Binary Code Optimized for Partial Encryption

Mehrshad Kafi and Sorina Dumitrescu, *Senior Member, IEEE*

Abstract

A common technique for the partial encryption of compressed images and videos encrypts only the sign bits of some syntax elements such as the quantized transform coefficients or the motion vector differences. The sign bit can be interpreted as the most significant bit (MSB) in the binary representation of the syntax element. Our work is motivated by the key observation that the binary code used for this representation has an impact on the quality of the reconstruction at the eavesdropper and on the size of the stream to be encrypted. Therefore, we address the problem of optimal binary code design for partial encryption. Ideally, the goal is to simultaneously maximize the eavesdropper's distortion and minimize the length of the compressed MSB stream. Since these two objectives are conflicting in general, we formulate the problem as the maximization of a weighted sum of the eavesdropper's distortion and of the probability of the MSB being 0. We cast the problem as a binary integer linear program equivalent to a weighted non-bipartite graph matching problem, which has a polynomial-time solution algorithm. We show that, when the source to be quantized and the quantizer are symmetric, the problem can be converted to a linear program of smaller size, for a family of distortion metrics. Extensive experiments assess the performance of the optimized binary code in comparison with existing approaches. The results reveal that certain existing partial encryption schemes could benefit from the proposed design.

Index Terms

Partial/selective encryption, binary code, weighted graph matching, linear programming.

I. Introduction

Every day, a huge amount of multimedia data are transmitted over the Internet or wireless networks. The Compression of these data is necessary in order to meet bandwidth limitations. In addition, ensuring privacy and protection against illegal use or unauthorized access is a major concern. The traditional approach for reaching both compression and security first encodes the data by a standard compression algorithm and then encrypts the whole compressed stream using a standard encryption algorithm. This approach provides the highest level of security, which is necessary for certain applications, such as military applications. Nevertheless, the encryption and decryption operations are computationally intensive. Therefore, using full encryption (FE),

The authors are with the Department of Electrical and Computer Engineering, McMaster University, Hamilton, Canada (Emails:kafim1@mcmaster.ca; sorina@mail.ece.mcmaster.ca).

i.e., encryption of the whole data stream, increases the power consumption and delay at both the transmitter and receiver. Thus, FE cannot be supported by applications involving real-time communication of large amounts of data and involving end users with limited computational resources, such as wireless sensors or hand-held devices. Partial encryption (PE), also called selective, soft, or perceptual encryption [1]–[3], has emerged as a means of reducing the computational cost of encryption. The general idea is to cipher only a smaller portion of the data stream. The reduction in complexity is typically achieved at the expense of some loss in terms of security. However, complete security (i.e., where no information about the data is leaked) is not always required. In certain applications, ensuring only some degree of content security is sufficient (for instance, hiding the details in an image, while the shapes or the general structure are still recognizable). In addition, some applications require only a sufficient degradation of the content at the eavesdropper's side in order to make the content not consumable, i.e., to prevent an enjoyable experience [3].

Extensive efforts have been devoted to the PE of compressed images. A PE method for SPIHT images was designed by encrypting the significance information related to pixels or sets in the two highest pyramid levels [1]. For JPEG 2000, one approach for PE uses randomized arithmetic coding [4]. Another approach for the PE of JPEG 2000 images is to encrypt the most significant layer of low resolutions bands for hard visual degradation [2]. For JPEG images, PE methods that include the encryption of higher order bitplanes of the discrete cosine transform (DCT) coefficients as a part of the algorithm were proposed [5], [6].

Video data has been subjected to PE too, due to its size, real-time applications, the necessity of format-compliance, and multi-user different quality demands. A widespread strategy is the encryption of the sign bits of key syntax elements such as the quantized transform coefficients (QTC) and/or the motion vector differences (MVD). This strategy was used for the PE of MPEG-compressed video [7]–[10], for the H.264/AVC standard [12]–[16] and for HEVC-compressed video [17]–[19]. More recently, the encryption of the prediction modes for intra blocks for H.264/AVC and intra units for HEVC was considered too [18].

Besides the PE of compressed images and videos, recent years have witnessed a growing interest in the development of PE techniques for uncompressed images [21]–[25]. In the aforementioned works, the encryption is applied only to the higher order bitplanes and the focus is on designing the encryption algorithms based on chaotic systems and DNA computing.

II. Our Contribution

This work is motivated by the observation that many PE approaches proposed to date for compressed images and videos use the encryption of the sign bits of some syntax elements (such as QTCs or MVDs) alone or in combination with other techniques. Our key insight is that the way of assigning binary codewords to these syntax elements must influence the performance of the PE method. Prior work on the PE of compressed images and videos based on sign bit encryption uses the assignment of binary codewords to the syntax elements that is specified by the respective compression algorithm or standard.

In this work, we consider the possibility of going beyond the conventional approach and applying a different binary code to represent these syntax elements. In order not to change the compression performance, the new binary codewords should have the same length as those specified by the compression algorithm or standard. Since the purpose of PE is to degrade the reconstruction at the eavesdropper's side, we are interested in designing a binary code such that this degradation is maximized. Another goal of PE is to decrease the amount of the encrypted portion. This is already partly achieved by selecting only a portion of the whole data stream for encryption. However, in situations where the portion chosen for encryption is further compressed before being encrypted, the binary code could also affect the length of this compressed bitstream. In such a situation it might be of interest to further decrease the length of the bitstream to be encrypted (for low encryption complexity) while maintaining a high enough degradation at the eavesdropper (i.e., high secrecy). For simplicity, we will refer to the eavesdropper as Eve, while Alice is the sender, and Bob is the legitimate receiver, as is common practice in the literature on information security.

In order to investigate this problem, we consider a general framework where a signal is first applied a scalar quantizer. Each quantized level is converted into a binary codeword consisting of b bits, where b is a fixed integer. Let N be the number of signal samples. Thus, at the end of the process, a sequence of N binary codewords is obtained, which are concatenated to produce a codestream. We consider two scenarios, A and B. In scenario A, Alice encrypts the most significant bits (MSB) of all codewords, while the remaining portions are not encrypted. Then Alice sends the resulted bitstream to Bob. To perform the encryption, the MSBs are concatenated and this stream is applied a strong enough cipher, for instance by utilizing a standard encryption algorithm such as AES. We will assume that the cyphertext contains the same number of bits

as the input sequence of MSBs. After that the MSB of each codeword is replaced by the corresponding bit in the cyphertext.

In scenario B, the MSB is separated from the rest of the codeword. The sequence of MSBs is further compressed using an entropy coder and the resulted bitstream is further encrypted. The sequence of remaining $(b-1)$-bit portions of the codewords is further compressed, but not encrypted. Alice appends the resulted codestream after the cyphertext and transmits it to Bob.

Note that scenario A is encountered in the PE of JPEG-compressed images where the sign bits of the non-zero quantized AC coefficients are encrypted. The non-zero values are divided into categories and the values within each category are represented by a fixed length binary code (i.e., where all codewords have the same number of bits). The MSB of each codeword represents the sign bit. Thus, for each category, the PE process falls under scenario A. Another case is the encryption of the sign bits of the MVDs in video streams compressed with H.264/AVC. In the baseline profile, the non-zero MVDs are divided into the same categories as for JPEG and the MVDs within each category are coded using a fixed-length binary code. By considering the sign bit as the MSB, this process also falls under scenario A. In addition, wavelet-based compression algorithms tend to use bitplane coding. A potential PE method is to encrypt the MSB plane after it is entropy-coded. Such an approach falls under scenario B.

We will assume that Eve is not able to break the encryption, but she is able to obtain a degraded reconstruction of the signal and will measure the secrecy of the scheme by the distortion achieved at Eve's side. Thus, in scenario A, we are interested in designing a binary code that maximizes the distortion at Eve's. In scenario B, we will use the entropy of the random variable S_0 that represents the MSB as a measure of the complexity of the encryption. This is accurate when the input signal samples are are i.i.d. (identically and independently distributed) and entropy coding is used to compress the MSB plane. We address the problem of designing the binary code such that to maximize the secrecy, while keeping the encryption complexity as low as possible. These two objectives are generally conflicting requirements, thus we will resort to maximizing a utility function which accounts for both objectives, namely the weighted sum of the distortion at Eve's side and the probability of the MSB being 0.

We show that for both scenarios the optimization problem can be cast as a weighted non-bipartite graph matching problem, which is known to have a solution algorithm that runs in $O(M^3)$ time, where M is the total number of quantizer bins. We additionally prove that, when the source probability density function (pdf) and the quantizer are symmetric, the problem can

be formulated as a linear program of smaller size for a class of distortion measures that includes the squared error distortion. The latter formulation allows for more efficient and for a larger variety of solution algorithms to be used.

Next, we proceed to assess the practical performance of the optimized binary codes in comparison with the binary codes commonly used, namely the natural binary code (NBC) and the folded binary code (FBC). This comparison can also be regarded as assessing how effective the conventional codes are relative to the optimum in ensuring secrecy and lowering the encryption complexity. To this end, we perform experiments on three sources, namely a Gaussian source, a Laplacian source, and a Gaussian mixture. The first two sources are chosen since they both have been used to model the distribution of transform coefficients and of prediction residuals. We also consider real DCT coefficients obtained from the Lena image. Our results indicate that existing PE methods based on sign bit encryption could benefit from the optimization of the binary code.

Although the proposed design is for the scenario when the data stream is compressed before encryption, the concept can also be applied to the PE of uncompressed images. Here the binary code is applied to obtain a binary representation of each pixel value. The main difference in terms of problem modeling resides in the fact that in the former case the input samples are i.i.d., while in the latter case they are correlated. We consider an adaptation of the proposed technique to account for the correlation between adjacent pixels and present experimental results on several images. The PE method applied consists of 1) encrypting the first MSB plane and 2) encrypting the first two MBS planes. We show that higher visual secrecy can be obtained in comparison with the conventional approach.

Finally, we would like to mention that our conference paper [26] is a shorter version of this work, which does not include the linear programming formulation of the problem for the symmetric case. Moreover, the current work includes a more extensive experimental analysis.

The rest of the paper is organized into six sections. The following section introduces the definitions, notations, and the problem set-up. Section IV formulates the problem of optimizing the binary code for PE and shows that it is equivalent to a weighted non-bipartite graph matching program. Section V demonstrates that the problem can be equivalently cast as linear program in the case of a symmetric source with the symmetric quantizer. In sections VI and VII, extensive experimental results for several i.i.d. sources, respectively for uncompressed images, are presented and discussed. Finally, section VIII concludes the paper.

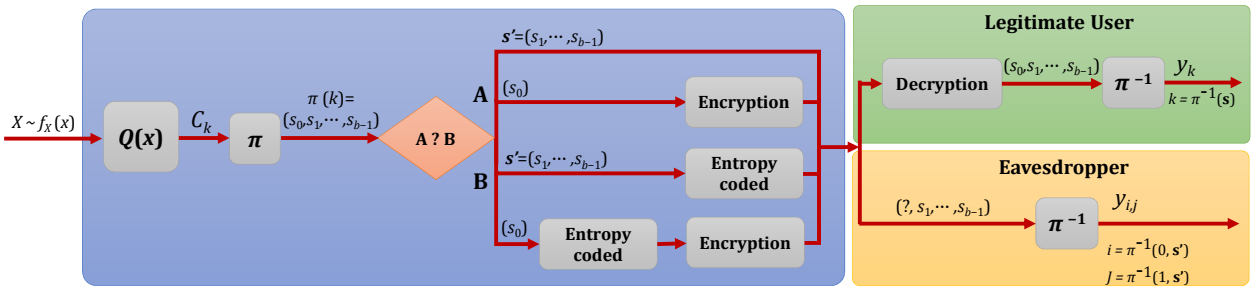


Fig. 1: Block diagram of the proposed scheme.

III. Preliminaries

Let X denote the random variable (RV) representing the values to be quantized, with continuous pdf $f(x)$, $x \in \mathbf{R}$, mean μ and finite variance σ^2. The scalar quantizer Q is specified by the encoder partition thresholds $b_1 < b_2 < \cdots < b_{M-1}$, and by the reconstruction values $y_0, \cdots, y_{M-1}$, where $M = 2^b$, for some positive integer b. The quantizer cells are denoted $C_0, C_1, \cdots, C_{M-1}$, with $C_k = (b_k, b_{k+1}]$, for $0 \leq k \leq M-2$, and $C_{M-1} = (b_{M-1}, b_M)$, where $b_0 = -\infty$ and $b_M = \infty$. For $0 \leq k \leq M-1$, let $P(C_k) = \int_{C_k} f(x)\, dx$. As illustrated in Figure 1, the encoding proceeds as follows. For each input sample x, the quantizer determines the cell C_k such that $x \in C_k$. Next the binary code $\pi : \{0, \cdots, M-1\} \rightarrow \{0,1\}^b$ assigns to the integer k a b-bit binary index $\pi(k)$. Let $\pi(k) = (s_0, s_1, \cdots, s_{b-1})$, where s_0 denotes the MSB. Next, in scenario A, the MSBs of all output binary codewords are encrypted, while the remaining $(b-1)$-bit portions are left unchanged. The resulted bitstream is sent to the destination. In scenario B, the MSBs s_0 and the remaining $(b-1)$-bit index $(s_1, \cdots, s_{b-1})$ are losslessly encoded separately. Specifically, the sequence of MSBs is encoded using an entropy coder, thus achieving a rate close to the entropy of S_0, denoted by $H(S_0)$. This bitstream is further encrypted. The remaining $(b-1)$-bit indexes are also encoded using some encoding mechanism. The encrypted and the unencrypted portions are concatenated and transmitted to the destination.

