Journal of Imaging Science and Technology® 68(6): 1–11, 2024.

A Consideration of JPEG Resistance Verification of Correlation-based Steganography

Aikawa Mariko
Shibaura Institute of Technology, Tokyo, Japan
E-mail: ma23001@shibaura-it.ac.jp

Miyata Sumiko
Institute of Science Tokyo, Tokyo, Japan

Hosono Kaito
Kanagawa University, Kanagawa, Japan

Miyata Takamichi
Chiba Institute of Technology, Chiba, Japan

Kinoshita Hirotsugu
Kanagawa University, Kanagawa, Japan

Abstract. *With large amount of personal information being managed over the Internet, privacy protection in communication channels has become essential. Thus, steganography, a secret communication technique that conceals information in an image, is garnering attention. Using this method to communicate with embedded ciphertext, the detection rate of encrypted communication can be reduced and privacy protection can be strengthened by making it appear to a third party that only image communication is taking place. Currently, many steganography methods with improved capacity and robustness have been proposed. In addition, JPEG compression resistance verification is required to extend its versatility. Correlation-based BMP steganography in previous studies has improved confidentiality by embedding and extracting secret information using correlation. However, the compression resistance of generated images has not been verified. In this study, we evaluate compression resistance based on image quality and information recovery rate. Moreover, we show the minimum compression quality that satisfies the required acceptable retention conditions for JPEG compression of cover images.*
Keywords: *robust steganography, privacy, JPEG compression, reed solpmon codes, characteristics analysis*

[DOI: 10.2352/J.ImagingSci.Technol.2024.68.6.060402]

1. INTRODUCTION

Today, everything from shopping to accessing public services and medical care is done online. With the development of social networking services, a large amount of video content is exchanged and utilizes a significant portion of bandwidth. In such services, confidential information such as users' personal information and transaction information is encrypted for transmission. However, this encrypted communication is visible to a third party and there is a risk that the information can be intercepted by decrypting the encrypted data. Steganography [1, 2] is a technique for achieving secret communication by embedding confidential information in multimedia data unrelated to the secret information. We focus on image steganography, in which an image is used as a cover object (cover image) for embedding information. By applying image steganography to encrypted communications and embedding the ciphertext in the cover image, a third party is led to recognize the image as a typical multimedia communication. Thus, image steganography is an effective privacy protection measure.

Several conventional methods in image steganography have been proposed [3–14]. These methods are classified based on the embedded area of information and the format of the cover image used [15]. Moreover, few methods that use JPEG images as cover images, focusing on minimizing the embedding distortion, are also proposed [6, 7, 10]. However, there is limited discussion on the confidentiality of embedded information in these methods, and there are concerns about the robustness of steganography, if its use is discovered. On the other hand, Correlation-based steganography [8, 11, 12] can improve confidentiality, since embedded information is shifted by using M-sequences, also known as pseudo-random sequence consisting of -1 and 1 [16, 17]. Since the cover image of these correlation-based steganography methods uses a high-resolution BMP image, these methods can be applied to medical and testing images that handle high-definition images, and the evaluation of image quality change is more rigorous.

Recently, many deep learning-based steganography methods have been proposed [18]. In particular, methods using GANs (Generative Adversarial Networks) [19–21]

Received July 31, 2024; accepted for publication Dec. 2, 2024; published online Dec. 31, 2024. Associate Editor: Kuo-Ping Lin.
1062-3701/2024/68(6)/060402/11/$25.00

employ generators to select areas with rich textures or high-frequency bands, embedding data into appropriate pixels less susceptible to the influence of embedding. Additionally, discriminators are used to evaluate whether the stego images are visually detectable. This technique allows for the generation of robust stego images by iteratively generating and evaluating until the detection rate decreases. However, such deep learning methods require extensive datasets for the training process and impose a significant computational cost. Furthermore, the high degree of black-box nature of these models makes it difficult to troubleshoot when errors occur. In addition, deep learning-based methods are highly dependent on the image dataset used during training. As a result, the detection tolerance may be weak for images with features that are not given at training time due to the inability to evaluate conflicts well. However, classical methods such as CoR do not require such a learning process and their detection tolerance is independent of the images used. The high transparency of the algorithm also makes it easier to troubleshoot, thereby ensuring system stability. In addition, compression resistance for information-embedded images (stego images) is essential for expanding the versatility of image steganography because image-based communications are more popular than text-based communications [22]. Depending on the application used, images may be automatically compressed, however, the information must be correctly extracted after compression and steganography must not be detected [13, 14]. In general, JPEG compression reduces the amount of data by removing high-frequency band components, which have coefficients close to zero, after DCT and quantization. This is because the high-frequency components correspond to the complex textures in the image, and even if changes occur in these components, the human eye cannot easily recognize the deterioration. Therefore, it is necessary to embed information by selecting appropriate pixel values (embedding areas) that are less susceptible to the effects of high-frequency components, since embedded information in stego images is easily deleted in high-frequency bands.

The bias of the frequency components that compose an image differs from image to image, so the necessary embedding distortion and appropriate embedding target coefficients vary even for the same compression quality and secret data volume. Therefore, if area selection is performed by focusing only on the information loss rate, image quality degradation will occur. Therefore, it is necessary to design embedding parameters that consider the trade-off between tolerance and image quality [23] by using error-correcting codes [24, 25]. In particular, correlation-based methods that use uncompressed images in BMP format, which have large data volume, are likely to be subject to compression. Therefore, we focus on the JPEG compression resistance of correlation-based methods.

Our earlier studies focused on verifying the JPEG compression resistance of correlation-based methods [26, 27], which check the behavior after compression of stego images created by varying the embedding parameters based on PSNR and BER. These two previous studies verify compression resistance when using the method that introduces RS codes in LSB (least significant bit) methods.

In addition, by fixing the embedding parameter in our method [26] proposed earlier, we captured the characteristics of the impact of the correlated method with RS codes on JPEG compression, called as correlation-based steganography using M'-sequence with RS codes by considering JPEG compression (CoRC).

In Ref. [27], the image quality and BER after compression are set to a threshold value and extract the combination of the minimum compression quality and embedding parameters that satisfy the thresholds. This technique is called correlation-based steganography using M'-sequence with RS codes by considering JPEG compression and minimum quality value (CoRCQ). However, there are a few limitations: the number of experimental images is small; there is no discussion of compression resistance and embedding capacity; and the performance of the RS code is not mentioned. In addition, some of the images could not be used as cover images due to the strict condition of BER $= 0$ %.

In this study, we analyze the JPEG compression resistance of the correlation-based method by changing the BER threshold value, and identify the embedding conditions and minimum compression quality for each image. We label this method as CoRCB (Correlation-based Steganography using M'-sequence with RS code introduction based on BER). We also compare the results with and without the use of RS codes, and determine whether existing RS code-based methods are effective as a JPEG compression measure. The position of this study is shown in Table I, and the contributions are as follows.

