PAPER *Special Section on Picture Coding and Image Media Processing*

WPE-MO: Prediction Error-Propagated Encryption with Modulo Operator for JPEG Texture Protection

Kosuke SHIMIZU[†a)] ***and*** **Taizo SUZUKI**[††b)]**,** ***Members***

SUMMARY We propose a JPEG format-compliant encryption method in the quantized discrete cosine transform (QDCT) domain for texture protection, called Prediction Error-Propagated Encryption with Modulo Operator (PEPE-MO = WPE-MO, by pronouncing 'W' as 'double'). In the QDCT domain, both the direct current (DC) coefficients, which contain structure information, and alternating current (AC) coefficients, which contain texture information, are encrypted with newly placed prediction, encryption, and reconstruction modules. The resulting propagated prediction error reinforces texture protection. To ensure JPEG compatibility, WPE-MO incorporates a modulo operator into the prediction and reconstruction modules, circulating coefficients within the JPEG-encodable value range. Additionally, to balance attack resilience and coding efficiency, two adjustable parameters are introduced: random length interval (RLI) and random step size (RSS). Experiments on JPEG image encryption demonstrate that WPE-MO exhibits high attack resilience with minimal degradation in coding efficiency. In particular, WPE-MO resists ciphertext-only attacks, including brute-force and replacement attacks, with approximately 19.55% degradation in coding efficiency, as measured by the Bjøntegaard-delta rate, through careful selection of RLI and RSS.

key words: *format-compliant encryption, JPEG texture protection, modulo operator, prediction error propagation*

1. Introduction

Format-compliant encryption (FE) is a technology used to visually protect images[i] while preserving their content format, such as JPEG, the de-facto standard for image coding. Protected (encrypted) images can be displayed with a normative decoder that can decode only the original format. Since JPEG is widely used for storing and sharing photos on social networking services (SNSs) such as 𝕏 (formerly Twitter), Instagram, and Facebook, JPEG format-compliant encryptions (JPEG-FEs) are particularly useful for protecting images shared on these platforms. Note that some existing JPEG-FEs may introduce unintended additional distortions in decompressed and decrypted images in exchange for high visual confidentiality. To mitigate these distortions, several JPEG-FEs [1]–[6] have been proposed. However, due to its structure, the encryption-then-compression approach [1], [2] cannot completely avoid these distortions. Additionally, the syntax domain approach [3]–[6] is limited to using only a Huffman coder, although an arithmetic coder is available in JPEG.

To minimize additional distortions, the quantized discrete cosine transform (QDCT) domain approach [7]–[10] has received attention. The QDCT domain is obtained by decomposing an image into direct current (DC) and alternating current (AC) coefficients through the discrete cosine transform (DCT) and quantizing them. Since FEs are typically expected to achieve high confidentiality regarding the statistical properties of the original image, we review JPEG-FEs in the QDCT domain based on the following criteria:

1) Changing values (of original nonzero coefficients)
2) Changing positions (of original nonzero coefficients)
3) Changing the ratio of zero and nonzero coefficients

and aim to meet all of these criteria.[ii] Once differential pulse-code modulation (DPCM) and run-length encoding (RLE) are applied after the DCT, the positions of the original coefficients are fixed, making criterion 2) somewhat difficult to meet. Thus, we utilize the QDCT domain immediately before applying the DPCM, RLE, and either Huffman or arithmetic coding to the DC and AC coefficients. Table 1 summarizes how JPEG-FEs in the QDCT domain [7]–[11][iii] related to the criteria. Many existing methods, such as random sign flip (RSF) [7], full inter-block shuffling (FIBS) [8], and run-level pair scrambling (RPS) [9], [11], only partially meet the criteria. Whereas bitcuboid-based encryption (BE) [10] meets all criteria without introducing additional distortions, it was originally designed to fine-tune the perceptual degradation in encrypted images rather than ensuring high confidentiality.

Table 1 JPEG-FEs in the QDCT domain and the criteria.

Criteria	RSF [7]	FIBS [8]	RPS [9]	BE [10]	Ours
1)	✓			✓	✓
2)		✓	✓	✓	✓
3)				✓	✓

Manuscript received January 10, 2025.
Manuscript revised April 30, 2025.
Manuscript publicized June 9, 2025.

[†]Faculty of Engineering, Gifu University, Gifu-shi, 501–1193 Japan.
[††]Institute of Systems and Information Engineering, University of Tsukuba, Tsukuba-shi, 305–8573 Japan.
a) E-mail: shimizu.kosuke.x5@f.gifu-u.ac.jp
b) E-mail: taizo@cs.tsukuba.ac.jp

DOI: 10.1587/transinf.2025PCP0005

[i]While FE can also protect videos, this study focuses on its use with images.

[ii]Criterion 2) refers to generally changing the position of coefficients, either within a subband or across subbands. It differs from criterion 1) in that the original values are preserved while their positions are altered.

[iii]Partial approaches [9], [11] are implemented in the post-DPCM QDCT domain, where only DPCM (without RLE or Huffman/arithmetic coding) is applied.

We revisit the concept of resilient JPEG-FE. The JPEG-FEs are designed to protect both structure and texture information because humans often recognize objects by perceiving these types of information. Many existing JPEG-FEs encrypt the DC coefficients, which contain structure information, in the residual state generated by DPCM. These encryptions are highly resilient against various attacks and also conceal the AC coefficients, which contain texture information. However, since the AC coefficients are not encrypted, these approaches are vulnerable to attacks such as the DC deletion attack described later; the unencrypted texture information may reveal potential vulnerabilities. In addition, *direct* encryptions for AC coefficients that ignore the statistical properties of the original images remain vulnerable to attacks. To achieve higher confidentiality for texture information, a new *residual* encryption for AC coefficients should be designed, similar to many DC coefficient encryptions.

We propose a JPEG-FE in the QDCT domain for texture protection, called Prediction Error-Propagated Encryption with Modulo Operator (PEPE-MO = WPE-MO, by pronouncing 'W' as 'double'). Both the DC and AC coefficients are encrypted with newly placed prediction (DPCM), encryption, and reconstruction (inverse DPCM) modules in the QDCT domain. The prediction module generates predicted residuals, the encryption module converts the predicted residuals into encrypted residuals (prediction errors), and the reconstruction module converts them into encrypted coefficients. This process propagates the prediction errors in the encoder to reinforce texture protection. WPE-MO meets the three criteria (i.e., changing values, positions, and ratio of zero and nonzero coefficients) for texture protection. Furthermore, it is highly customizable because each module works independently. To ensure compatibility with JPEG, i.e., JPEG-encodable encrypted coefficients, we introduce a modulo operator that circulates the coefficients within the acceptable range for JPEG in the prediction and reconstruction modules; here, the term "circulate" refers to cycling the processed value within the specified range (let one cycle between the value range). Additionally, to balance attack resilience and coding efficiency, we use two types of adjustable parameters: a random length interval (RLI) and a random step size (RSS). Experiments on a JPEG coder demonstrate both its attack resilience and its coding efficiency.

