INFORMATICA, 2023, Vol. 34, No. 3, 449–464

DOI: https://doi.org/10.15388/23-INFOR521

A Robust and High-Capacity Coverless Information Hiding Based on Combination Theory

Kurnia ANGGRIANI[1,2], Shu-Fen CHIOU[3], Nan-I WU[4], Min-Shiang HWANG[1,5,*]

[1] *Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan*
[2] *Department of Information System, University of Bengkulu, Indonesia*
[3] *Department of Information Management, National Taichung University of Science and Technology, Taiwan*
[4] *Department of Information Management, Lunghwa University of Science and Technology, Taiwan*
[5] *Department of Medical Research, China Medical University Hospital, China Medical University, Taiwan*
e-mail: mshwang@asia.edu.tw

Received: January 2023; accepted: May 2023

Abstract. Many confidential multimedia, such as personal privacy, commercial, and military secrets, are transmitted on the Internet. To prevent this confidential multimedia from being eavesdropped on by illegal users, information-hiding technology is a leading research topic nowadays. One of the important research topics of information-hiding technology is coverless information hiding, which utilizes the unchanged property of its multimedia carrier to hide secret information. In this paper, we propose two schemes that employ the average pixel value of an image. The first is an extension of the Coverless Information Hiding Based on the Most Significant Bit (CIHMSB) scheme, referred to as E-CIHMSB. In the E-CIHMSB, we build an extended matrix containing the image fragment's average pixel value. The second scheme is a combination theory-based CIHMSB, referred to as CB-CIHMSB. In the CB-CIHMSB, we construct the combined matrix. E-CIHMSB and CB-CIHMSB embed the secret bits by changing the most significant bits of the chosen pixel in the matrix. Experimental results show that our schemes achieved higher hiding capacity than previous related schemes. Moreover, the proposed scheme is more robust against steganalysis tools and image quality attacks such as Additive Gaussian White Noise (AWGN), Salt & Pepper noise, low-pass filtering attacks, and JPEG compression attacks than CIHMSB.

Key words: coverless information hiding, image data hiding, image steganography, most significant bit.

1. Introduction

The need for information security in the internet age is inevitable. This is because sensitive information such as military, health care, economic, and personal data is exposed in many

[*] Corresponding author.

applications (Stillman and Defiore, 1980; Liang *et al.*, 2020; Oh *et al.*, 2019; Iwaya *et al.*, 2020; Coleti *et al.*, 2020). One solution to this issue is to implement data-hiding techniques. There are two types of data hiding mechanisms: covered and coverless. Covered information hiding is a well-known and widely investigated topic. In a covered information hiding scenario, the sender must provide a cover media to embed secret messages and create stego media. Cover media include images, audio, and video formats (Mahmoud and Elshoush, 2022; Cogranne *et al.*, 2022; Yi *et al.*, 2019; Liu Y. *et al.*, 2022; Mstafa *et al.*, 2020; Wang *et al.*, 2019). The stego media is then delivered to the recipient. The alteration of the stego media causes distortion and leaves a trace for steganographic analysis tools. Moreover, the hiding capacity of the covered information hiding method has certain limitations due to balancing the stego image quality. Because the greater the hiding capacity, the lower the image quality.

On the other side, the coverless information hiding offers higher hiding capacity without affecting the image quality. The secret messages and cover images are sent as a code stream to the recipient. Furthermore, the coverless information hiding method is more robust against the steganographic analysis tools. The coverless information hiding method utilizes the unchanged property of its multimedia carrier to hide secret information such as pixel value, brightness, and texture. There are several current researches in coverless data hiding (Qin *et al.*, 2019; Peng *et al.*, 2022; Zhou *et al.*, 2019; Wang and Gao, 2019; Luo *et al.*, 2021; Zhou *et al.*, 2022; Chen *et al.*, 2022; Zhang *et al.*, 2018; Liu *et al.*, 2022; Yang *et al.*, 2020; Long *et al.*, 2019; Saad *et al.*, 2021; Anggriani *et al.*, 2023a, 2023b).

In 2020, Peng *et al.* (2022) proposed a coverless information-hiding method based on the Most Significant Bit (MSB) of the cover image (CIHMSB). Their scheme was fragment-based calculation. Begin by segmenting the cover image into several fragments, calculating the average intensity of each fragment, and using the MSB to represent the secret information. As a result, the mapping sequence is used to establish a mapping between the image fragment's MSB and the confidential data. This process generates a mapping flag sent along with the stego image by the sender.

Yang *et al.*'s scheme (2020) is highly resistant to all steganalysis tool attacks because the cover image is the same as the stego image. This scheme, however, has a lower embedding capacity. This is because each segment only embeds one bit—the larger the fragment, the lower the embedding capacity. To address this issue, we propose a change in which the fragment value is used. In addition, we add more average value of the fragment by implementing the concept of combination theory. We can improve the embedding capacity by conducting this approach. Moreover, the proposed scheme is more robust against steganalysis tools and image attacks.

The remainder of the work is presented: Section 2 presents the criteria for evaluating the information-hiding method's performance. Section 3 explains our proposed method. Then, Section 4 discusses the experimental results. Finally, Section 5 addresses the conclusions.

2. The Evaluation Criteria

This section presents some of the parameters used to measure the performance of the information-hiding method. Three evaluation criteria are generally used: image quality assessment, hiding capacity assessment, and robustness analysis.

2.1. *Image Quality Assessment*

The image quality was assessed using the structural similarity (SSIM) index and universal image quality (Q_i) index.

