Optimization Based Adaptive Tagged Visual Cryptography

Pei-Ling Chiu
Department of Risk Management & Insurance
Ming Chuan University
Taiwan, ROC
plchiu@mail.mcu.edu.tw

Kai-Hui Lee
Department of Computer Science & Information Engineering
Ming Chuan University
Taiwan, ROC
khlee@mail.mcu.edu.tw

ABSTRACT

The Tagged Visual Cryptography Scheme (TVCS) [1] adds tag images to the noise-like shares generated by the traditional VCS to improve the shares management of the traditional VCS. However, the existing TVCSs suffers visual quality of the recovered secret image may be degraded and there may be pixel expansion. This study proposes a Threshold Adaptive Tagged Visual Cryptography Scheme ((k,n)-ATVCS) to solve the above-mentioned problems. The ATVCS encryption problem is formulated in a mathematical optimization model, and an evolutionary algorithm is developed to find the optimal solution to the problem. The proposed (k,n)-ATVCS enables the encryptor to adjust the visual quality between the tag image and the secret image by tuning parameters. Experimental results show the correctness and effectiveness of this study.

CCS CONCEPTS

•**Security and privacy** → Visual Cryptography; •**Computing Methodologies** →Genetic programming

KEYWORDS

Visual cryptography, tagged visual cryptography, adaptive tagged visual cryptography, optimization, genetic algorithm.

1 INTRODUCTION

The Threshold Visual Cryptography Scheme ((k,n) -VCS) encrypts a secret image into n meaningless noise-like shares [1]. During decryption, the secret image can be recovered by stacking any k of n shares in order to restore a secret image. The Tagged Visual Cryptography Scheme (TVCS), which adds an additional tag image to the shares, and folds each share can reveal the tag image such that the shares can be identified to improve the friendliness of VCSs [2, 3]. This study proposes a pixel-expansion-free Threshold Adaptive Tagged Visual Cryptography Scheme ((k,n)-ATVCS) that uses a systematic encoding method to provide adjustability for TVCS.

2 THE (k,n)-ATVCS ENCRYPTING PROCESS

The proposed (k,n) -ATVCS uses a two-phased encryption process, as shown in Fig. 1. The first phase embeds each tag-image (TM) by (2,2)-ProbVCS [4] and generates a Transient-share (T) which has the same size of secret image, i.e. double the size of the tag-image. A tag-pixel is encrypted as two share-pixels by (2,2)-ProbVCS; then the two corresponding share-pixels will be placed in two coordinates symmetrized to the folding line in the T-Share. Phase 2 modifies the pixels of T-Shares to yield Tagged-Shares (TSs). Finally, folds a TS can reveal the embedded tag image and stacks k TSs can recover the secret image.

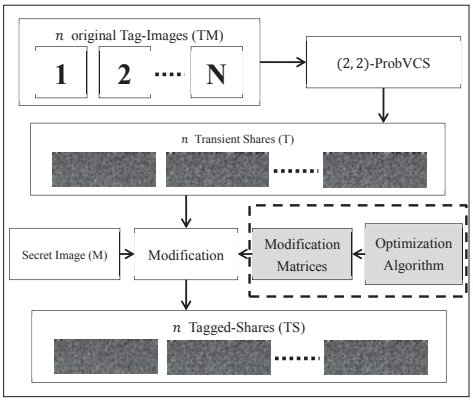

Fig. 1: ATVCS encrypting procedure

As shown in Fig. 1, although both Transient Shares (T) and shares of VCS have the same noise-like appearance, the pixel distributions for a set of T and for shares of a specific VCS (or ATVCS) are quite different. For example, codebook ($C_0 = \{[1\ \ 0\ \ 1]^T, [1\ \ 1\ \ 1]^T\}$ and $C_1 = \{[1\ \ 1\ \ 0]^T, [1\ \ 0\ \ 1]^T, [0\ \ 1\ \ 1]^T\}$) and chosen-probability set ($F^0 = \{0.5, 0.5\}$ and $F^1 = \{1/3, 1/3, 1/3\}$) are used to construct a (2,3)-ProbVCS. The pixel distribution pattern, iB$(n-i)$W, indicates there are i black pixels and $n-i$ white pixels distributed among n shared pixels. Vector $[1\ \ 1\ \ 0]^T$ was selected from C_1 for sharing a black secret pixel, shares 1, 2 and 3 will get a black, black and white pixels, respectively. The pixel distribution pattern for the shares will be 2B1W. On the other hand, the pixel distribution in n T-shares that were generated independently is totally independent in Phase 1. Suppose each T has the same pixel

GECCO '18 Companion, July 15–19, 2018, Kyoto, Japan

ACM ISBN 978-1-4503-5764-7/18/07.
https://doi.org/10.1145/3205651.3208767

density d, the probability of pixel distribution pattern $i\mathrm{B}(n-i)\mathrm{W}$ can be calculated as following:

$$P_{i,n}^{d} = \binom{n}{i} \times d^{i} \times (1-d)^{n-i}.$$

In general, while any two T-shares are stacked, each pixel distribution pattern will uniformly appear in the stacked image. Hence, it is almost impossible to reveal any meaningful image by stacking two shares together. Hence, in Phase 2, the encryption process generates n Tagged-Shares by modifying the pixels of the T-Shares based on Modification-Matrices that are designed for sharing a secret image [5]. Modification-Matrix $\mathrm{M}^0(\mathrm{M}^1)$ is a $(n+1)\times(n+1)$ matrix for sharing white (black) secret pixels in a secret image. Modification probability $m_{i,j}^{0}$ $(m_{i,j}^{1})$, $0 \le i \le n, 0 \le j \le n$, is an element of M^0 (M^1) and is used to alter the distribution pattern of n pixels that have the same coordinates in n T-shares from $i\mathrm{B}(n-i)\mathrm{W}$ to $j\mathrm{B}(n-j)\mathrm{W}$. The Modification-Matrices not only influence the visual quality of the tag image and the recovered secret image, but also relate to the construction of a secure VCS. In this study, the Modification-Matrices designing problem is formulated as a mathematical optimization model, and an evolutionary algorithm is developed to solve the problem [6]. The proposed algorithm encodes candidate solutions, M^0 and M^1, as chromosomes as below. The fitness function is defined as contrast of the recovered secret image directly. Tuning parameters, ρ_{max} and d, are used to verify feasibility of a new chromosome.