A preliminary study [12] focused on encrypting only the AC coefficients and showed that the method is not fully compatible with the JPEG format. In this study, we propose a new method that encrypts both the DC and AC coefficients while theoretically ensuring JPEG format compatibility. In particular, we use a modulo operator to ensure compatibility and introduce adjustable parameters (i.e., RLI and RSS) to balance resilience and coding efficiency.

The remainder of this paper is organized as follows: Section 2 reviews fundamental techniques, including JPEG and WPE. Section 3 details our WPE-MO. Section 4 presents experimental results evaluating the attack resilience and coding efficiency of WPE-MO. Section 5 concludes this paper.

2. Review

2.1 JPEG and DPCM

JPEG is a lossy image compression algorithm, though some parts use lossless techniques. The algorithm consists of following steps:

1) Convert the input RGB image into luma and chroma (YCbCr) components using a color transform; the chroma components are downsampled[iv].
2) Apply the DCT to each 8×8 block of YCbCr components, producing DCT coefficients with one DC coefficient and 63 AC coefficients.
3) Quantize the DCT coefficient blocks using a quality factor Q. The resulting domain is reffered to as "QDCT domain."
4) Apply DPCM to DC coefficients and RLE to AC coefficients, followed by Huffman encoding.
5) Packetize the encoded DC and AC coefficients into the entropy-coded segment (ECS) of the JFIF file structure.

Steps 1) to 3) are lossy due to chroma downsampling and precision reduction, while the steps 4) and 5) are lossless. The Huffman encoder can be replaced with an arithmetic encoder.

To incorporate the encryption into the lossless process in step 4), we provide more details on the DPCM in that step. The DPCM calculates the residuals of quantized DC coefficients (DC residuals) between blocks. Here, let $\{c_i(1,1)\}_{i=1}^n$ and $\{\widetilde{c}_i(1,1)\}_{i=1}^n$ denote the DC coefficients from the 8×8 QDCT coefficient blocks $\{\mathbf{c}_i\}_{i=1}^n$, where $\mathbf{c}_i := \{c_i(j,k)\}_{j,k=1,1}^{8,8}$ ($c_i(j,k)$: a (j,k) subband coefficient in the i-th block), and the DC residuals, respectively. DPCM is performed as

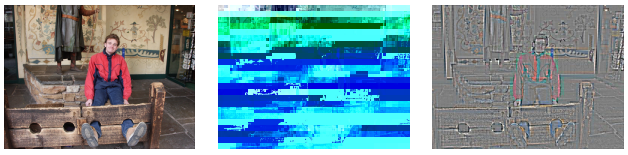
$$\widetilde{c}_i(1,1) = \begin{cases} c_i(1,1) & \text{if } i = 1 \\ c_i(1,1) - c_{i-1}(1,1) & \text{if } i > 1 \end{cases}. \tag{1}$$

Since the DC residual magnitudes $\{|\widetilde{c}_i(1,1)|\}_{i=1}^n$ are typically smaller than the original DC coefficients $\{|c_i(1,1)|\}_{i=1}^n$, the residuals can be efficiently compressed with Huffman encoding and packed into the ECS segment.

2.2 Prediction Error-Propagated Encryption for DC Coefficients

Since DPCM is a predictor, the encrypted DC residuals can

[iv] JPEG officially supports three downsampling options, [4 : 2 : 0] (default), [4 : 2 : 2], and [4 : 4 : 4]. In this study, we used the default option [4 : 2 : 0], which indicates to downsample the sizes of chroma components by 2x both vertically and horizontally.



(a) (b) (c)

Fig. 1 Encrypted and attacked images: (a) original, (b) encrypted with DC-WPE, and (c) attacked with DC deletion attack.

be regarded as "prediction errors". These prediction errors propagate sequentially through inverse DPCM in the decoder. This WPE for DC coefficients (DC-WPE), also known as the masking effect [13], visually protects the texture information of the original image (Fig. 1 (b)). Here, the inverse DPCM to the DPCM (without encryption) in (1) is performed as

$$c_i(1,1) = \begin{cases} \widetilde{c}_i(1,1) & \text{if } i = 1 \\ \widetilde{c}_i(1,1) + \widetilde{c}_{i-1}(1,1) & \text{if } i > 1 \end{cases} \tag{2}$$

and the inverse DPCM to the DPCM with encryption (without decryption) is performed as

$$c_i(1,1) \neq c'_i(1,1) = \begin{cases} \mathcal{E}(\widetilde{c}_i(1,1)) & \text{if } i = 1 \\ \mathcal{E}(\widetilde{c}_i(1,1)) + c'_{i-1}(1,1) & \text{if } i > 1 \end{cases}, \tag{3}$$

where $\mathcal{E}(\cdot)$ is an encryption function. In other words, encrypting DC residuals disrupts inverse DPCM.

2.3 DC Deletion Attack and Its Countermeasure

The DC deletion attack is a type of replacement attacks that replaces all DC coefficient values with zeros to reveal the texture information in the AC coefficients (Fig. 1) [3]. Although DC-WPE conceals the original image texture (Fig. 1 (b)), it is easily removed by the DC deletion attack (Fig. 1 (c)). This highlights the need for AC coefficient encryption, as DC coefficient encryption alone cannot resist this attack. Nonetheless, the number of nonzero AC coefficients per block can be exploited by sketch attack, if the block-wise ratio of zero and nonzero AC coefficient numbers remains unchanged [9]; the relationship between the number of nonzero coefficients and the sketch attack is discussed in Sect. 3.5. Consequently, the encryption should simultaneously change the values, positions, and ratio of zero and nonzero coefficients, even at the expense of JPEG coding efficiency. In contrast, lightweight approaches for AC coefficients, e.g., RSF [7], only change the sign of coefficients, leaving their absolute values unchanged. Other approaches, e.g., FIBS [8], shuffle the AC coefficients, changing their positions but preserving the original values unchanged. However, the unchanged absolute and/or original values may still allow attackers to recover some texture information. Even when RSF and FIBS are combined, the ratio of zero and nonzero coefficients remains a statistical property that can be exploited.