The structural similarity (SSIM) index measures the similarity between the cover and stego images. Its value ranges from -1 to $+1$. When the cover image is the same as the stego image, SSIM is equal to 1, which is also the optimal value of SSIM. It can be expressed by (1):

$$SSIM = \frac{(2\bar{p}\bar{q} + c_1)(2\sigma_{xy} + c_2)}{[(\bar{p})^2 + (\bar{q})^2 + c_1](\sigma_x^2 + \sigma_y^2 + c_2)}, \tag{1}$$

where $\bar{p}$ and $\bar{q}$ represent the average pixel values of the cover and stego images, σ_x^2 and σ_y^2 represent the standard deviation of the cover image and the stego image, respectively. And σ_{xy} represents the covariance between the cover and stego images. Constant $c_1 = 2.55$, $c_2 = 7.65$.

The universal image quality index (Q_i) is another important parameter to measure the similarity between the cover and stego images. When the cover image is the same as the stego image, Q_i can get the optimal value of 1. The definition of Q_i is as (2):

$$Q_i = \frac{4\sigma_{xy}\bar{p}\bar{q}}{(\sigma_x^2 + \sigma_y^2)[(\bar{p})^2 + (\bar{q})^2]}, \tag{2}$$

where $\bar{p}$ and $\bar{q}$ represent the average pixel values of the cover and stego images, σ_x^2 and σ_y^2 represent the standard deviation of the cover and stego images. In contrast, σ_{xy} represents the covariance between the cover and stego images.

2.2. *Hiding Capacity Assessment*

Hiding capacity is defined as the number of secret bits carried in an image. The measurement is ($bits * carrirer^{-1}$).

2.3. *Robustness Analysis*

Robustness analysis is done by providing an attack on the image. Some commonly used image attacks are Additive Gaussian White Noise (AGWN), salt & pepper noise, Low-pass filtering, and JPEG compression. The attack is done on multiple tests. The final results are averaged over multiple tests.

Bit Error Rate (*BER*) is used as the criterion to evaluate the robustness. BER is defined as:

$$BER = \frac{N_m}{N_n} \times 100\%, \tag{3}$$

where N_m represents the number of bits with errors when extracting secret information from the stego image, and N_n represents the total number of bits of secret information to be hidden. The smaller the BER, the more robust the information-hiding method.

3. The Proposed Method

To address the limitation of hiding capacity in Peng *et al.* (2022), we propose two improvement schemes: An extension of Yang *et al.*'s scheme and the combination theory-based scheme. The flowchart of the proposed schemes is depicted in Fig. 1 and Fig. 4, respectively. Furthermore, the proposed schemes can be classified into embedding and extracting procedures explained in the following subsections.

3.1. *An Extension of Yang et al.'s Scheme*

We extend Yang *et al*.'s scheme (2020) by adding an extra average of the fragments; for convenience, we call it E-CIHMSB. The proposed embedding procedures consist of three main steps: cover image preparation, secret data preparation, and mapping. Firstly, preprocess the cover image into fragment image S_i. Then form an extended matrix that contains the average value of the fragment. Secondly, preprocess the secret data into binary format M_i so that it can be operated with the MSB of V_i. Finally, a mapping operation between the MSB of v_i and M_i is conducted. The embedding procedure is detailed and presented below:

- **Preparation of Cover Image**

  1. Segment the cover image T of size $W \times H$ pixels into $(w \times h)$ non-overlapping fragment, S_i.
  2. Form a *Matrix* $1 = \{v_1, v_2, \ldots, v_e\}$

     $$v_i = \textit{avg pixel of the sub-block} \tag{4}$$

     $i = 1$ to e, where $e =$ the number of the sub-block S_i in image.
  3. Extend the *Matrix* 1 by adding one value of the average of Matrix-1.
  4. Convert v_i into the eight-binary format.
  5. Compute the embedding capacity of the cover image using (5):

$$EC = \left(\frac{W \times H}{w \times h}\right) + 1. \tag{5}$$

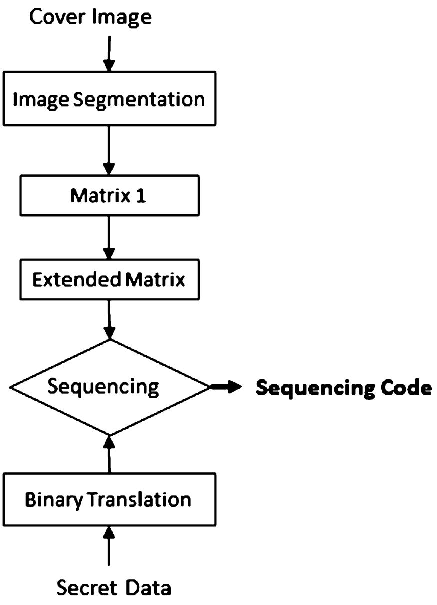


Fig. 1. The flowchart of an extension of Yang *et al.*'s scheme.

Table 1
The mapping rule of embedding procedure.

