XOR-ed Based Friendly-Progressive Secret Sharing

by Joni Welman

Submission date: 01-Aug-2022 05:30PM (UTC+0700)
Submission ID: 1877666188
File name: XOR-ed_Based_Friendly-Progressive.pdf (3.32M)
Word count: 1069
Character count: 6202

2019 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)

XOR-ed Based Friendly-Progressive Secret Sharing

Heri Prasetyo
Department of Informatics
Universitas Sebelas Maret
Surakarta, Indonesia
heri.prasetyo@staff.uns.ac.id

Joni Welman Simatupang
Study Program of Electrical Engineering
President University
Bekasi, Indonesia
joniwsmtp@president.ac.id

***Abstract*— This paper presents a simple approach for secret sharing under the bitwise eXclusive-OR (XOR) framework. The proposed method extends the effectiveness of Progressive Secret Sharing (PSS) into the Friendly Secret Sharing (FSS). The PSS produces a set of shared images in noisy-like form, while FSS generates shared images into more-visually-friendly appearance. The proposed method offers lossless ability in the recovery result of secret image. At the same time, it shows superiority compared to the former existing scheme in the secret sharing task.**

Keywords*— *friendly, lossless, progressive, secret sharing

I. INTRODUCTION

Several methods have been developed for secret sharing such as PSS [1], multiple secret sharing [2], lossless PSS [3], etc. Most of them yield promising results on secret sharing systems. This section presents the proposed XOR-ed based FPSS. It extends the usability of PSS [1] into FSS. The proposed method offers lossless ability on secret image reconstruction. Let I be a quantized secret image of size $M \times N$. This image is obtained after performing the scalar quantization with coefficient Q. Suppose that this quantized image is in RGB color space. Each pixel is denoted as $I(x, y, c)$, where $x = 1,2, \dots, M$ and $y = 1,2, \dots, N$ are spatial positions. The symbol c is color channel, i.e. $c = 1,2,3$.

The proposed method generates n shared images denoted as $\{S^1, S^2, \dots, S^n\}$, where S^i is the i-th shared image. The PSS [1] produces a set of shared images in noise-like form. The shared image can be easily recognized by investigating its content. The proposed method overcomes this problem by rendering the secret image into the cover image. Let C be a color cover image of size $M \times N$. This image size should be identical to that of I. Each pixel of C is denoted as $C(x, y, c)$.

The computation of shared image generation can be explained as follow. For each pixel on spatial position (x, y, c) with $x = 1,2, \dots, M$, $y = 1,2, \dots, N$, and $c = 1,2,3$, the proposed method firstly computes the masking coefficient R as follow:

$$R \leftarrow U_I(0, \left\lceil \frac{255}{Q} \right\rceil), \tag{1}$$

where $U_I(a, b)$ denotes the random number generator which uniformly produces an integer in range $[a, b]$. The symbols $\lceil \cdot \rceil$ and $\leftarrow$ are ceiling and assignment operators, respectively. The proposed method subsequently determines the indices of two selected shared images, i.e. r_1 and r_2, with constraint $1 \leq r_1, r_2 \leq n$ and $r_1 \neq r_2$. These two indices are randomly chosen. The first selected shared image, i.e. S^{r_1} is determined as:

$$S^{r_1}(x, y, c) \leftarrow C(x, y, c) \oplus I(x, y, c) \oplus R, \tag{2}$$

where $\oplus$ represents the bitwise-based XOR operation. Whereas, the second selected shared image, i.e. S^{r_2} is computed as:

$$S^{r_2}(x, y, c) \leftarrow C(x, y, c) \oplus R. \tag{3}$$

For the rest of shared images with $i = 1,2, \dots, n$ and $i \neq r_1, r_2$, we perform the following process;

$$S^i(x, y, c) \leftarrow C(x, y, c). \tag{4}$$

At the end of this process, one obtains a set of shared images $\{S^1, S^2, \dots, S^n\}$.

The secret image can be reconstructed by stacking several shared images as follow:

$$\hat{I}(x, y, c) \leftarrow S^{t_1}(x, y, c) \oplus S^{t_2}(x, y, c) \oplus \dots \oplus S^{t_T}(x, y, c), \tag{5}$$

where $\hat{I}(x, y, c)$ is the recovered secret image at spatial position (x, y, c) and $\{t_1, t_2, \dots, t_T\}$ is the index of stacked shared image. The symbol T denotes the number of stacked shared images with condition $T \leq n$. The proposed method achieves FSS since the content of S^i is almost similar to C under some extends, while it gives PSS based on the facts that the quality of recovered secret image is improved by stacking more shared images. Thus, the proposed method can be categorized as friendly and progressive secret sharing.