2.4 Range-Exceeding Problem

Reconsidering that DC-WPE results from reconstructing encrypted residuals, we find that any form of WPE can be induced by arbitrary prediction and reconstruction modules. However, encoding the reconstructed AC coefficients after WPE is challenging because the original values oscillate (i.e., lack smoothness), causing the propagated values easily exceed the encodable range for the JPEG coder. This range-exceeding problem can lead to not only coding failure but also incorrect decryption of the encrypted QDCT coefficients. Thus, the reconstructed coefficients must remain strictly within the encodable range.

3. Prediction Error-Propagated Encryption with Modulo Operator

3.1 Motivation

As discussed earlier, encryption in the QDCT domain is essential. While common JPEG-FEs are often implemented after Huffman encoding, they lack versatility for other domains, such as arithmetic encoding. Encrypting AC coefficient positions after RLE encoding is also challenging because RLE groups AC coefficients into run-level pairs. Therefore, encryption should be applied in the QDCT domain to protect as many statistical properties as possible. As described in Sect. 2.3, QDCT domain encryption is required for both DC and AC coefficients.

As described in Sect. 1, the QDCT domain approach must simultaneously change the values, positions, and ratio of zero and nonzero coefficients. One way to achieve this is by camouflaging the coefficient values. To this end, we developed a method that propagates the prediction errors for both DC and AC coefficients by newly placing prediction, encryption, and reconstruction modules in the QDCT domain. Additionally, as discussed in Sect. 3.3, we theoretically ensure that the range-exceeding problem will not occur by incorporating a modulo operator, which circulates the reconstructed values within the JPEG-encodable range, into the prediction and reconstruction modules. Furtheremore, we balance attack resilience and coding efficiency by introducing RLI and RSS into the prediction and reconstruction modules.

3.2 Encryption Framework

This subsection describes the prediction, encryption, and reconstruction modules that compose WPE-MO (Fig. 2). To address the range-exceeding problem, we incorporate a modulo operator that circulates reconstructed coefficients within the encodable range in the prediction and reconstruction modules.

The prediction module converts a given coefficient c into a predicted residual $\widetilde{c}$ using another coefficient. The procedure is as follows. First, the signed coefficient range is

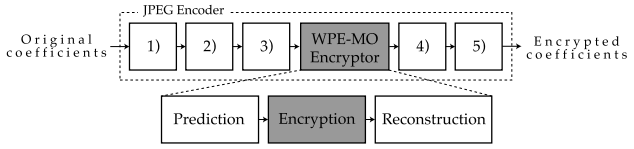


Fig. 2 Framework of WPE-MO (encryptor): prediction, encryption, and reconstruction modules; the process of 1) to 5) means the JPEG encoding process of Sect. 2.1.

shifted into an unsigned range as

$$c_i^+(j,k) = c_i(j,k) + 2^{D-1}, \tag{4}$$

where $c_i^+(j,k)$ is a nonnegative D-bit QDCT coefficient. Next, $\{c_i^+(j,k)\}_{i=1}^n$ is predicted with modulo-operated DPCM[v] as

$$\widetilde{c}_i^+(j,k) = \begin{cases} c_i^+(j,k) & \text{if } i = 1 \\ \left(c_i^+(j,k) - c_{i-1}^+(j,k)\right) \bmod 2^D & \text{if } i > 1 \end{cases}. \tag{5}$$

Finally, the range is shifted back as

$$\widetilde{c}_i(j,k) = \widetilde{c}_i^+(j,k) - 2^{D-1}. \tag{6}$$

The encryption module converts the residual $\widetilde{c}$ into the encrypted version $\widetilde{c}'$. The predicted residual $\widetilde{c}_i(j,k)$ is encrypted as

$$\widetilde{c}_i'(j,k) = \mathcal{E}(\widetilde{c}_i(j,k)). \tag{7}$$

While various encryption algorithms can be used for the encryption function $\mathcal{E}(\cdot)$ in WPE-MO, we chose RSF as a lightweight algorithm:

$$\mathcal{E}(\widetilde{c}_i(j,k)) := \begin{cases} \widetilde{c}_i(j,k) & \text{if } \text{rand}(i)\&1 = 0 \\ -\widetilde{c}_i(j,k) & \text{if } \text{rand}(i)\&1 = 1 \end{cases}, \tag{8}$$

where rand(i) (i is the block order) is a random number generated by a pseudo random number generator (PRNG) initialized with an encryption key. While RSF alone induces limited texture degradation, WPE-MO reinforces this effect through its propagation property, as described below.

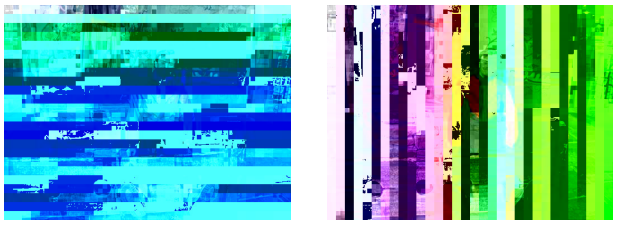
The reconstruction module converts the encrypted residual $\widetilde{c}'$ into an encrypted coefficient c'. To address the range-exceeding problem, a modulo operator is incorporated as follows. First, the coefficient range of $\widetilde{c}_i'(j,k)$ is re-shifted as

$$\widetilde{c}_i'^+(j,k) = \widetilde{c}_i'(j,k) + 2^{D-1}. \tag{9}$$

Second, inverse DPCM is applied to $\widetilde{c}_i'^+(j,k)$ as

$$c_i'^{1/\epsilon}(j,k) = \begin{cases} \widetilde{c}_i'^+(j,k) & \text{if } i = 1 \\ \widetilde{c}_i'^+(j,k) + c_{i-1}'^{1/\epsilon}(j,k) & \text{if } i > 1 \end{cases}, \tag{10}$$

[v]Throughout this paper, we use the modulo operator mod in combination with abs() to denote the distance from a reference point in the modular ring. In particular, we treat the sign separately and interpret mod as the C-style remainder.



(a) (b)

Fig. 3 Different directional DPCMs in WPE-MO: (a) horizontal DPCM and (b) vertical DPCM.

Table 2 QDCT coefficient ranges in each module of WPE-MO.

