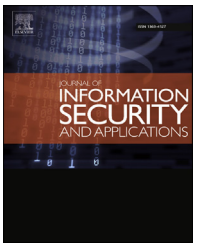
Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa



Scalable secret sharing of compressed multimedia

Shreelatha Bhadravati [a], *Pradeep K. Atrey* [a,b,*], *Majid Khabbazian* [c]

[a] *University of Winnipeg, MB, Canada*
[b] *University at Albany - State University of New York, Albany, NY, USA*
[c] *University of Alberta, AB, Canada*

ARTICLE INFO

Article history:
Available online 19 August 2015

Keywords:
Secret sharing
Scalable reconstruction
Compressed media

ABSTRACT

Traditional secret image sharing methods have an all-or-nothing property, which is not suitable for applications which require gradual reconstruction. In this paper, we propose a scalable secret image sharing (SSIS) method that provides gradual reconstruction with smooth scalability. Furthermore, we extend this method to videos and propose a scalable secret video sharing (SSVS) method. These two methods are designed for compressed multimedia (i.e. JPEG images and H.264 videos). In both methods, the size of the shadow images (shares) is reduced to an optimal value. Experimental results and analyses show that the proposed methods are computationally and semantically secure.

1. Introduction

Addressing the security concerns of multimedia data is a challenging problem as the size of the data is huge, therefore processing in real time is a constraint (Su et al., 2012). Furthermore, the diversified application areas of the digital content make it more challenging to develop security measures as each application can have different end users and specific requirements. For example, in the case of digital videos, in one scenario a low quality video is made available to all users as a means to promote the content as in pay-TV, HDTV. Adversely, in applications like video conferencing and surveillance, the video must be completely unintelligible to unauthorized users in order to preserve the privacy of the people and objects involved.

The task of securing digital images and videos has been studied extensively in the past. The conventional method of ensuring security is to encrypt the data using block encryption methods such as Advanced Encryption Standard (AES) (National Institute of Standards and Technology, 2001). Applying these block encryption methods, and therefore considering image (Subramanyan et al., 2011; Zeghid et al., 2007) or video (Liu and Koenig, 2010; Shi et al., 1999; Wu and Kuo, 2005) data to be byte data, is not a practical solution because of the computational complexity involved in the traditional encryption methods. To overcome this problem, selective encryption methods were proposed in which only certain parts of the image (Cheng and Xiaobo, 2000) or video (Shi and Bhargava, 1998) are encrypted, as opposed to encrypting the entire image or video data. However, these methods were insufficient in protecting the confidentiality of the data, as the unencrypted portions of the image and video revealed considerable amount of information. Further, the encryption methods require the use of a secret key. Storing the cryptographic key is also problematic as a single person cannot be entrusted with the security of the key. Storage of the key at a single place can lead to single point failure (Blakley, 1979) and if the key is corrupted or lost, there is no way to reconstruct the original data. The key is further vulnerable to security attacks and can be compromised if stored at multiple places.

* *Corresponding author.* State University of New York, Albany, NY, USA. Tel.: +1 518 442 4281; fax: 518-442-5638.
E-mail address: patrey@albany.edu (P.K. Atrey).
http://dx.doi.org/10.1016/j.jisa.2015.06.004
2214-2126/

In 1979, Shamir (1979) developed the secret sharing scheme (we call it "Shamir's Secret Sharing" (SSS) scheme throughout this paper) to overcome the problem of cryptographic keys. This method is said to be information theoretically secure. In this (k, n), $(2 \le k \le n)$ threshold scheme, the secret is divided into n shares and any k shares are required to reconstruct the secret. Any number of shares less than k cannot reconstruct the secret. Furthermore, the minimum size of the shares has to be equal to the size of the secret to be information theoretically secure (Jhanwar and Safavi-Naini, 2013). Using SSS on digital data can make it information theoretically secure, provided the size of the shares is at least the same as the size of the secret data. However, this causes an increase in the storage space as it is similar to keeping n copies of the secret data. Hence, it would be ideal if the size of the shares was reduced to $1/k$ of the size of the secret data. Unfortunately, by reducing the size of the shares, the information theoretic security property of SSS is lost. Recently many methods have been proposed to reduce the size of the shares in the computationally secure model (Alharthi and Atrey, 2010; Thien and Lin, 2002). The main idea in these methods, though not mentioned, is to use the Reed–Solomon error correction (RSEC) scheme (Lacan et al., 2009), which is similar to SSS. The RSEC scheme can be used for information dispersal but it cannot be used for hiding information because it does not provide semantic security, as was shown in our previous work (Bhadravati et al., 2013).