M_i	MSB of v_i	Z_i
0	0	1
0	1	0
1	0	0
1	1	1

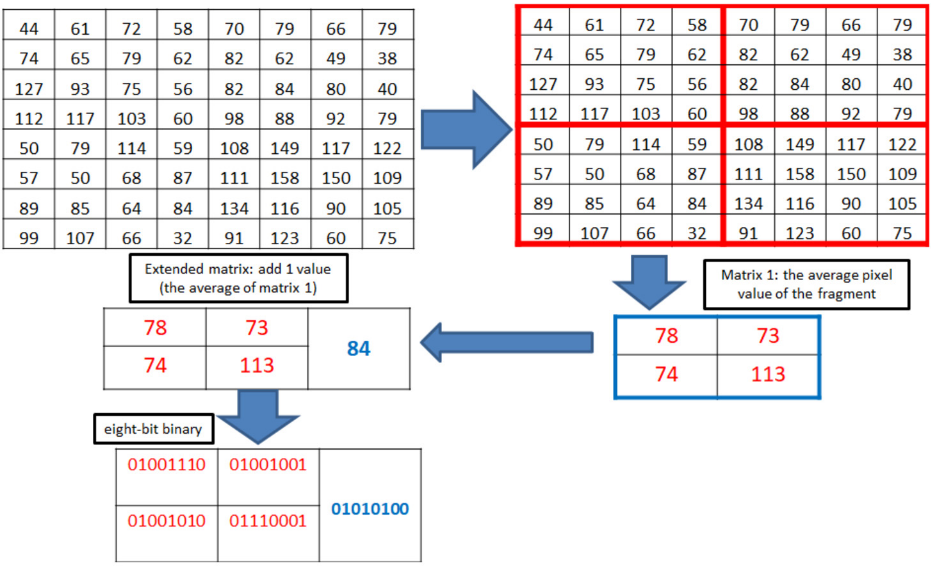
- **Preparation of Secret Data**

1. Convert the secret data into a seven-binary format M_i;
2. Prepare $M_i = EC$.

- **Mapping**

1. Identify the predefined key Q between a sender and receiver, where the length of $Q = EC$.
2. Organize a mapping between M_i and MSB of v_i according to Q. Resulting mapping code Z_i. The rule is shown in Table 1.

Suppose we have a cover image I of size 8×8 pixels. Firstly, preprocess the cover image into a 4×4 non-overlapping fragment, so the number of fragment $S_i = 4$. Then, form a Matrix 1 and extended matrix. The cover image preparation is presented in Fig. 2. Therefore, based on equation (5), we can embed 5 bits of secret data. Suppose the character of secret data is A (the decimal value is 65). Convert into seven-binary format $\boldsymbol{M_i} =$



44	61	72	58	70	79	66	79
74	65	79	62	82	62	49	38
127	93	75	56	82	84	80	40
112	117	103	60	98	88	92	79
50	79	114	59	108	149	117	122
57	50	68	87	111	158	150	109
89	85	64	84	134	116	90	105
99	107	66	32	91	123	60	75

Matrix 1: the average pixel value of the fragment

78	73
74	113

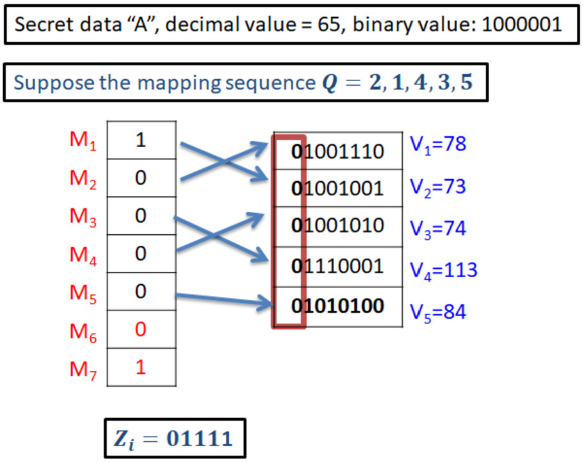
Extended matrix: add 1 value (the average of matrix 1)

78	73	84
74	113	

eight-bit binary

01001110	01001001	01010100
01001010	01110001	

Fig. 2. An example of cover image preparation.



Secret data “A”, decimal value = 65, binary value: 1000001

Suppose the mapping sequence $Q = \mathbf{2, 1, 4, 3, 5}$

M_1	1
M_2	0
M_3	0
M_4	0
M_5	0
M_6	0
M_7	1

01001110	V_1=78
01001001	V_2=73
01001010	V_3=74
01110001	V_4=113
01010100	V_5=84

$Z_i = \mathbf{01111}$

Fig. 3. An example of mapping.

1, **0**, **0**, **0**, **0**, **0**, **1**. Then, the embeddable $M_i = 1, 0, 0, 0, 0$. Suppose the mapping key $\boldsymbol{Q} = \mathbf{2}, \mathbf{1}, \mathbf{4}, \mathbf{3}, \mathbf{5}$. Finally, based on the rule in Table 1, $Z_i = \mathbf{0\ 1\ 1\ 1\ 1}$, as shown in Fig. 3.

3.2. *The Combination Theory-Based Scheme*

The combination theory-based scheme adds more averages of the fragments with a combination theory; for convenience, we call it CB-CIHMSB. The proposed embedding pro-

Table 2
The example of a combined matrix.

$n = 4, r = 1$, $NC = 4$	$n = 4, r = 2$, $NC = 6$	$n = 4, r = 3$, $NC = 4$	$n = 4, r = 4$, $NC = 1$
I_1	$I_1\ I_2$	$I_1\ I_2\ I_3$	$I_1\ I_2\ I_3\ I_4$
I_2	$I_1\ I_3$	$I_1\ I_2\ I_4$	
I_3	$I_1\ I_4$	$I_1\ I_3\ I_4$	
I_4	$I_2\ I_3$	$I_2\ I_3\ I_4$	

cedures consist of three main steps: cover image preparation, secret data preparation, and mapping. Firstly, preprocess the cover image into fragment image S_i. Then form a combined matrix by implementing the concept of combination without repetition. Secondly, preprocess the secret data into binary format M_i so that it can be operated with the MSB of v_i'. Finally, a mapping operation between the MSB of v_i' and M_i is conducted. The embedding procedure is detailed and presented below:

- Preparation of Cover Image

  1. Segment the cover image T of size $W \times H$ pixels into $(w \times h)$ non-overlapping fragment, S_i.
  2. Form the combined matrix without repetition.