A chromosome

$m_{0,0}^{0}\ldots m_{0,n}^{0}$	…	$m_{n,0}^{0}\ldots m_{n,n}^{0}$	$m_{0,0}^{1}\ldots m_{0,n}^{1}$	…	$m_{n,0}^{1}\ldots m_{n,n}^{1}$
Matrix M^0			Matrix M^1		

3 EXPERIMENTAL RESULTS

In the experiment, an encryption results are demonstrated for evaluating visual effects of the ATVCS. Then, the visual quality of ATVCS are compared with previous studies. The population size is 50. The crossover and mutation probabilities are 75% and 0.05% (for each row of modification matrix). The parent and survivor selection mechanisms are best 2 out of random and replace worst, respectively. The algorithm stops when the fitness improvement remains under 0.1% in last 10 generations.

Given the space limitation, (2,3)-ATVCS is used as an example in this paper. In this experiment, images "IMAGE", "TAG 1", "TAG 2, and "TAG 3" are used as the secret image and three tag images, respectively. First, the $(2,3)$-ATVCS encryption result of the proposed method is validated. Parameters ρ_{max} (maximum pixel altering probability) and d (pixel density for Tagged-Shares) are set to 0.15 and 0.5, respectively. Fig. 2 shows that the proposed (k,n)-ATVCS algorithm is proved feasible.

Experiment 2 presents comparison results of the previous studies of Wang&Hsu [2], Wu&Sun [3], and the proposed (k,n)-ATVCS. Taking the $(2,3)$ sharing scheme as an example, the preset parameters are $\rho_{max}=0.15$ and $d=0.5$. The experimental results are shown in Fig. 3. In terms of the visual quality of the recovered secret images (Fig. 3(a)~(c)) and the recovered tag images (Fig. 3(d)~(f)), the performance of the proposed ATVCS is better than others.

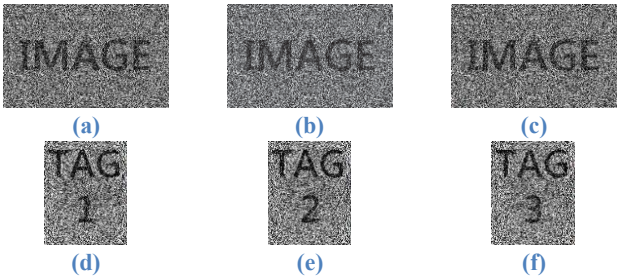

Fig. 2: $(2,3)$-ATVCS experimental results. (a)~(c) results of stacking any two tagged shares. (d)~(f) recovered tag images.

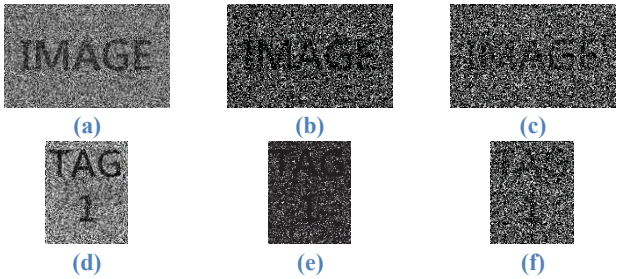

Fig. 3: Comparison results of $(2,3)$-ATVCS. (a)~(c) recovered secret images of ATVCS, Wang&Hsu, and Wu&Sun, respectively. (d)~(f) recovered tag images of ATVCS, Wang&Hsu, and Wu&Sun, respectively.

4 CONCLUSION

In order to provide TVCS with an adjustable encryption mode, this paper proposes an ATVCS for users to tune parameters (ρ_{max} and d), meaning trade-off can be implemented for the secret and tagged recovered image contrast, and the encryption scheme is more flexible. According to the experimental results, the shares generated by the adjustable method are free of the pixel expansion problem, and the recovered secret and tag images have better visual quality than previous methods.

ACKNOWLEDGMENTS

This work was supported in part by the Ministry of Science Technology of Taiwan under Contracts MOST 106-2221-E-130-016 and MOST 105-2221-E-130-007-MY2.

REFERENCES

[1] M. Naor, and A. Shamir, "Visual cryptography," *Advances in Cryptology — EUROCRYPT'94*, Lecture Notes in Computer Science, pp. 1-12: Springer, 1995.
[2] W. Ran-Zan, and H. Shuo-Fang, "Tagged visual cryptography," *Signal Processing Letters, IEEE,* vol. 18, no. 11, pp. 627-630, 2011.
[3] X. Wu, and W. Sun, "Improved tagged visual cryptography by random grids," *Signal Processing,* vol. 97, pp. 64-82, 2014.
[4] C. N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognition Letters,* vol. 25, no. 4, pp. 481-494, 2004.
[5] K.-H. Lee, and P.-L. Chiu, "Sharing visual secrets in single image random dot stereograms," *IEEE Transactions on Image Processing,* vol. 23, no. 10, pp. 4336-4347, 2014.
[6] T. Back, *Evolutionary algorithms in theory and practice: evolution strategies, evolutionary programming, genetic algorithms*: Oxford University Press, 1996.