II. ANALYSIS OF PROPOSED XOR-ED BASED FPSS

This section supports the correctness of the proposed method with the theoretical analysis. It considers the lossless ability of the proposed method on recovering secret image. For simplicity, we omit the spatial position of an image. Then, the formal analysis is given as follow.

Theorem 1: *The proposed XOR-ed Based FPSS is lossless if* $T \leq n$ *and* $1 \leq r_1, r_2 \leq T$.

Proof: Stacking several shared images $\{S^{t_1}, S^{t_2}, \dots, S^{t_T}\}$ produces a recovered secret image as:

$$\hat{I} \leftarrow S^{t_1} \oplus S^{t_2} \oplus \dots \oplus S^{t_T}.$$

For $T \leq n$ and $1 \leq r_1, r_2 \leq T$, the value $\hat{I}$ is then obtained as:

$$\hat{I} \leftarrow S^{t_1} \oplus S^{t_2} \oplus \dots \oplus S^{r_1} \oplus \dots \oplus S^{r_2} \oplus \dots \oplus S^{t_T}.$$

This form can be alternatively rewritten as follow:

$$\hat{I} \leftarrow S^{r_1} \oplus S^{r_2} \oplus \underbrace{S^{t_1} \oplus S^{t_2} \oplus \dots \oplus S^{t_T}}_{T-2},$$

$$\hat{I} \leftarrow S^{r_1} \oplus S^{r_2} \oplus \underbrace{C \oplus C \oplus \dots \oplus C}_{T-2}.$$

If $T - 2$ is even number, the XOR property [3] gives the following result:

$$\hat{I} \leftarrow S^{r_1} \oplus S^{r_2} \oplus 0 = S^{r_1} \oplus S^{r_2}. \tag{6}$$

The recovered secret image $\hat{I}$ can be simply obtained by performing XOR operation between S^{r_1} and S^{r_2}.

Since $S^{r_1} \leftarrow C \oplus I \oplus R$ and $S^{r_2} \leftarrow C \oplus R$, the form in (6) can be further rewritten as follow:

$$\hat{I} \leftarrow S^{r_1} \oplus S^{r_2} = C \oplus I \oplus R \oplus C \oplus R,$$

$$\hat{I} \leftarrow C \oplus C \oplus R \oplus R \oplus I.$$

The XOR property [3] simplifies the computation as:

978-1-7281-3038-5/19/$31.00 ©2019 IEEE

$$\hat{I} \leftarrow 0 \oplus 0 \oplus I = I. \quad (7)$$

Simplification in (7) indicates that the proposed method is lossless, i.e. $\hat{I} = I$. It completes a proof. ■

III. Experimental Results

We report some experiments in this section. Two color images (for cover and secret image) are used in this experiment as shown in Fig. 1. Herein, the quantization coefficient is simply set as $Q = 25$ indicating that each pixel of secret image is represented with four bits. The number of shared images is $n = 10$. Fig. 2 depicts two shared images obtained by the proposed method. As it can be seen, the proposed method effectively generates a set of shared images, in which the contents of shared image are almost identical to that of the cover image.

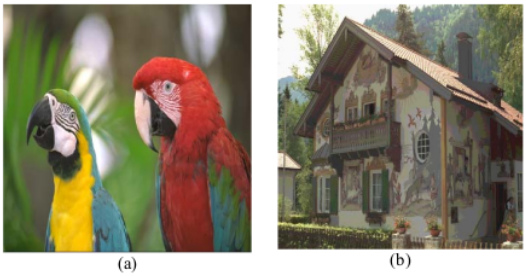
Fig. 3 displays the performance comparison between the proposed method and extended PSS [1] for FSS in terms of visual investigation on the quality of $\hat{I}$. The number of stacked shared images are set as $T = \{2, 4, 6, 8, 10\}$. It can be deducted from Fig. 3 that the proposed method achieves PSS and FSS criteria for a good secret sharing scheme. The proposed method yields lossless recovered secret image if all shared images are stacked by XOR operation. In addition, the proposed method is superior compared to that of the extended PSS [6] for FSS.

