A Novel Progressive Secret Image Sharing Scheme Based on Arithmetic Mean

Lintao Liu, Hefei Electronic Engineering Institute, Hefei, China
Yuliang Lu, Hefei Electronic Engineering Institute, Hefei, China
Xuehu Yan, Hefei Electronic Engineering Institute, Hefei, China
Song Wan, Hefei Electronic Engineering Institute, Hefei, China

ABSTRACT

The current researches in secret sharing techniques have limitations of lossy recovery for binary images, complex computation for grayscale images, and “All-or-Nothing”. In this paper, we propose a novel progressive secret image sharing (PSS) scheme based on arithmetic mean. In the proposed scheme, the more shares are collected, the better recovered visual quality will be. Furthermore, it can realize lossless recovery with all the shares. It can be directly used to share grayscale images and can be easily extended to deal with binary and color images. In the recovery process, it only needs simple computing (arithmetic mean). Simulations show the advantages and effectiveness of the proposed scheme.

KEYWORDS

Arithmetic Mean, Greyscale Images, Lossless Recovery, Progressive Secret Sharing

INTRODUCTION

Nowadays, the wide use of media data such as digital images or videos attracts the attention to the security issues. In the past few years, various cryptographic schemes have been proposed as possible solutions to the security of digital images. Cryptography provides a very powerful method to protect both confidentiality and robustness. Traditional cryptographic algorithms (Li et al., 2012; Li et al., 2007; Torrubia & Mora, 2002; Yang et al., 2009) can be directly applied to protect the images, audios and videos in these applications. But these schemes are not loss-tolerant, and need a great lot of calculation. At the meanwhile, users need to pay attention on the security of the key used for encryption.

Secret sharing techniques are able to solve these issues above, which are the natural drawbacks of the traditional cryptography. Secret sharing (SS) was first proposed by Blakley (1979) and Shamir (1979) independently. In the encryption process, it splits the secret image into noise-like shadow images (also called shares or shadows), and then distributes them among the authorized participants. When collecting sufficient shadow images, authorized participants can recover the secret. This technique has value of better theoretical and practical research.

Visual secret sharing (VSS) and Shamir’s polynomial-based scheme are mainstreams of secret sharing. Except for simple recovery and alternative order of the shadow images, the traditional VSS
and random grids-based VSS (RGVSS) (Chen & Tsao, 2011; Kafri & Keren, 1987; Shyu, 2007) can realize many other good properties, such as no pixel expansion, meaningful shares and so on. Since they are designed only for the binary images, it still has a long way to be applied in encryption for the grayscale image. In addition, their recovered secret images are usually lossy. At the same time, some other schemes based on Shamir’s polynomial and Lagrange interpolation, have been proposed (Thien & Lin, 2003; Zhao et al., 2009) to realize the secret image sharing. These schemes have the advantages of \((k,n)\) threshold, lossless recovery and less pixel expansion. However, they suffer from “All-or-Nothing”, complex recovery and known order of the shadow images.

Along with the development of many business applications like pay-per-view videos, Pay-TV/Music, artwork image vending, and video on demand (VOD), the following feature namely “progressive or perceptual property” is more and more valuable (Yan et al., 2014). This feature requires that the visual quality of media data could be controlled by a control factor, which can be determined by the senders. Progressive property makes it possible for potential users to view low-quality copies of the media data products before buying them. By controlling the number of shares sent to users, secret sharing scheme with special construction may effectively achieve the goal of visual quality control.

Currently, progressive visual secret sharing (PVSS) schemes based on VCS (Hou & Quan, 2011; Hou & Quan, 2013; Chen, 2009), Shamir’s polynomial (Chen & Lin, 2005) or transformation (Huang et al., 2010) have the progressive or perceptual property. Progressive property means better perceptual quality will be gained when more shadow images are collected. However, they overall suffer from the same disadvantages as VCS, RG and Shamir’s polynomial-based secret sharing.

In this paper, we propose a PSS scheme based on arithmetic mean. The proposed scheme satisfies large number of valuable features in secret sharing, including progressive visual quality with more shares, lossless recovery with all the shares, and simple computation (only addition and division). It can be directly applied to share grayscale images, and can be extended to deal with the binary and color images. Besides, it can realize other features such as alternative order of shadow images in recovery, avoiding the pixel expansion and no codebook design. Experimental results show the effectiveness of the proposed scheme.

The rest of the paper is organized as follows. Section 2 presents the basic definitions and main ideas of the proposed PSS scheme. Section 3 introduces the proposed PSS scheme. Section 4 is devoted to the experimental results and analysis. Finally, Section 5 concludes this paper.

**PRELIMINARIES**

The grayscale secret image is denoted as \(S\) with the pixel value \(S(i, j)\), \(1 \leq i \leq M, 1 \leq j \leq N\), and size \((S) = (M, N)\), where function size means size of \(S\).

The original grayscale secret image \(S\) is distributed to \(n(n \geq 2, n \in \mathbb{Z}^+)\) shadow images (shares) \(SC_1, SC_2, \ldots, SC_n\) by the generation function \(GF\), that is:

\[
(SC_1, SC_2, \ldots, SC_n) = GF(S, n)
\]

The recovered secret image \(S'\) is recovered from \(t(1 \leq t \leq n, t \in \mathbb{Z}^+)\) shadow images by the recovery function \(RF\), that is \(S' = RF(SC_{i_1}, \ldots, SC_{i_t})\), where \(i_1, i_2, \ldots, i_t\) is the subsequence of \(1, 2, \ldots, n\).
Related Content

Internet Crime: How Vulnerable Are You? Do Gender, Social Influence and Education play a Role in Vulnerability?
[www.igi-global.com/chapter/internet-crime-vulnerable-you-gender/60937?camid=4v1a](www.igi-global.com/chapter/internet-crime-vulnerable-you-gender/60937?camid=4v1a)

E-Behaviour Trends and Patterns among Malaysian Pre-Adolescents and Adolescents

Biometric Controls and Privacy
[www.igi-global.com/chapter/biometric-controls-privacy/60966?camid=4v1a](www.igi-global.com/chapter/biometric-controls-privacy/60966?camid=4v1a)
Identification of Natural Images and Computer Generated Graphics Based on Hybrid Features
www.igi-global.com/article/identification-natural-images-computer-generated/65733?camid=4v1a