models, cheating prevention in Visual Cryptography, etc.

Regarding the focused review of the literature, we identified the most appropriate present methods, where we considered found two important algorithms that were modified to developing our scheme. We achieved to built and prove the correctness of our algorithm in this regard. In later stages, we expect to program and test this algorithm to show also practical whether it presents an advantage compared to other contemporary algorithms in Visual Cryptography.

References

[1] M. Naor and A. Shamir, *Visual Cryptography*, Advances in Cryptology-EUROCRYPT'94, LNCS 950, Springer-Verlag, pages 1-12, 1994.

[2] E. R. Verheul and H. C. A. Van Tilborg, *Constructions and properties of k out of n visual secretsharing schemes*, Designs, Codes and Cryptography, Vol. 11, No. 2 (1997) pp. 179–196.

[3] R. Youmaran, A. Adler and A. Miri, *An improved visual cryptography scheme for secret hiding*, School of Information Technology and Engineering (SITE), University of Ottawa, Ontario, Canada

[4] C. Chang, C. Tsai, and T. Chen, *A new scheme for sharing secret color images in computer network*, In the Proceedings of International Conference on Parallel and Distributed Systems, pages 21–27, July 2000.

[5] C. Yang and C. Laih., *New colored visual secret sharingschemes*, Designs, Codes and Cryptography,20:325–335,2000.

[6] C. C. Chang and Yu. T. X., *Sharing a Secret Gray Image in Multiple Images*, In the Proceedings of International Symposium on Cyber Worlds: Theories and Practice, Tokyo, Japan, Nov. 2002, pp.230-237.

[7] D. S. Wang, L. Zhang, N. Ma, and X. Li. *Two secret sharing schemes based on Boolean operations*, Pattern Recognition 2007,

[8] C. C. Thien and J. C. Lin, *An image-sharing method with user-friendly shadow images*, IEEE Trans. Circuits Syst. Video Technol. 13 (12) (2003)1161–1169.

[9] R. Z. Wang and C. H. Su, *Secret image sharing with smaller shadow images*, Pattern Recognition Lett. 27 (6) (2006) 551–555.

[10] Y. S. Wu, C. C. Thien and J. C. Lin, *Sharing and hiding secret images with size constraint*, Pattern Recognition 37 (7) (2004) 1377–1385.

[11] C. C. Chang and I.C. Lin, *A new (t, n) threshold image hiding scheme for sharing a secret color image*, in: Proceedings of the ICCT2003, vol. 1, Beijing, China, 2003, pp. 196–202.

[12] V. Goebel, Th. Plagemann, *Research / Scientific Methods in Computer Science*, Department of Informatics, University of Oslo.

[13] J. Weir and W. Yan, *Visual Cryptography and Its Applications*, Jonathan Weir and WeiQi Yan &Ventus Publishing ApS, 2012

[14] S. Cimato and Ch. Yang, *Visual Cryptography and Secret Image Sharing*, August 2011, CRC Press.

[15] K. Pachiappan, S. Annaji and N. Jayakumar, *Security in Medical Images using enhanced Visual Secret Sharing Scheme*, ISSN 2319-8885, Vol.03,Issue.09, May-2014, Pages:1642-1645, International Journal of Scientific Engineering and Technology Research.

[16] A. Bhise, N. Borate, A. Garje and Y. Karkal, *Security Internet Voting System*, The international Journal of Engineering and Science, Volume 4, pp.71-75, 2015

[17] A.B Rajendra and H. S. Sheshadri, *Visual Cryptography in Internet Voting System*, Innovative Computing Technology (INTECH), pp. 60 - 64, 2013.

[18] N. Askari, H. M. Heys and C.R. Moloney, *An extended visual cryptography scheme without pixel expansion for Halftone images*, 2013.

[19] M. Ulutas, G. Ulutas and V. Nabiyev, *Medical image security and EPR hiding using Shamir's secret sharing scheme*, The Journal of Systems and Software, 2011@Elsevier.

[20] A. S. Akotkar and Ch. Choudhary, *Security of Face Authentication using Visual Cryptography*,

[21] A. Ross and A. Othman, *Visual Cryptography for Biometric Privacy*, IEEE Transactions on Information Forensics and Security (Volume:6 , Issue: 1), May 2011.

[22] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson,*Extended Capabilities for VisualCryptography*, TheoreticalComputer Science, vol. 250, pp. 143-161, 2001.

[23] C. C. Wu and L. H. Chen, *A study on visual cryptography*, Mater Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998.

[24] R. Z. Wang and C. H. Su, *Secret image sharing with smaller shadow images*, Pattern Recognition Lett. 27 (6) (2006) 551–555.

[25] Y. S. Wu, C. C. Thien and J. C. Lin, *Sharing and hiding secret images with size constraint*, Pattern Recognition 37 (7) (2004) 1377–1385.

[26] C. C. Chang and I. C. Lin, *A new (t, n) threshold image hiding scheme for sharing a secret color image*, in: Proceedings of the ICCT2003, vol. 1,Beijing, China, 2003, pp. 196–202.

[27] Tzung-Her Chen and Chang-Sian Wu, *Efficient multi-secret image sharing based on Boolean operations*, Elsevier@2011.

[28] L. S. Reddy and M. V. N. K. Prasad, *Extended Visual Cryptography Scheme for Multi-secret Sharing*, Springer@2016, Volume 44 of the series Smart Innovation, Systems and Technologies, pp 249-257

[29] C.-N. Yang and C.-S. Laih, *Some new types of visual secret sharing schemes*, In Proc. Nat. Computer Symp., 1999, vol. 3, pp. 260–268.

[30] G. B. Horng, T.-G. Chen and D.-S. Tsai, *Cheating in visual cryptography*, Designs, Codes, Cryptog., vol. 38, no. 2, pp. 219–236, 2006.

[31] Chih-Ming Hu and Wen-GueyTzeng, *Cheating Prevention in Visual Cryptography*, IEE Transactions on Image Processing, vol. 16, no. 1, January 2007.

[32] M. Lisi, *Some remarks on the Cantor pairing function*, Le Matematiche, Vol. LXII (2007) - Fasc. I, pp. 55-65

[33] S. Lu, D. Manchala, and R. Ostrovsky, *Visual cryptography on graphs*, J Comb Optim 21, 47–66 (2011). https://doi.org/10.1007/s10878-009-9241-x

[34] M. Davarzani, *Visual cryptography scheme on graphs with m*(G) = 4*, Transactions on Combinatorics, Vol. 8 No. 2 (2019), pp. 53-66.