Rewritable Data Insertion in Encrypted JPEG using Coefficient Prediction Method

KuanYew Tan∗, KokSheik Wong†, Simying Ong‡ and Kiyoshi Tanaka§
∗ University of Malaya, Kuala Lumpur, Malaysia
E-mail: daryltan0202@siswa.un.edu.my
† Monash University Malaysia, Selangor, Malaysia
E-mail: wong.koksheik@monash.edu
‡ Tunku Abdul Rahman University College, Kuala Lumpur, Malaysia
E-mail: ongsy@acr.tarc.edu.my
§ Shinshu University, Nagano, Japan
E-mail: ktanaka@shinshu-u.ac.jp

Abstract—This paper proposes a data insertion method using DCT coefficient prediction algorithm in encrypted JPEG image. First, a sequence of quantized AC coefficients are removed, and the remaining nonzero coefficients are shifted to the left, hence ensuring sufficient room for data insertion. Next, the external data is mapped to a set of Huffman codewords, and the external data is inserted into the image by introducing the corresponding Huffman codewords. At the receiver’s side, the hidden data can be extracted by referring to the pre-defined table without the need to decrypt the image. To restore the image, the decrypted JPEG image is segmented using the Superpixel function, and further processed using the prediction algorithm for recovering the removed AC coefficients. Experimental results show the recovered images resemble their original counterparts. In the best case scenario, up to 19% compression gain is achieved while 24,576 bits of external data can be inserted into the image.

I. INTRODUCTION

The unification of data insertion and encryption has received much attention in recent years thanks to its application value. For example, user prefer to mask the perceptual meaning of their personal contents before storing them online (e.g., cloud storage) for ubiquitous access, while administrator may insert some tag or control data to better manage these contents. In another application, content provider prefers to transmit the paid content to the rightful viewer, while ensuring some form of identification information (e.g., watermark, fingerprint) remains intact even after dejections [1].

Among multimedia contents, image is the mostly communicated one. According to Zephoria Digital Marketing [2], there are 300 millions images posted online per day in Facebook itself. Therefore, there are many joint data insertion and encryption methods specifically designed to handle image. There are at least two ways to achieve a joint method. For example, in sequential approach, an image with hidden data can be encrypted, and vice versa. On the other hand, the content can be separated into two parts, where one is reserved for data insertion, and another for encryption. Other approaches include independent operations [3] where the outcome is exactly the same regardless of the order of operations (i.e., commutative), and combined method where the data insertion and encryption operations cannot be separated [4].

Specifically, Lian et al.’s method [1] encrypts a H.264/AVC video by randomizing the sign of the DCT coefficients and the motion vectors, and inserts data by modulating the magnitude of the DCT (discrete cosine transformation) coefficients. On the other hand, Zhang proposed to encrypt an image, block-by-block, by randomizing the five most significant bit-planes to mask the image, while the remaining 3 bit-planes are further divided into two sub-groups, where the uniformity in these bit-planes are exploited for data insertion purpose. Later on, Rad et al. [5] put forward a joint method by predicting 75% of the pixels of an image, where the prediction errors are first manipulated (to control the quality of recovered image) then stored as side information into the image. Encryption is achieved by replacing the predicted pixel by the actual data to be hidden. Recently, Ong et al. [6] encrypt a JPEG (Joint Picture Expert Group) image by shuffling the coefficients, and the cardinality (of coefficient) of each block is manipulated to encode data.

In this work, a data insertion method is proposed to complement our previous work in JPEG encryption [7] for achieving a joint data insertion-encryption method. JPEG is considered because it is the mostly deployed compression standard despite the introduction of more efficient compression standards such as JPEG2000 and JPEG-XR. Specifically, selected DCT coefficients are removed, and the available room is utilized to host external data. Here, the data is pre-processed by dividing the binary sequence into segments, and each segment is mapped to a Huffman code for data insertion purpose. For image recovery, the processed image (i.e., with hidden data and encrypted) is decrypted, and the removed coefficients are predicted using our previous work [8], where some minor modifications are introduced. The proposed joint method has the following property: (a) rewritable, where the hide-recover cycle does lead to any quality degradation from the 2nd cycle onwards; and; (b) commutative, where the output is exactly the same regardless of the order of operations, i.e., encrypt-first-then-insert-data yields the same output as insert-data-first-then-encrypt.