- We determined that the method of embedding RS codes in LSBs proposed in correlation-based method with RS codes [11] in not enough to improve JPEG compression resistance.
- We determined the minimum compression quality that satisfies the required acceptable retention conditions for JPEG compression of cover images created by the correlation-based image steganography based on correlation-based method [8, 11, 12].

This paper is organized as follows. First, we classify the main steganography methods as related studies and introduce DCRAS [13] and ESS [14] as examples of steganography with verified compression resistance. Then, in preparation for the experiments, we introduce the correlation-based method [8, 11, 12], which is the subject of this validation. We also introduce the JPEG compression resistance verification considering embedding parameters [26, 27]. Next, through numerical analysis, we conduct brute force experiments to investigate the conditions under which the correlation-based method satisfies compression tolerance and achieves minimum compression quality. In addition, the effect of RS codes in the correlation method and suggestions for improvement in its use are proposed. Finally, we present the conclusions and the future prospects.

Table I. Comparison of existing and proposed methods.

Method	Error correction	Compression resistance verification	Minimum Q check	Allowance of BER > 0
Co [8]	—	—	—	—
CoR [11]	✓	—	—	—
CoRC [26]	✓	✓	—	—
CoRCQ [27]	✓	✓	✓	—
CoRCB (Ours)	✓	✓	✓	✓

2. RELATED WORK

In this section, we first classify image steganography to define the position of the methods [15] used in this study. Then, we introduce DCRAS [13] and ESS [14], which are methods for verifying compression resistance.

2.1 *Steganography Classification*

2.1.1 *Classification based on Embedded Area*

There are two main types of information embedding methods: pixel substitution and frequency domain embedding. The former method embeds secret information by directly changing the pixel values, and the LSB method is a typical example [3, 4]. Steganography that examines the correlation of neighboring pixels before embedding and selects bits higher than LSB has also been proposed [5]. This method takes advantage of the fact that the degradation caused by pixel value changes in complex textures, such as noisy regions, is difficult for the human eye to perceive. For each local region, the effect on vision is considered, and the appropriate bit plane for embedding and the amount of embedding are adjusted. This enables embedding that takes into account both the embedding capacity and the image quality. However, the information embedded by the pixel replacement method is easily lost due to the distortion of the lossy image compression. On the other hand, the frequency domain method embeds the secret information in the transform coefficients obtained by a transform such as DFT, DCT, etc. Using this method to identify the embedding position is difficult [6–9], and can also provide compression resistance by avoiding embedding in high-frequency bands, taking into account the effects of embedding distortion design and quantization of JPEG compression [13].

2.1.2 *Classification based on use of Cover Image*

There are two types of cover image file format classifications: those that use uncompressed BMP images, and those that use JPEG images, which compress images by removing high-frequency areas that are difficult for the human eye to perceive [15]. Many JPEG steganography methods have been proposed because the JPEG format is suitable for image communication due to its small data size [6, 7, 10]. These methods improve the statistical detection of visual changes and steganalysis by minimizing the distortion function and considering the position of embedded information. However, their robustness against image processing has not been confirmed at the time of study. BMP images are expected to be used for personal information management in inspection images that require complex texture representation, but they may be compressed due to their large data volume. However, the effect of compression on image quality is greater than that of JPEG images, which have already degraded the image quality, hence it is necessary to validate the robustness.

2.2 *Steganography Methods*

2.2.1 *DCRAS*

DCRAS [13] is a JPEG-tolerant adaptive steganography that provides compression tolerance to J-UNIWARD [7], which is widely used in JPEG steganography, by calculating the relationship between DCT coefficients and concentrating the embedding frequencies in the low frequency range, which is not affected by JPEG compression. The JPEG-tolerant steganography is achieved by calculating the relationship between DCT coefficients and concentrating the embedding frequencies in the low frequency band, which is not affected by JPEG compression. STC is used for information embedding to efficiently encode messages, and the Viterbi algorithm is used to find the optimal encoding path. This minimizes embedding distortion. In addition, the RS code (31, 15) is embedded with the information to aid in information recovery after compression. With these introductions, the detected error rate at compression quality $Q = 75$ is maintained at near 0%, which is an overwhelming improvement of 40% compared to J-UNIWARD [7]. Steganalysis detection tolerance using CCPEV548 [28] is also improved. However, no mention is made on the use of lossless formats such as BMP for cover images. Another problem is that there is no evaluation of image distortion from embedding, and the characteristics of compression resistance are not sufficiently obtained because there are no evaluation metrics for JPEG quality factors other than $Q = 75$.

2.2.2 *ESS*

ESS [14] makes JPEG compression permissive by incorporating the compression characteristics of the application in which it is used. The main idea of this method is as follows.

The image quality factor of the JPEG image before information embedding is QF1, and the image quality factor to be recompressed after embedding is QF2. Then, the image is recompressed with QF2, and the DCT coefficients are checked. The non-zero coefficients after recompression are used as cover elements for embedding secret information along with error correction codes. The method is tolerant by selecting DCT coefficients according to the quality of the compressed image. It is also stated that the cover image to be used is appropriate to use an image that contains many non-zeros after compression with an arbitrary QF2, but even if the information can be retained, the tolerance can be increased by avoiding images with large visual degradation.

As a result of this tolerance verification, J-UNIWARD achieves a lower information loss rate, a lower detection rate due to steganalysis, and a higher image quality retention rate at each compression quality compared to other methods.

In addition, while J-UNIWARD has not succeeded in communicating even a single image, ESS has been confirmed to be able to communicate secretly with WeChat and Twitter for 48 out of 50 images. Thus, it is shown that multifaceted security-resistant embedding and application-appropriate cover image selection are possible.

3. PREPARATIONS

The correlation method used in this study is frequency domain steganography, using BMP images as cover images, and four methods have been proposed [12]. Based on Method 1, the following methods describe the way to suppress the intensity coefficient, which is the cause of image quality degradation. In this section, we describe the embedding and extraction procedures using correlation in Method 1, the basic method, and then introduce the method using RS [11], which was the subject of compression resistance verification in [26, 27].

3.1 *Correlation-based Method*

3.1.1 *Method 1: Correlation-based Steganography Using M'-sequence without RS Codes (Co)*

The correlation-based method improves data confidentiality by focusing not only on the method of embedding secret information but also on the encryption of the secret information itself. M'-sequences, which are pseudo-random sequences, are used for encryption, and information is represented by shifting the source sequence. Since the M'-sequence consists of $-1, 1$ binary values, there are 2^m peak positions in the m-dimensional M'-sequence. The total number of correspondences between m bits consisting of $-1, 1$ and 2^m ways is $2^m!$ [16, 17].