  Firstly, obtain the number of combined matrix (NC_r) by (6):

$$NC_r = \frac{n!}{r!(n-r)!}, \tag{6}$$

where n is the number of things to choose from, we choose r of them, with no repetition.

Table 2 presents an example of the combination with no repetition under $n = 4$, $r = 1, 2, 3, 4$, and the NC_r value.

Next, calculate the hiding capacity which is the same as the total number of a combined matrix and is defined by (7):

$$EC = \sum_{i=1}^{r} NC_i = 2^n - 1. \tag{7}$$

Finally, form a *Combined Matrix* $= \{v_1', v_2', \dots, v_e'\}$

$$v_i' = \text{avg pixel of the } NC_i \tag{8}$$

$i = 1$ to e,

where $e =$ the number of the EC.

- Preparation of Secret Data

  1. Convert the secret data into a seven-binary format M_i;
  2. Prepare $M_i = EC$.

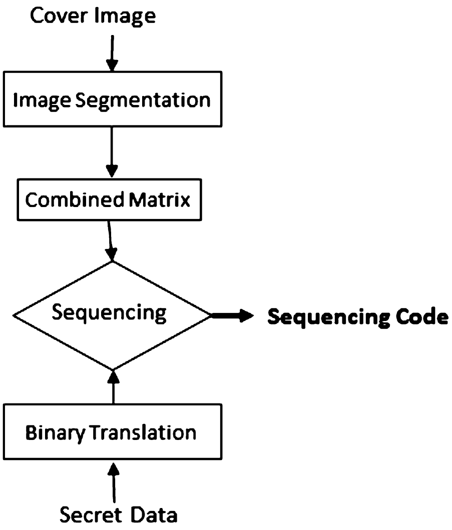


Fig. 4. The flowchart of the proposed combination theory-based scheme.

- Mapping

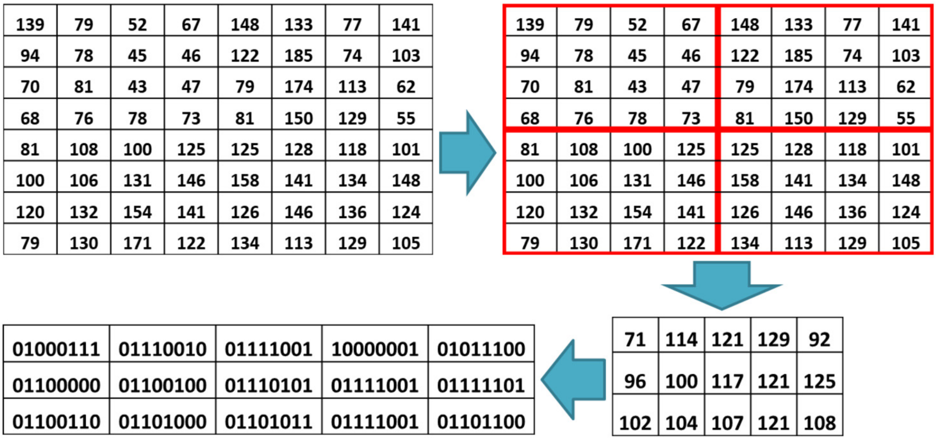
1. Identify the predefined key Q between a sender and receiver, where the length of $Q = EC$.
2. Organize a mapping between M_i and MSB of v_i' according to Q. Resulting mapping code Z_i. The rule is shown in Table 2.

Suppose we have a cover image I of size (8×8) pixels. Firstly, preprocess the cover image into a (4×4) non-overlapping fragment, so the number of fragment $S_i = 4$. Then form the combined matrix. The cover image preparation is presented in Fig. 5. Therefore, based on (7), we can embed 15 bits of secret data. Suppose the character of secret data is A, B, and C, and the decimal value is 65, 66, and 67, respectively. Convert into seven-binary format $M_i = 1, 0, 0, 0, 0, 0, 1,\ 1, 0, 0, 0, 0, 1, 0,\ 1, 0, 0, 0, 0, 1, 1$. The embeddable $\boldsymbol{M_i} = \mathbf{1, 0, 0, 0, 0, 0, 1,\ 1, 0, 0, 0, 0, 1, 0, 1}$.

Suppose the mapping key $Q = 7, 8, 1, 2, 3, 4, 6,\ 5, 10, 9, 11, 12, 14, 13, 15$. Finally, based on the rule in Table 1, $Z_i = \mathbf{0\,1\,1\,1\,1\,1\,0\,0\,1\,1\,1\,1\,0\,1\,0}$, as shown in Fig. 6.

4. Experimental Results

Experimental results were obtained by comparing the performance of CIHMSB (2022), CIHLHF (2023b), LMICS (2022), E-CIHMSB, and CB-CIHMSB. We experimented on the six test grayscale images: Airplane, Baboon, Barbara, Boat, Lena, and Pepper, as shown in Figs. 7(a)–(f), respectively.



