Abstract—Although ScaScraIH [1] is able to scalably scramble image/video and offer scalable carrier capacity for reversible data embedding [2], the product of ScaScraIH suffers from bitstream size increment of $\sim 9.17\%$ on average. The main cause of bitstream size increment in ScaScraIH is storing the number of nonzero coefficients in each $8 \times 8$ block which is utilized during the descrambling process. This paper proposes two techniques in suppressing bitstream size increment for ScaScraIH. The first technique exploits the distribution of nonzero DCT coefficients in the image to construct a scanning order, aiming to shorten the distance between nonzero coefficients in a block. For the second technique, combination of predictive and entropy coding is used to encode the number of nonzero coefficients. Experiments are conducted by using standard test images to verify the effectiveness of both techniques in suppressing bitstream size increment. On average, bitstream size increment is significantly suppressed to $\sim 0.91\%$, with some of the processed images assuming smaller bitstream size than its original counterpart.

I. INTRODUCTION

Encryption and external information insertion are the two main disciplines in information hiding [3]. Encryption is the translation of plaintext message into unintelligible ciphertext [4]. It plays very important roles, ranging from encrypting our daily password to encrypting highly confidential data such as military image, copyrighted multimedia content, medical image, etc. However, it requires high complexity when multimedia content such as image, video and audio are treated and encrypted in the bitstream level [5]. Thus, partial encryption is applied in most of the information hiding schemes to ensure format compliance as well as to preserve bitstream size.

Some representative partial encryption schemes for DCT compressed image/video include modification on intra prediction mode [6], intra-block shuffle and sign flipping. However, these partial encryption (hereinafter scrambling) schemes suffer from leakage of information of the original content. For example, Li et. al [7] proposed NZCA (nonzero counting attack) that generates a rough sketch of the original image without prior knowledge on the scrambling algorithm used. To counter NZCA, FLBS (Full Inter-Block Shuffle) [7] is proposed to scramble all the AC coefficients from the same subband for destroying the information on the number of nonzero coefficients in a block. However, when the AC coefficients are scrambled within the respective subbands (as in FLBS), correlations exploited by the zigzag ordering is completely destructed. This causes a significant increase in the bitstream size, which is a classical problem in existing scrambling schemes in the compressed domain [4].

External information insertion methods embed additional information such as metadata, fingerprint [4], watermark [8], etc. into a host content for various purposes, including quick content retrieval, legal distribution of copyrighted content, claim of ownership, etc. Recently, reversible information hiding (some authors use the terms lossless, restorable, invertible, etc.) has received much attention because of its attractive feature that can perfectly restore the original content after extraction of payload. This is particularly useful in applications where any form of permanent distortion in the content is not permitted.

In recent years, some joint techniques of scrambling and external information insertion are proposed. Zhang proposed an information hiding method in encrypted images where the inserted information can be extracted without decrypting the encrypted image, and vice versa [9]. Joint work is also proposed for broadcasting paid video content [4]. Specifically, a video is scrambled prior to transmission and a unique fingerprint of the buyer is inserted into the decoded video prior to actual display. Both techniques proposed in [4] and [9] are not reversible. The joint work in ScaScraIH [1] addressed this issue to completely restore the original content and offer scalable carrier capacity [2]. However, it suffers from bitstream size increment.

In this work, two techniques are proposed to suppress bitstream size increment in ScaScraIH [1], [2]. The first technique exploits the distribution of nonzero DCT coefficients in the image to construct a scanning order, aiming to shorten the distance between nonzero coefficients in a block. The second technique combines predictive and entropy coding to encode the number of nonzero coefficients. Experiments are then conducted by using standard test images to verify the effectiveness of both techniques in suppressing bitstream size increment.

II. REVIEW OF SCA SCRAIH [1], [2]

Let $G(x,y)$ be the $(x,y)$-th DCT coefficient block in a JPEG image $G$, and let $G_{ij}(x,y)$ be the $(i,j)$-th coefficient in $G(x,y)$ where $1 \leq i,j \leq 8$. Here, $1 \leq x \leq M$ and $1 \leq y \leq N$ where $M \times N$ is the dimension of $G$. The