The legitimate receiver, Bob, is able to decrypt the cypher and therefore can recover the transmitted b-bit index $\mathbf{s}$. Then he applies the inverse mapping π^{-1} to find the label $\pi^{-1}(\mathbf{s})$ of the quantizer cell the original sample belongs to, and uses $y_{\pi^{-1}(\mathbf{s})}$ as reconstruction.

The eavesdropper, Eve, intercepts the communication between Alice and Bob, but she is not able to decipher the encrypted portion. Thus, she is able to recover only the least significant $(b-1)$-bit portion $\mathbf{s}' = (s_1, \cdots, s_{b-1})$ of each encoded index, but not the MSB s_0. Eve knows the

binary code π since this information is not encrypted. As there are only two possibilities for the value of s_0, she concludes that the transmitted index is either $i = \pi^{-1}((0, \mathbf{s}'))$ or $j = \pi^{-1}((1, \mathbf{s}'))$, i.e., the original coefficient belongs to $C_i \cup C_j$. Based on her knowledge about the source statistics and the quantizer, Eve can select different strategies to decode the received bits. The strategies we consider in this work are listed below.

Strategy 1: When Eve knows the quantizer partition and the source pdf ($f(x)$) she can use as reconstruction the value which minimizes the distortion, i.e.,

$$y_{i,j}^{(1)} = \arg\min_{y \in \mathbb{R}} \int_{C_i \cup C_j} d(x, y) f(x)\ dx, \tag{1}$$

where $d : \mathbb{R} \times \mathbb{R} \to [0, \infty)$ denotes the distortion function, chosen such that the integral in (1) exists. Note that when $d(x, y) = (x - y)^2$, the integral exists since σ^2 is finite.

Strategy 2: If Eve does not know the source pdf, but she knows the reconstruction values y_i and y_j, a reasonable strategy is to use as reconstruction their average, i.e.,

$$y_{i,j}^{(2)} = \frac{y_i + y_j}{2}. \tag{2}$$

Strategy 3: There is also the possibility that Eve is not aware that encryption took place. In this case, she just assumes that the recovered b-bit index is correct and uses the reconstruction of the corresponding quantizer cell.

Let us evaluate now the distortion that Eve achieves. We will denote it by $D_E^{(l)}$, where $l = 1, 2, 3$, indicates the decoding strategy which she uses. Then the following holds, for $l = 1, 2, 3$,

$$D_E^{(l)} = \sum_{\mathbf{s}' \in \{0,1\}^{b-1}} D_{\pi^{-1}((0,\mathbf{s}')), \pi^{-1}((1,\mathbf{s}'))}, \tag{3}$$

where, for any pair (i, j), $0 \leq i < j \leq M - 1$, $D_{i,j}^{(l)}$ is defined as follows

$$D_{i,j}^{(l)} = \int_{C_i \cup C_j} d(x, y_{i,j}^{(l)}) f(x)\ dx, \text{ for } l = 1, 2, \tag{4}$$

$$D_{i,j}^{(3)} = 0.5 \int_{C_i \cup C_j} d(x, y_i) f(x)\ dx + 0.5 \int_{C_i \cup C_j} d(x, y_j) f(x)\ dx. \tag{5}$$

It should be noted that equation (5) holds under the assumption that the encryption randomly flips 0s and 1s with probability 0.5.

Finally, another strategy that Eve can use is the so-called replacement or error-concealment attack. Namely, Eve is aware that encryption of the MSBs took place, and to decode the codestream she either replaces all MSBs with 0 or replaces all MSBs with 1. The arithmetic

average of the distortions achieved for the two reconstructions equals $D_E^{(3)}$. Therefore, we will also use $D_E^{(3)}$ as a measure of secrecy for this decoding strategy.

By analyzing the distortion formulas for strategies 2 and 3 when $d(x,y)=(x-y)^2$ we find that they are closely related. More specifically, it can be shown that for any pair i,j

$$\begin{aligned} D_{i,j}^{(2)} =&(y_j-y_i)\left(\int_{C_j}(x-y_j)f(x)\ dx-\int_{C_i}(x-y_i)f(x)\ dx\right)\\ &+\int_{C_i}(x-y_i)^2f(x)\ dx+\int_{C_j}(x-y_j)^2f(x)\ dx+1/4(y_j-y_i)^2(P(C_i)+P(C_j)), \end{aligned}$$

$$D_{i,j}^{(3)}=D_{i,j}^{(2)}+1/4(y_j-y_i)^2(P(C_i)+P(C_j)).$$

When $|y_j-y_i|$ is large enough, the dominant term in $D_{i,j}^{(2)}$ is the last term, thus, $D_{i,j}^{(2)}\approx 1/4(y_j-y_i)^2(P(C_i)+P(C_j))$. This observation further implies that if $|y_j-y_i|$ is for all connected pairs then $D_E^{(3)}\approx 2D_E^{(2)}$. We conclude that the difference in terms of secrecy between two binary codes under strategies 2 and 3 is similar. For this reason, in the sequel, we will focus our attention on strategies 1 and 3 only.

The definitions in this section can be extended in a straightforward manner to the case of finite-alphabet sources. A particular case is when each cell consists of only one element, i.e., $C_k=\{y_k\}$. We will say that the *trivial* quantizer is applied. In this situation, we have for each pair i,j

$$D_{i,j}^{(3)}=1/2(y_j-y_i)^2(P(C_i)+P(C_j)). \tag{6}$$

We will say that two quantizer cells C_i and C_j, $0\le i<j\le M-1$, are *connected* by the binary code π (alternatively, we say that integers i and j are connected by the binary code) if their b-bit binary representations $\pi(i)$ and $\pi(j)$ differ only in the MSB. Thus, the binary code π connects each cell with exactly one other cell. An important observation made by analyzing the definition (3) is that the distortion at Eve's side only depends on the way the cells are connected. Thus, all binary codes which result in the same connections lead to the same value of $D_E^{(l)}$.

The example in Figure 2 illustrates what a high difference the binary code can make in terms of Eve's distortion. Here, strategy 1 is assumed, which is the worst case in terms of security since it leads to the best reconstruction at Eve's side (i.e., the reconstruction which minimizes the distortion). A Gaussian source with $\mu=0$ and $\sigma^2=1$ is used. The squared error is the distortion measure. The quantizer is the optimal 4-level uniform quantizer for the aforementioned source.

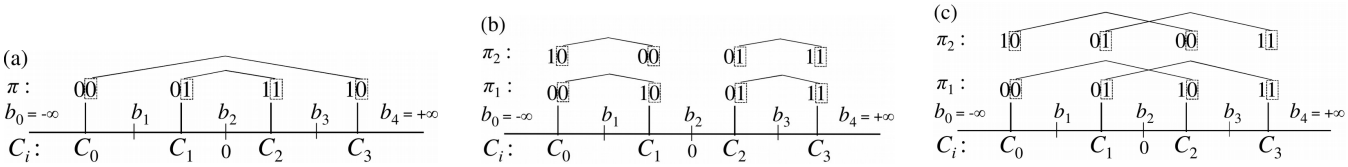


Fig. 2: Different binary codes for a 4-level quantizer.

The distortion incurred at Eve's in case (a) equals the variance of the source, thus it is as worse as if no information where available. This is the highest distortion achieved with an optimized decoder. On the other hand, in case (b) $D_E^{(1)}$ is much smaller (0.3634), while in case (c) $D_E^{(1)}$ is only slightly lower than the maximum (0.9697).

As pointed out earlier, all binary codes that generate the same set of connected pairs of quantizer cells lead to the same $D_E^{(l)}$. The way the MSB is assigned to the two cells in each pair affects the entropy $H(S_0)$. In scenario B, we are interested in reducing $H(S_0)$. Therefore, we will assign the MSB 0 to the cell with the higher probability. In this way, we obtain a binary code that maximizes $P_0 = \mathbb{P}(S_0 = 0)$ (hence minimizes $H(S_0)$) among all binary codes with the same set of connected pairs. We will say that such a binary code is an *entropy-optimized* binary code and we will understand that it is entropy-optimized for the given set of connected pairs. Let us analyze the binary codes in Figure 2 from the point of view of P_0 and $H(S_0)$.

For the 4-level quantizer in Figure 2, $P(C_0) = P(C_3) \approx 0.16$ and $P(C_1) = P(C_2) \approx 0.34$. In case (a) π is entropy-optimized for the given set of connected pairs and has $P_0 = 0.5$, hence $H(S_0) = 1$. In cases (b) and (c), π_1 and π_2 have the same set of connected pairs but only π_2 is entropy-optimized achieving $P_0 = 0.68$ and $H(S_0) = 0.9037$, while for π_1, $H(S_0) = 1$.

IV. Problem Formulation

In this section, we formulate the problem of optimal binary code design for PE and show that it is equivalent to a weighted non-bipartite graph matching problem.

In scenario A the goal is to maximize the security by maximizing the distortion at Eve's side. In scenario B, we are also interested in reducing the entropy of the MSB as much as possible. As the example in Figure 2(a) illustrates, these two objectives are conflicting in general. Therefore, we need to settle for a trade-off between them. Such a trade-off can be achieved by choosing as an objective function to be maximized a weighted sum of $D_E^{(l)}$ and P_0.

Consequently, we formulate the problem of designing the binary code optimized for PE as

$$\max_{\pi} \; D_E^{(l)} + \lambda P_0, \tag{7}$$

where $\lambda = 0$ in scenario A, while $\lambda \geq 0$ in scenario B.

Next, we show that problem (7) can be formulated as a binary integer linear program. To this end, notice first that when $\lambda > 0$ the solution to the problem (7) has to be an entropy-optimized binary code for the given set of connected cells. For such a binary code, the value of the objective function depends only on the set of pairs of connected cells. Thus, problem (7) can be recast as the optimization of the set of connected pairs. Let us consider, for each pair (i, j), $0 \leq i < j \leq M-1$, a binary variable $x_{i,j}$, which equals 1 if the pair (C_i, C_j) is connected by π, and equals 0 otherwise. Then the distortion $D_E^{(l)}$ can be written as

$$D_E^{(l)} = \sum_{i=0}^{M-2} \sum_{j=i+1}^{M-1} D_{i,j}^{(l)} x_{i,j}. \tag{8}$$

In addition, for an entropy-optimized binary code, if C_i and C_j are connected, then the cell assigned the MSB 0 must be the one with higher probability. Thus, $P_0 = \sum_{i=0}^{M-2} \sum_{j=i+1}^{M-1} P_{0,i,j} x_{i,j}$, where $P_{0,i,j} = \max(P(C_i), P(C_j))$. Consequently, the objective function in (7) becomes

$$D_E^{(l)} + \lambda P_0 = \sum_{i=0}^{M-2} \sum_{j=i+1}^{M-1} D_{i,j}^{(l)} x_{i,j} + \lambda \sum_{i=0}^{M-2} \sum_{j=i+1}^{M-1} P_{0,i,j} x_{i,j} = \sum_{i=0}^{M-2} \sum_{j=i+1}^{M-1} w_{i,j}^{(l)} x_{i,j}, \tag{9}$$

where $w_{i,j}^{(l)} = D_{i,j}^{(l)} + \lambda P_{0,i,j}$, for $l = 1, 2, 3$.

Further, for each cell C_i, the constraint that it occurs in exactly one connected pair is equivalent to the constraint that all $x_{i,j}, i < j \leq M-1$, and all $x_{k,i}, 0 \leq k < i$, equal 0, except for one of them, which equals 1. Given that the variables are binary, the aforementioned condition is equivalent to the equality $\sum_{j=i+1}^{M-1} x_{i,j} + \sum_{k=0}^{i-1} x_{k,i} = 1$. Consequently, problem (7) can be formulated as the following binary integer linear program,

$$\begin{aligned} \max_{(x_{i,j})_{i,j}} \quad & \textstyle\sum_{i=0}^{M-2} \sum_{j=i+1}^{M-1} w_{i,j}^{(l)} x_{i,j} \\ \text{subject to} \quad & x_{i,j} \in \{0,1\}, \; 0 \leq i < j \leq M-1 \\ & \textstyle\sum_{j=i+1}^{M-1} x_{i,j} + \sum_{k=0}^{i-1} x_{k,i} = 1, \; 0 \leq i \leq M-1. \end{aligned} \tag{10}$$

The above problem is a weighted non-bipartite graph matching problem and can be solved in $O(M^3)$ time [29].