In a computationally secure model, a basic method is to encrypt the image using a secret key and then apply SSS on the secret key. In this method, every user gets the same copy of the encrypted image and a share of the secret key. Though this method may be computationally more efficient (depending on k, n and the encryption method), the size of the shares is still the same as the size of the original image. In Krawczyk (1994), it was proposed to use the information dispersal methods along with the basic method discussed above in order to reduce the size of the shares to $1/k$ of the size the secret image.

The SSS scheme also has the property that either the secret image is reconstructed completely when k shares are available or it is not reconstructed at all. This all-or-nothing (Fatemi et al., 2009) property might not be suitable for certain applications, which require the secret data to be gradually reconstructed based on the number of shares available.

1.1. *Paper goal and contributions*

The goal of this paper is to provide a semantically and computationally secure method for scalable sharing of compressed images and videos. The proposed method can be used in the applications where a gradual reconstruction of secret images and videos is required.[1]

The main contributions of this paper are described as follows:

1. We propose a (k, n) scalable secret image sharing (SSIS) method which provides scalability, such that when k shares are available the image reconstructed is of low quality, achieving the highest quality when all n shares become available. This method possesses semantic security and it reduces the size of the share images by $1/k$.
2. We extend this scalable method of image sharing to provide (k, n) scalable secret video sharing (SSVS) for compressed videos, where k shares are required to reconstruct the base layer of the video. As the number of shares available increases, enhancement layers of the video are reconstructed. To the best of our knowledge, this is the first attempt to propose a scalable secret sharing method on compressed videos.

We demonstrate the utility of the proposed method on compressed images (JPEG) and videos (H.264/SVC). We choose JPEG and H.264/SVC because these are the most widely used encoding standards for images and videos.

1.2. *Paper organization*

The rest of this paper is organized as follows. Section 2 contains the background details of image and video standards that are used in this paper. Also the existing secret sharing methods for images and videos are discussed, and the novelty of the proposed methods against them is highlighted. In Section 3, the proposed SSIS and SSVS methods are described. Section 4 provides the implementation details, performance results and security analysis of the SSIS and SSVS methods. Section 5 concludes this paper.

2. Background and literature review

In this section, the background details of compressed images and videos and the existing works related to secret image sharing are presented. In Section 2.1, JPEG and H.264/SVC compression standards are elaborated to get an understanding of how scalability is achieved. In Section 2.2, SSS, RSEC and the existing methods on SSIS and some of the encryption methods on compressed videos are discussed.

2.1. *Background*

2.1.1. *JPEG*

JPEG is the acronym for Joint Photographic Experts Group (Wallace, 1992), which is the most widely used compression standard for images. In JPEG format, the encoding can be done in four modes. Baseline mode is the most widely used encoding method for JPEG. The second mode of encoding in JPEG format is progressive mode, which is gaining importance recently due to the development of devices with varying bandwidth requirements, though it has not been universally accepted. In the progressive mode of encoding, the images are compressed in multiple passes. The complete image is rendered in the first scan but with low quality and the quality of the image increases with respective scans. For the proposed SSIS method, the progressive mode of JPEG encoding is used, which helps to provide scalability for the compressed images.

There are two types of progressive mode JPEG encoding, which make use of the spectral characteristics of the discrete cosine transform (DCT) coefficients. In each scan, the

[1] A motivation video for this work can be found at: http://youtu.be/XGVXF9Rh3kU.