In addition, to extract the embedded information, it is necessary to extract the correlation peaks from the original series to obtain the number of shifts in the M'-sequence. Correct correlation values must also be obtained for correct secret information extraction. However, while DCT coefficients take many different values, the M'-sequence takes only two values, -1 and 1. Therefore, when the DCT coefficients to be embedded are large, the influence of the M'-sequence becomes small and correlation extraction becomes difficult. Changing embedding strength for each block of DCT coefficients enables correct restoration.

The embedding and detection procedures for correlation-based methods are shown below.

3.1.2 *Embedding Procedure*

For embedding, we implemented a correlation-based method based on few studies [8, 17, 29]. Figure 1 shows the embedding process.

(E1) Converts embedded data from hexadecimal to decimal.

(E2) Generate one M'-sequence A^0, which is extended to represent information up to $2^m - 1$ by adding "-1" to the end of the M-sequence. Shift it t times to represent the information and obtain the shifted series A^{t_M} $(M = 0, 1, \ldots; t_M = 2^m - 1)$.

The next step is to embed the shifted M' series representing the secret information into the image. For this purpose, DCT is performed on the original image to derive a series of DCT coefficients.

(E3) The original image N^{ori} of size $W \times W$ is divided into $N_B = \frac{W^2}{W_{\text{sub}}^2}$, where size of sub-block is $W_{\text{sub}} \times W_{\text{sub}}$. Perform DCT on each sub-block to obtain a one-dimensional series Y_u $(u = 0, 1, \ldots, N_B - 1)$. where u is a sub-block number.

(E4) A zigzag scan is performed on each sub-block Y_u to obtain a one-dimensional series $Y_{u,j}$ $(j = 0, 1, \ldots, W_{\text{sub}}^2 - 1)$ where the DCT coefficients are aligned from low to high frequency, where j is an index of DCT coefficient in the block.

(E5) From the created one-dimensional series $Y_{u,j}$, extract a series $Y'_{u,j}$ $(j = S, S+1, \ldots, S+L-1)$ consisting of DCT coefficients to be used for embedding, where S $(1 \le S \le W_{\text{sub}}^2 - L + 1)$ is the starting position, and L is the M' series length. $Y'_{u,j}$ are extracted from all the sub-blocks and concatenated to obtain $\widetilde{Y}_j$ $(j = 0, 1, \ldots, N_B \times L - 1)$.

(E6) For the extracted series $\widetilde{Y}_j$ $(j = 0, 1, \ldots, N_B \times L - 1)$, multiply the M' series by a strength factor G to change the embedding strength required to extract the correct correlations, G is a value that depends on the size of the DCT coefficients used, i.e., it is determined by S. Here, the strength coefficient is taken when BER$= 0$, which is the information error rate during information extraction. Essentially, the magnitude of the required gain is different because the magnitude of the DCT coefficients contained in each series $Y'_{u,j}$ $(u = 0, 1, \ldots, N_B - 1; j = S, S+1, \ldots, S+L-1)$ extracted from each sub-block differs for information recovery. However, the largest value of the gain G is commonly applied to all sub-blocks. Embedding is performed by replacing the extracted series $\widetilde{Y}_j$ $(j = 0, 1, \ldots, N_B \times L - 1)$ with $\widehat{Y}_j$. The embedding formula is as follows.

$$\widehat{Y}_j = \widetilde{Y}_j + G \times A_j^{t_M} \tag{1}$$

(E7) Inverse zigzag scan is performed to return to a block of $W \times W$. Then, inverse DCT is performed to generate a stego image N^{stego}.

3.1.3 *Detection Procedures*

(F1) Perform (E3)–(E5) on the stego image to obtain $\widehat{Y}_j$. Calculating the correlation coefficient between this embedded series and the original M'-sequence A^0, the maximum peak occurs at the position indicating t, the number of shifts.

(F2) The extracted location information t is converted to hexadecimal numbers, and the M'-sequence is

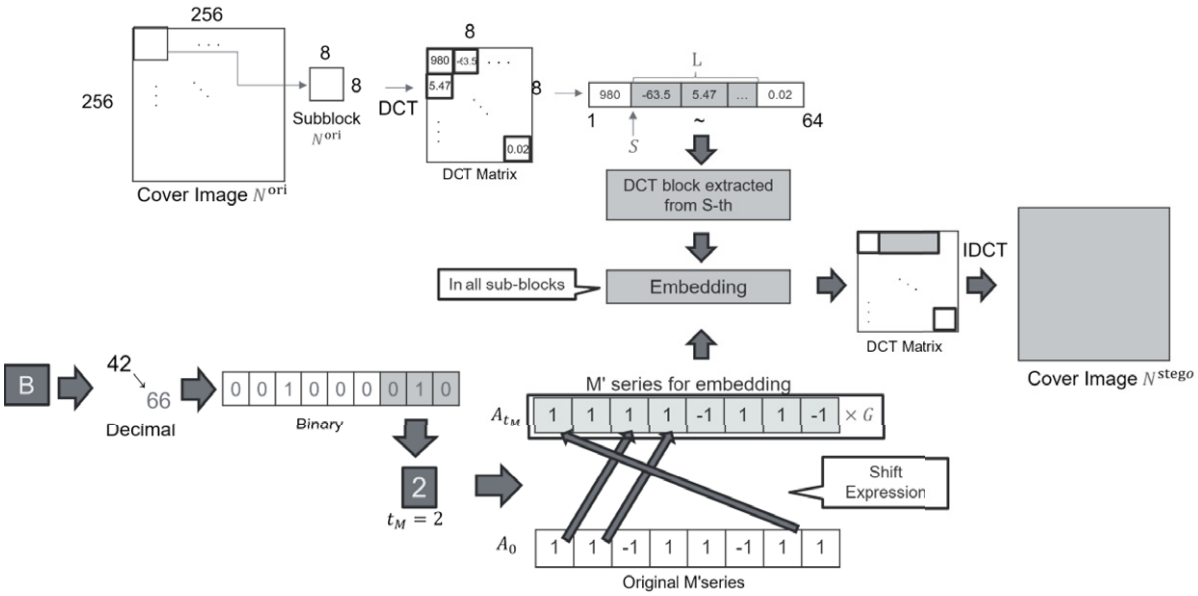

Figure 1. Secret information "B" (UTF-8) is expressed and embedded with the correlation-based method.

re-shifted based on the obtained t. This is how the secret information is extracted.

3.1.4 *Method. 2 Correlation-based Steganography Using M'-sequence with RS codes (CoR)*

In Method 2 [11], we considered increasing the amount of information embedded without degrading image quality, and focused on suppressing the intensity coefficient G, which is the cause of image quality degradation. However, if G is suppressed, there is a possibility that information extraction will not be complete because correct correlation cannot be obtained. Therefore, the key idea is to correct detection errors by using RS codes during information recovery.