V. Linear Programming Formulation for Symmetric Source and Quantizer

In this section, we consider the case of a symmetric source with a symmetric quantizer and show that, for certain distortion measures, problem (10) can be formulated as a linear program (LP) of approximately half the size. Specifically, we will show that the above claim holds for $l = 1, 3$, when $d(x, y) = \rho(|x - y|)$, for any nondecreasing function ρ, while for $l = 2$, it holds when $d(x, y) = (x - y)^2$ and some additional conditions are satisfied.

The idea is to show that the optimal binary code has connections only from the left side to the right side. Then we can formulate the problem with this constraint from the start, which is a weighted bipartite graph matching problem. It is known that the LP relaxation of the latter problem necessarily has an integer solution (to be exact, any basic feasible solution has integer components) [29], leading to the conclusion that problem (7) can be cast as an LP.

Let $\mathcal{I} = \{0, 1, \cdots, M/2 - 1\}$ and $\bar{\mathcal{I}} = \{M/2, \cdots, M - 1\}$. Consider now the problem formulation where connections are allowed only from the left side to the right side (i.e., $i \in \mathcal{I}, j \in \bar{\mathcal{I}}$). To this end, for each pair (i, j) with $i \in \mathcal{I}$, $j \in \bar{\mathcal{I}}$, let $z_{i,j}$ be a binary variable which takes the value 1 if the pair (C_i, C_j) is connected by π and takes the value 0 otherwise. In this case, the problem can be formulated as follows

$$\begin{aligned} \max_{(z_{i,j})_{i\in\mathcal{I},j\in\bar{\mathcal{I}}}} \quad & \sum_{i\in\mathcal{I}}\sum_{j\in\bar{\mathcal{I}}} w_{i,j}^{(l)} z_{i,j} \\ \text{subject to} \quad & z_{i,j} \in \{0,1\},\ i \in \mathcal{I}, j \in \bar{\mathcal{I}},\ \sum_{j\in\bar{\mathcal{I}}} z_{i,j} = 1,\ i \in \mathcal{I}, \sum_{i\in\mathcal{I}} z_{i,j} = 1,\ j \in \bar{\mathcal{I}}. \end{aligned} \tag{11}$$

By dropping the integrality constraint in problem (11) we obtain the following linear program

$$\begin{aligned} \max_{(z_{i,j})_{i\in\mathcal{I},j\in\bar{\mathcal{I}}}} \quad & \sum_{i\in\mathcal{I}}\sum_{j\in\bar{\mathcal{I}}} w_{i,j}^{(l)} z_{i,j} \\ \text{subject to} \quad & z_{i,j} \geq 0,\ i \in \mathcal{I}, j \in \bar{\mathcal{I}},\ \sum_{j\in\bar{\mathcal{I}}} z_{i,j} = 1,\ i \in \mathcal{I}, \sum_{i\in\mathcal{I}} z_{i,j} = 1,\ j \in \bar{\mathcal{I}}. \end{aligned} \tag{12}$$

It is known that problem (12) has a solution which satisfies the integer constraint $z_{i,j} \in \{0, 1\},\ i \in \mathcal{I}, j \in \bar{\mathcal{I}}$, and therefore is also a solution to problem (11) [29].

Clearly, any feasible solution $\mathbf{z} = (z_{i,j})_{i\in\mathcal{I},j\in\bar{\mathcal{I}}}$ to problem (11) can be augmented to a feasible solution $\mathbf{x}(\mathbf{z}) = (x(z)_{i,j})_{0\leq i<j\leq M-1}$ to problem (10), where $x(z)_{i,j} = z_{i,j}$ for $i \in \mathcal{I}, j \in \bar{\mathcal{I}}$ and $x(z)_{i,j} = 0$ otherwise. The fact that $\mathbf{x}(\mathbf{z})$ is a feasible solution to problem (10) can be easily checked. Likewise, it follows that $F_1(\mathbf{x}(\mathbf{z})) = F_2(\mathbf{z})$, where F_1 and F_2 denote the cost functions of problems (10) and (11), respectively.

In order to present the main result of this section, we need to establish some new terminology and notations. We say that source X (or the pdf $f(x)$) is symmetric about μ if $f(x) = f(\mu - x)$ for each $x \in \mathbf{R}$. For each $i, 0 \leq i \leq M-1$, denote $\bar{i} = M - 1 - i$. For each set $S \subseteq \mathbb{R}$, denote $\mu - S = \{\mu - x | x \in S\}$. We say that the M-level quantizer Q is symmetric about μ if $b_{M/2} = \mu$, $C_i = \mu - C_{\bar{i}}$ and $y_i = \mu - y_{\bar{i}}$, for each $0 \leq i \leq M-1$. Finally, for each $0 \leq i \leq M-1$, denote $\mu_i = \frac{\int_{C_i} xf(x)\ dx}{P(C_i)}$. In the sequel, we assume that for each $0 \leq i \leq M-1$, $y_i \in [b_i, b_{i+1}]$.

Proposition 1: Assume that the source X and the quantizer Q are symmetric about μ. Then, for any solution $\mathbf{z}^{(0)}$ to problem (11), $\mathbf{x}(\mathbf{z}^{(0)})$ is a solution to problem (10), for $l \in \{1, 2, 3\}$, when one of the following holds:

i) $l \in \{1, 3\}$ and $d(x, y) = \rho(|x - y|)$, where ρ is nondecreasing;

ii) $l = 2$, $d(x, y) = (x - y)^2$ and, for any $i \in \mathcal{I}$, one has $y_i - \mu \geq 2(\mu_i - \mu)$.

Proof: When $d(x, y) = \rho(|x - y|)$, shifting both the pdf and the quantizer by the same amount does not change the values $w_{i,j}^{(l)}$, $0 \leq i < j \leq M-1$. Thus, we may assume that $\mu = 0$.

In the following argument we will use Lemmas (1)-(5), stated and proved in the appendix. Let $F_{1,opt}$ and $F_{2,opt}$ denote the optimal cost for problems (10) and (11), respectively. Since for any feasible solution $\mathbf{z} = (z_{i,j})_{i \in \mathcal{I}, j \in \bar{\mathcal{I}}}$ to problem (11), $\mathbf{x}(\mathbf{z}) = (x(z)_{i,j})_{0 \leq i < j \leq M-1}$ is also a feasible solution for problem (10) and $F_1(\mathbf{x}(\mathbf{z})) = F_2(\mathbf{z})$, it follows that

$$F_{1,opt} \geq F_{2,opt}. \tag{13}$$

Next we prove that, when one of conditions i) and ii) is satisfied, one has $F_{1,opt} \leq F_{2,opt}$. For this, let $\mathbf{x}^{(0)} = (x_{i,j}^{(0)})_{0 \leq i < j \leq M-1}$ be a solution to problem (10) and define $\bar{\mathbf{x}}^{(0)} = (\bar{x}_{i,j}^{(0)})_{0 \leq i < j \leq M-1}$, where $\bar{x}_{i,j}^{(0)} = x_{\bar{j},\bar{i}}^{(0)}$, $0 \leq i < j \leq M-1$. Lemma 1 implies that $w_{i,j}^{(l)} = w_{\bar{j},\bar{i}}^{(l)}$, for all $0 \leq i < j \leq M-1$. Then $\mathbf{x}^{(0)}$ is also a solution to problem (10). Consider now $\mathbf{x}^{(1)} = (x_{i,j}^{(1)})_{0 \leq i < j \leq M-1}$, where $x_{i,j}^{(1)} = \frac{1}{2}\left(x_{i,j}^{(0)} + \bar{x}_{i,j}^{(0)}\right)$, $0 \leq i < j \leq M-1$. (Notice that $x_{i,j}^{(1)}$ are not necessarily integer values anymore.) Since $\mathbf{x}^{(1)}$ is a convex combination of two solutions to problem (10), it follows that $F_1(\mathbf{x}^{(1)}) = F_{1,opt}$ and that $\mathbf{x}^{(1)}$ satisfies the equality constraints, i.e., for any $0 \leq i \leq M-1$,

$$\sum_{j=i+1}^{M-1} x_{i,j}^{(1)} + \sum_{k=0}^{i-1} x_{k,i}^{(1)} = 1. \tag{14}$$

Additionally, notice that $\mathbf{x}^{(1)}$ has the following symmetry property:

$$x_{i,j}^{(1)} = x_{\bar{j},\bar{i}}^{(1)}, \text{ for all } 0 \leq i < j \leq M-1. \tag{15}$$

Let us construct now the tuple $\mathbf{z}^{(1)} = (z_{i,j}^{(1)})_{i\in\mathcal{I},j\in\bar{\mathcal{I}}}$ as follows

$$z_{i,j}^{(1)} = \begin{cases} x_{i,\bar{i}}^{(1)} & \text{if} \quad j = \bar{i} \ (\iff i = \bar{j}) \\ x_{i,j}^{(1)} + x_{i,\bar{j}}^{(1)} & \text{if} \quad j < \bar{i} \ (\iff i < \bar{j}) \\ x_{i,j}^{(1)} + x_{\bar{j},i}^{(1)} & \text{if} \quad j > \bar{i} \ (\iff i > \bar{j}) \end{cases} . \tag{16}$$

According to Lemma 2, $\mathbf{z}^{(1)}$ is a feasible solution to problem (12). Since problem (12) has a solution which satisfies the integer constraints of problem (11) [29], it follows that the two problems achieve the same cost at optimality, i.e., $F_{2,opt}$, and further that $F_2(\mathbf{z}^{(1)}) \leq F_{2,opt}$. On the other hand, according to Lemmas 3 and 4, one has $w_{i,j}^{(l)} \leq w_{i,\bar{j}}^{(l)}$ and $w_{i,j}^{(l)} \leq w_{\bar{j},\bar{i}}^{(l)}$, for all $0 \leq i < j \leq M/2-1$. In addition, Lemma 5 can be further applied leading to the conclusion that $F_2(\mathbf{z}^{(1)}) \geq F_1(\mathbf{x}^{(1)})$. Since $F_{1,opt} = F_1(\mathbf{x}^{(1)})$, it follows that $F_{1,opt} \leq F_{2,opt}$. Combining with (13), one obtains that $F_{1,opt} = F_{2,opt}$. Now let $\mathbf{z}^{(0)}$ be a solution to problem (11). Then one has $F_1(\mathbf{x}(\mathbf{z}^{(0)})) = F_2(\mathbf{z}^{(0)}) = F_{2,opt} = F_{1,opt}$, which completes the proof. ■

Remark 1: Note that the condition $y_i - \mu \geq 2(\mu_i - \mu)$ is satisfied for all $i \in \mathcal{I}$ when the pdf and the quantizer are symmetric about μ and the codebook of the quantizer Q is optimized for the squared error distortion, since in this case $y_i = \mu_i < \mu$. Moreover, if Q is uniform with step size $\Delta > 0$, then $b_{i+1} = \mu + (-M/2 + i + 1)\Delta$, and $y_i = b_{i+1} - \Delta/2$, for each $i \in \mathcal{I}$. Clearly, for $0 \leq i \leq M/2-2$, one has $(y_i - \mu)/2 > b_{i+1} - \mu > \mu_i - \mu$. Thus, the only situation when the condition is not automatically guaranteed is for $i = M/2-1$.

VI. Experimental Results I

In this section, we assess the practical performance of the optimized binary code for several i.i.d. sources. Specifically, we consider the Gaussian and Laplacian sources with $\mu = 0$ and $\sigma^2 = 1$ since they are commonly used to model the distribution of transform coefficients and of prediction residuals [20]. In addition, we consider a mixed Gaussian source with pdf

$$f(x) = 0.7\left(\frac{1}{\sqrt{2\pi}}e^{-(x-\nu_1)^2/2}\right) + 0.3\left(\frac{1}{\sqrt{2\pi}}e^{-(x-\nu_2)^2/2}\right),$$

where $\nu_1 = -2$, and $\nu_2 = 2$ (the mean is -0.80 and the variance is 4.36).

The distortion measure is the squared error. In each case, we consider uniform quantizers with M bins for each $M \in \{4, 8, 16, 32, 64, 128\}$. In a uniform quantizer, all bounded cells are intervals of the same size and the reconstruction values are the midpoints of the bounded intervals. Each such quantizer is characterized by the step size Δ and the shift δ.

Then $b_{i+1} = \delta + (-M/2 + i + 1)\Delta$, and $y_i = b_{i+1} - \Delta/2$, for each $0 \leq i \leq M-2$, while $y_{M-1} = b_{M-1} + \Delta/2$. The values of Δ and δ are chosen such that the distortion is minimized for the corresponding source and number of levels. Specifically, the values of Δ (in increasing order of M) are $0.9957, 0.586, 0.3352, 0.1881, 0.1041, 0.0569$, for the Gaussian source, $1.0873, 0.7309, 0.4609, 0.2799, 0.1657, 0.0961$ for the Laplacian source and $1.81, 1, 0.54, 0.29$, 0.16, 0.08 for the mixed Gaussian pdf. The shift δ is 0 for the Gaussian and Laplacian pdfs, while for the mixed Gaussian it takes the values $-0.21, -0.17, -0.15, -0.14, -0.12, -0.12$. Note that in the Gaussian and Laplacian cases, both the pdf and the quantizer are symmetric about 0, which is not true for the mixed Gaussian distribution. Besides the abovesources, we will also perform experiments with real data consisting of the DCT coefficients of the Lena image.