Prediction and encryption modules	
Module	Range
1) Original	$[-2^{D-1},\ 2^{D-1}-1]$
2) Range-shifted	$[0,\ 2^D-1]$
3) Predicted	$[-2^D+1,\ 2^D-1]$
4) Modulo-applied	$[-2^D+1,\ 2^D-1]$
5) Range-shifted back	$[-1.5\cdot 2^D+1,\ 2^{D-1}-1]$
6) RSF-applied	$[-1.5\cdot 2^D+1,\ 1.5\cdot 2^D-1]$
Reconstruction module	
Module	Range
1) Input	$[-1.5\cdot 2^D+1,\ 1.5\cdot 2^D-1]$
2) Range-reshifted	$[-2^D+1,\ 2^{D+1}-1]$
3) Reconstructed	$\mathbb{Z}^+$ in most cases
4) Modulo-applied	$[0,\ 2^D-1]$
5) Range-reshifted back	$[-2^{D-1},\ 2^{D-1}-1]$

where the superscript $1/\epsilon$ ($\epsilon \simeq 0$) indicates a huge value that may exceed the JPEG-encodable range. Third, the value of $c_i'^{1/\epsilon}(j,k)$ is circulated using the modulo operator as

$$\{c_i'^+(j,k)\}_{i=1}^n = \left\{c_i'^{1/\epsilon}(j,k) \bmod 2^D\right\}_{i=1}^n. \tag{11}$$

Finally, the range of $c_i'^+(j,k)$ is reconstructed as

$$c_i'(j,k) = c_i'^+(j,k) - 2^{D-1}. \tag{12}$$

Since arbitrary encrypted residuals propagate during reconstruction, as shown in (10), WPE-MO disrupts all statistical properties in the QDCT coefficient domain.

Remarks: Prediction error propagation, a key property in this study, is induced by the reconstruction module. Thus, any encryption module, such as RSF and FIBS, and any prediction module, such as DPCM and LOCO-I [14], can be placed without constraint. The direction of propagation errors can propagate horizontally and vertically for DC coefficients, as shown in Fig. 3. For simplicity, this study uses DPCM and RSF, two of the simplest prediction and encryption algorithms.

3.3 Range Preserving Feature

The ranges of the QDCT coefficients in the WPE-MO modules are summarized in Table 2. Each case is described below. RSF encryption between the prediction and reconstruction modules does not change the range.

In the prediction and encryption modules, the input QDCT coefficient range $[-2^{D-1},\ 2^{D-1}-1]$ is initially shifted to $[0,\ 2^D-1]$ by adding 2^{D-1}. As a result, the range of predicted QDCT coefficient residuals becomes $[-2^{D-1}+1,\ 2^D-1]$ due to subtracting the maximum coefficient $2^{D-1}-1$ from 0 in the worst case. The residual range remains unchanged after applying the modulo operator, which calculates the remainder when divided by 2^D as

$$\beta = \mathrm{sgn}(\alpha)\left(\mathrm{abs}(\alpha) \bmod 2^D\right) \quad (\alpha, \beta \in \mathbb{Z}), \tag{13}$$

where α and β are input and output values, respectively. The residual range in the reconstruction becomes $[-1.5 \cdot 2^D + 1,\ 2^{D-1}-1]$ due to subtracting 2^{D-1} from the range $[-2^D+1,\ 2^D-1]$. Flipping the minimum value $-1.5\cdot 2^D+1$ with RSF may extend the range to $[-1.5\cdot 2^D+1,\ 1.5\cdot 2^D-1]$ in the worst case.

In reconstruction module, the range of encrypted residuals is re-shifted to $[-2^D+1,\ 2^{D+1}-1]$ by adding 2^{D-1}. Although this range allows negative values, experiments confirm that all residuals become positive during propagation. Negative values are eliminated due to the following:

- Propagation involves simple addition, accumulating values from previous (reconstructed) coefficients.
- Large-magnitude samples rarely appear in the early stages of propagation.
- Positive sums quickly surpass and eliminate negative residuals.

Positive values are circulated within the range $[0,\ 2^D-1]$ by the modulo operator and reconstructed to $[-2^{D-1},\ 2^{D-1}-1]$ by subtracting 2^{D-1}. Thus, the final QDCT coefficient range is $[-2^{D-1},\ 2^{D-1}-1]$, ensuring JPEG compatibility for both encryptor and decryptor in WPE-MO.

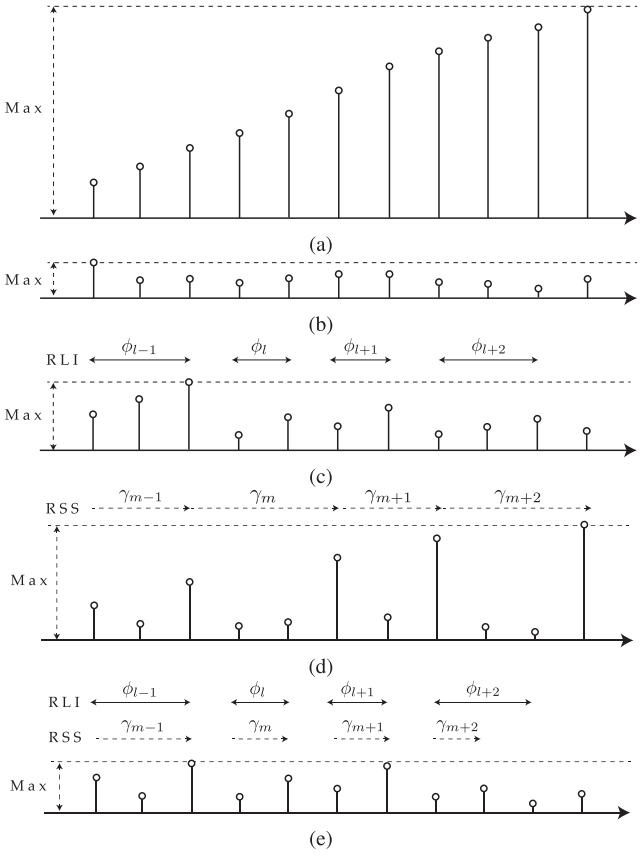


Fig. 4 Variance of prediction and reconstruction modules: (a) original signal, (b) original residual signal, (c) reconstruction with only RLI, (d) random discrete reconstruction with only RSS, and (e) random discrete reconstruction with a combination of RLI and RSS.

3.4 Balancing Attack Resilience and Coding Efficiency

Encryption techniques often disrupt coding efficiency, requiring JPEG-FEs, especially in the QDCT domain, to carefully balance attack resilience and coding efficiency. The modulo operator in WPE-MO ensures that reconstructed coefficient values remain within the acceptable JPEG range, ensuring full format compatibility and correct decryption. However, despite of the use of the modulo operator, the magnitudes of nonzero AC coefficients can increase significantly, leading to a substantial rise in the file size of encrypted-compressed image tends to increase significantly as well. To address this, we introduce two adjustable parameters for the prediction and reconstruction modules in WPE-MO: RLI and RSS.