The embedding procedure of RS codes is as follows.

(R1) The RS code (h, c) to be used is used to divide the secret information into pieces of a certain length of information symbols according to the set code length h. For each partitioned secret information, a Galois array, which is a code word, is generated. Redundant symbols are extracted from the code word.

(R2) LSBs are extracted from the stego image created by Method. 1. Each LSB is replaced with an RS code and embedded. The image is then reconstructed.

Compared to Method 1, this method can embed information even in small G by performing error correction with RS codes at the time of information extraction, and also achieves an increase in embedding capacity. In addition, since the low-frequency band is an important part of the image that contains rough features, a large intensity factor is required. However, this is suppressed in this method, resulting in an improvement in image quality of about 0.4 in structural similarity index measure (SSIM) for small S.

3.2 *Summary of our Previous Verification for Compression Resistance*

We analyzed JPEG compression resistance verification to ensure that the correlation-based method worked with data compression. In the verification, the post-compression quality change (PSNR), the information loss rate (BER), and the embedding capacity were used as indices. In this subsection, we summarize the JPEG compression tolerance verification of the correlation-based method [26, 27]. In both cases, embedding and extraction were performed using the Method 2 for correlation-based method.

3.2.1 *Embedding Parameters S, G*

The important parameters in the correlation-based embedding methods are the start position S and the strength coefficient G. S represents the coefficient number within the sub-block, which determines from which DCT coefficient among $N_B - 1$ coefficients in the sub-block, the information will be embedded when rearranged into a one-dimensional sequence $Y_{u,j}$ by the zig-zag scan order. Note that if the S is large, the secret information is embedded in the high-frequency band, and vice versa. The strength coefficient G is the value multiplied by the M' sequence to adjust the embedding strength. If G is not strong enough, it will be difficult to correctly obtain the correlation before and after the shift of the M'-sequence, making information recovery difficult. On the other hand, since G is added to the DCT coefficients along with the M'-sequence, an excessively large G will cause significant changes to the original DCT coefficient values, resulting in image quality degradation. Therefore, embedding with the minimum necessary G is desirable to minimize the image quality degradation while maintaining robustness. In addition, preliminary experiments [27] have shown that information recovery is

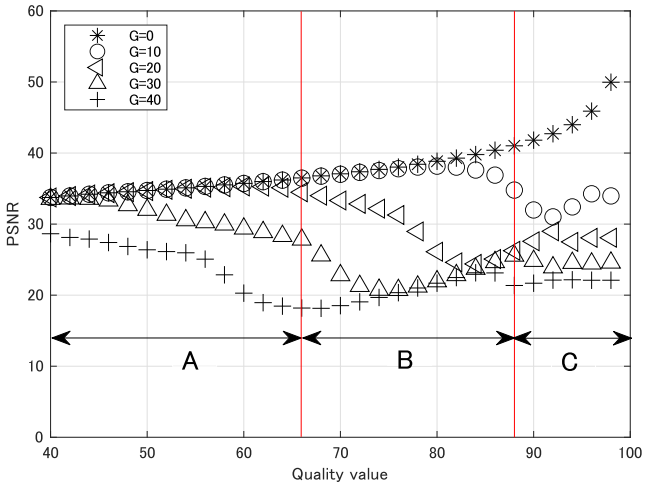

Figure 2. Change in PSNR at each G during Q-value change and ABC of region segmentation by characteristics focused on $G = 40$ (from reproduction experiment [26] using image Boat).

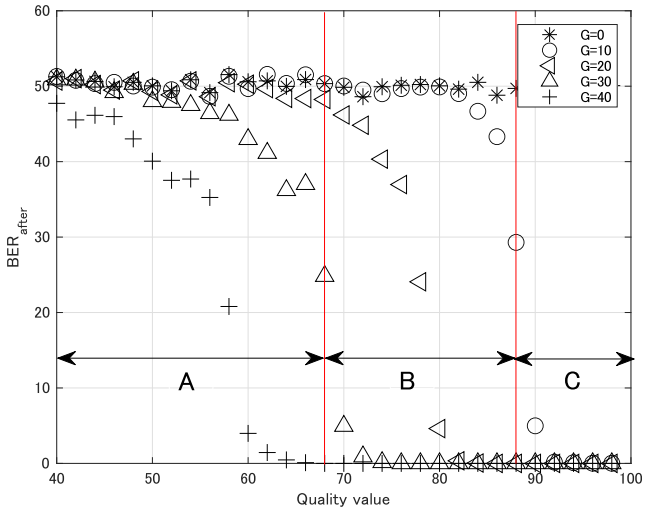

Figure 3. Change in BER at each G when Q-value changes and ABC of region segmentation by characteristics focused on $G = 40$ (from reproduction experiment [26] using image Boat).

possible even with a small G in the higher frequency bands (larger S) compared to the lower frequency bands (smaller S).

3.2.2 *Confirmation of Resistance by Fixing Embedded Parameters*

Miyata's method [26] makes it easy to understand the characteristics of the effect of compression by fixing the embedding strength factor G and the embedding start position S in each block of DCT coefficients. This verification is called CoRC (correlation-based steganography using M'-sequence with RS codes by considering JPEG compression).

This verification confirms that compression resistance varies in three stages depending on the change in compression quality Q ($G \neq 0$). In particular, when we divide the regions focusing on $G = 40$ (Figures 2 and 3), the BER begins to exceed 0% from the boundary between regions A and B (red line) as Q decreases. Furthermore, PSNR improves more than when compression was performed with a high quality factor. Experimental condition 1 was used in this experiment. In addition, the source of the test images is from a Standard Image Database called SIDBA.

Experimental condition 1	
Embedded information	512 Bytes
Embedding start position	$S = 64 - L + 1$
M' series length	$L = 16$
Compression quality	$Q = 40 \sim 100$
Embedded strength factor	$G = 0, 10, 20, 30, 40$
Test Images (BMP 256 × 256)	Boat, Babara, Girl
RS Code	$(h, c) = (255, 127)$

3.2.3 *Search for Parameters to Minimize Compression Quality*

The verification by Miyata [26] clarified the characteristics of changes in image quality and BER when compression quality changes by fixing the embedding parameters S and G, which have a trade-off relationship. However, there is a possibility that a larger size than necessary is used in the rough setting where G is every 10. In addition, since S uses a relatively high-frequency value ($S = 49$) derived from the M'-sequence length, it is possible that the embedding parameter is set in a state susceptible to JPEG compression. Therefore, more detailed parameters had to be set to check the tolerance in other frequency bands. In addition, there was no discussion of the degree of compression quality each cover image could tolerate.