In the sequel, the distortion will be represented in dB, i.e., as $10\log_{10} D$. We will use the acronym OPT for the optimized binary code. When we need to specify the strategy l and the value of λ we add (l) as a superscript and λ as a subscript. Thus, $\text{OPT}_{\lambda}^{(l)}$ refers to the binary code obtained by solving the problem (7) for $l = 1, 3$. After converting the problem to the form (10) we use the MATLAB linear programming solver, unless otherwise specified.

For comparison with the state of the art, we choose NBC and FBC. Before proceeding to the presentation of the experimental results, we first provide the definition of the binary codes NBC and FBC and justify why we use them for the performance comparison.

A. NBC and FBC

NBC is the binary code π defined as follows: for $0 \leq k \leq M-1$, $\pi(k) = (s_0, \cdots, s_{b-1})$, where $k = \sum_{i=1}^{b} s_{i-1} 2^{b-i}$. The reversed NBC (RNBC) is the binary code obtained from NBC by flipping the MSB s_0. FBC is the binary code π, where $\pi(k)$ is the same as the RNBC codeword for $k \geq M/2$, while for $k < M/2$, $\pi(k)$ equals the NBC codeword corresponding to $M-1-k$. Table I illustrates the three binary codes when $b = 3$.

TABLE I: Binary codes NBC, RNBC, and FBC, for $M = 8$.

k	0	1	2	3	4	5	6	7
NBC	000	001	010	011	100	101	110	111
RNBC	100	101	110	111	000	001	010	011
FBC	111	110	101	100	000	001	010	011

Notice that NBC and RNBC have the same set of connected pairs of integers, namely $\{(k, k+M/2) : 0 \leq k \leq M/2-1\}$. Thus, they have the same values for $D_E^{(l)}$ and $H(S_0)$. For FBC, the

set of connected pairs of integers is $\{(k, M-1-k) : 0 \leq k \leq M/2-1\}$.

In the JPEG standard, the amplitudes of the non-zero AC coefficients are encoded by dividing them into categories and using a fixed-length binary code for each category. Specifically, for $t \geq 1$, category t is the set $\mathcal{I}_t = \{k \in \mathbb{N} : 2^{t-1} \leq |k| \leq 2^t - 1\}$. The elements in $\mathcal{I}_t$ are encoded with a t-bit binary code. Consider relabeling these integers in their increasing order with labels from 0 to $2^b - 1$ and let π denote the binary code applied to these labels. Then the code π specified by the standard is RNBC. Since NBC and RNBC have the same values of $D_E^{(l)}$ and $H(S_0)$, we use NBC in our comparison. Note that PE methods that encrypt the sign bit of the non-zero AC coefficients can be regarded as the application of scenario A in each category.

In the baseline profile of the H.264/AVC standard, the MVDs are encoded using the 0th order Exp-Golomb code [30]. As a result, all integers in the set $\mathcal{I}_t$ are encoded with a $(2t+1)$-bit binary code. For fixed t, only the last t bits of the codeword are different for different integers in $\mathcal{I}_t$. Therefore, we can consider the portion formed of the last t bits as the effective binary code π applied to $\mathcal{I}_t$. The last bit of the codeword is the sign bit. Thus, if we interpret the last bit as the MSB, the PE methods that encrypt the sign bits of the MVDs correspond to scenario A applied to each category. If we consider that π is applied to the labels 0 to 2^b-1 after relabeling the integers in $\mathcal{I}_t$ in their increasing order, then the binary code π specified by the H.264/AVC standard corresponds to FBC (with the provision that the MSB is moved to the last position, while all the other bits remain in the same order).

In the main profile of the H.264/AVC standard, the MVDs are first binarized, i.e., converted to intermediate binary codewords, which are subsequently encoded with a binary arithmetic coder. The binarization process uses a third order Exp-Golomb code, which divides all MVDs with the absolute value larger than 9 into categories, and assigns binary codewords of the same length within each category. Like in the previous case, the effective code within each category corresponds to FBC. PE methods that encrypt the sign bit of the MVDs before applying the arithmetic coder can also be regarded as an instance of scenario A applied to each category, with the code π being FBC.

B. Gaussian and Laplacian Sources

Tables II presents the distortion at Eve's obtained by the optimized binary code in scenario A in comparison with NBC and FBC for the Gaussian and Laplacian sources. The results show that for both sources FBC is optimal under strategy 1, but has very poor performance under strategy

3. The performance gap from the optimum when $l = 3$ increases as M increases and is more pronounced for the Laplacian source, reaching more than 9 dB at $M = 128$. Interestingly, NBC is optimal or very close to optimal under strategy 3 but has weak performance under strategy 1 for the higher values of M. The gap in performance relative to optimum is also higher for the Laplacian source.

TABLE II: Value of $D_E^{(l)}$ for $\text{OPT}_0^{(l)}$, NBC, and, FBC when $l = 1, 3$, for the Gaussian and Laplacian sources.

		M	4	8	16	32	64	128
$l = 1$	Gaussian	$\text{OPT}_0^{(1)}$, FBC	0	0	0	0	0	0
		NBC	-0.13	-0.03	-0.16	-0.50	-1.00	-1.66
$l = 1$	Laplacian	$\text{OPT}_0^{(1)}$, FBC	0	0	0	0	0	0
		NBC	-0.01	-0.15	-0.76	-1.65	-2.78	-4.13
$l = 3$	Gaussian	$\text{OPT}_0^{(3)}$	3.15	4.41	5.560	6.562	7.444	8.217
		NBC	3.15	4.41	5.559	6.559	7.441	8.215
		FBC	2.74	2.93	2.99	3.003	3.008	3.010
$l = 3$	Laplacian	$\text{OPT}_0^{(3)}$, NBC	3.82	6.25	8.29	10.00	11.48	12.77
		FBC	2.56	2.85	2.95	2.99	3.00	3.01

TABLE III: Value of $H(S_0)$ for $\text{OPT}_0^{(1)}$, $\text{OPT}_0^{(3)}$, NBC, EONB, and, FBC for the Gaussian and Laplacian sources.

	M	4	8	16	32	64	128
Gaussian	$\text{OPT}_0^{(1)}$, NBC, FBC	1	1	1	1	1	1
	$\text{OPT}_0^{(3)}$, EONB	0.90	0.80	0.68	0.56	0.46	0.36
Laplacian	$\text{OPT}_0^{(1)}$, NBC, FBC	1	1	1	1	1	1
	$\text{OPT}_0^{(3)}$, EONB	0.75	0.55	0.38	0.25	0.16	0.10

Let us discuss now the performance of $\text{OPT}_\lambda^{(1)}$ in scenario B. Figures 3 and 4 plot the value of $D_E^{(1)}$ versus the entropy $H(S_0)$, obtained in scenario B when $M = 4, 8, 16, 32, 64, 128$, in the case of the Gaussian source, respectively the Laplacian source. For each M, various points are obtained by gradually increasing λ from 0 up to some very large value. For both sources, $\text{OPT}_0^{(1)}$ achieves the highest secrecy since $D_E^{(1)}$ is the largest, but also the highest encryption complexity as $H(S_0) = 1$ is also the largest. As λ gradually increases above 0, the complexity of the encryption decreases at the expense of decreasing the secrecy. However, it is noteworthy that at the beginning, $H(S_0)$ decreases at a high rate, while the reduction in $D_E^{(1)}$ is very slow. In particular, when $M \geq 8$, $H(S_0)$ can be reduced from 1 to 0.8 or less, while decreasing $D_E^{(1)}$

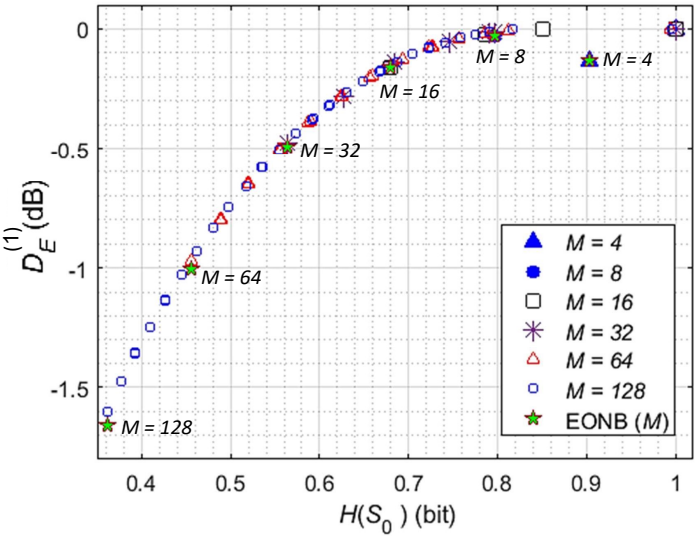


Fig. 3: Plot of $D_E^{(1)}$ versus $H(S_0)$ for $M = 4, 8, 16, 32, 64, 128$, for the Gaussian source.

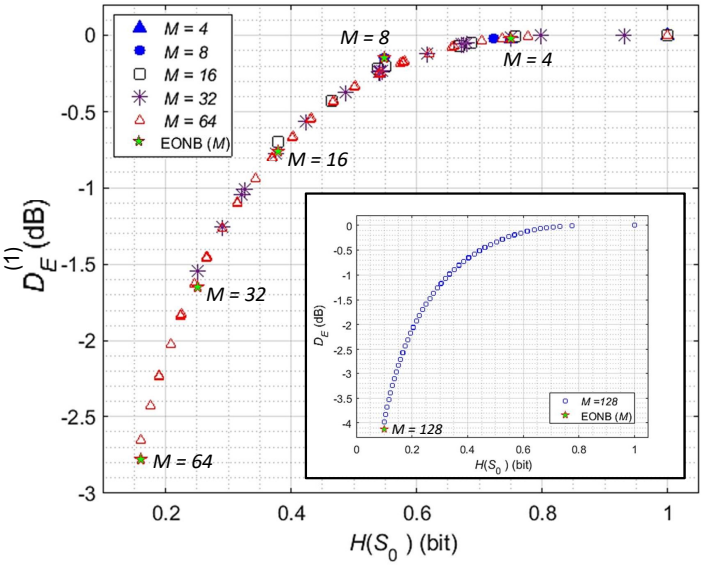
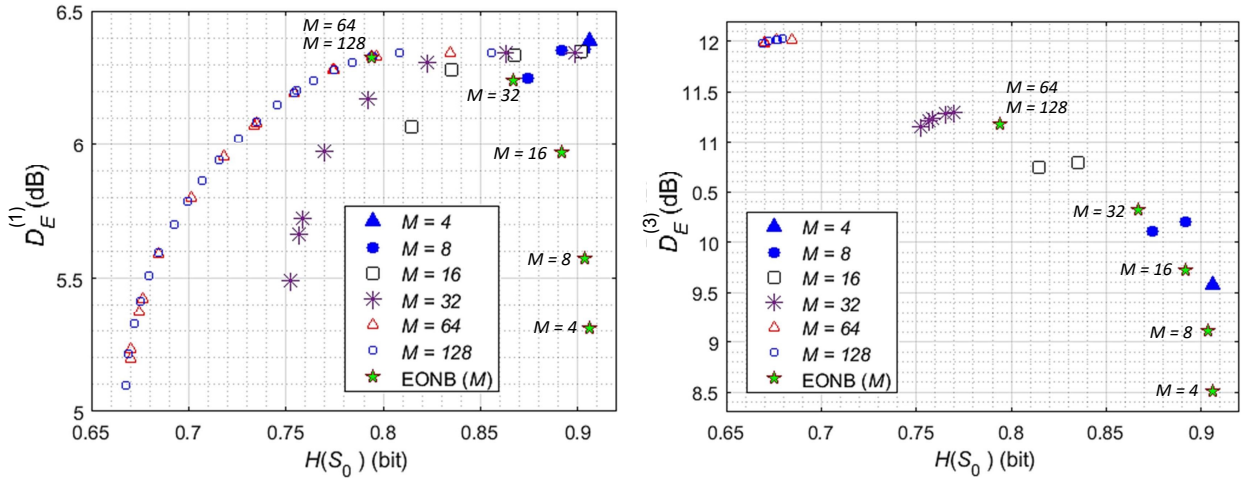


Fig. 4: Plot of $D_E^{(1)}$ versus $H(S_0)$ for $M = 4, 8, 16, 32, 64, 128$, for the Laplacian source.

by only ≈ 0.025 dB. Based on this observation, it follows that NBC and FBC have very poor performance in scenario B since they have $H(S_0) = 1$, i.e., the largest encryption complexity.