The random length interval (RLI) is an adjustable parameter $\phi_l \in \mathbb{Z}_{[N_1,\ N_2]} (1 \le l \le n)$ that intermittently or randomly blocks prediction error propagation (Fig. 4 (c)). In WPE-MO with RLI, $N_1 \le \phi_l \le N_2$ coefficients are predicted at a time. The value of ϕ_l is determined randomly by PRNG. Therefore, $N_1 \in \mathbb{Z}_{[0,\,n-1]}$ and $N_2 \in \mathbb{Z}_{[1,\,n]}$, with the condition $N_1 < N_2$. This irregular blocking suppresses increases in the magnitudes of propagated signals, preserving coding efficiency. However, there is a trade-off between attack resilience and coding efficiency depending on the interval range. Shorter intervals better outline the original image, making it easier to identify attack points, while longer intervals increase magnitudes of AC coefficients, raising bitrate overhead. Without the modulo operators in the prediction and reconstruction modules, the lower/upper interval bounds $[N_1,\ N_2]$ must be set experimentally to ensure reconstructed coefficient values stay within range. Let $\mathbf{I}_{DC}$ and $\mathbf{I}_{AC}$ be predefined sections for the DC and AC coefficients, respectively, where intervals for the prediction and reconstruction modules are randomly determined. For example, $\mathbf{I}_{AC} = [0,\ 15]$ means that $\phi_l (\in \mathbb{Z}_{[0,\ 15]})$ AC coefficients are predicted each time through the encryption and decryption.

The random step size (RSS) is an adjustable parameter $\gamma_m \in \mathbb{Z}_{[1,\ n]}$ $(m \in \mathbb{Z}_{[1,\ n]})$ that determines the positions of the same subband of the QDCT coefficients to be predicted and reconstructed (Fig. 4 (d)). It controls how often the magnitudes of propagated signals increase. Specifically, the target coefficient is predicted using a previous coefficient at a random position:

$$\widetilde{c}^{+}_{i+\gamma_m}(j,k) = \begin{cases} c^{+}_{i}(j,k) & \text{if } i = 1 \\ (c^{+}_{i+\gamma_m}(j,k) - c^{+}_{i}(j,k)) \bmod 2^{D} & \text{if } i > 1 \end{cases}. \quad (14)$$

The predicted residual $\widetilde{c}^{+}_{i(j,k)}$ is reconstructed as

$$c'^{1/\epsilon}_{i+\gamma_m}(j,k) = \begin{cases} \widetilde{c}'^{+}_{i}(j,k) & \text{if } i = 1 \\ \widetilde{c}'^{+}_{i+\gamma_m}(j,k) + c'^{1/\epsilon}_{i}(j,k) & \text{if } i > 1 \end{cases}. \quad (15)$$

Since γ_m is the m-th random number generated by the PRNG, the same RSS values can be generated synchronously in both the prediction and reconstruction modules. Increasing γ_m propagates encrypted residuals to more distant residuals, resulting in moderate bitrate overhead. By mixing residual signals with original signals during random discrete prediction, it becomes difficult for attackers to distinguish between propagated and non-propagated signals. Let $\mathbf{S}_{DC}$ and $\mathbf{S}_{AC}$ be predefined sections for DC and AC coefficients, respectively, where step sizes for the prediction and reconstruction modules are randomly determined. For example, $\mathbf{S}_{AC} = [1,\ 10]$ means $\gamma_m \in \mathbb{Z}_{[0,\ 10]}$ in (15) for AC coefficients.

We recommend using RLI and RSS in combination (Fig. 4 (e)). This combination is more effective than using either method alone, as RLI suppresses the magnitudes of propagated signals, while RSS suppresses the frequency of magnitude increases. RLI does not control how often magnitudes increase within intervals, and RSS does not control the number of coefficients predicted or reconstructed. Thus, combining RLI and RSS allows for better control of the total number of coefficients predicted and the total number of predictions.

3.5 Against Attacks

Since most JPEG-FEs are classified as symmetric-key cryptosystems, they are vulnerable to ciphertext-only attacks (COAs) that attempt to approximate the original content (plaintext) from encrypted content (ciphertext). Existing COAs against JPEG-FEs include replacement and brute-force attacks, as discussed below. To ensure security, FEs must resist these COAs.

A replacement attack replaces encrypted coefficient values with constant values. This study focuses on the DC deletion attack described in Sect. 2.3 and the sketch attack [9]. Since AC residuals encrypted with WPE-MO are further propagated by the reconstruction module, the RSF used in WPE-MO provides stronger texture protection against DC deletion attacks than conventional RSF alone. In the sketch attack, each 8×8 QDCT coefficient block is assigned a uniform shade, representing a single "point" from a global perspective; these points can sometimes outline the original image. WPE-MO is effective against sketch attacks as it changes the number of nonzero QDCT coefficients per block. It has been shown in [9] that if the ratio of zero to non-zero coefficients remains unchanged, this ratio can be exploited for sketch attacks that use the number of zero and non-zero coefficients. By proposing an encryption method that does not alter the number of non-zero coefficients per block, the bit length of DC residual values, or the DC/AC categories, [9] appears to have nearly optimized the balance between visual obfuscation strength and coding efficiency. Nevertheless, the number of non-zero coefficients in each block of the encrypted JPEG file remains the same as in the original image. In [9], although the positions of AC blocks are shuffled, the number of non-zero AC coefficients within each block after shuffling is not changed, in order to preserve coding efficiency. On the other hand, WPE-MO randomizes the absolute values of the AC coefficients to modify this count (or ratio) as an alternative, while maintaining a balance with coding efficiency by tuning the encryption parameters, RLI and RSS. Section 4.1 discusses WPE-MO's resilience against DC deletion and sketch attacks.

Next, consider WPE-MO's resilience against brute-force attacks. Suppose all AC coefficients in the same subband are predicted at once using DPCM, without RLI or RSS, and RSF is applied as the encryption module. To decrypt, an attacker must guess the signs of N coefficients, requiring 2^N attempts. If $2^N \geq 2^{256} \Rightarrow N \geq 256$, i.e., more than 256 signs are encrypted, brute-force guessing becomes practically impossible in real time[vi]. Thus, WPE-MO is inherently secure against brute-force attacks and no further measures are needed.

4. Experiments

The experiments examined WPE-MO's attack resilience and its effect on coding efficiency. Section 4.1 shows resilience against COAs, while Sect. 4.2 shows coding efficiency under different conditions. Section 4.3 presents statistical analyses of WPE-MO's properties. Table 3 summarizes the tested versions of WPE-MO. The UCID dataset [17] was used for the test images, and *libjpeg* [18] was used for the standard JPEG software. The procedure was as follows:

1) Compress a test image with the JPEG encoder while encrypting QDCT coefficients using JPEG-FEs. The JPEG quality factor was set to $Q = 10, 20, \cdots, 90$.

