International Journal of Digital Crime and Forensics
Volume 10 • Issue 1 • January-March 2018

Secure Steganography in JPEG Images Based on Histogram Modification and Hyper Chaotic System

Shun Zhang, College of Software, Nankai University, Tianjin, China
Liang Yang, College of Software, Nankai University, Tianjin, China
Xihao Xu, College of Software, Nankai University, Tianjin, China
Tiegang Gao, College of Software, Nankai University, Tianjin, China

ABSTRACT

Security always plays an important role in the communication. Steganography, which conceals the process of communication, is another efficient way to achieve secure communication besides encryption. This paper proposes a secure steganography scheme in JPEG images with high embedding capacity and low distortion to the cover image. It embeds the additional information by modifying the DCT coefficients in JPEG images. Considering the size of the additional information, some DCT coefficients are adaptively selected in the embedding process. Two chaotic encryption strategies are designed based on the hyper-chaotic system to encrypt the additional information before the embedding to enhance the security. Extensive experiments have demonstrated the validity and efficiency of this proposed scheme. Compared with some existing schemes, it offers larger embedding rate and lower distortion with stronger security.

KEYWORDS

DCT Coefficients, Hyper-Chaotic Encryption, JPEG Steganography, Secure Communication

1. INTRODUCTION

The security in communication is important. Especially in the modern times, more and more information has been transmitted on the Internet. However, the Internet is insecure due to its original design in the transfer protocols. Therefore, it is of vital importance to guarantee the safety of private and secret information in the Internet Era. Various methods have been proposed ever since ancient times to ensure the secure communication. Encryption and steganography are two of the most important strategies, generally. The encryption strategy makes original information meaningless, which may arouse invaders' attention. Therefore, it is easier detected and even, decrypted. The steganography (Marvel, Boncelet & Retter, 1999) strategy hides the secure information into a cover media, while only the intended receiver is aware of the existence of the hidden information. Therefore, nobody perceives the invisible information, and without the keys, nobody can extract this information. It offers better invisibility and security.

Many steganography schemes in the spatial domain have been proposed in the past decades. However, steganography in the compressed domain seems to have a broader application prospect in the Internet times, because compression offers less space-consumption and more efficiency. JPEG

DOI: 10.4018/IJDCF.2018010104

images are the most frequently used image format on the Internet. Therefore, many data hiding scheme used JPEG images as the cover media (Chang, Chen, & Chung, 2002; Tseng & Chang, 2004; Chang, Lin, Tseng et al., 2007; Li & Wang, 2007; Xuan, Shi, Ni et al., 2007; Qian & Zhang, 2012; Hu, Wang, & Lu, 2013; Wang, Lu, & Hu, 2013; Holub & Fridrich, 2014; Li, Zhang, Lu et al., 2014; Nguyen, Arch-int, & Arch-int, 2014; Xu, Xiong, Xu, et al., 2014; Westfeld, 2001; Fridrich, Goljan, & Du, 2001; Fridrich, Goljan, & Du, 2002). Data hiding in JPEG images, or JPEG steganography, mainly embeds the secure information into the blocked DCT coefficients. There are many ways to realize the hiding process. Schemes evolved from early proposed methods in the spatial domain, such as LSB (Least Significant Bit) substitution (Chang, Chen, & Chung, 2002; Tseng & Chang, 2004; Li & Wang, 2007), usually regard the DCT coefficients as the pixels in the spatial domain. For example, the Jpeg-Jsteg hiding tool embeds the additional information into the LSB (Least Significant Bit) of the quantized DCT coefficients, whose values do not equal to 0, 1, or -1. It is obvious the hiding capacity is rare, because the quantized DCT coefficients satisfying such conditions are rare. After that, Westfeld et al. (2001) developed the F5 algorithm, which improved the embedding efficiency by employing the matrix encoding strategy. An invertible watermarking scheme for authentication of digital JPEG images was proposed by Fridrich et al. (2001), which modified the quantization matrix to enable the reversibility. Besides, Fridrich et al. (2002) provided a lossless compression method to compress the LSB of some selected DCT coefficients to make room for the embedding. Chang et al. (2002) improved the Jpeg-Jsteg method by modifying the standard quantization table. The modified quantization table keeps some middle frequency DCT coefficients of every block in JPEG images. Therefore, it offered higher embedding capacity and better security. Tseng et al. (2004) proposed a capacity table, according to the HVS (Human Visual System) and JPEG quantization table, to estimate the number of bits that can be embedded into each DCT coefficients. Then additional information was adaptively embedded into the LSB of each eligible coefficient. Some optimization was also introduced to improve the performances in JPEG steganography. The PSO (Particle Swarm Optimization) strategy was employed to improve the quality of stego-images in Li & Wang (2007). Similar to Chang et al. (2002), the proposed scheme embedded the additional information into the middle frequency sub-bands of the quantized DCT coefficients. Besides, it also modified the quantized JPEG quantization table, and employed the matrix embedding, which gained larger hiding capacity compared with Chang et al. (2002). All these above-mentioned methods are generally based on the improvements of LSB-based steganography. Some newly proposed schemes modified the histograms of JPEG images in the DCT domain to embed additional information. Chang et al. (2007) proposed a novel steganography by embedding the secure information into the successive zero sequences in the middle frequency quantized DCT coefficients. Some special sub-bands were selected and evaluated to determine the position and capacity of the steganography. The quantization tables were modified sometimes to accommodate the steganography. Xuan et al. (2007) proposed a JPEG steganography based on histogram pairs. The scheme analyzed the optimum threshold and optimum region of the DCT coefficients in JPEG compressed images for the histogram pairs based steganography. Obvious higher hiding capacity was achieved compared with LSB based technology (Chang, Chen, & Chung, 2002; Tseng & Chang, 2004; Li & Wang, 2007). Recently, some schemes embed the additional information into the JPEG bit-streams (Qian & Zhang, 2012; Hu, Wang, & Lu, 2013). In Wang, Lu, & Hu (2013), both the quantization table and the quantized DCT coefficients were modified to embed additional information. Only a fraction of DCT coefficients were selected for the embedding process. Based on an optimized distortion function, Li et al. (2014) designed an adaptive steganography in JPEG images. Nguyen, Arch-int, & Arch-int (2014) modified the matrix encoding scheme to improve the embedding efficiency. Besides, cellular automata were employed to encrypt the additional information before embedding. A content protection scheme combining encryption and digital fingerprint was proposed in the JPEG compressed domain in Xu et al. (2014).

High hiding capacity, low distortion and strong security are three important concerns in designing a secure steganography scheme. Based on the JPEG compression, this paper proposes a high capacity