Another interesting observation is that the entropy-optimized NBC (EONB) has the smallest value of $H(S_0)$. This is because the $M/2$ cells with the largest probabilities are $C_{M/4}, \cdots, C_{3M/4-1}$, and each of them is connected by EONB to a cell which is not in this set, thus each of them



(a) $l = 1$ (b) $l = 3$

Fig. 5: Plot of $D_E^{(l)}$ versus $H(S_0)$ when $M = 4, 8, 16, 32, 64, 128$, for the mixed Gaussian source.

is assigned the MSB 0 by EONB. Table III shows the values of $H(S_0)$ for $\text{OPT}_0^{(l)}$, $l = 1, 3$, NBC, FBC and EONB for all M. The pairs $(H(S_0, D_E^{(1)})$ corresponding to EONB are marked by red stars in Figures 3 and 4. We see that they are very close to the pairs obtained by $\text{OPT}_\lambda^{(1)}$ corresponding to similar values of $H(S_0)$.

Finally, another key observation for strategy 1 is that there is a large number of trade-off pairs $(H(S_0), D_E^{(1)})$ and they cover a wide range of values of $H(S_0)$ and $D_E^{(1)}$, especially for higher M. Under strategy 3, on the other hand, $\text{OPT}_0^{(3)}$ already achieves the highest distortion $D_E^{(3)}$ and the lowest entropy $H(S_0)$, for both the Gaussian and Laplacian sources. In other words, maximizing the secrecy and minimizing the complexity of encryption can be done simultaneously and there is no further impact by increasing λ above 0. Also note that EONB has the same performance as $\text{OPT}_0^{(3)}$ in scenario B, while NBC and FBC are considerably inferior since their entropy $H(S_0)$ is much lower than that of $\text{OPT}_0^{(3)}$.

C. Mixed Gaussian Source

Table IV illustrates the comparison in performance between the optimized binary code, NBC, and FBC for the mixed Gaussian source in scenario A. It can be seen that under strategy 1, FBC is optimal or very close to optimal. NBC is suboptimal, but the gap to the optimal performance narrows as M increases, unlike for the Gaussian and Laplacian sources. Under strategy 3 both NBC and FBC have weaker performance than $\text{OPT}_0^{(3)}$, except for FBC when $M = 4$. The gap

between NBC and $\text{OPT}_0^{(3)}$ is between 0.8 and 1.1 dB, while the gap between FBC and $\text{OPT}_0^{(3)}$, for $M \geq 16$, is between 1 and 2.16 dB.

TABLE IV: Value of $D_E^{(l)}$ for $\text{OPT}_0^{(l)}$, NBC, and FBC when $l = 1, 3$, for the mixed Gaussian source.

	M	4	8	16	32	64	128
$l=1$	$\text{OPT}_0^{(1)}$	6.39	6.36	6.35	6.34	6.344	6.345
	NBC	5.31	5.57	5.97	6.24	6.32	6.32
	FBC	6.39	6.36	6.35	6.34	6.341	6.340
$l=3$	$\text{OPT}_0^{(3)}$	9.58	10.21	10.79	11.30	12.02	12.02
	NBC	8.51	9.11	9.72	10.33	11.18	11.18
	FBC	9.58	9.74	9.79	9.81	9.84	9.84

TABLE V: Value of $H(S_0)$ for $\text{OPT}_0^{(1)}$, $\text{OPT}_0^{(3)}$, NBC, EONB, and FBC for the mixed Gaussian source.

M	4	8	16	32	64	128
$\text{OPT}_0^{(1)}$	0.91	0.90	0.90	0.898	0.83	0.86
$\text{OPT}_0^{(3)}$	0.91	0.89	0.84	0.77	0.66	0.68
NBC, FBC	0.91	0.90	0.90	0.901	0.90	0.90
EONB	0.91	0.90	0.89	0.86	0.79	0.79

Let us consider now scenario B. Figures 5(a) and 5(b) plot the value of $D_E^{(l)}$, for $l = 1$, respectively $l = 3$, versus $H(S_0)$, for $\text{OPT}_\lambda^{(l)}$ with various values of λ, when $M = 4, 8, 16, 32, 64, 128$. We can observe that by varying λ, a various trade-off pairs $(H(S_0), D_E^{(3)})$ can be obtained. The number of these pairs and the range of values covered are larger for strategy 1. As seen from Table V, $\text{OPT}_0^{(1)}$ achieves a high entropy $H(S_0)$. As Figure 5(a) shows, for $M \geq 16$, a large decrease of $H(S_0)$ can be obtained with only a small decrease of $D_E^{(1)}$. Since according to Table V, NBC and FBC have the value of $H(S_0)$ larger than or equal to that of $\text{OPT}_0^{(1)}$, it follows that both are inferior to $\text{OPT}^{(1)}$ in scenario B for $M \geq 16$. The same conclusion holds for NBC when $M = 4, 8$ since in this case, NBC has the value of $D_E^{(1)}$ much smaller than that of $\text{OPT}_0^{(1)}$, while $H(S_0)$ is the same. Under strategy 3, when $M \geq 8$, we observe that NBC and FBC have a larger value of $H(S_0)$ than $\text{OPT}_0^{(3)}$, while the distortions $D_E^{(3)}$ are much lower, thus they have poorer performance than $\text{OPT}_0^{(3)}$ in scenario B. This conclusion extends to the case when $M = 4$ for NBC.

Figures 5(a) and 5(b) also contain the pairs $(H(S_0, D_E^{(1)})$ corresponding to EONB. Notice that they are far away from the pairs corresponding to $\text{OPT}_\lambda^{(l)}$, for all M under strategy 3 and all

$M \leq 32$ under strategy 1. We conclude that EONB is inferior to $\text{OPT}_{\lambda}^{(l)}$ in these cases. The exception is when $M \geq 64$ in strategy 1. In this case EONB is very close to the optimum.

D. DCT Coefficients Data

In this subsection, we assess the performance of the optimized binary code on practical data consisting of quantized DCT coefficients. We use the 512-by-512 Lena gray-level image with 8-bit pixel intensity values. The DCT transform is applied on 8-by-8 blocks as in the JPEG standard. We apply a fine quantizer to the DCT coefficients by rounding them to the closest integer, then record the frequencies of the non-zero quantized AC coefficients within the range from -256 to 256. Let Z denote the discrete RV with this probability distribution. Thus Z takes as values the non-zero integers in the interval $[-256, 256]$.

TABLE VI: Performance of $\text{OPTA}^{(3)}$, NBC, EONB, and FBC for Z_t, $2 \leq t \leq 8$.

	Size	2	3	4	5	6	7	8
$D_E^{(3)}$	$\text{OPT}_0^{(3)}$	10.97	17.82	24.22	30.4322	36.5556	42.669	48.82
	$\text{OPT}_{10^6}^{(3)}$	10.97	17.82	24.22	30.4322	36.5554	42.666	48.75
	NBC	10.97	17.82	24.22	30.4316	36.54	42.61	48.65
	FBC	10.81	17.19	23.62	29.93	36.03	42.08	47.74
$H(S_0)$	$\text{OPT}_0^{(3)}$	0.97	0.89	0.90	0.92	0.9145	0.889	0.70
	$\text{OPT}_{10^6}^{(3)}$	0.97	0.89	0.90	0.92	0.9141	0.885	0.64
	NBC, FBC	≈ 1	≈ 1	≈ 1	≈ 1	≈ 1	≈ 1	≈ 1
	EONB	0.97	0.89	0.90	0.92	0.9145	0.90	0.73

TABLE VII: Performance of $\text{OPTA}^{(3)}$, NBC, EONB, and FBC for Z.

Measure	$\text{OPT}_0^{(3)}$	$\text{OPT}_{10^6}^{(3)}$	NBC	EONB	FBC	NBC_{cat}	FBC_{cat}
$D_E^{(3)}$	45.1556	45.1555	45.1545	45.1545	27.1	27.78	27.09
$H(S_0)$	0.0314	0.0311	≈ 1	0.0319	≈ 1	≈ 1	≈ 1

We further construct more distributions as follows. For any integer t, $1 \leq t \leq 8$, let Z_t denote the RV obtained by truncating Z to the set $\mathcal{I}_t$ defined in subsection VI-A.

For the sources Z and Z_t, $2 \leq t \leq 8$, we apply the trivial quantizer, i.e., the quantizer for which each cell consists of only one element. Then we solve the problem (7) for $\lambda = 0$ and $\lambda = 10^6$ under strategy 3. For this, the problem is converted to the form (10) and solved with an integer programming package in Python 3 (the MIP package). The binary codes obtained using

our design are compared with NBC and FBC. Table VI contains the results for Z_t, fro $2 \leq t \leq 8$, while Table VII contains the results for Z. Notice first that $\text{OPT}_0^{(3)}$ and $\text{OPT}_{10^6}^{(3)}$ are very close in performance. Only for Z_8 a non-negligible difference between them can be noticed.

Let us discuss now the results for the sources Z_t. We observe that NBC performs very well in scenario A for all Z_t, with identical or very close performance to $\text{OPT}^{(3)}$, while FBC lags behind with a gap between 0.5 and 1 dB for $t \geq 3$.

Recall that FBC is used to encode the non-zero MVDs in the set $\mathcal{I}_t$ by the H.264/AVC standard. The above result suggests that the secrecy of the PE scheme that encrypts the MVDs sign bits can be improved simply by replacing FBC with NBC. On the other hand, RNBC is used in JPEG to encode the quantized AC coefficients in the set $\mathcal{I}_t$. Since RNBC has the same performance in terms of secrecy as NBC, our result shows that the PE scheme that encrypts the sign bits of the non-zero AC coefficients cannot be further improved by changing the binary code.

However, in scenario B, both NBC and FBC are inferior to $\text{OPT}^{(3)}$ for all Z_t since they have a larger value of the entropy $H(S_0)$, while EONB has a performance close to $\text{OPT}_0^{(3)}$. This suggests that, if in the aforementioned PE schemes, the sign bits were to be compressed by an entropy coder before being encrypted, a performance improvement could be obtained by replacing the binary code for each category by EONB. The improvement would consist of a decreased complexity of encryption for both PE schemes, while for the PE scheme for H.264/AVC an additional increase in secrecy could be obtained.

Let us discuss now the experiments with the source Z. In Table VII we also include the results for NBC_{cat} and FBC_{cat}, where NBC_{cat} (respectively FBC_{cat}) is a variable-length binary code for Z that assigns the t-bit NBC (respectively FBC) to the integers in the set $\mathcal{I}_t$. We see that in scenario A, NBC has an excellent performance, i.e. extremely close to the optimum $\text{OPT}_0^{(3)}$, while FBC, NBC_{cat} and FBC_{cat} are very far away from the optimum. In scenario B, even NBC performs poorly since is entropy $H(S_0)$ is approximately 1, while $H(S_0) \approx 0.03$ for $\text{OPT}_0^{(3)}$. The results for the source Z suggest that the aforementioned PE schemes could achieve high improvements in terms of secrecy and complexity of encryption if the variable-length code were to be changed by a PE optimized fixed-length code. Since this change would increase the rate of the bitstream, further compression would have to be applied to reduce the bitrate.

VII. Experimental Results II

In this section, the performance of the proposed optimized binary code will be investigated for the PE of uncompressed or "lightly" compressed images. The PE is obtained by encrypting

(a) (b) (c) (d) (e)

Fig. 6: Images (a) Camera Man, (b) Gold Hill, (c) Lena, (d) Living Room, (e) Zelda.

one or two MSB planes. In scenario A, the images are not compressed. In scenario B, only the MSB plane is compressed before being encrypted.

We consider five gray-level images of size 512×512, with 8-bit pixel values. Thus, the intensity values of the pixels are integers ranging from 0 to 255. The images are shown in Figure 6. The binary code π maps each integer in this range to an 8-bit sequence. We will consider two cases, i.e., encryption of one MSB plane (1BPE) and encryption of two MSB planes (2BPE). The binary code will be optimized for 1BPE, but its practical performance will be assessed for both 1BPE and 2BPE.

We assume that Eve uses a replacement attack. Thus, in the case of 1BPE, she uses two reconstructions, obtained by replacing all MSBs by 0, respectively by 1. Under 2BPE, Eve uses four reconstructions, obtained by replacing the two unknown MSB bits by 00, 01, 10 and 11, respectively.

To optimize the binary code, we solve the optimization problem (7) for $l = 3$, $\lambda = 0$ and $\lambda = 10^6$. For this, we convert the problem to the form (10) and solve it using an integer programming package in Python 3 (the MIP package). Note that the solution to the problem (10) only specifies the connected pairs i, j, i.e., the pairs having the same 7-bit LSB (least significant bit) representation. It does not specify how to assign the 7-bit LSB sequences to these pairs. This assignment does not impact the image degradation under 1BPE, but it does under 2BPE. Our intuition is that a random assignment will increase the correlation between adjacent pixels in the reconstruction, which is desired for higher secrecy. Therefore, we will use a random assignment of 7-bit LSB sequences to the connected pairs for both scenarios A and B. Likewise, the assignment of the MSB value to each element in a connected pair does not affect the value of $D_E^{(3)}$. However, it influences the visual distortion since adjacent pixels in an image are correlated. Therefore, in scenario A, we will randomly assign the MSB to each integer in a

connected pair.