2) Measure the bitrate [bits/pixel (bpp)] of the JPEG image.

3) Decompress the JPEG image while decrypting the QDCT coefficients using JPEG-FEs.

Table 3 Tested versions of WPE-MOs.

Method name	RLI		RSS	
	$\mathbf{I}_{DC}$	$\mathbf{I}_{AC}$	$\mathbf{S}_{DC}$	$\mathbf{S}_{AC}$
W/o All	n/a	n/a	n/a	n/a
W/o RSS	[0, 500]	[0, 15]	n/a	n/a
W/o RLI	n/a	n/a	1	[1, 5]
Type-I	[400, 500]	[20, 40]	1	[1, 5]
Type-II	[100, 200]	[10, 20]	1	[1, 5]

[vi] 2^{256} represents the number of attempts required to break 256-bit Secure Hash Algorithm (SHA) digests [15], which the National Institute of Standards and Technology (NIST) considers secure [16].

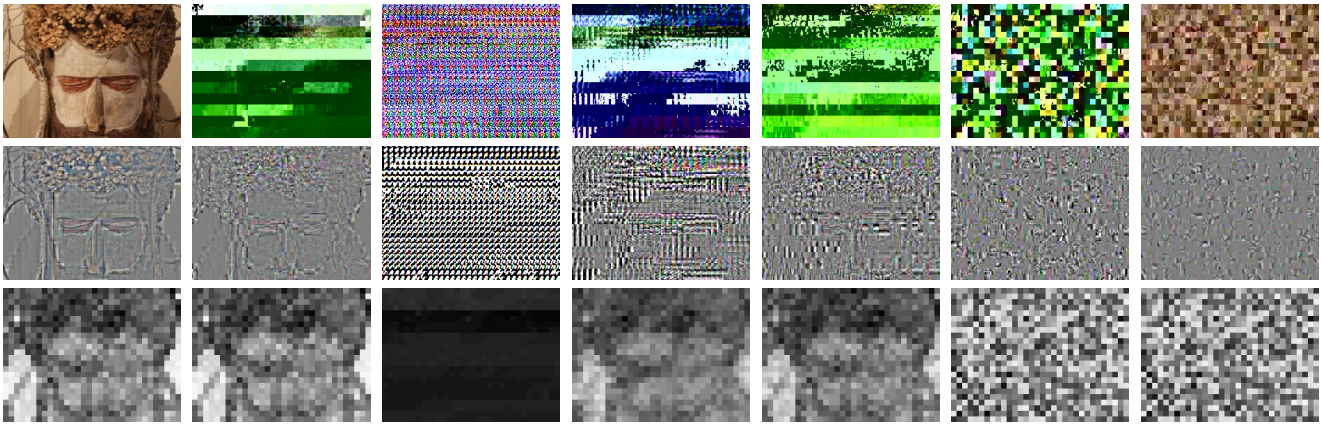


Fig. 5 Resilience against replacement attacks (*#045*, JPEG $Q = 70$): (top-to-bottom) original and encrypted images, DC-deletion-attacked ones, and sketch-attacked ones and (left-to-right) original, RSF [7], W/o All, W/o RSS, Type-I, Type-I+global shuffling, and only global shuffling.

Table 4 BD-rates [%] and BD-PSNRs [dB] at the different directional DPCMs in WPE-MO for DC coefficients.

Image	Horizontal DPCM		Vertical DPCM	
	BD-rate	BD-PSNR	BD-rate	BD-PSNR
#001	**0.06**	**−0.00**	5.97	−0.30
#021	**0.09**	**−0.00**	3.10	−0.14
#041	**0.12**	**−0.01**	5.22	−0.25
#061	**0.05**	**−0.00**	6.55	−0.29
#081	**0.04**	**−0.00**	4.67	−0.27
⋮	⋮	⋮	⋮	⋮
Avg.	**0.09**	**−0.00**	4.81	−0.24

4) Measure the peak signal-to-noise ratio (PSNR) [dB] between the original and decompressed images.

5) Iterate steps 1)–4) for all test images and compute the average values.

The value of D is empirically determined by checking the encoding profile and the actual output of the software implementation. In this study, we set $D = 10$, since in our preliminary examination with Q values up to 90, the test images were fully decrypted when $D = 10$.

4.1 Resilience against Replacement Attacks

This subsection analyzes WPE-MO's resilience against replacement attacks on JPEG images.

First, we analyzed resilience against DC deletion attack by examining the results. As shown in the first and second columns of Fig. 5, simple RSF offered limited texture protection. While W/o All provided the strongest texture protection, it was ineffective in terms of coding efficiency, as described in Sect. 4.2. While W/o RSS appeared to offer sufficient texture protection, it was ineffective for smooth images because propagating AC residuals to adjacent blocks thickened image contours. Type-I moderately obscured contours, even in such cases.

Next, we analyzed WPE-MO's resilience against sketch attack by reviewing the results. The sketch attack counts the number of nonzero AC coefficients in each block [9]. As shown in the first and second columns of Fig. 5, simple RSF provided minimal texture protection. While W/o All largely removed sketch contours, W/o RSS moderately blurred them. Type-I distributed shading of the sketched image from the foreground to the background, efficiently blurring areas where multiple blocks were adjacent. The combination of WPE-MO and existing global shuffling approaches [8], [9] completely prevents this attack, as shown in the right-most two columns of Fig. 5.[vii] Type-I provides the option to propagate the signal over longer intervals compared to Type-II, and the longer the propagation interval, the stronger the visual obfuscation effect becomes. For this reason, Type-II is expected to cause weaker visual obfuscation

Table 5 BD-rates [%] at the different $\mathbf{I}_{AC}$ in WPE-MO Type-II.

Image	[0, 15]	[10, 15]	[0, 10]	[0, 5]	[0, 3]	W/o All
#001	14.42	18.98	8.41	2.78	**0.86**	654.45
#021	11.01	14.43	6.81	2.33	**0.68**	460.82
#041	13.41	17.89	8.27	2.72	**0.95**	544.20
#061	13.04	18.06	8.29	2.69	**1.03**	682.42
#081	12.86	17.04	7.75	2.56	**0.71**	632.11
⋮			⋮			
Avg.	12.19	16.30	7.53	2.57	**0.79**	570.82

Table 6 BD-rates [%] at the different $\mathbf{S}_{AC}$ in WPE-MO Type-II.

