Chapter 32
A Novel Pixel Merging-Based Lossless Recovery Algorithm for Basic Matrix VSS

Xin Liu
Harbin Institute of Technology, China & Harbin University of Science and Technology, China

Shen Wang
Harbin Institute of Technology, China

Jianzhi Sang
Harbin Institute of Technology, China

Weizhe Zhang
Harbin Institute of Technology, China

ABSTRACT

Lossless recovery in visual secret share (VSS) is very meaningful. In this paper, a novel lossless recovery algorithm for the basic matrix VSS is proposed. The secret image is reconstructed losslessly by using simple exclusive XOR operation and merging pixel. The algorithm not only can apply to the VSS without pixel expansion but also can apply to VSS with pixel expansion. The condition of lossless recovery of a VSS is given by analyzing the XOR all columns of basic matrixes. Simulations are conducted to evaluate the efficiency of the proposed scheme.

INTRODUCTION

One of efficient secure methods for secret image protection is the visual secret sharing (VSS), also called visual cryptography scheme (VCS) (Wang, Zhang, Ma, & Li, 2007) (Naor, & Shamir, 1999). The original secret image is divided into different meaningless or meaningful shadows (shares) in VSS generating phase. The generated shares are distributed to a group of participants (Yang, 2004) (Cimato, Prisco & Santis, 2006) (Kafri, & Keren, 1987). If enough shadows collected, the secret image is performed by superposing all or some of shares. Based on human visual system (HVS) we can easily obtain the original secret image. However, less than th threshold coefficient$^{(k)}$ participants give nothing about the secret image.

DOI: 10.4018/978-1-7998-1763-5.ch032

Literature on VSS is quite rich (Liu, Guo, Wu, & Qian, 2012) (Shyu, 2009) (Li, El-Latif, & Niu, 2012) (Chen, & Tsao, 2011) (Yan, Jin, & Kankanhalli, 2004) (Li, Ma, Su, & Yang, 2012). The concept of the VSS is first introduced by Naor and Shamir (Naor, & Shamir, 1999), the shadow images are generated according to the basic matrixes and are expanded to the larger size than the secret image. Following Naor and Shamir's work, many research works focus on VSS own physical properties and problems of the VSS mechanism. The probabilistic VSS (ProbVSS) (Yang, 2004) and Random grid (RG)-based VSS (Kafri, & Keren, 1987) (Liu, Guo, Wu, & Qian, 2012) (Shyu, 2009) (Li, El-Latif, & Niu, 2012) (Chen, & Tsao, 2011) are proposed to solve the problem of the pixel expansion. The (Blundo, D'Arco, Santis, & Stinson, 2003) (Hou, & Quan, 2011) focus on the basic matrixes, (Yan, Jin, & Kankanhalli, 2004) (Li, Ma, Su, & Yang, 2012) (Yan, Liu, & Yang, 2015) and XOR-based VSS (XVSS) (Tuyls, Hollmann, & Lint, 2005) concentrate on improving the visual quality. The basic matrix-based VSS scheme is our research object.

It is worth noting that in a lot of situations the lossless recovery of secret image is necessary such as for transmission and storage of military secret images, private medical images, and so on. It is very meaningful to research the lossless recovery scheme which only uses simple computation in the phase of decrypting (recovering).

In the following, we discuss some related works and scope of the proposed work. Lossless recovery can reconstruct the secret losslessly if the light-weight computation device is available.

Chen et al. (Chen, Wang, Yan, & Li, 2014) proposed a progressive$^{(2, n)}$ VSS and the secret will be reconstructed losslessly by additive operation. Wu and Sun (Wu, & Sun, 2013) proposed a scheme having the abilities of OR and exclusive OR (XOR) decryptions and the secret could be recovered losslessly at the condition of collecting all n shares. Utilizing XOR operation, Yan et al. (Yan, Wang, El-Latif, & Niu, 2015) proposed a scheme which needs all n shares to reveal the distortion-less secret image. Nevertheless, none of these schemes (Chen, Wang, Yan, & Li, 2014) (Wu, & Sun, 2013) (Yan, Wang, El-Latif, & Niu, 2015) could recover the secret losslessly when the size of shadow images is expanded. The two-in-one VSS (TiOISS) (Lin, & Lin, 2007) only needs k shares to reconstruct the distortion-less secret image. However, it still requires knowing the order of shadow images and needing complicated computations, i.e., Lagrange interpolations, in the second decoding phase. In addition, in most literatures, the visual quality of the recovered image is always low and the secret image could not be losslessly recovery.

In this paper, a novel pixel merging-based lossless recovery algorithm for basic matrix-based VSS is proposed. The proposed algorithm just needs to use simple XOR operation and pixel merging in order to lossless recover the original secret image. In addition, the algorithm can be applied to the VSS with and without pixel expansion.

In our algorithm, firstly to analysis the ability of lossless recovery of a VSS by performing the simple XOR operation on all n columns of basic matrixes. According to the XOR theory, we can obtain the following conclusion. If all the XOR-ed result of the basic matrix M^0 is 0 and all the result of the basic matrix M^1 is 1, the secret image can be recovered losslessly for a VSS scheme. Otherwise, the secret image cannot be recovered losslessly for a VSS scheme. In the phase of recovery, the original secret image could be losslessly revealed by XOR-ing all the shadows. For the VSS scheme with pixel expansion, the recovery phase needs a pixel merging phase. The algorithm has lossless recovery feature at the same time maintains the merits of the original VSS scheme. Simulation results show the effectiveness of the proposed scheme. Comparisons with the previous approaches show the advantages of the proposed algorithm.