Recall that in scenario B, our optimization procedure uses $H(S_0)$ as a measure of the encryption complexity. Since the pixel values are correlated, the entropy of the MSB plane is no longer guaranteed to be equal to $H(S_0)$. However, we expect that by increasing $H(S_0)$, the entropy of the MSB plane to increase too. The assignment of the MSB value to the elements in a connected pair influences $H(S_0)$. Therefore, in scenario B we use the entropy-optimized binary code, i.e., the MSB 0 is assigned to the integer in the pair having the largest probability.

We use the acronyms OPTA and OPTB for the binary codes obtained as specified above in scenario A, respectively B. When we are interested in specifying the value of λ, we add it as a subscript to OPTB. The performance of OPTA and OPTB will be compared against NBC, which is the binary code used in the prior work on PE schemes that encrypt the high order MSBs of the pixel values [21]–[25].

To measure the degradation in the reconstruction at Eve's side, we will use both the visual assessment and the objective assessment based on evaluating the PSNR and SSIM [32]. We will also consider the correlation between adjacent pixel values as a measure of security of each technique. In Table VIII the PSNR, SSIM, and the diagonal correlation (dCorr) for the reconstructions at Eve's side are presented for the binary codes under investigation. The PSNR is computed based on the average MSE over all reconstructions used at Eve's side. The SSIM and dCorr values are also averaged over all reconstructions.

We observe from Table VIII that the PSNR values for OPTA and OPTB are always smaller than for NBC in case of 1BPE. This is expected since the maximization of the distortion, hence the minimization of the PSNR, under 1BPE is accounted for in the optimization objective. For all images except Zelda, this observation holds for 2BPE, too. While the difference in terms of PSNR between the optimized binary codes and NBC is not that dramatic, we see a significant difference in SSIM. Note that for NBC, the SSIM values are at least 0.2 in most of the cases, while for OPTA the SSIM is extremely low (≤ 0.01). The SSIM for OPTB, although higher than for OPTA, is still lower than half of the SSIM value of the NBC in all cases except for Camera Man under 1BPE. As for the diagonal correlation, it can be noticed that NBC has high values (over 0.5 for 1BPE and over 0.3 for 2BPE), while OPTA significantly decreases the correlation. More specifically, for four out of the five images, dCorr for OPTA is very low, i.e., at most 0.12. The values of dCorr for OPTB, although higher than for OPTA, are still lower than for NBC with only one exception (Camera Man at 1BPE).

TABLE VIII: Performance comparison in terms of secrecy using objective measures.

Images	**Measure**	NBC		OPTA		OPTB_0		OPTB_{10^6}	
		1BPE	2BPE	1BPE	2BPE	1BPE	2BPE	1BPE	2BPE
Camera Man	PSNR(dB)	9.00	8.96	7.38	7.83	7.38	7.83	7.64	8.01
	SSIM	0.23	0.44	0.01	0.01	0.41	0.06	0.44	0.05
	dCorr	0.65	0.64	0.40	0.18	0.81	0.32	0.84	0.30
Gold Hill	PSNR(dB)	9.00	8.96	8.76	8.88	8.76	8.88	8.83	8.88
	SSIM	0.20	0.25	0.01	0.01	0.09	0.09	0.08	0.08
	dCorr	0.55	0.37	0.07	0.07	0.18	0.18	0.23	0.23
Lena	PSNR(dB)	9.00	8.97	8.69	8.95	8.69	8.95	8.71	8.96
	SSIM	0.25	0.35	0.01	0.01	0.05	0.05	0.04	0.04
	dCorr	0.69	0.51	0.11	0.11	0.23	0.23	0.19	0.19
Living Room	PSNR(dB)	9.00	9.37	8.69	9.00	8.69	9.00	8.72	9.02
	SSIM	0.15	0.26	0.01	0.01	0.07	0.07	0.07	0.07
	dCorr	0.60	0.41	0.10	0.10	0.23	0.23	0.21	0.21
Zelda	PSNR(dB)	9.00	8.86	8.84	8.89	8.84	8.89	8.84	8.90
	SSIM	0.27	0.38	0.00	0.00	0.08	0.08	0.08	0.08
	dCorr	0.78	0.59	0.12	0.12	0.29	0.29	0.30	0.30

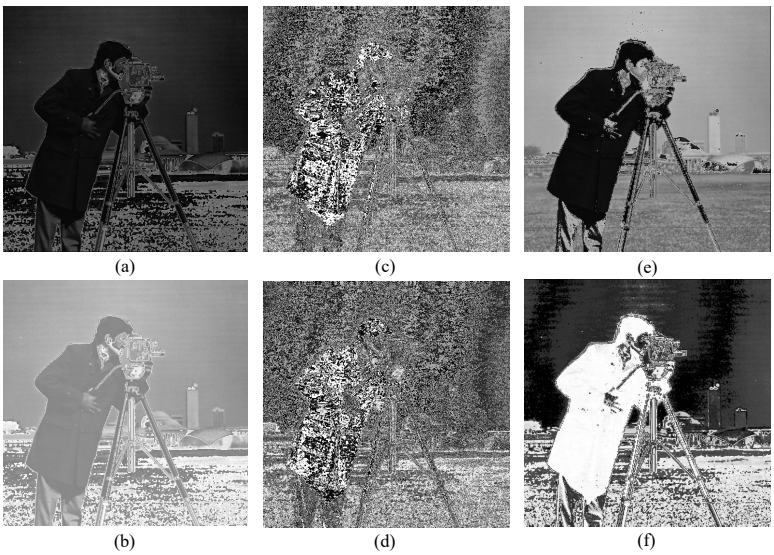


Fig. 7: Eve's reconstruction of Camera Man in 1-bitplane encryption (a) NBC MSB0, (b) NBC MSB1, (c) OPTA MSB0, (d) OPTA MSB1, (e) OPTB_{10^6} MSB0, (f) OPTB_{10^6} MSB1.

Figures 7 and 8 show the reconstructions at Eve's side for the image Camera Man, for the three binary codes under comparison in the case of 1BPE, respectively 2BPE. The reconstructions corresponding to the remaining images are provided in the supplementary material [33]. It can be seen that OPTA leads to significant image degradation in both 1BPE and 2BPE. NBC, on the

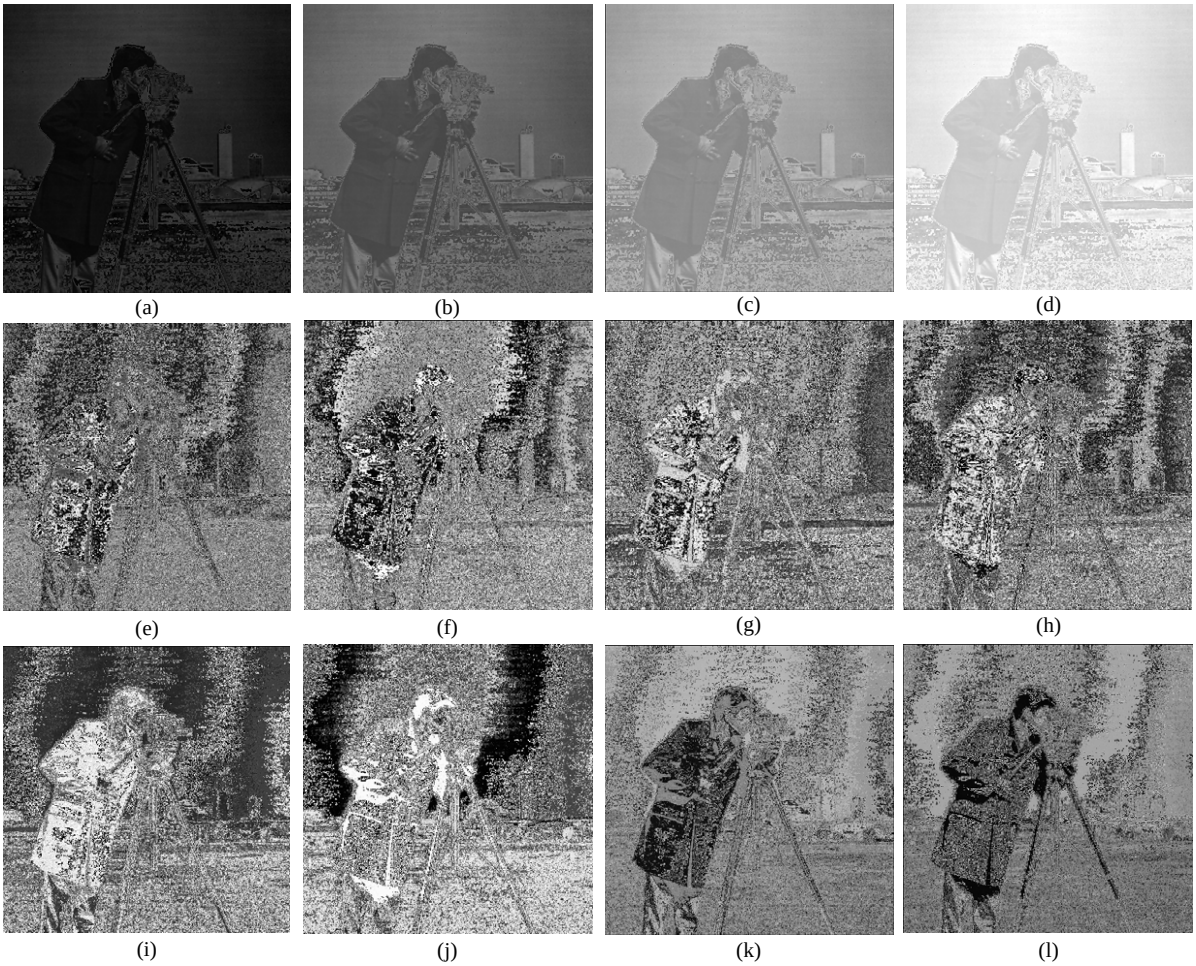


Fig. 8: Eve's reconstruction of Camera Man under 2BPE (a) NBC 00, (b) NBC 01, (c) NBC 10, (d) NBC 11, (e) OPTA 00, (f) OPTA 01, (g) OPTA 10, (h) OPTA 11, (i) OPTB_{10^6} 00, (j) OPTB_{10^6} 01, (k) OPTB_{10^6} 10, (l) OPTB_{10^6} 11 .

other hand, fails at obscuring all the details, even in the case of 2BPE. The same conclusions can be drawn for the other images, based on the reconstructions shown in [33]. We conclude that OPTA ensures a high level of content secrecy even when only one MSB plane is encrypted.

The quality degradation achieved with OPTB in case of 1BPE is similar to that corresponding to NBC. On the other hand, in the case of 2BPE, OPTB ensures a much higher secrecy level than NBC by hiding much more detail. For instance, in the reconstruction with NBC, the landscape in the background is visible, while with OPTB it is blurred. The person's fingers are also clearly distinguishable in the former case, but very blurry in the latter case.

Table IX illustrates the size of the compressed MSB plane, as a measure of encryption

complexity. The compression is performed by using the WebP standard as one of the most efficient lossless compression techniques [34]. Note that the size of the uncompressed MSB plane is 32 KB. We see from the table that the MSB plane of OPTA is not compressible, which is expected since OPTA randomizes the MSBs. We conclude that OPTA is not suitable for use in scenario B. NBC achieves a high compression ratio of the MSB plane (between $3:1$ and $4.8:1$). Recall that in OPTB, the MSB 0 is assigned to intensity values that have high probability. This technique is not guaranteed to remove the correlation between adjacent bits in the MSB plane, therefore, $H(S_0)$ is no longer an accurate measure of the compressibility of the MSB plane. Thus, OPTB is not guaranteed to decrease the size of the compressed MSB plane in comparison with NBC. However, as we see from the table, in five out of the ten cases (five images with two values of λ for each image) the size of the compressed MSB plane for OPTAB is smaller than for NBC, while in the remaining cases the two sizes are close, except for Lena. Since in most cases the sizes of the compressed MSB planes for NBC and OPTB are comparable, while OPTB provides higher secrecy than NBC in case of 2BPE, we conclude that OPTB is a good candidate in scenario B.

TABLE IX: The size of the MSB plane (KB) as the measure of the encryption complexity.

Images	NBC	OPTA	OPTB_0	OPTB_{10^6}
Camera Man	6.6	32.2	7.2	7.1
Gold Hill	9.0	32.8	7.3	6.8
Lena	8.2	32.4	15.4	14.9
Living Room	11.1	32.6	9.8	12.1
Zelda	6.8	32.7	6.9	6.1

VIII. Conclusion

In this work, we consider the scenario where partial encryption (PE) is applied to a sequence of compressed quantization indexes. Specifically, only the plane of MSBs (possibly after being entropy-coded) is encrypted. This corresponds to existing PE schemes for compressed images or videos, where only the sign bits of some syntax elements are encrypted. We observe that the binary code, i.e, the mapping of binary sequences to quantization cells, can control the level of security by influencing the distortion at the eavesdropper's side, while also impacting the amount of computation needed for encryption by affecting the length of the compressed MSB stream. Therefore, we formulate the problem of optimal binary code design for PE as the maximization of a weighted sum of the eavesdropper's distortion and of the probability of the MSB being

0. We show that the problem is equivalent to a maximum weighted graph matching problem, which can be solved in polynomial time. Moreover, we prove that, when the source and the quantizer are symmetric, the problem can be cast as a linear program. Experimental comparison with binary codes used in existing PE schemes shows that in certain situations the proposed design could bring considerable improvement.