Image	[0, 10]	[0, 7]	[0, 5]	W/o All
#001	**8.95**	14.49	23.18	654.45
#021	**6.13**	10.26	16.99	460.82
#041	**8.59**	14.20	21.98	544.20
#061	**8.07**	13.21	21.38	682.42
#081	**8.02**	13.35	20.65	632.11
⋮		⋮		
Avg.	**7.26**	12.25	19.53	570.82

[vii]The global shuffling added to Type-I consisted of independently and globally shuffling DC coefficients and 63 AC coefficient blocks globally, where the 63 AC coefficient blocks were shuffled while preserving their positions within the blocks.

Table 7 BD-rates [%] and BD-PSNRs [dB] at the different types of WPE-MOs.

Image	W/o All		W/o RSS		W/o RLI		Type-I		Type-II	
	BD-rate	BD-PSNR	BD-rate	BD-PSNR	BD-rate	BD-PSNR	BD-rate	BD-PSNR	BD-rate	BD-PSNR
#001	654.45	−10.69	60.00	−2.43	265.90	−7.12	42.84	−1.85	**23.20**	**−1.08**
#021	460.82	−8.55	53.40	−1.94	162.34	−4.89	28.58	−1.14	**16.99**	**−0.70**
#041	544.20	−10.20	59.65	−2.29	207.78	−5.62	41.33	−1.71	**22.01**	**−0.98**
#061	682.42	−9.84	60.11	−2.07	260.60	−5.89	39.52	−1.49	**21.40**	**−0.87**
#081	632.11	−12.71	57.07	−2.57	245.14	−7.61	36.59	−1.79	**20.67**	**−1.07**
⋮	⋮		⋮		⋮		⋮		⋮	
Avg.	570.82	−10.15	56.35	−2.26	220.77	−6.36	34.58	−1.51	**19.55**	**−0.90**

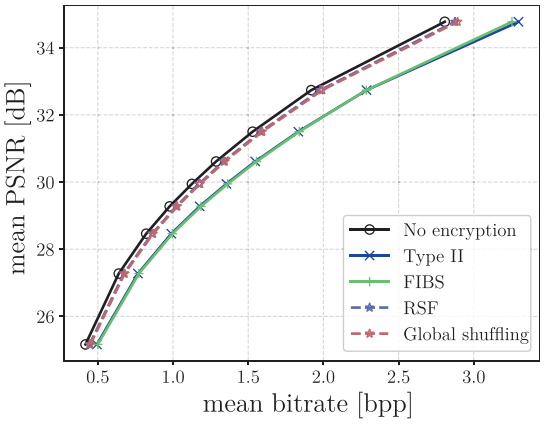


Fig. 6 R-D curves for Type-II and conventional JPEG-FEs including global shuffling.

than Type-I (while better preserving coding efficiency discussed in Sect. 4.2), and thus has been omitted from Fig. 5. This trade-off between encryption strength and coding efficiency is a key aspect of WPE-MO, but the values of RLI and RSS can be adjusted by the user.

4.2 Coding Efficiency

This subsection analyzes the coding efficiency of JPEG images encrypted with WPE-MO. Coding efficiency was analyzed by drawing rate-distortion (R-D) curves and computing the Bjøntegaard delta (BD) metrics [19].

First, we analyzed the effect of DC encryption modules in WPE-MO on coding efficiency. Table 4 shows the results when different directional (horizontal and vertical) DPCMs were applied to DC coefficients, with no AC encryption modules used. The results indicate that prediction error propagation from reconstructing encrypted DC residuals, particularly in the vertical direction, slightly degraded JPEG coding efficiency but not significantly. In other words, DC coefficients encrypted with DC-WPE remain efficiently encoded, regardless of horizontal or vertical propagation. Therefore, we selected horizontal DPCM and inverse DPCM for each WPE-MO method in subsequent experiments.

Second, we analyzed the effect of varying intervals in RLI on coding efficiency in WPE-MO. As shown in Table 5, shorter intervals more effectively reduced the degradation in coding efficiency, indicating that propagation was blocked more frequently.

Table 8 Ratio of zero and nonzero DC coefficients in the QDCT domain encrypted with WPE-MOs (JPEG $Q = 70$).

Image	No encrypt.	W/o All	W/o RSS	W/o RLI	Type-I	Type-II	FIBS	RSF
#001	**48.02**	657.29	106.16	417.91	101.40	229.40	**48.02**	**48.02**
#021	**79.84**	767.00	169.67	459.80	127.00	138.64	**79.84**	**79.84**
#041	241.53	208.45	241.53	287.00	328.14	**130.66**	241.53	241.53
#061	**176.23**	241.53	575.00	353.46	417.91	241.53	**176.23**	**176.23**
#081	**29.52**	287.00	58.84	169.67	38.05	71.00	**29.52**	**29.52**
⋮				⋮				
Avg.	**36.03**	204.16	105.47	222.47	74.71	96.59	**36.03**	**36.03**

Table 9 Ratio of zero and nonzero AC coefficients in the QDCT domain encrypted with WPE-MOs (JPEG $Q = 70$).

Image	No encrypt.	W/o All	W/o RSS	W/o RLI	Type-I	Type-II	FIBS	RSF
#001	**0.18**	1.11	0.27	0.44	0.23	0.21	**0.18**	**0.18**
#021	**0.42**	1.46	0.63	0.76	0.51	0.47	**0.42**	**0.42**
#041	**0.16**	0.44	0.23	0.34	0.20	0.18	**0.16**	**0.16**
#061	**0.13**	0.39	0.20	0.31	0.16	0.15	**0.13**	**0.13**
#081	**0.21**	0.97	0.30	0.48	0.26	0.24	**0.21**	**0.21**
⋮				⋮				
Avg.	**0.20**	0.62	0.29	0.41	0.24	0.22	**0.20**	**0.20**

Third, we analyzed the effect of varying step sizes in RSS on coding efficiency in WPE-MO. As shown in Table 6, increasing the step size more effectively reduced the effect of WPE-MO on coding efficiency. In particular, larger step sizes reduced the frequency of signal propagation.

Finally, we analyzed the effect of DC and AC encryption modules on coding efficiency. As shown in Table 7, WPE-MO for AC coefficients significantly effected coding efficiency. However, RLI reduced this effect, and RSS further improved efficiency by skipping prediction/reconstruction intervals.

We also compared the coding efficiency of Type-II with other JPEG-FEs. As shown in Fig. 6, Type-II had a similar effect on coding efficiency as FIBS. However, RSF and FIBS do not conceal statistical features as effectively as WPE-MO because they only change the values or positions of nonzero coefficients without changing the ratio of zero and nonzero coefficients, as discussed in Sect. 4.3.