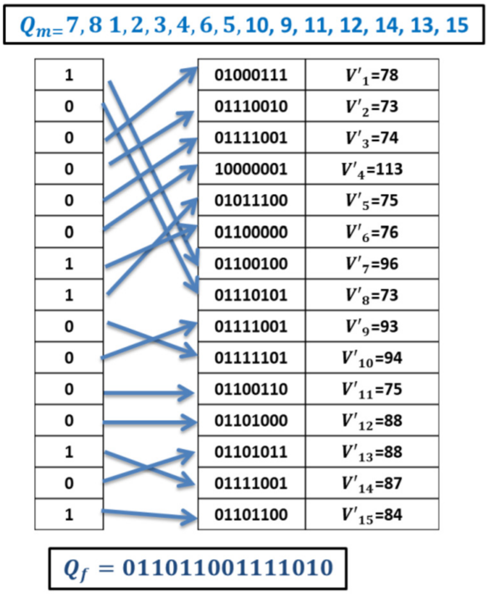
139	79	52	67	148	133	77	141
94	78	45	46	122	185	74	103
70	81	43	47	79	174	113	62
68	76	78	73	81	150	129	55
81	108	100	125	125	128	118	101
100	106	131	146	158	141	134	148
120	132	154	141	126	146	136	124
79	130	171	122	134	113	129	105

139	79	52	67	148	133	77	141
94	78	45	46	122	185	74	103
70	81	43	47	79	174	113	62
68	76	78	73	81	150	129	55
81	108	100	125	125	128	118	101
100	106	131	146	158	141	134	148
120	132	154	141	126	146	136	124
79	130	171	122	134	113	129	105

71	114	121	129	92
96	100	117	121	125
102	104	107	121	108

01000111	01110010	01111001	10000001	01011100
01100000	01100100	01110101	01111001	01111101
01100110	01101000	01101011	01111001	01101100

Fig. 5. An example of cover image preparation.



$Q_{m=}7, 8\ 1, 2, 3, 4, 6, 5, 10, 9, 11, 12, 14, 13, 15$

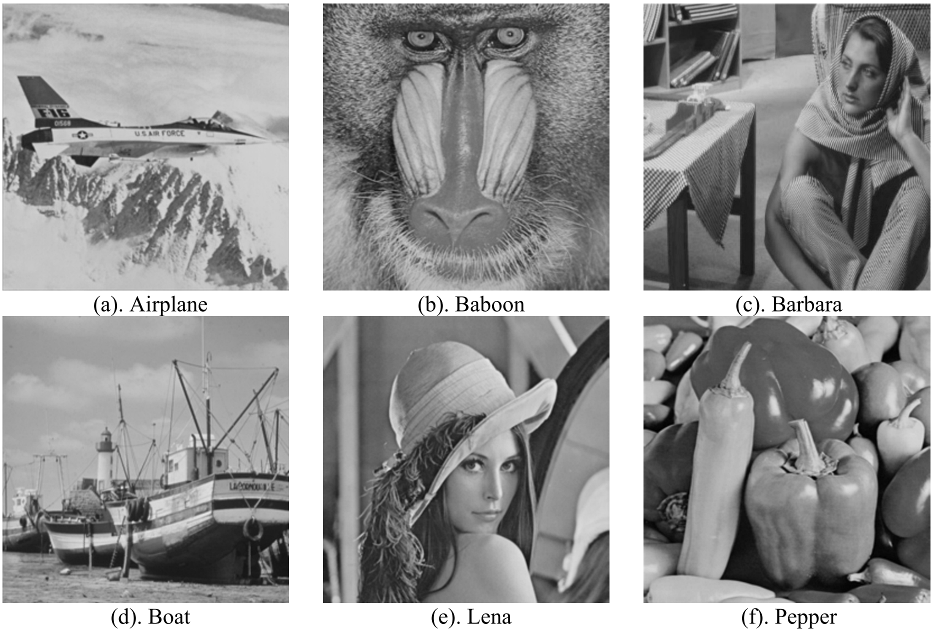
1	01000111	$V'_1=78$
0	01110010	$V'_2=73$
0	01111001	$V'_3=74$
0	10000001	$V'_4=113$
0	01011100	$V'_5=75$
0	01100000	$V'_6=76$
1	01100100	$V'_7=96$
1	01110101	$V'_8=73$
0	01111001	$V'_9=93$
0	01111101	$V'_{10}=94$
0	01100110	$V'_{11}=75$
0	01101000	$V'_{12}=88$
1	01101011	$V'_{13}=88$
0	01111001	$V'_{14}=87$
1	01101100	$V'_{15}=84$

$Q_f = 011011001111010$

Fig. 6. An example of mapping.

4.1. *Image Quality Assessment*

The image quality assessment is shown in Table 4. As seen in Table 4, the SSIM and Q_i of CIHMSB, LMICS, the proposed E-CIHMSB, and CB-CIHMSB schemes are equal to 1, which is also the optimal value. Therefore, it means the cover image is the same as the stego image. It indicated the schemes are coverless.



(a). Airplane (b). Baboon (c). Barbara

(d). Boat (e). Lena (f). Pepper

Fig. 7. Test images.

Table 3
The comparison of image quality between CIHMSB, the proposed E-CIHMSB, and CB-CIHMSB schemes.

Methods	SSIM	Q_i
CIHMSB (2020)	1	1
LMICS (2022)	1	1
E-CIHMSB	1	1
CB-CIHMSB	1	1

4.2. *Hiding Capacity Assessment*

As seen in Table 4, for cover image size 512 × 512 and the fragment size 8 × 8, the hiding capacity is 16384, 20480, and 61440 for CIHMSB (2020), CIHLHF (2023b), E-CIHMSB, and CB-CIHMSB, respectively. Figure 8 presents the hiding capacity comparison of CIHMSB E-CIHMSB and CB-CIHMSB. It can be seen that E-CIHMSB's capacity is 25% higher than CIHMSB's. Moreover, CB-CIHMSB's hiding capacity is 275% higher than CIHMSB and 125% higher than CIHLHF.

4.3. *Robustness Analysis*

In the AGWN attack, we define different intensities σ^2 0.1, 0.5, and 1. In the robustness analysis under salt & pepper noise attack, the noise density increases from 0.001 to

Table 4
The comparison of hiding capacity between CIHMSB, the proposed E-CIHMSB, and CB-CIHMSB schemes.