IX. Appendix

Lemma 1: If the pdf $f(x)$ and the quantizer Q are symmetric about 0, and the distortion measure is $d(x,y)=\rho(|x-y|)$, then $w_{i,j}^{(l)}=w_{\bar{j},\bar{i}}^{(l)}$, $0\le i<j\le M-1$, $l\in\{1,2,3\}$.

Proof: For each measurable set $S\subseteq\mathbb{R}$ and $y\in\mathbb{R}$ let $L(S,y)=\int_S\rho(|x-y|)f(x)\,dx$. Then the following property holds:

Property A: For any measurable set $S\subseteq\mathbb{R}$ and $y\in\mathbb{R}$, $L(S,y)=L(-S,-y)$.

The proof relies on the symmetry about 0 of the pdf and of the absolute value function. Specifically, one has $L(S,y)=\int_S\rho(|-x+y|)f(-x)\,dx=\int_{-S}\rho(|z+y|)f(z)\,dz=L(-S,-y)$, where the second equality is based on the change of variable $z=-x$.

Property A, together with the fact that $C_{\bar{j}}\cup C_{\bar{i}}=-(C_i\cup C_j)$, leads to $y_{\bar{j},\bar{i}}^{(1)}=\arg\min_{y\in\mathbb{R}}L(C_{\bar{j}}\cup C_{\bar{i}},y)=\arg\min_{y\in\mathbb{R}}L(C_i\cup C_j,-y)=-y_{i,j}^{(1)}$. On the other hand, the symmetry of the quantizer readily implies that $y_{\bar{j},\bar{i}}^{(2)}=-y_{i,j}^{(2)}$. Then, for $l=1,2$, one has $D_{\bar{j},\bar{i}}^{(l)}=L(C_{\bar{j}}\cup C_{\bar{i}},y_{\bar{j},\bar{i}}^{(l)})=L(-(C_i\cup C_j),-y_{i,j}^{(l)})=L(C_i\cup C_j,y_{i,j}^{(l)})=D_{i,j}^{(l)}$, where the second last equality is based on Property A. Let us consider now $l=3$. Using again Property A in conjunction with $y_{\bar{i}}=-y_i$, $y_{\bar{j}}=-y_j$ and $C_{\bar{j}}\cup C_{\bar{i}}=-(C_i\cup C_j)$, one obtains $D_{\bar{j},\bar{i}}^{(3)}=0.5L(C_{\bar{j}}\cup C_{\bar{i}},y_{\bar{i}})+0.5L(C_{\bar{j}}\cup C_{\bar{i}},y_{\bar{j}})=0.5L(C_i\cup C_j,y_i)+0.5L(C_i\cup C_j,y_j)=D_{i,j}^{(3)}$. Further, for each $k,0\le k\le M-1$,

$$P(C_{\bar{k}})=\int_{C_{\bar{k}}}f(x)\,dx=\int_{-C_k}f(-x)\,dx=\int_{C_k}f(z)\,dz=P(C_k). \tag{17}$$

This implies that $P_{0,\bar{j},\bar{i}}=P_{0,i,j}$. Now the conclusion of the lemma follows immediately. ■

Lemma 2: The tuple $\mathbf{z}^{(1)}$ defined in (16) is a feasible solution to problem (12).

Proof: Let us first fix some arbitrary $i\in\mathcal{I}$. Based on (16), one obtains

$$\sum_{j\in\bar{\mathcal{I}}}z_{i,j}^{(1)}=\sum_{j=M/2}^{\bar{i}-1}z_{i,j}^{(1)}+z_{i,\bar{i}}^{(1)}+\sum_{j=\bar{i}+1}^{M-1}z_{i,j}^{(1)}=\sum_{j=M/2}^{\bar{i}-1}\left(x_{i,j}^{(1)}+x_{i,\bar{j}}^{(1)}\right)+x_{i,\bar{i}}^{(1)}+\sum_{j=\bar{i}+1}^{M-1}\left(x_{i,j}^{(1)}+x_{\bar{j},i}^{(1)}\right)$$
$$=\sum_{j=M/2}^{\bar{i}-1}x_{i,\bar{j}}^{(1)}+\sum_{j=M/2}^{\bar{i}-1}x_{i,j}^{(1)}+x_{i,\bar{i}}^{(1)}+\sum_{j=\bar{i}+1}^{M-1}x_{i,j}^{(1)}+\sum_{j=\bar{i}+1}^{M-1}x_{\bar{j},i}^{(1)}.$$

By making the substitutions $m=\bar{j}$ in the first summation and $k=\bar{j}$ in the last one, leads to

$$\sum_{j\in\bar{\mathcal{J}}} z_{i,j}^{(1)} = \underbrace{\sum_{m=i+1}^{M/2-1} x_{i,m}^{(1)}}_{\text{rename } m \text{ by } j} + \sum_{j=M/2}^{M-1} x_{i,j}^{(1)} + \sum_{k=0}^{i-1} x_{k,i}^{(1)} = \sum_{j=i+1}^{M-1} x_{i,j}^{(1)} + \sum_{k=0}^{i-1} x_{i,j}^{(1)} = 1, \tag{18}$$

where the last equality is based on (14). Let us fix some arbitrary $j\in\bar{\mathcal{J}}$. Using (16) leads to

$$\begin{aligned}\sum_{i\in\mathcal{J}} z_{i,j}^{(1)} &= \sum_{i=0}^{\bar{j}-1} z_{i,j}^{(1)} + z_{\bar{j},j}^{(1)} + \sum_{i=\bar{j}+1}^{M/2-1} z_{i,j}^{(1)} = \sum_{i=0}^{\bar{j}-1}\left(x_{i,j}^{(1)} + x_{i,\bar{j}}^{(1)}\right) + x_{\bar{j},j}^{(1)} + \sum_{i=\bar{j}+1}^{M/2-1}\left(x_{i,j}^{(1)} + x_{\bar{j},i}^{(1)}\right)\\ &= \sum_{i=0}^{\bar{j}-1} x_{i,\bar{j}}^{(1)} + \sum_{i=0}^{\bar{j}-1} x_{i,j}^{(1)} + x_{\bar{j},j}^{(1)} + \sum_{i=\bar{j}+1}^{M/2-1} x_{i,j}^{(1)} + \sum_{i=\bar{j}+1}^{M/2-1} x_{\bar{j},i}^{(1)}.\end{aligned} \tag{19}$$

According to (15), one has $x_{i,\bar{j}}^{(1)} = x_{j,\bar{i}}^{(1)}$. Applying the above, then performing the substitution $n=\bar{i}$, yields

$$\sum_{i=0}^{\bar{j}-1} x_{i,\bar{j}}^{(1)} = \sum_{i=0}^{\bar{j}-1} x_{j,\bar{i}}^{(1)} = \sum_{n=j+1}^{M-1} x_{j,n}^{(1)}. \tag{20}$$

Similarly, using $x_{\bar{j},i}^{(1)} = x_{\bar{i},j}^{(1)}$ followed by the substitution $m=\bar{i}$, one obtains

$$\sum_{i=\bar{j}+1}^{M/2-1} x_{\bar{j},i}^{(1)} = \sum_{i=\bar{j}+1}^{M/2-1} x_{\bar{i},j}^{(1)} = \sum_{m=M/2}^{j-1} x_{m,j}^{(1)}. \tag{21}$$

By plugging (20) and (21) in (19) leads to

$$\sum_{i\in\mathcal{J}} z_{i,j}^{(1)} = \sum_{n=j+1}^{M-1} x_{j,n}^{(1)} + \sum_{i=0}^{M/2-1} x_{i,j}^{(1)} + \sum_{m=M/2}^{j-1} x_{m,j}^{(1)} = \sum_{m=0}^{j-1} x_{m,j}^{(1)} + \sum_{n=j+1}^{M-1} x_{j,n}^{(1)} = 1,$$

where the last equality follows by replacing in (14) i with j, j with n and k with m. With this, the proof is complete. ■

Lemma 3: Assume that the pdf $f(x)$ and the quantizer Q are symmetric about 0. Let the distortion function satisfy $d(x,y)=\rho(|x-y|)$, where ρ is a nondecreasing function. Then, $w_{m,n}^{(l)} \le w_{m,\bar{n}}^{(l)}$ and $w_{m,n}^{(l)} \le w_{n,\bar{m}}^{(l)}$ for all $0\le m<n\le M/2-1$ and $l\in\{1,3\}$.

Proof: In virtue of Lemma 1, one has $w_{m,\bar{n}}^{(l)} = w_{n,\bar{m}}^{(l)}$. Therefore, it is sufficient to prove only that $w_{m,n}^{(l)} \le w_{m,\bar{n}}^{(l)}$. Additionally, $P_{0,m,n} = P_{0,m,\bar{n}}$ since $P(C_n) = P(C_{\bar{n}})$ according to (17). We conclude that we only need to prove that

$$D_{m,n}^{(l)} \le D_{m,\bar{n}}^{(l)}. \tag{22}$$

For this, we first prove the following property.

Property B: For any $y \leq 0$ and measurable set $S \subseteq (-\infty, 0]$, $L(S, y) \leq L(S, -y)$.

To prove the above claim it is sufficient to show that $\rho(|x-y|) \leq \rho(|x+y|)$ for any $x, y \leq 0$. Indeed, when $x, y \leq 0$, one has $-|x+y| = x+y \leq x-y \leq -x-y = |x+y|$, which implies that $|x-y| \leq |x+y|$ and further leads to $\rho(|x-y|) \leq \rho(|x+y|)$ since ρ is nondecreasing.

Let us prove now (22) for the case $l = 1$. Consider first the situation when $y_{m,\bar{n}}^{(1)} \geq 0$. Since $C_m \subseteq (-\infty, 0]$, according to Property B, one has

$$L(C_m, -y_{m,\bar{n}}^{(1)}) \leq L(C_m, y_{m,\bar{n}}^{(1)}). \tag{23}$$

Moreover, the fact that $C_{\bar{n}} = -C_n$, combined with Property A, implies that

$$L(C_n, -y_{m,\bar{n}}^{(1)}) = L(C_{\bar{n}}, y_{m,\bar{n}}^{(1)}). \tag{24}$$

It follows that $D_{m,n}^{(1)} \overset{(a)}{\leq} L(C_m \cup C_n, -y_{m,\bar{n}}^{(1)}) = L(C_m, -y_{m,\bar{n}}^{(1)}) + L(C_n, -y_{m,\bar{n}}^{(1)}) \overset{(b)}{\leq} L(C_m, y_{m,\bar{n}}^{(1)}) + L(C_{\bar{n}}, y_{m,\bar{n}}^{(1)}) = L(C_m \cup C_{\bar{n}}, y_{m,\bar{n}}^{(1)}) = D_{m,\bar{n}}^{(1)}$, where (a) follows from the definition of $D_{m,n}^{(1)}$, while (b) is based on (23) and (24).

Consider now the case $y_{m,\bar{n}}^{(1)} < 0$. Since $C_n \subseteq (-\infty, 0]$, by using Property B followed by Property A, one obtains $L(C_n, y_{m,\bar{n}}^{(1)}) \leq L(C_n, -y_{m,\bar{n}}^{(1)}) = L(C_{\bar{n}}, y_{m,\bar{n}}^{(1)})$. Then the following sequence of relations holds

$$D_{m,n}^{(1)} \leq L(C_m \cup C_n, y_{m,\bar{n}}^{(1)}) = L(C_m, y_{m,\bar{n}}^{(1)}) + L(C_n, y_{m,\bar{n}}^{(1)}) \leq L(C_m, y_{m,\bar{n}}^{(1)}) + L(C_{\bar{n}}, y_{m,\bar{n}}^{(1)}) = D_{m,\bar{n}}^{(1)}.$$

Consider now the case $l = 3$. Since $C_m \subseteq (-\infty, 0]$, $y_n \leq 0$ and $y_{\bar{n}} = -y_n$, according to Property B, one has

$$L(C_m, y_n) \leq L(C_m, y_{\bar{n}}), \tag{25}$$

while Property A implies that

$$L(C_n, y_n) = L(C_{\bar{n}}, y_{\bar{n}}). \tag{26}$$

Applying again Properties B and A leads to

$$L(C_n, y_m) \leq L(C_n, -y_m) = L(C_{\bar{n}}, y_m). \tag{27}$$

Further, relations (25), (26) and (27) imply that $D_{m,n}^{(3)} - D_{m,\bar{n}}^{(3)} = 0.5(L(C_m, y_m) + L(C_m, y_n) + L(C_n, y_m) + L(C_n, y_n)) - 0.5(L(C_m, y_m) + L(C_m, y_{\bar{n}}) + L(C_{\bar{n}}, y_m) + L(C_{\bar{n}}, y_{\bar{n}})) \leq 0$. This completes the proof of the lemma. ■

Lemma 4: Assume that $f(x)$ and the quantizer Q are symmetric about 0 and $y_i \geq 2\mu_i$, for $i \in \mathcal{I}$. Let $d(x, y) = (x-y)^2$. Then, $w_{m,n}^{(2)} \leq w_{m,\bar{n}}^{(2)}$ and $w_{m,n}^{(2)} \leq w_{n,\bar{m}}^{(2)}$ for all $0 \leq m < n \leq M/2 - 1$.