4.3 Statistical Analysis

This subsection discusses the statistical variation in the ratio of zero and nonzero coefficients in the QDCT domain. Ta-

bles 8 and 9 list the ratios of zero and nonzero DC coefficients and AC coefficients, calculated as

$$\text{ratio} = \frac{\text{number of the nonzero coefficients}}{\text{number of the zero coefficients}}, \tag{16}$$

i.e., a lower ratio shows that more number of zero coefficients are contained in the image. The results show that WPE-MO significantly changes the ratio of zero and nonzero coefficients.

5. Conclusion

To reinforce the protection of JPEG images, particularly their texture information, we proposed Prediction Error-Propagated Encryption with Modulo Operator (WPE-MO). WPE-MO encrypts both the direct current (DC) coefficients, which contain structure information, and the alternating current coefficients, which contain texture information, by newly placing prediction, encryption, and reconstruction modules in the QDCT domain. Additionally, WPE-MO incorporates a modulo operator to ensure JPEG format compatibility and employs random discrete processing through a random length interval (RLI) and a random step size (RSS) parameters in the prediction and reconstruction modules, preserving JPEG coding efficiency. Experiments demonstrated that WPE-MO maintained moderate coding efficiency and provided strong resilience against ciphertext-only attacks, including brute-force and replacement attacks such as sketch and DC deletion attacks. Especially, WPE-MO Type-II reduced coding efficiency by only 19.55% in terms of the Bjøntegaard-delta (BD)-rate, while achieving texture protection.

Acknowledgments

This work was supported by the Japan Society for the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (C) under Grant 22K04084.

References

[1] K. Shimizu, T. Suzuki, and K. Kameyama, "Cube-based encryption-then-compression system for video sequences," IEICE Trans. Fundamentals, vol.E101-A, no.11, pp.1815–1822, Nov. 2018.
[2] T. Chuman, W. Sirichotedumrong, and H. Kiya, "Encryption-then-compression systems using grayscale-based image encryption for JPEG images," IEEE Trans. Inf. Forensics Security, vol.14, no.6, pp.1515–1525, Nov. 2019.
[3] J. He, S. Huang, S. Tang, and J. Huang, "JPEG image encryption with improved format compatibility and file size preservation," IEEE Trans. Multimedia, vol.20, no.10, pp.2645–2658, Oct. 2018.
[4] V. Itier, P. Puteaux, and W. Puech, "Recompression of JPEG crypto-compressed images without a key," IEEE Trans. Circuits Syst. Video Technol., vol.30, no.3, pp.646–660, March 2020.
[5] N.A. Khan, M. Altaf, and F.A. Khan, "Selective encryption of JPEG images with chaotic based novel S-box," Multimed. Tools. Appl., vol.80, no.6, pp.9639–9656, March 2021.
[6] M. Hirose, S. Imaizumi, and H. Kiya, "Encryption method for JPEG bitstreams for partially disclosing visual information," Electronics, vol.13, no.11, May 2024.
[7] P. Li and K.-T. Lo, "Joint image compression and encryption based on order-8 alternating transforms," J. Vis. Commun. Image, vol.44, pp.61–71, April 2017.
[8] W. Li and Y. Yuan, "A leak and its remedy in JPEG image encryption," Int. J. Comput. Math, vol.84, no.9, pp.1367–1378, Sept. 2007.
[9] K. Minemura, K. Wong, Q. Xiaojun, and T. Kiyoshi, "A scrambling framework for block transform compressed image," Multimed. Tools. Appl., vol.76, no.5, pp.6709–6729, March 2017.
[10] K. Shimizu and T. Suzuki, "Finely tunable bitcuboid-based encryption with exception-free signed binarization for JPEG standard," IEEE Trans. Inf. Forensics Security, vol.16, pp.4985–4908, Sept. 2021.
[11] C. Qin, J. Hu, F. Li, Z. Qian, and X. Zhang, "JPEG image encryption with adaptive DC coefficient prediction and RS pair permutation," IEEE Trans. Multimedia, vol.25, pp.2528–2542, Feb. 2022.
[12] K. Shimizu, Q. Wang, and T. Suzuki, "AC prediction error propagation-based encryption for texture protection of JPEG compressed images," Proc. PCS, (Bristol, UK), pp.166–170, June 2021.
[13] J. Ting, K. Wong, and S. Ong, "Format-compliant perceptual encryption method for JPEG XT," Proc. ICIP, (Taipei, Taiwan), pp.4559–4563, Sept. 2019.
[14] M. Weinberger, G. Seroussi, and G. Sapiro, "The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS," IEEE Trans. Image Process., vol.9, no.8, pp.1309–1324, Aug. 2000.
[15] National Institute of Standards and Technology, FIPS PUB 180-4: Secure Hash Standard (SHS), pub-NIST, Aug. 2015.
[16] E. Barker, NIST Special Publication 800-57 Part 1, Revision 5, NIST, 2020.
[17] G. Schaefer and M. Stich, "UCID: An uncompressed color image database," Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia, vol.5307, (San Jose, CA), pp.472–480, Jan. 2004.
[18] "JPEG software," https://jpeg.org/jpeg/software.html.
[19] G. Bjøntegaard, Calculation of average PSNR differences between RD-curves, VCEG-M33, 2001.

Kosuke Shimizu received the B.E. of the Computer Science Program of the Advanced Course, Tokyo Metropolitan College of Industrial Technology (TMCIT), Japan, in 2017, and the M.E. and D.E. degrees from the Department of Computer Science, University of Tsukuba, Japan, in 2019 and 2022, respectively. From 2020 to 2022, he was a Research Fellow of the Japan Society for the Promotion of Science (JSPS). In 2022, he was a Ph.D. Research Fellow in University of Tsukuba, Japan, and later joined the Faculty of Engineering, Gifu University, Japan, as an Assistant Professor. His current research interest is image and video processing.

Taizo Suzuki received the B.E., M.E., and Ph.D. degrees in electrical engineering from Keio University, Japan, in 2004, 2006, and 2010, respectively. From 2006 to 2008, he was with Toppan Printing Co., Ltd., Japan. From 2008 to 2011, he was a Research Associate at the Global Center of Excellence (G-COE), Keio University, Japan. From 2010 to 2011, he was a Research Fellow at the Japan Society for the Promotion of Science (JSPS) and a Visiting Scholar at the Video Processing Group, University of California, San Diego, La Jolla, CA, USA. From 2011 to 2012, he was an Assistant Professor at Nihon University, Japan. In 2012, he joined the University of Tsukuba, Japan, as an Assistant Professor, where he has been an Associate Professor since 2019. Since 2024, he has been a Science and Technology Policy Fellow at the Council for Science, Technology, and Innovation, Cabinet Office, Government of Japan. His current research interests include signal processing and its applications to media content. From 2017 to 2021, he was an Associate Editor of the *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, where he has served as an Area Editor since 2023.