Experimental condition 2	
Embedded information	512 Bytes
Embedding start position	$S = 20 \sim 49$
M' series length	$L = 16$
Compression quality	$Q = 75 \sim 100$
Embedded strength factor	$G = 5 \sim 20$
Test Images (BMP 256 × 256)	Boat, Babara, Girl, Lax
RS Code	$(h, c) = (255, 127)$
Resistant conditions	PSNR $\geq$ 30 dB $\wedge$ BER = 0%

Our second verification [27] derives minimum compression quality and adjusts the parameter by brute force. After compression, PSNR $\geq$ 30 dB $\wedge$ BER = 0% is set as the threshold for compression resistance, and the combination of S, G, and compression quality Q is extracted when these conditions are satisfied. The minimum compression quality $Q_{\min}$ was determined from among the tolerant combinations, and the extent to which each image can be compressed using the correlation-based method was checked. This verification is called as CoRCQ (correlation-based steganography using M'-sequence with RS codes by considering JPEG compression and minimum quality value). If there are multiple combinations of embedding parameters

Table II. Q_{min} and PSNR and embedding conditions for each image.

Image	Q_{min}	PSNR (dB)	G	S
Boat	91	30.31	15	33
Babara	93	30.42	15	49
Girl	92	30.43	14	41
Lax	—	—	—	—

that satisfy $Q_{\min}$, the one with the highest image quality PSNR is selected. Experimental condition 2 was used in this experiment and the source of the test Images are SIDBA.

Table II shows the combination of parameters and $Q_{\min}$ when the threshold is satisfied by brute force. The results show that Boat, Babara, and Girl images found parameters and minimum compression quality that satisfy both image quality and BER thresholds. There is no significant difference in G which can modify the impact (magnitude of change) on the pixel and cause degradation of image quality. This study used same source M'-sequence. Thus, the same intensity coefficient around $G = 15$ was required, and the intensity coefficient started to deviate from the PSNR threshold at this intensity coefficient. On the other hand, S was different for each image, and Boat was better suited for embedding at lower frequencies than other images. This is because the magnitudes of the DCT coefficients are unevenly distributed among the images, and the frequency response of the same S varies.

In addition, Lax could not find a combination of embedding conditions that could achieve tolerance within the embedding conditions used. This is because the bias of DCT coefficients that make up Lax is different from that of the other three pieces. It is also stated that $G = 50$ was needed to achieve BER $= 0$ even at low compression ratios of $S = 49$ and $Q = 99$. In addition, even when the amount of embedded information was reduced to 256 Bytes, no combination satisfying the threshold was found within the experimental conditions.

This compression tolerance test [27] using thresholds determined the minimum compression quality for the tolerant state. However, certain images are not suitable for compression. Thus, next section, we propose CoRCB (correlation-based steganography using M'-sequence with RS code introduction based on BER) and analyze the characteristics.

4. CONSIDERATION FOR ANALYSIS OF CORCB

In the previous section, we accomplished compression tolerance verification, specifically examining the impact of JPEG compression in the high-frequency range. Additionally, we determined the minimum compression quality through detailed parameter adjustments and thresholds setting. However, there was no evaluation of the effect of RS codes on compression resistance despite the use of Method 2. In addition, the evaluation was insufficient that Lax was an inappropriate image to be used. Therefore, as an extension of the previous study [26, 27], this study continued the verification using other images and confirmed the effect of the RS code.

4.1 *Performance Evaluation of RS Code for JPEG Compression*

In Method 2, RS codes were embedded in the LSB to assist in information restoration, thereby suppressing strength coefficients. However, the verification in the previous section did not state whether the RS codes are still functional after compression, and it was insufficient to verify whether Method 2 is compression-resistant or not.

Therefore, in order to confirm whether RS code helps the recovery even after compression using Method 2, we first checked the parameters after compression with and without the RS code using other images based on the existing study [27]. This resistance test also used the parameters of experimental condition 2, but used the eight images shown in Figure 4 as cover images.

4.1.1 *Verification Procedure*

(T1) Validation Procedure Correlation type method 2 (R1, R2) and experimental condition 2, 8 cover images (Fig. 4) are used for embedding and compression with compression quality Q for each parameter.

(T2) After compression, check whether the resistance requirement PSNR $\geq$ 30 dB $\wedge$ BER $= 0\%$ is satisfied. If so, record the embedding parameters G, S, $Q_{\min}$ and PSNR at the given time.

(T3) To compare the effect of RS codes, we performed a similar search for parameters by brute force (T2) using Method 1 ($E1 \sim F2$).

4.1.2 *Effectiveness and Tolerance Evaluation of RS Code for Method 2*

The results obtained from the analysis are shown in Table III. ✓/× indicates whether the embedded image has parameters that satisfy the threshold, i.e., whether the image can be compressed while maintaining security. As a result, the parameter combinations, PSNR, and compression quality were consistent when comparing the results obtained with methods 1 and 2. Thus, it was found that the RS code is not effective in the case of compression and that Method 2 is not compression tolerant.

In Method 2, the RS code was embedded using the LSB of the stego image. However, the nature of JPEG compression, which modifies LSBs during JPEG encoding and decoding process, might be the reason why the RS code did not function effectively. It also showed that half of the images did not survive compression after embedding. Auxiliary experiments show that images unsuitable for embedding all have very large G for information extraction, and multiplying that G to the M'-sequence for information restoration reduces the PSNR, and the threshold cannot be met even with low compression quality. They are also not suitable for JPEG compression due to low inter-pixel correlation.

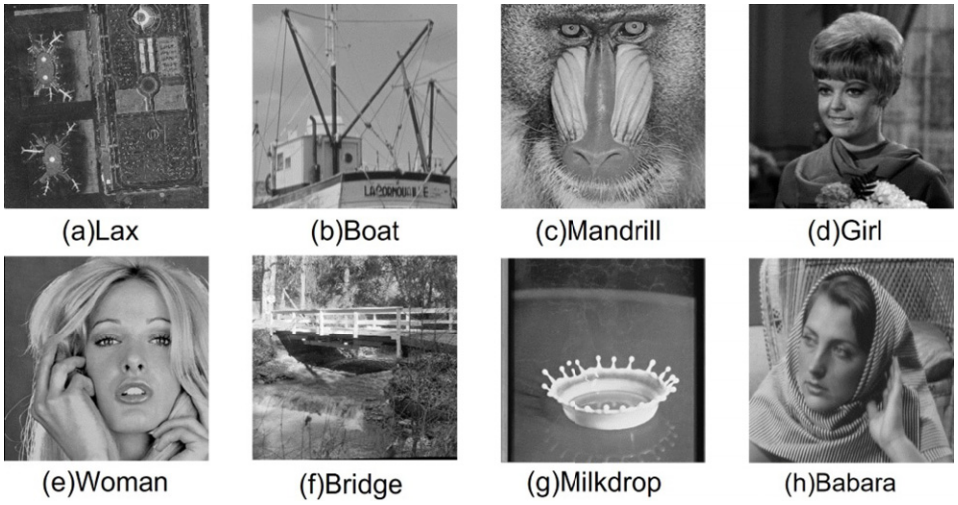

Figure 4. BMP image dataset from SIDBA (Standard Image Database) used in the numerical analysis.