Proof: As in the proof of Lemma 3, we only need to show that $D^{(2)}_{m,n} \leq D^{(2)}_{m,\bar{n}}$. Note that, since $y_{\bar{n}} = -y_n$ and $C_{\bar{n}} = -C_n$, using the definition of $D^{(2)}_{m,\bar{n}}$ and Property A, one obtains

$$\begin{aligned} D^{(2)}_{m,\bar{n}} &= \int_{C_m} \left(x - \tfrac{y_m + y_{\bar{n}}}{2}\right)^2 f(x)\, dx \quad + \int_{C_{\bar{n}}} \left(x - \tfrac{y_m + y_{\bar{n}}}{2}\right)^2 f(x)\, dx \\ &= \int_{C_m} \left(x - \tfrac{y_m - y_n}{2}\right)^2 f(x)\, dx \quad + \int_{C_n} \left(x + \tfrac{y_m - y_n}{2}\right)^2 f(x)\, dx. \end{aligned}$$

Combining the above with the definition of $D^{(2)}_{m,n}$ and using straightforward algebra, leads to $D^{(2)}_{m,n} - D^{(2)}_{m,\bar{n}} = -y_n P(C_m)\,(2\mu_m - y_m) - y_m P(C_n)\,(2\mu_n - y_n) \leq 0$, where the last inequality follows from $y_n, y_m \leq 0$, $y_m \geq 2\mu_m$ and $y_n \geq 2\mu_n$. Now the proof is complete. ■

Lemma 5: Let $l \in \{1, 2, 3\}$. If $w^{(l)}_{m,n} \leq w^{(l)}_{m,\bar{n}}$ and $w^{(l)}_{m,n} \leq w^{(l)}_{n,\bar{m}}$ for all $0 \leq m < n \leq M/2 - 1$, then $F_2(\mathbf{z}^{(1)}) \geq F_1(\mathbf{x}^{(1)})$.

Proof: Recall that F_1 and F_2 denote the cost functions of problems (10) and (11), respectively. Using the definition of $\mathbf{z}^{(1)}$, one obtains

$$F_2(\mathbf{z}^{(1)}) = \sum_{i=0}^{M/2-1} \left(\sum_{j=M/2}^{\bar{i}-1} w^{(l)}_{i,j} \left(x^{(1)}_{i,j} + x^{(1)}_{i,\bar{j}} \right) + w^{(l)}_{i,\bar{i}} x^{(1)}_{i,\bar{i}} \quad + \sum_{j=\bar{i}+1}^{M-1} w^{(l)}_{i,j} \left(x^{(1)}_{i,j} + x^{(1)}_{\bar{j},i} \right) \right). \tag{28}$$

According to the hypothesis, one has $w^{(l)}_{i,j} \geq w^{(l)}_{i,\bar{j}}$ when $M/2 \leq j < \bar{i}$, and $w^{(l)}_{i,j} \geq w^{(l)}_{\bar{j},i}$ when $M/2 \leq \bar{i} < j \leq M - 1$. Plugging these in (28) leads to

$$\begin{aligned} F_2(\mathbf{z}^{(1)}) &\geq \sum_{i=0}^{M/2-1} \left(\sum_{j=M/2}^{\bar{i}-1} w^{(l)}_{i,\bar{j}} x^{(1)}_{i,\bar{j}} + \sum_{j=M/2}^{\bar{i}-1} w^{(l)}_{i,j} x^{(1)}_{i,j} \quad + w^{(l)}_{i,\bar{i}} x^{(1)}_{i,\bar{i}} + \sum_{j=\bar{i}+1}^{M-1} w^{(l)}_{i,j} x^{(1)}_{i,j} + \sum_{j=\bar{i}+1}^{M-1} w^{(l)}_{\bar{j},i} x^{(1)}_{\bar{j},i} \right) \\ &= \sum_{i=0}^{M/2-1} \left(\sum_{j=i+1}^{M-1} w^{(l)}_{i,j} x^{(1)}_{i,j} + \sum_{k=0}^{i-1} w^{(l)}_{k,i} x^{(1)}_{k,i} \right), \end{aligned} \tag{29}$$

where the last equality is obtained in the same manner as (18). Further, relation (15) and Lemma 1 imply that $w^{(l)}_{k,i} x^{(1)}_{k,i} = w^{(l)}_{\bar{i},\bar{k}} x^{(1)}_{\bar{i},\bar{k}}$. By applying this in (29), it follows that

$$\begin{aligned} F_2(\mathbf{z}^{(1)}) &\geq \sum_{i=0}^{M/2-1} \sum_{j=i+1}^{M-1} w^{(l)}_{i,j} x^{(1)}_{i,j} + \sum_{i=0}^{M/2-1} \sum_{k=0}^{i-1} w^{(l)}_{\bar{i},\bar{k}} x^{(1)}_{\bar{i},\bar{k}} \\ &= \sum_{i=0}^{M/2-1} \sum_{j=i+1}^{M-1} w^{(l)}_{i,j} x^{(1)}_{i,j} + \sum_{m=M/2}^{M-1} \sum_{j=m+1}^{M-1} w^{(l)}_{m,j} x^{(1)}_{m,j} = F_1(\mathbf{x}^{(1)}), \end{aligned} \tag{30}$$

where the first equality is obtained by making the substitutions $m = \bar{i}$ and $j = \bar{k}$ in the second nested sum. This observation completes the proof. ■

ACKNOWLEDGMENT

The authors would like to thank the Editor and the anonymous reviewers for their valuable comments and suggestions, which helped improve the quality of the work.

REFERENCES

[1] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Trans. on Sig. Process.*, vol. 48, no. 8, pp. 2439-2451, Aug. 2000.

[2] A. Massoudi, F. Lefebvre, and C. De Vleeschouwer, "Secure and low cost selective encryption for JPEG 2000," *IEEE Int. Symp. on Multimedia*, USA, Dec. 2008, pp. 31-38.

[3] S. Jenisch and A. Uhl, "A Detailed Evaluation of Format-compliant Encryption Methdos for JPEG XR-compressed Images", *EURASIP J. Inform. Security* 2014, 2014:6.

[4] M. Grangetto, E. Magli, and G. Olmo, "Multimedia selective encryption by means of randomized arithmetic coding," *IEEE Trans. Multimedia*, vol. 8, no. 5, pp. 905-917, Oct. 2006.

[5] S. Lian, J. Sun, and Z. Wang, "A novel image encryption scheme based-on JPEG encoding," *Proc. IEEE 8th Int. Conf. Inf. Visualisation*, UK, July 2004, pp. 217-220.

[6] L. Tawalbeh, M. Mowafi, and W. Aljoby, "Use of elliptic curve cryptography for multimedia encryption," *IET Information Security*, vol. 7, no. 2, pp. 67-74, Nov. 2012.

[7] C. Shi, and B. Bhargava, "A fast MPEG video encryption algorithm," *ACM Int. Conf. Multimedia*, pp. 81-88, Sep. 1998.

[8] J. Wen, M. Severa, W. Zeng, M. H. Luttrell, and W. Jin, "A format-compliant configurable encryption framework for access control of video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 12, no. 6, pp. 545-557, June 2002.

[9] B. B. Zhu, C. Yuan, Y. Wang, and S. Li, "Scalable protection for MPEG-4 fine granularity scalability," *IEEE Trans. Multimedia*, vol. 7, no. 2, pp. 222-233, Apr. 2005.

[10] S. Li, G. Chen, A. Cheung, B. Bhargava, and K.-T. Lo, "On the design of perceptual MPEG-video encryption algorithms," *IEEE Trans. on Circuits and Syst. for Video Technol.*, vol. 17, no. 2, pp. 214-223, Feb. 2007.

[11] F. Dufaux and T. Ebrahimi, "Scrambling for privacy protection in video surveillance systems," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 8, pp. 1168-1174, Aug. 2008.

[12] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Secure advanced video coding based on selective encryption algorithms," *IEEE Trans. on Consumer Electron.*, vol. 52, no. 2, pp. 621-629, May 2006.

[13] H. Yin, C. Lin, F. Qiu, J. Liu, G. Min, and B. Li, "CASM: A content-aware protocol for secure video multicast," *IEEE Trans. on Multimedia*, vol. 8, no. 2, pp. 270-277, Nov. 2006.

[14] W. Wang, M. Hempel, D. Peng, H. Wang, H. Sharif, and H.-H. Chen, "On energy efficient encryption for video streaming in wireless sensor networks," *IEEE Trans. on Multimedia*, vol. 12, no. 5, pp. 417-426, Aug. 2010.

[15] Y. Wang, M. Ob-Neill, and F. Kurugollu, "A tunable encryption scheme and analysis of fast selective encryption for CAVLC and CABAC in H.264/AVC," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 9, pp. 1476-1490, Sep. 2013.

[16] M. N. Asghar and M. Ghanbari, "An efficient security system for CABAC bin-strings of H.264/SVC," *IEEE Trans. on Circuits and Syst. for Video Technol.*, vol. 23, no. 3, pp. 425-437, Nov. 2013.

[17] Z. Shahid and W. Puech, "Visual protection of HEVC video by selective encryption of CABAC binstrings," *IEEE Trans. on Multimedia*, vol. 16, no. 1, pp. 24-36, Jan. 2014.

[18] B. Boyadjis, C. Bergeron, B. Pesquet-Popescu, and F. Dufaux, "Extended selective encryption of H.264/AVC (CABAC)- and HEVC-encoded video streams," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 27, no. 4, pp. 892-906, Apr. 2017.

[19] A. I. Sallam, O. S. Faragallah , and E. M. El-Rabaie "HEVC selective encryption using RC6 block cipher technique," *IEEE Trans. on Multimedia*, vol. 20, no. 7, pp. 1636-1644, July 2018.

[20] E. Lam and J. Goodman, "A mathematical analysis of the DCT coefficient distributions for images," *IEEE Trans. Image Process.*, vol. 9, no. 10, pp. 1661–1666, Oct. 2000.

[21] T. Xiang, K. Wong, and X. Liao, "Selective image encryption using a spatiotemporal chaotic system," *Chaos*, vol. 17, no. 2, 2007.

[22] A. Kulsoom, D. Xiao, and A. U. Rehman, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," *Multimedia Tools and Applications*, no. 75, pp. 1-23, 2016.

[23] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," Eur. Phys. J. Plus, vol. 133, no. 8, p. 331, Aug. 2018.

[24] Y. Liu, Z. Qin, and J. Wu, "Cryptanalysis and Enhancement of an Image Encryption Scheme Based on Bit-Plane Extraction and Multiple Chaotic Maps," *IEEE Access*, vol. 7, pp. 74070-74080, May. 2019.

[25] Q. U. Rehman, H. Wang, M. M. A. Shahid, and S. Iqbal, Z. Abbas, and A. Firdous, "A Selective Cross-Substitution Technique for Encrypting Color Images Using Chaos, DNA Rules and SHA-512," *IEEE Access*, vol. 7, pp. 162786-162802, Nov. 2019.

[26] M. Kafi and S. Dumitrescu, "Index assignment optimized for partial encryption," *16th Canadian Workshop on Information Theory (CWIT)*, Canada, 2019, vol.1.

[27] J. Max, "Quantizing for minimum distortion," *IRE Trans. on Inf. Theory*, vol. 6, no. 1, pp. 7-12, Mar. 1960.

[28] J. C. Kieffer, "Uniqueness of locally optimal quantizer for log-concave density and convex error weighting function," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 1, pp. 42-47, Jan. 1983.

[29] C. H. Papadimitriou and K. Steiglitz, *Combinatorial Optimization: Algorithms and Complexity*, Prentice-Hall, Englewood Cliffs, New Jersey, 1982.

[30] I. E. G. Richardson *H.264 and MPEG-4 Video Compression. Video Coding for Next-generation Multimedia*, John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, England, 2003.

[31] D. Marpe, H. Schwarz, and T.Wiegand, "Context-adaptive binary arithmetic coding in the H.264/AVC video compression standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, pp. 620–636, July 2003.

[32] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," *IEEE Trans. Image Proc.*, vol. 13, no. 4, pp. 600-612, Apr. 2004.

[33] M. Kafi and S. Dumitrescu, "Binary code optimized for partial encryption. Supplementary figures", http://www.ece.mcmaster.ca/∼sorina/papers/TCOMPE2020SUP.pdf.

[34] https://developers.googleblog.com/2012/08/lossless-and-transparency-modes-in-webp.html.