Methods	Bits	$carrirer^{-1}$	Hiding capacity $(bits * carrirer^{-1})$
CIHMSB (2020)	4	$\frac{512\times512}{8\times8} = 4096$	16384
CIHLHF (2023b)	12		49152
E-CIHMSB	5		20480
CB-CIHMSB	15		61440

Table 5
The type of attacks.

Attack type	Parameters
Additive Gaussian White Noise (AGWN)	Variance = {0.1, 0.5, 1}
Salt & Pepper Noise (SPN)	Variance = {0.001, 0.005}
Low Pass Filtering: Average Filtering (AF)	Window size = {3 × 3, 5 × 5}
JPEG Compression	Quality factor = {50, 70, 90}

Table 6
The comparison of attacks performance.

Attack	CIHMSB	LMICS	E-CIHMSB	CB-CIHMSB
AGWN 0.1	10.7583	N.A	9.6700	7.9700
AGWN 0.5	23.2117	N.A	21.2600	18.4400
AGWN 1	29.4633	N.A	27.1533	24.5517
SPN 0.001	0.1333	0.0083	0.12667	0.12500
SPN 0.005	0.4450	0.0167	0.42500	0.40667
AF (3 × 3)	0.9250	0.0334	0.8367	0.6950
AF (5 × 5)	2.0767	0.0520	1.8450	1.5000
JPEG 50	0.4817	0.0134	0.4517	0.3833
JPEG 70	0.2983	0.0115	0.2683	0.2400
JPEG 90	0.1117	0.0074	0.1033	0.1000

0.005. This experiment uses the average filtering technique to perform a robustness analysis against low-pass filtering attacks. The average filter's size parameters range 3 × 3 and 5 × 5, with 3 × 3 representing the lowest attack and 5 × 5 representing the highest attack. The compression quality (Q) is used in this experiment to perform a robustness analysis against JPEG compression attacks. The JPEG compression quality (Q) ranged 50, 70, and 90 in this experiment. Table 5 provides information about the attack type and used parameters.

Table 6 presents the BER tendency of the CIHMSB, LMICS, E-CIHMSB, and B-CIHMSB. As shown in Table 6, the higher the noise intensity, the higher the BER.

Figure 8 shows the BER comparison value between CIHMSB, LMICS, E-CIHMSB, and CB-CIHMSB under AGWN attack. BER tendency of CB-CIHMSB and E-CIHMSB is lower than CIHMSB. It is proven that E-CIHMSB and CB-CIHMSB are more robust than CIHMSB under the AGWN attack.

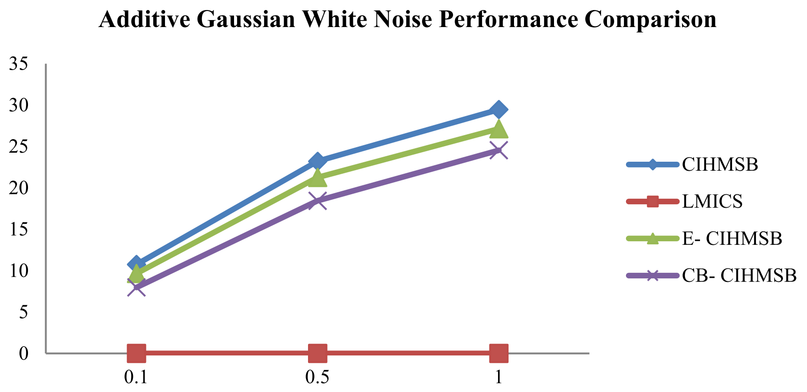


Fig. 8. AGWN performance comparison.

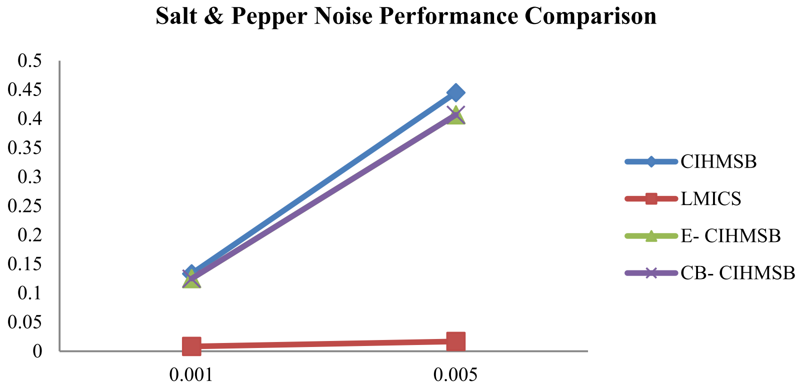


Fig. 9. SPN performance comparison.

Figure 9 shows the BER comparison value between CIHMSB, LMICS, E-CIHMSB, and CB-CIHMSB under the Salt & Pepper attack. BER tendency of CB-CIHMSB and E-CIHMSB is lower than CIHMSB. Generally, the proposed E-CIHMSB and CB-CIHMSB schemes are more robust than CIHMSB under the Salt & Pepper attack.

Figure 10 shows the BER comparison value between CIHMSB, LMICS, E-CIHMSB, and CB-CIHMSB under a low-filtering attack. Again, the BER increases as the filtering size increases. BER tendency of CB-CIHMSB and E-CIHMSB is lower than CIHMSB. Therefore, the robustness of the proposed E-CIHMSB and CB-CIHMSB schemes under a low-filtering attack is greater than that of CIHMSB.

