A Reversible Data Hiding Method for Encrypted Images

W. Puech, M. Chaumont and O. Strauss

LIRMM Laboratory, UMR CNRS 5506, University of Montpellier II
161, rue Ada, 34392 MONTPELLIER CEDEX 05, FRANCE

ABSTRACT

Since several years, the protection of multimedia data is becoming very important. The protection of this multimedia data can be done with encryption or data hiding algorithms. To decrease the transmission time, the data compression is necessary. Since few years, a new problem is trying to combine in a single step, compression, encryption and data hiding. So far, few solutions have been proposed to combine image encryption and compression for example. Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images. In this paper we propose an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step. We have applied our method on various images, and we show and analyze the obtained results.

1. INTRODUCTION

The amount of digital images has increased rapidly on the Internet. Image security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. For example, the necessity of fast and secure diagnosis is vital in the medical world.[1, 2] Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks. To decrease the transmission time, the data compression is necessary. The protection of this multimedia data can be done with encryption or data hiding algorithms. Since few years, a problem is to try to combine compression, encryption and data hiding in a single step. For example, some solutions was proposed in[3] to combine image encryption and compression. Two main groups of technologies have been developed for this purpose. The first one is based on content protection through encryption. There are several methods to encrypt binary images or gray level images.[3–6] In this group, proper decryption of data requires a key. The second group bases the protection on digital watermarking or data hiding, aimed at secretly embedding a message into the data.[7, 8] These two technologies can be used complementary[9, 10] and mutually commutative.[11] Sinha and Singh proposed a technique to encrypt an image for secure image transmission.[12] In their approach the digital signature of the original image is added to the encoded version of the original image. The encoding of the image is done using an appropriate error control code. At the receiver end, after the decryption of the image, the digital signature can be used to verify the authenticity of the image. Encryption and watermarking algorithms rely on the Kerckhoffs principle[13]: all the details of the algorithm are known, and only the key to encrypt and decrypt the data should be secret.

Nowadays, a new challenge consists to embed data in encrypted images. Previous work proposed to embed data in an encrypted image by using an irreversible approach of data hiding.[14] The challenge was to find an encryption method robust to noise. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity,[15, 16] but these methods are not applicable on encrypted images. In this paper we propose an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step.

william.puech@lirmm.fr, marc.chaumont@lirmm.fr, olivier.strauss@lirmm.fr

Security, Forensics, Steganography, and Watermarking of Multimedia Contents X
edited by Edward J. Delp III, Ping Wah Wong, Jana Dittmann, Nasir D. Memon
Proc. of SPIE-IS&T Electronic Imaging, SPIE Vol. 6819, 68191E, © 2008 SPIE-IS&T · 0277-786X/08/$18