Table III. Embedding conditions for each image satisfying PSNR $\geq$ 30 dB $\wedge$ BER = 0% (results are the same with and without RS code).

Image	✓/×	Q_{min}	S	G	PSNR
Lax	×	—	—	—	—
Boat	✓	91	33	15	30.31
Mandrill	×	—	—	—	—
Girl	✓	92	41	14	30.43
Woman	×	—	—	—	—
Bridge	×	—	—	—	—
Milkdrop	✓	91	36	15	30.02
Babara	✓	93	49	15	30.42

4.2 *Relaxation of BER Limits and Changes to RS Embedding Process*

The experiments in the previous section showed that RS codes do not work after compression, and that evaluation by thresholds indicates that half of the experimental cover images cannot be safely used in environments subject to compression. However, we revisited the threshold and modified the process of introducing RS codes in order to use them in real applications of sensitive information communication using correlation-based methods on arbitrary images.

First, the better the PSNR, the less likely steganalysis or visual steganography will be detected, so the threshold is not changed. On the other hand, since there are many images for which a threshold of BER = 0 can only be achieved by increasing G, which has a trade-off relationship with image quality; we propose a solution. Specifically, we change the threshold to BER $\leq$ 5.5%. CoRCB is a compression-resistant correlation-based method that increases the variety of cover images by reducing the intensity coefficient used and improving image quality.

Experimental conditions with different threshold values are shown in Experimental Condition 3. The image dataset consists of 8 images from SIDBA, Kodak Lossless True Color Image Suite, a dataset of all 24 images called Kodak [30], and 50 images from Berkeley Segmentation Dataset and Benchmark 500 called BSDS [31]. All grayscale images were resized and center-cropped to have an image size 512 × 512. By using these three datasets, we compare the existing method CoRCQ [27] with the proposed method CoRCB to confirm whether there is any change in the parameters obtained even for the images used. In addition, we will also experiment with downsampling to 128 × 128 size for SIDBA. Note that since we have not changed the sub-block size and the amount of embedded information, the payload per sub-block does not change, even in the case of an image size of 128 × 128. The embedding procedure is illustrated in Figure 5.

Experimental condition 3	
Embedded information	512 Bytes
Embedding start position	$S = 20 \sim 49$
M′ series length	$L = 16$
Compression quality	$Q = 75 \sim 100$
Embedded strength factor	$G = 5 \sim 20$
Test Images (bmp 256 × 256)	SIDBA, BSDS, Kodak
Resistant conditions	PSNR $\geq$ 30 dB $\wedge$ BER $\leq$ 5.5%

4.2.1 *Verification Procedure*

(M1) Embedding is performed using the correlation-type Method 1 ($(E1)\sim(F2)$) and the embedding parameters of experimental condition 3.

(M2) Compress the stego image with the compression quality of experimental condition 3 and check if PSNR $\geq$ 30 dB $\wedge$ BER $\leq$ 5.5% is satisfied. Record the embedding parameters G, S, Q_{min}, PSNR and BER at the given time.

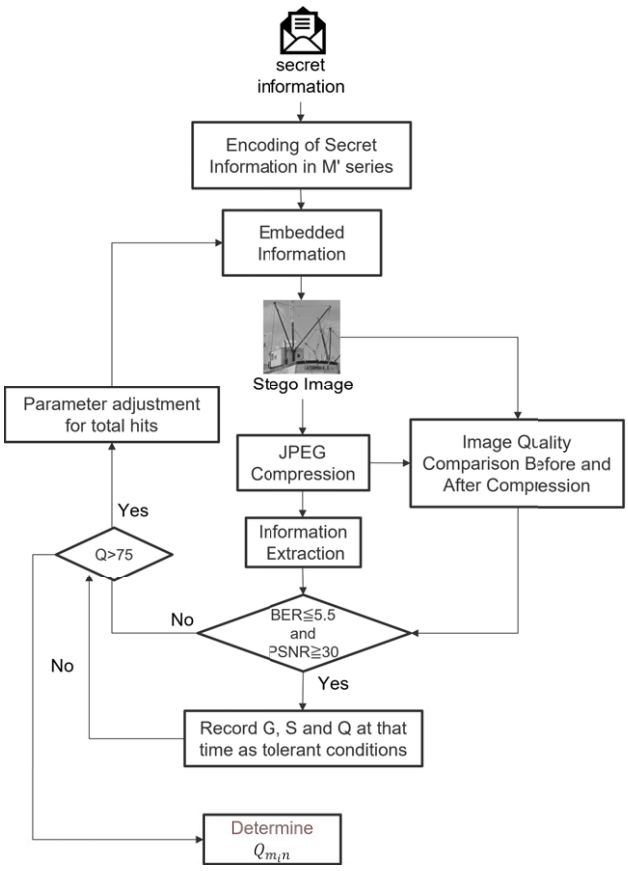

Figure 5. Verification flow with the method of changing the threshold to BER $\leq$ 5.5% and introducing RS codes later.

Table IV. Embedding condition for each image satisfying PSNR $\geq$ 30 dB $\wedge$ BER $\leq$ 5.5% (without RS code).

Image	Q_{min}	S	G	BER	PSNR
Lax	98	47	16	5.05	30.00
Boat	79	20	12	5.37	30.49
Mandrill	90	47	13	4.93	30.00
Girl	76	22	13	5.00	30.06
Woman	81	21	12	5.22	30.14
Bridge	93	49	15	5.15	30.08
Milkdrop	76	21	13	4.27	30.27
Babara	86	32	12	5.32	30.24

(M3) Calculate the required RS code length and real embedding capacity from the obtained BER at minimum quality $Q_{\min}$.

4.2.2 *Enlargement of the Image used by BER Mitigation*

The results of the reverification with the BER loosened according to this proposed method are shown in Table IV.

Table IV confirms that Table III allows the use of images that could not satisfy the threshold and were rated "×" due to the large required intensity coefficient. Therefore, it was found that loosening the BER threshold and designing the RS code to match the information loss after compression is effective in selecting the cover image. Comparing Table III with the parameters obtained, it is evident that the minimum compression quality $Q_{\min}$ of the image that originally showed "✓" has been reduced, indicating that higher compression is possible. The reason for this is that the image quality threshold PSNR $\geq$ 30 dB is not satisfied when the value of G becomes larger than this.