Figure 11 depicts the BER between CIHMSB, LMICS, E-CIHMSB, and CB-CIHMSB schemes when subjected to a JPEG compression attack with varying Q. The BER increases as Q decreases. The proposed E-CIHMSB and CB-CIHMSB schemes are more resistant to JPEG compression than CIHMSB.

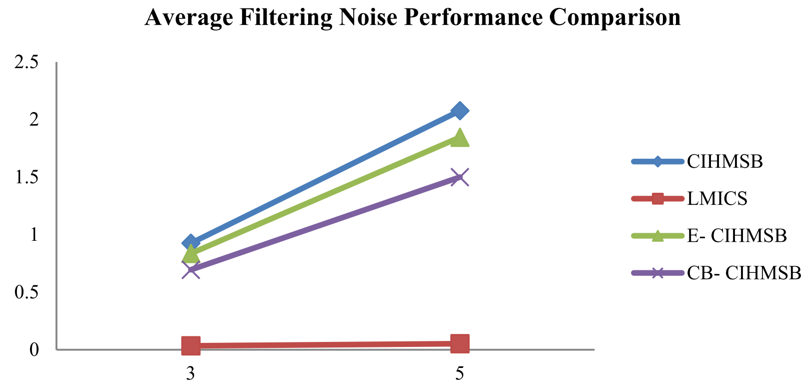


Fig. 10. AF performance comparison.

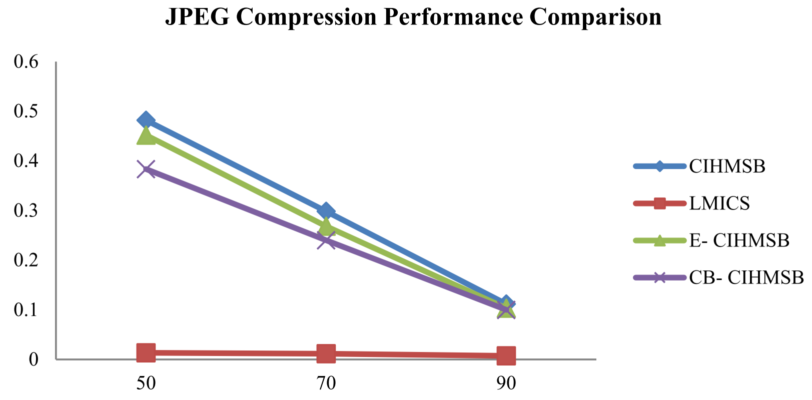


Fig. 11. JPEG compression performance comparison.

5. Conclusion

This study proposed two coverless information hiding methods, E-CIHMSB and CB-CIHMSB, to improve the CIHMSB method's hiding capacity. The difference between the two methods is in creating the cover image. The first proposed method uses image segmentation to compute each average, after which the extended average value is calculated. The second proposed method, with the combination theory, is used to obtain a higher average value. The greater the number of average value, the greater the hiding capacity. We follow the mapping and sequencing operations for the first and second methods, respectively. We investigate the robustness of the proposed method under AWGN, Salt & Pepper noise, low-pass filtering, and JPEG compression attacks. It has been demonstrated that the proposed method is resistant to steganalysis attacks. The experimental results show that our proposed method's hiding capacity outperforms CIHMSB.

References

Anggriani, K., Wu, N.-I., Hwang, M.-S. (2023a). Research on coverless image steganography. *International Journal of Network Security*, 25(1), 25–31. https://doi.org/10.6633/IJNS.202301_25(1).03.

Anggriani, K., Chiou, S.-F., Wu, N.-I., Hwang, M.-S. (2023b). A high-capacity coverless information hiding based on the lowest and highest image fragments. *Electronics*, 12, 395. https://doi.org/10.3390/electronics12020395.

Chen, X., Zhang, Z., Qiu, A., Xia, Z., Xiong, N.N. (2022). Novel coverless steganography method based on image selection and StarGAN. *IEEE Transactions on Network Science and Engineering*, 9(1), 219–230. https://doi.org/10.1109/TNSE.2020.3041529.

Cogranne, R., Giboulot, Q., Bas, P. (2022). Efficient steganography in JPEG images by minimizing performance of optimal detector. *IEEE Transactions on Information Forensics and Security*, 17, 1328–1343. https://doi.org/10.1109/TIFS.2021.3111713.

Coleti, T.A., Luiz, P., Corrêa, P., Vilela, L., Filgueiras, L., Morandini, M. (2020). TR-model. A metadata profile application for personal data transparency. *IEEE Access*, 8, 75184–75209. https://doi.org/10.1109/ACCESS.2020.2988566.

Iwaya, L.H., Ahmad, A., Babar, M.A. (2020). Security and privacy for mHealth and uHealth systems: a systematic mapping study. *IEEE Access*, 8, 150081–150112. https://doi.org/10.1109/ACCESS.2020.3015962.

Liang, Y., Quan, D., Wang, F., Jia, X., Li, M., Li, T. (2020). Financial big data analysis and early warning platform: a case study. *IEEE Access*, 8, 36515–36526. https://doi.org/10.1109/ACCESS.2020.2969039.

Liu, Q., Xiang, X., Qin, J., Tan, Y., Zhang, Q. (2022). A robust coverless steganography scheme using camouflage image. *IEEE Transactions on Circuits and Systems for Video Technology*, 32(6), 4038–4051. https://doi.org/10.1109/TCSVT.2021.3108772.

Liu, X., Li, Z., Ma, J., Zhang, W., Zhang, J., Ding, Y. (2022). Robust coverless steganography using limited mapping images. *Journal of King Saud University – Computer and Information Sciences*, 34(7), 4472–4482. https://doi.org/10.1016/j.jksuci.2022.05.012.

