Exploiting the Homomorphic Property of Visual Cryptography

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

ABSTRACT

In this paper, homomorphic visual cryptographic scheme (HVCS) is proposed. The proposed HVCS inherits the good features of traditional VCS, such as, loss-tolerant (e.g., (k, n) threshold) and simply reconstructed method, where simply reconstructed method means that the decryption of the secret image is based on human visual system (HVS) without any cryptographic computation. In addition, the proposed HVCS can support signal processing in the encrypted domain (SPED), e.g., homomorphic operations and authentication, which can protect the user's privacy as well as improve the security in some applications, such as, cloud computing and so on. Both the theoretical analysis and simulation results demonstrate the effectiveness and security of the proposed HVCS.

KEYWORDS

Cloud Computing, Homomorphic Encryption, Homomorphic Visual Cryptography, Signal Processing in the Encrypted domain (SPED), Visual Cryptography

INTRODUCTION

Secret sharing encrypts the user data into different secret shadows (also called shares or shadow images) and distributes them to multiple participants, which has attracted more attention of scientist and engineers. Shamir's polynomial-based scheme (Li, Ma, Su & Yang, 2012; Li, Yang, Wu, Kong & Ma, 2013; Lin et al., 2007; Shamir, 1979; Thien & Lin, 2002; Yang & Ciou, 2010) and visual cryptographic scheme (VCS) (Naor et al., 1994; Tuyls et al., 2005; Wang et al., 2007, Wang, Arce, & Di, 2009, Weir & Yan, 2010; Yan et al., 2014), are the primary branches in secret sharing. A (k,n) threshold secret sharing scheme was first proposed by Shamir (1979) through encrypting the secret into the constant coefficient of a random (k -1)-degree polynomial. The secret image can be perfectly reconstructed using Lagrange's interpolation. Inspired by Shamir's scheme, Thien and Lin (2002) reduced share size 1/k times to the secret image utilizing all coefficients of the polynomial for embedding secret. The advantage of Shamir's polynomial-based schemes (Li, Ma, Su & Yang, 2012; Li, Yang, Wu, Kong & Ma, 2013; Lin et al., 2007; Shamir, 1979; Thien & Lin, 2002; Yang & Ciou, 2010) is that, the secret image can be recovered losslessly. Although Shamir's polynomial-based schemes only need k shares for reconstructing the distortion-less secret image, it requires more complicated computations, i.e., Lagrange interpolations, for decoding. The limitation makes it useless

DOI: 10.4018/IJDCF.2017040105

without computational device and unsuitable for light-weight devices, such as, mobile phone, smart device and so on.

Naor and Shamir [14] first proposed the threshold-based VCS. In their scheme, a secret image is generated into n random shares which separately reveals nothing about the secret other than the secret size. The n shares are then printed onto transparencies and distributed to n associated participants. The secret image can be visually revealed based on human visual system (HVS) and probability by stacking any k or more shares, while less than k shares give no clue about the secret, even if infinite computational power is available.

Unfortunately, traditional VCS has the limitation of the pixel expansion 错误!未找到引用源. The pixel expansion will increase storage and transmission bandwidth. In order to remove the pixel expansion, probabilistic VCSs (Cimato, 2006; Ryo et al., 1999; Yang, 2004) and random grids (RG)-based VCSs (Chen & Tsao, 2013; Guo et al., 2013; Kafri & Keren, 1987; Shyu, 2007; Weir & Yan, 2010; Wu & Sun, 2013) were proposed. Main properties of VCS are simple recovery method and the alternative order of the shadow images. Simply reconstructed method means that the decryption of secret image is light-weighted or completely based on HVS without any cryptographic computation.

On the other hand, recently, rapid technological developments in areas such as cloud computing, online applications, social networking, and distributed processing have raised important concerns about the security (privacy) of user-related content (Lagendijk et al., 2013).

Traditional cryptographic technologies aim to protect data, but fail if the processor itself is untrusted (Lagendijk et al., 2013). In providing a service that needs personal information, the service provider may gain a lot about a user's past behavior, preferences, and biometrics. On the one hand, in order to use the service, the user must trust the service provider requiring his personal data. On the other hand, the service provider may be untrusted. Thus, the use of personal information becomes more varied with more flexibility in presentation and processing.

In particular, biometric techniques (Rao et al., 2008; Revenkar et al., 2010; Ross & Othman, 2011) such as, face recognition/authentication, are increasingly employed to verify the identity of a person with digital photos. Aiming to automatically match the faces of people shown on surveillance images against a database of known suspects, surveillance cameras in public areas led to the high interest in face recognition technologies (Lagendijk et al., 2013). The widespread use of biometrics raises privacy risks if the face recognition process is performed or stored at untrusted or only a central server. The faces might be used in criminal behavior.

To address this issue, signal processing in the encrypted domain (SPED) technologies (Barni, 2012) such as, homomorphic encryption (Bao & Zhou, 2015; Erkin et al., 2007; Li et al., 2012; Naehrig et al., 2011; Smart & Vercauteren, 2014) and authentication, are proposed, whose main motivator is to process the sensitive signals at potentially untrusted sites, minimally or without leaking information.

However, similarly as traditional cryptography, homomorphic encryption and authentication are not loss-tolerant and require more complicated computations for decryption. Homomorphic VCS (HVCS) may be an alternative way to solve the problem, which will be introduced in this paper. In addition, in HVCS, secret images are processed through the shares, i.e., in the encrypted domain, which shows the security of the proposed HVCS compared with traditional VCS.

The main motivation of this paper is to introduce HVCS which exploits the homomorphic property of traditional VC, thus the proposed HVCS achieves the features of both homomorphic encryption and visual secret sharing. The contribution of this paper lies in: 1) HVCS is first introduced; 2) the homomorphic property of traditional VC is exploited; 3) some operations of traditional VCS are proved or validated to support HVC operations. As an example, the proposed schemes exploit traditional RG-based VCS to support HVC operations. The proposed schemes have homomorphic property where the result of a specific signal processing operation performed on the secret image is equivalent to that of the decryption of the same (probably different) signal processing operation performed on the shares. In addition, they allow the authentication to be carried out by utilizing the

BP-Neural Network for Plate Number Recognition

Jia Wang and Wei Qi Yan (2016). *International Journal of Digital Crime and Forensics (pp. 34-45).*

www.igi-global.com/article/bp-neural-network-for-plate-number-recognition/158900?camid=4v1a