References

[1] H.-C. Chao and T.-Y. Fan, "XOR-based progressive visual secret sharing using generalized random grids," *Displays*, vol. 49, pp. 6-15, 2017.

[2] H. Prasetyo and J. M. Guo, "A note on multiple secret sharing using Chinese remainder theorem and exclusive-OR," *IEEE Access*, vol. 7, 1, pp. 37473-37497, 2019.

[3] H. Prasetyo and C. H. Hsia, "Lossless progressive secret sharing for grayscale and color images," *Multimed. Tools App.*, 2019. https://doi.org/10.1007/s11042-019-7710-5.



(a) (b)

Fig. 1. Two testing color images: (a) cover image, and (b) quantized secret image.

(a) (b)

Fig. 2. Two shared images generated by proposed method with $n = 10$: (a-d) $\{S^1, S^2, \ldots, S^4\}$.

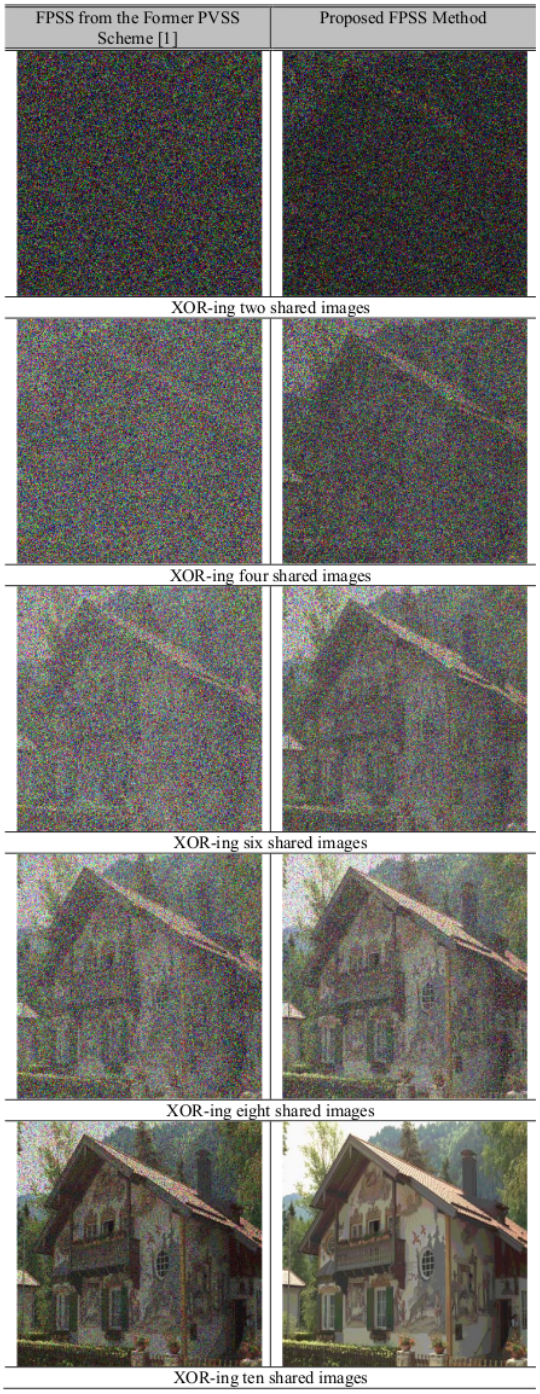


Fig. 3. The reconstruction process of secret image.

978-1-7281-3038-5/19/$31.00 ©2019 IEEE

XOR-ed Based Friendly-Progressive Secret Sharing

ORIGINALITY REPORT

20%	15%	15%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	mdpi-res.com Internet Source	5%
2	Jing-Ming Guo, Dwi Riyono, Heri Prasetyo. "Improved Beta Chaotic Image Encryption for Multiple Secret Sharing", IEEE Access, 2018 Publication	3%
3	www.computingonline.net Internet Source	2%
4	koreascience.or.kr Internet Source	2%
5	scholars.ncu.edu.tw Internet Source	2%
6	aivc.ntust.edu.tw Internet Source	2%
7	"Improved Beta Chaotic Image Encryption for Multiple Secret Sharing", IEEE Access, 2018 Publication	2%
8	doaj.org Internet Source	1%

9	Chen, W.Y.. "Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation", Applied Mathematics and Computation, 20070201 Publication	1 %
10	WWW.MDPI.COM Internet Source	1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		