Securing Digital Image from Malicious Insider Attacks

Rahul Saranjame, Dhirubhai Ambani Institute of Information and Communication Technology, Gandhinagar, India
Manik Lal Das, Dhirubhai Ambani Institute of Information and Communication Technology, Gandhinagar, India

ABSTRACT

Protection of digital images from malicious (and dishonest) insider entities is an important concern in modern digital space. A malicious entity can alter some important features of an image to mislead the target recipient of the image, which can cause harm in applications such as healthcare, insurance, product description and so on. In order to protect digital images, cryptographic primitives such as pseudo-random function and digital signature have been used in practice for image protection. In this article, the authors present a method of image protection from malicious image manipulation. The authors use the concept of secret sharing and public key primitives in the proposed method. This article discusses on attacks involving generation of fake shares to cheat honest user(s) and a demonstration of the proposed system employing a centralized server to generate shares and authenticate them on the basis of requests is made as a counter to the described attack.

KEYWORDS
Data Confidentiality, Image Security, Public Key Cryptography, Random Grids, Visual Cryptography

INTRODUCTION

Modern Information and Communication Technology facilitates easy accessibility of digital contents (Furht, & Kirovski, 2004). While providing flexible content access anywhere and anytime, manipulation of digital image for distorting facts is also found an easy attempt, but detecting and protecting such acts become a challenging problem in scientific community (Muraharirao, & Das, 2012). In order to protect multimedia data, techniques like digital watermarking, scrambling, authentication, integrity or a combination of these could protect digital content from content tampering (Saranjame, & Das, 2017). Many techniques (Walton, 1995), (Yeung, & Mintzer, 1997), (Wong, & Memon, 2001), (Tang, Hwang, & Yang, 2002), (Chang, Hu, & Lu, 2006), (Ahmed, Siyal, & Abbas, 2010) have been proposed for protecting multimedia data, piracy detection, and copyright and ownership control.

Visual Cryptography is an interesting cryptographic art, introduced by Naor and Shamir (Naor, & Shamir, 1995), in which a secret image is divided into n shares (Shamir, 1979) using a codebook which basically prescribed what each pixel in the share would look like according to the pixel in the secret image. However, the system has a major drawback of pixel expansion where each pixel in the secret image is mapped to an $n \times n$ pixel leading to expansion of the shares. Furthermore, the requirement of the codebook is another downside that this technique has. The main advantage of Visual Cryptography as an encryption technique is that it renders any computation for decryption unnecessary (Naor, & Pinkas, 1997). The only computational cost involved is in the encryption phase whereas decryption is simply carried out by the Human Visual System by superimposing the shares. Kafri and Keren (Kafri, & Keren, 2004) proposed the method of encryption using Random

DOI: 10.4018/IJCVIP.2018040103
Grids. This eliminates the two drawbacks of the earlier scheme whilst retaining its computational simplicity. The secret image is broken down into noise like grids called shares that are the same size as the image. This eliminates the need for a codebook and does not require pixel expansion. The decryption process occurs by simple superimposition. A \((2, n)\)-threshold visual cryptography scheme is presented in (De Prisco and De Santis, 2006), in which they address cheating immune schemes without the use of extra information. The authors in (De Prisco and De Santis, 2014) also proposed a scheme using random grid. In Ogata et al.’s scheme (Ogata, Kurosawa and Stinson, 2006), a lower bound on the size of shares is provided for secret sharing that protects against malicious participants forging an honest participant in the scheme. Chen and Tsao (Chen, & Tsao, 2008) further proposed the \((2, n)\) and \((n, n)\) secret sharing scheme based on Random Grids. In \((2, n)\) RG based method, the image is broken down into \(n\) random grids and only on the acquisition of 2 or more shares can it be reconstructed. In \((n, n)\) RG based method, all \(n\) need to be acquired and superimposed to recreate the secret image. They then came up with the novel method of \((k, n)\) secret sharing which is what this paper primarily uses as a basis. The principle remains the same: on getting at least \(k\) out of the \(n\) shares the image can be recovered by simple visual detection but having \(k-1\) or less shares reveals absolutely nothing about the secret image. Guo et al. present a \((k, k)\) extended visual cryptography scheme using random grids (Guo, Liu and Wu, 2014), in which a secret image and \(k\) cover images are encoded into \(k\) share images. One of the major fields where visual cryptography has applications is in medical sciences where patient data confidentiality is of prime importance (Padmavathi, Sharma, Khan, & Krishnareddy, 2015) (Sagar, 2016). Assuming a typical hospital scenario where patient records are stored on a central database and there is need for strict confidentiality, this project makes use of the \((k, n)\) secret sharing technique to achieve the purpose. Each patient may have a number of scans and image records that are supposed to be available only to a certain number of doctors along with the patient. The work in (Yu, Zhang and Fu, 2017) provided an \((n, n)\) extended color visual cryptography scheme using XOR cipher, where a color secret image and \(k\) color cover images are encoded into \(n\) shares.

In this paper, we present a technique of image encryption and authentication using the notion of visual cryptography and public key encryption. For data integrity and authentication, message authentication codes are used, which can achieve the intended goal and provide efficiency in comparison to conventional digital signature-based data authentication. The paper discusses some prominent attacks involving generation of fake shares to cheat honest users and a demonstration of the proposed system employing a centralized server to generate shares and authenticate them on the basis of requests is made as a counter to the described attack.

The remaining of the paper is organized as follows. Section 2 gives a brief insight into the way shares are developed in \((2, n)\) and \((k, n)\) Random Grid (RG)-based share generation and describes why in the considered context of healthcare the need for share generation arises and how it is carried out. Section 3 elucidates in detail the attack that exploits vulnerabilities in the considered \((2, n)\) and \((k, n)\) RG based visual cryptography. The section also discusses the practical problems of such an attack being successful and the damage caused. Section 4 provides a detailed illustration of the proposed technique for preventing the attack and expounds upon the practical applications of the new scheme. Section 5 concludes the paper.

SHARE GENERATION

This section elaborates on the process of share generation in \((2, n)\) and \((k, n)\) Random Grid (RG) based visual cryptography and weaknesses involved in the technique (Shyu, 2007) (Chen, & Tsao, 2011) (Wu, & Sun, 2012) (Lee, & Chen, 2012).
Related Content

Applications of Image Compression on Agricultural Image Data Analysis
[www.igi-global.com/chapter/applications-of-image-compression-on-agricultural-image-data-analysis/224081?camid=4v1a](www.igi-global.com/chapter/applications-of-image-compression-on-agricultural-image-data-analysis/224081?camid=4v1a)

Bio-Inspired Techniques in Rehabilitation Engineering for Control of Assistive Devices
[www.igi-global.com/chapter/bio-inspired-techniques-in-rehabilitation-engineering-for-control-of-assistive-devices/197041?camid=4v1a](www.igi-global.com/chapter/bio-inspired-techniques-in-rehabilitation-engineering-for-control-of-assistive-devices/197041?camid=4v1a)
Significant Enhancement of Object Recognition Efficiency Using Human Cognition based Decision Clustering

A Robust Skeletonization Method for Topological Complex Shapes
[www.igi-global.com/article/a-robust-skeletonization-method-for-topological-complex-shapes/177198?camid=4v1a](www.igi-global.com/article/a-robust-skeletonization-method-for-topological-complex-shapes/177198?camid=4v1a)