Chapter 27
An Improved Size Invariant (n, n) Extended Visual Cryptography Scheme

Rahul Sharma
Indian School of Mines, India

Ayush Khare
Indian School of Mines, India

Nitesh Kumar Agrawal
Indian School of Mines, India

Arup Kumar Pal
Indian School of Mines, India

ABSTRACT

In this paper, the authors have presented a (n, n) extended visual cryptography scheme where n numbers of meaningful shares furnish a visually secret message. Initially they have converted a grayscale image into binary image using dithering method. Afterwards, they have incorporated pixel's eight neighboring connectivity property of secret image during formation of meaningful shares. The scheme is able to generate the shares without extending its size. This approach has enhanced the visual quality of the recovered secret image from n numbers of shares. The scheme has been tested with some images and satisfactory results are achieved. The scheme has improved the contrast of the recovered secret image than a related (n, n) extended visual cryptography scheme.

1. INTRODUCTION

A *n* out of *n* visual cryptography scheme *((n,n)*-VCS*)*, defined by Naor and Shamir (1994) in which the image is first encrypted into n shares and someone with all *n* shares can only decrypt the secret image, while stacking less than *n* number of shares will not reveal any information about the secret image. In a *(2, 2) Visual Cryptography* experiment defined by Naor and Shamir (1994), a codebook comprising of all code words of size *(2, 2)* sub-pixels is taken. The secret image is then encrypted into two shares where the size of each share is four times the size of the original secret mage. An example illustrating

DOI: 10.4018/978-1-7998-1763-5.ch027

the *(2,2)* Visual Cryptography codebook is shown in Figure 1 where the secret image is shown in Figure 1(a) and the two shares are shown in Figure 1(b) and Figure 1(c). The final stacked result of the two generated shares is shown in Figure 1(d).

The overlapping of encrypted shares can be of two types; namely *Stack based* and *XOR-based* In *Stack based visual cryptography scheme*, the logical OR of the generated shares has been chosen whereas in *XOR-based visual cryptography scheme*, the XOR operation on the generated shares are performed to reveal the secret image (Ou et al., 2015). According to the research, many unresolved issues on OR-based visual cryptography scheme have been extensively studied, such as meaningless share, poor contrast quality of revealed secret image, perfect reconstruction of the black pixels and the cheating prevention issue (Chen and Tsao, 2009). To overcome the above mentioned problems, a random grid-based size-invariant visual cryptography scheme (RGVCS) was introduced by Kafri and Keren (1987) in which a secret image is encoded into two random-liked shares. The size of each share is same as that of the original secret image for solving the problem of pixel expansion. Furthermore, areas of research include improving the visual quality of RGVCS and constructing RGVCS with the abilities of OR and XOR decryption. Contrast is one of the main factor in evaluating the visual quality of the revealed secret image. In OR-based visual cryptography scheme, the contrast achieved is at most 50% of the secret image. In order to achieve better visual quality of the revealed secret image, XOR-based visual cryptography scheme was introduced (Ou et al., 2015). In XOR-based visual cryptography scheme, only small, cheap and lightweight computational devices are needed. Decryption of secret image using XOR-based operation improves the visual quality of the revealed secret image and solves the alignment problem, some drawbacks like meaningless shares still exist in this scheme. We can generate the meaningful shares with the help of multiple cover images. To generate meaningful shares, the light transmission of a share is adjusted according to an independent cover image. Moreover, the visual quality of both the shares and the revealed secret image is still poor.

To overcome the aforementioned problem, in this paper, a size invariant XOR-based visual cryptography scheme has been proposed with a notion of improved visual quality of the meaningful shares as well as the revealed secret image. Firstly, a basic algorithm for (n, n) XOR-based visual cryptography scheme has been presented. Teng Guo et. al. (2014) have suggested a (n,n) random grid based extended visual cryptography scheme. Introduction of randomness in share generation process of random-grid based visual cryptography scheme (RGVCS) have degraded the visual quality of the generated meaningful shares and the revealed secret image. To overcome the peculiarities associated with above problem, we have introduced a new method in which we have considered the probability of the neighboring pixel of cover image to determine whether a pixel should be black or white. The proposed method improves the visual quality of the generated shares and the revealed secret image considerably. In this paper, we have improved the to the algorithm proposed in Teng Guo et al. (2014) in terms of improvement of visual quality of the generated meaningful shares as well the revealed secret image by introducing some improvement in the above *(n, n) XOR-based Visual Cryptography* algorithm and secondly perfect regeneration of the black pixels associated with the black pixel in the revealed secret image.

This paper is organized as follows. In section 2, we provide the detailed method of RG-based VCS and RG-based EVCS. In section 3, we provide a proposed method of RG-based EVCS is given. In section 4, a performance analysis of the algorithm provided in section 3 is done. Section 4 provides the experimental results of algorithm proposed in section 3. The conclusion of the paper is given in section 5.