Finally, focusing on the embedding start position S, they show values that appear to be affected by the zigzag scan shown in Figure 6 and the length of the M' series when performing DCT. In particular, there are two major patterns: the mid-frequency range at 21 and 22 and the beginning of the high-frequency range from 47 and 49. Considering the M'-sequence length $L = 16$ used here, the embedding ends at the left end of 36 and 37, and at the right end of 63 and 64, which is a good position for a break. By comparing with the zigzag scan table, it is possible to visually see where the resistant embedding areas are and where the truncation of the most influential information occurs in each image. A low quality factor can also be achieved by selecting images with a mid-frequency embedding parameter of $S = 21, 22$.

Moreover, by using three different image data sets we examined how the detection rate of parameters varies with and without the constraint of BER = 0%. The results shown in Table V indicate that when compression is performed with BER = 0% of CoRCQ [27], the discovery rate of embedding parameters S, G, and $Q_{\min}$ is low, with an average probability of only 38%. In particular, in Kodak [30], the discovery rate is below 20%, which can be attributed to the required value of G for information recovery in Kodak is higher than in other datasets, causing the PSNR to relatively decrease. Table VI shows the results of a similar comparison experiment using images with SIDBA downscaled to 128 × 128. Table VI shows that as the image size decreased, the parameter discovery rate improved by 10% when CoRCQ was used. This is attributed to the fact that the number of parameters that can satisfy the PSNR condition increases. Regardless of the image size, the proposed method always finds parameters

Table V. Parameter discovery rate considering BER for each image set. All images were resized and clopped to 256 × 256.

	SIDBA	BSDS [31]	Kodak [30]	Average
CoRCQ [27]	0.50	0.48	0.17	0.38
CoRCB (ours)	1.0	1.0	1.0	1.0

Table VI. Difference in parameter discovery rate when image size is changed from 256 × 256 to 128 × 128.

	SIDBA (128 × 128)	SIDBA (256 × 256)
CoRCQ [27]	0.63	0.50
CoRCB (ours)	1.0	1.0

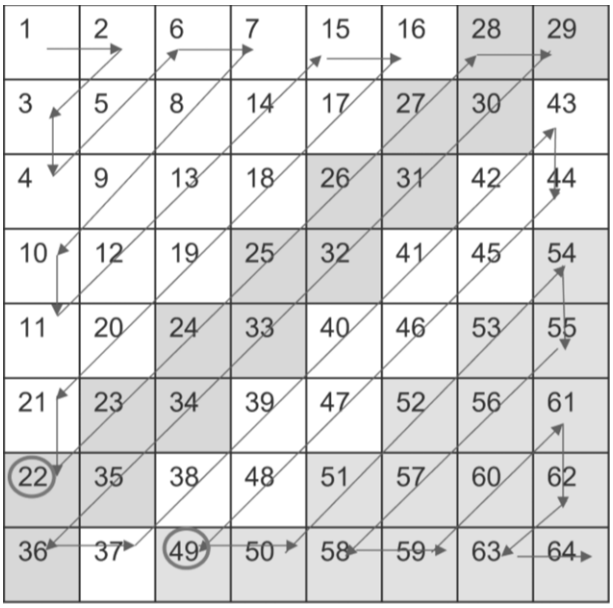

Figure 6. The zigzag scan and the block used for embedding by the detected $S = 22, 49$.

that satisfy the conditions, while the conventional method does not. On the other hand, if we allow for information loss as BER $\leq 5.5\%$ (CoRCB), we find that the parameters can be found in all image datasets and in the images after down sampling.

Therefore, by loosening the BER condition and searching for combinations that satisfy PSNR ≥ 30 dB and BER $\leq 5.5\%$, it was found that the embedding condition could be found for all experimental images. Although BER is allowed to occur in this case, the problem of information loss can be solved by introducing the RS code calculated from the BER, afterwards. In the case of introducing RS codes, only about 10% of the additional embedding capacity is needed to recover the information without significant change, if the error rate is about 5% [32].

Images with characteristics such as those in Kodak, which require large values of G, are more susceptible to BER constraints. By considering the introduction of RS codes after the fact, these images can be used as compression-resistant images.

5. SUMMARY AND FUTURE TASKS

This study confirmed the JPEG compression resistance of the correlation-based method after embedding, and found that the correlation-based method [11], which introduced RS codes in the LSB, had no effect because the error correction codes were removed during JPEG compression, and was not compression resistant. Comparison experiments with CoRCB also showed that the CoCRQ [27], which uses BER $= 0\%$ as the threshold, is an unrealistic method that does not admit information loss even though it assume applying JPEG compression, and the discovery rate of parameters that possess tolerance is less than 40% (Tables V, VI). Therefore, we proposed a new method (CoRCB) that adds redundancy to the secret information to be embedded by obtaining the necessary amount of RS codes from BER after the information is extracted, and re-verified the method. The proposed CoRCB is based on a correlation-based method, which is computationally less expensive than recently proposed deep learning models. Furthermore, classical approaches such as the proposed method have a high explainability for their outputs. Therefore, CoRCB is highly maintainable among methods that consider JPEG compression, and it is easy to implement due to its low dependency on the equipment used.

Experiments with a threshold value of BER $\leq 5.5\%$ showed that the compression resistance condition was satisfied for all images, and the combination of embedding parameters and minimum compression quality were found. The results also show that the minimum compression quality that can be achieved varies greatly depending on the cover image, hence the selection of the image to be used must be appropriate. Therefore, we should consider extending this experiment to generate images suitable for embedding and compression from the acquired features using a GAN model [19–21].

The JPEG compression resistance of the correlative method confirmed in this study will contribute to the increased use of steganography with high security performance in situations where high-resolution images are communicated, such as DICOM™ [33], which is used to exchange examination images in the medical field. In examination images, a single shadow or dot is important for disease detection, but the large data volume of these images makes it difficult to use them for high-speed communication or over ordinary communication channels. Therefore, it is important to consider compression resistance for high-resolution images such as BMP [34].

In future, we aim to improve PSNR in order to propose more secure steganography. For this purpose, it is necessary to consider how to set the BER threshold, which has a trade-off relationship with image quality. In addition, since images are exposed to third parties when used in applications, we plan to investigate the detection resistance of steganalysis [35, 36] to confirm whether it can be used safely in general communication channels.

REFERENCES

[1] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in *Information Hiding Techniques for Steganography and Digital Watermarking*, edited by S. Katzenbeisser and F. Petitcolas (Artech House, Norwood, MA, 2000), Vol. 355, pp. 43–78.

[2] T. Morkel, J. H. Eloff, and M. S. Olivier, "An overview of image steganography," *ISSA* (University of Pretoria, Pretoria, 2005), Vol. 1, pp. 1–11.

