Chapter 25
Basic Visual Cryptography Using Braille

Guangyu Wang
Chinese Academy of Sciences, China & Auckland University of Technology, New Zealand

Feng Liu
Chinese Academy of Sciences, China

Wei Qi Yan
Chinese Academy of Sciences, China & Auckland University of Technology, New Zealand

ABSTRACT

As a significant part of information security, Visual Cryptography (VC) is a secret sharing approach which has the advantage of effectively obscuring hints of original secret. In VC, a secret image is separated into partitions which are also known as VC shares. The secret is only able to be revealed by superimposing certain shares. Since Basic VC is in a structure which is similar to that of Braille where white and black dots are arranged in certain orders, it is feasible to utilize the feature of Braille for the authentication of VC. In this paper, the authors will conduct an experiment embedding Braille into grayscale and halftone images as well as VC shares. The result indicates that the embedding of Braille has little impact on VC secret revealing and enhances the security of VC shares.

1. INTRODUCTION

Visual Cryptography (VC) was firstly invented and researched by Naor and Shamir in 1994 to deal with the problem of secret sharing (Wei & Yan, 2012; Shamir, 1979; Yang & Laih, 1999). As equipped with the ability to divide secret image into several images which show no hint of the secret, VC is now playing an important role in information security. The aim of VC is to provide efficient approaches for image secret sharing (Naor & Pinkas, 1997). In VC, encryption and decryption are the two significant processes.

DOI: 10.4018/978-1-7998-1763-5.ch025

The decryption problem in VC is defined as a secret sharing problem. By stacking certain number of the shares together, secret image is revealed visually. VCS result is perceived by Human Visual System (HVS) (Naor & Shamir, 1995; Tuyls, Hollmann, Van Lint & Tolhuizen, 2005; Memon & Wong, 1998). On the contrary, secret remains undiscovered if the amount of given shares is fewer than the required number. Different from original secret image in which the secret can be easily identified, the stacked secret is perceived by using the contrast between the secret and its background.

There are three main types of VC: traditional VC, grayscale and color VC, multi-secret VC. Traditional VC aims at analyzing one secret image which has only black and white color. As two important expansions, while grayscale VC is studied to resolve the images consisting of multiple colors or intensity (Wei & Yan, 2010), multi-secret VC attempts to reveal more than one secret (Wei & Yan, 2010; Shyu et al, 2007).

Despite VC significantly assists secret protection, it appears to be difficult for participants to validate all shares and the secret, thereby given cheaters the opportunity to create unauthorized share. The role of cheater in VC as well as the authentication and successful cheat in VC are defined by Horng, Chen and Tsai (2006). According to their definition, a cheater is someone who releases a fake share that is different from the one (s)he received from the dealer during the process of secret reconstruction. Thus cheating prevention approaches are necessary in association with VC to prevent those cheating practices. There are two authentication methods available for checking shares and secret (Wei & Yan, 2012). The first type is to use an additional share to check the authentication of the revealed secret. This authentication method enables verification of the shares before the process of secret restoration. The other available authentication method is to use a blind authentication technique which aims at preventing the prediction of genuine shares' structure. As the inconvenience of producing and carrying additional shares, the first type of authentication is hard to be implemented. By contrast, using blind authentication methods such as cipher text is widely accepted in researches and applications.

In this paper, we will introduce Braille encoding and explain how it is applied to handle the authentication problem in VC. Our contribution is to use Braille for VC. To the best of our knowledge, this is the first time Braille has been applied to the area of VC. The remaining sections will be: Section 2 will introduce our related work, Section 3 will depict the contributions, our results will be provided in Section 4, discussions and conclusion will be presented in Section 5.

2. RELATED WORK

Even though the security nature of VC, attack approaches have been investigated and proved to be effective. Hu and Tzeng (Hahn & Jung, 2006) explained numerous cheating methods and each of the methods is capable of cheating VC schemes. A vast number of other researchers have also attempted to develop practical applications including one involving biometrics (Hegde et al, 2008; Hu & Tzeng, 2007; Jin, Yan & Kankanhalli, 2004; Lee & Chen, 2012; Tuyls et al, 2005; Weir 7 Yan, 2009; Liu, Wu & Lin, 2008; Horng et al, 2006).

In this paper, we focus on developing a new scheme of VC authentication method by using Braille as the cheating prevention tool. In 1824, a French visually impaired person Louis Blair invented Braille which is designed specifically for the visually impaired person to read by tactile perception (Yin, Wang & Li, 2010). In Braille, the alphabet is written in the form of blocks of the six dots which are also called Braille cells (Goldberg & Swan, 2011). Braille cells are small, flat, rectangular objects of a standard size.