[3] C.-K. Chan and L. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit. **37**, 469–474 (2004).

[4] S. Sugathan, "An improved LSB embedding technique for image steganography," *2016 2nd Int'l. Conf. on Applied and Theoretical Computing and Communication Technology (iCATccT)* (IEEE, Piscataway, NJ, 2016), pp. 609–612.

[5] T. Ei, M. Niimi, H. Noda, and E. Kawaguchi, "A study on data hiding of the BPCS-steganography," Technical Report of IEICE PRMU (IEICE, Tokyo, 1998), Vol. 98, pp. 181–188.

[6] A. Westfeld, "F5—a steganographic algorithm," in *Information Hiding*, edited by I. S. Moskowitz (Springer, Cham, 2001), pp. 289–302.

[7] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP J. Information Security* (Springer, Cham, 2014).

[8] K. Onuma and S. Miyata, "A proposal for correlation-based steganography using Shamir's secret sharing scheme and DCT domain," *2021 Int'l. Conf. on Information Networking (ICOIN)* (IEEE, Piscataway, NJ, 2021), pp. 255–260.

[9] T. Filler and J. Fridrich, "Gibbs construction in steganography," Trans. Info. For. Sec. **5**, 705–720.

[10] J. Wang, C. Yang, P. Wang, X. Song,, and J. Lu, "Payload location for JPEG image steganography based on co-frequency sub-image filtering," Int. J. Distrib. Sensor Netw. **16**, 1550147719899569 (2020).

[11] K. Onuma and S. Miyata, "A study of steganography based on error correction code and secret sharing scheme," *2020 3rd Int'l. Conf. on Signal Processing and Information Security (ICSPIS)* (IEEE, Piscataway, NJ, 2020), pp. 1–4.

[12] K. Onuma and S. Miyata, "An improved intensity factor of correlation-based steganography using M-sequence and DCT," SN Comput. Sci. **5**.

[13] Y. Zhang, X. Luo, C. Yang, D. Ye, and F. Liu, "A JPEG-compression resistant adaptive steganography based on relative relationship between dct coefficients," *2015 10th Int'l. Conf. on Availability, Reliability and Security* (IEEE, Piscataway, NJ, 2015), pp. 461–466.

[14] T. Qiao, S. Wang, X. Luo, and Z. Zhu, "Robust steganography resisting JPEG compression by improving selection of cover element," Signal Process. **183**, 108048 (2021).

[15] A. S. Ansari, M. S. Mohammadi, and M. T. Parvez, "A comparative study of recent steganography techniques for multiple image formats," Int. J. Comput. Netw. Inf. Secur. **11**, 11–25 (2019).

[16] M. Niimi, "*Study on Digital Steganography*," Ph.D. thesis (Kyusyu Institute of Technology, 2003).

[17] H. Koda and H. Furuta, "A study on correlation type watermarking scheme for images with RDS embedding in DCT domain," *Bulletin of the University of Electro-Communications* (UEC, Tokyo, 2018), Vol. 30, pp. 62–70.

[18] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image steganography: A review of the recent advances," IEEE Access **9**, 23409–23423 (2021).

[19] Z. Wang, O. Byrnes, H. Wang, R. Sun, C. Ma, H. Chen, Q. Wu, and M. Xue, "Data hiding with deep learning: a survey unifying digital watermarking and steganography," IEEE Trans. Comput. Soc. Syst. **10**, 2985–2999 (2023).

[20] Y. Wencui, Z. Tingge, and L. Ying, "A review of deep learning based image steganography methods," *2024 6th Int'l. Conf. on Natural Language Processing* (IEEE, Piscataway, NJ, 2024), pp. 630–637.

[21] J. Qin, J. Wang, Y. Tan, H. Huang, X. Xiang,, and Z. He, "Coverless image steganography based on generative adversarial network," Mathematics **8**, 1394 (2020).

[22] J. Tao, S. Li, X. Zhang, and Z. Wang, "Towards robust image steganography," IEEE Trans. Circuits Syst. Video Technol. **29**, 594–600 (2019).

[23] X. Duan, B. Li, Z. Yin, X. Zhang, and B. Luo, "Robust image steganography against lossy JPEG compression based on embedding domain selection and adaptive error correction," Expert Syst. Appl. **229**, 120416 (2023).

[24] M. Z. Konyar and S. Öztürk, "Reed solomon coding-based medical image data hiding method against salt and pepper noise," Symmetry **12**, 899 (2020).

[25] Y. Zhang, C. Qin, W. Zhang, F. Liu, and X. Luo, "On the fault-tolerant performance for a class of robust image steganography," Signal Process. **146**, 99–111 (2018).

[26] S. Miyata, "Detection of secret information in the processing of multimedia information," *Computing, Institution of Engineering and Technology* (Elsevier, Amsterdam, 2023), pp. 27–50.

[27] M. Aikawa, S. Miyata, and K. Hirotsugu, "JPEG compression quality setting considering image quality and information loss for correlated steganography," IEICE Technical Report CCS2023-50 (2024).

[28] T. Pevny and J. Fridrich, "Multiclass detector of current steganographic methods for JPEG format," IEEE Trans. Inf. Forensics Secur. **3**, 635–650 (2008).

[29] H. Koda and K. Kaminusi, "On a correlation-based scheme of digital watermarking for images exploiting 2-D LOT," Bull. Univ. Electro-Commun. **23**, 1–10 (2011).

[30] "Kodak lossless true color image suite." https://r0k.us/graphics/kodak/.

[31] D. Martin, C. Fowlkes, D. Tal, and J. Malik, "A database of human segmented natural images and its application to evaluating segmentation algorithms and measuring ecological statistics," *Proc. Eighth IEEE Int'l. Conf. on Computer Vision* (IEEE, Piscataway, NJ, 2001), Vol. 2, pp. 416–423.

[32] K. A. Zhang, A. Cuesta-Infante, L. Xu, and K. Veeramachaneni, "SteganoGAN: High capacity image steganography with GANs," Preprint, arXiv:1901.03892 (2019).

[33] D. R. Varma, "Managing DICOM images: Tips and tricks for the radiologist," Indian J. Radiology Imaging **22**, 4–13 (2012).

[34] P. K. and V. Jaitly, "Securing medical images using compression techniques with encryption and image steganography," *2023 3rd Int'l. Conf. on Intelligent Technologies (CONIT)* (IEEE, Piscataway, NJ, 2023), pp. 1–7.

[35] J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: dead ends challenges, and opportunities," *Proc. 9th Workshop on Multimedia & Security MMSec '07* (Association for Computing Machinery, New York, NY, 2007), pp. 3–14.

[36] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," IEEE Trans. Inf. Forensics Secur. **7**, 432–444 (2011).