Liu, Y., Ni, J., Zhang, W., Huang, J. (2022). A novel video steganographic scheme incorporating the consistency degree of motion vectors. *IEEE Transactions on Circuits and Systems for Video Technology*, 32(7), 4905–4910. https://doi.org/10.1109/TCSVT.2021.3135384.

Long, Y., Liu, Y., Zhang, Y., Ba, X., Qin, J. (2019). Coverless information hiding method based on web text. *IEEE Access*, 7, 31926–31933. https://doi.org/10.1109/ACCESS.2019.2901260.

Luo, Y., Qin, J., Xiang, X., Tan, Y. (2021). Coverless image steganography based on multi-object recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 31(7), 2779–2791. https://doi.org/10.1109/TCSVT.2020.3033945.

Mahmoud, M.M., Elshoush, H.T. (2022). Enhancing LSB using binary message size encoding for high capacity, transparent and secure audio steganography—an innovative approach. *IEEE Access*, 10, 29954–29971. https://doi.org/10.1109/ACCESS.2022.3155146.

Mstafa, R.J., Younis, Y.M., Hussein, H.I., Atto, M. (2020). A new video steganography scheme based on Shi-Tomasi corner detector. *IEEE Access*, 8, 161825–161837. https://doi.org/10.1109/ACCESS.2020.3021356.

Oh, H., Park, S., Lee, G.M., Heo, H., Choi, J.K. (2019). Personal data trading scheme for data brokers in IoT data marketplaces. *IEEE Access*, 7, 40120–40132. https://doi.org/10.1109/ACCESS.2019.2904248.

Peng, F., Chen, G., Long, M. (2022). A robust coverless steganography based on generative adversarial networks and gradient descent approximation. *IEEE Transactions on Circuits and Systems for Video Technology*, 32(9), 5817–5829. https://doi.org/10.1109/TCSVT.2022.3161419.

Qin, J., Luo, Y., Xiang, X., Tan, Y., Huang, H. (2019). Coverless image steganography: a survey. *IEEE Access*, 7, 171372–171394. https://doi.org/10.1109/ACCESS.2019.2955452.

Saad, A.H.S., Mohamed, M.S., Hafez, E.H. (2021). Coverless image steganography based on optical mark recognition and machine learning. *IEEE Access*, 9, 16522–16531. https://doi.org/10.1109/ACCESS.2021.3050737.

Stillman, R.B., Defiore, C.R. (1980). Computer security and networking protocols: technical issues in military data communications networks. *IEEE Transactions on Communications*, 28(9), 1472–1477. https://doi.org/10.1109/TCOM.1980.1094838.

Wang, K., Gao, Q. (2019). A coverless plain text steganography based on character features. *IEEE Access*, 7, 95665–95676. https://doi.org/10.1109/ACCESS.2019.2929123.

Wang, J., Jia, X., Kang, X., Shi, Y.-Q. (2019). A cover selection HEVC video steganography based on intra prediction mode. *IEEE Access*, 7, 119393–119402. https://doi.org/10.1109/ACCESS.2019.2936614.

Yang, L., Deng, H., Dang, X. (2020). A novel coverless information hiding method based on the most significant bit of the cover image. *IEEE Access*, 8, 108579–108591. https://doi.org/10.1109/ACCESS.2020.3000993.

Yi, X., Yang, K., Zhao, X., Member, S., Wang, Y., Yu, H. (2019). AHCM: adaptive Huffman code mapping for audio steganography based on psychoacoustic model. *IEEE Transactions on Information Forensics and Security*, 14(8), 2217–2231. https://doi.org/10.1109/TIFS.2019.2895200.

Zhang, X., Peng, F., Long, M. (2018). Robust coverless image steganography based on DCT and LDA topic classification. *IEEE Transactions on Multimedia*, 20(12), 3223–3238. https://doi.org/10.1109/TMM.2018.2838334.

Zhou, Z., Cao, Y., Wang, M., Fan, E., Wu, Q.M.J. (2019). Faster-RCNN based robust coverless information hiding system in cloud environment. *IEEE Access*, 7, 179891–179897. https://doi.org/10.1109/ACCESS.2019.2955990.

Zhou, Z., Su, Y., Zhang, Y., Xia, Z., Du, S., Gupta, B.B., Qi, L. (2022). Coverless information hiding based on probability graph learning for secure communication in IoT environment. *IEEE Internet of Things Journal*, 9(12), 9332–9341. https://doi.org/10.1109/JIOT.2021.3103779.

K. Anggriani received her BS degree in informatics from University of Bengkulu, Indonesia, in 2011, and the MS degree in informatics from Bandung Institute of Technology, Indonesia, in 2014. She is a lecturer at the Department of Information System, Engineering Faculty, University of Bengkulu, Indonesia. Currently, she is pursuing her PhD degree in Asia University, Taiwan. Her current research interests include steganography and image processing.

S.-F. Chiou received the BBA degree in information management from National Taichung Institute of Technology, Taichung, Taiwan, ROC, in 2004. She studied for a MS degree in computer science and engineering at the National Chung Hsing University for one year, and then started to pursue her PhD degree. She received her PhD in computer science and engineering from National Chung Hsing University in 2012. She is currently an assistant professor in the Department of Information Management, National Taichung University of Science and Technology. Her current research interests include information security, network security, data hiding, text mining and big data analysis.

N.-I Wu received his PhD from the Institute of Computer Science and Engineering, Nation Chung Hsing University (NCHU), Taichung, Taiwan 2009. From 2010 to 2011, he was a post-doctoral research fellow at the Academia Sinica Institute of Information Science. He was an assistant professor at the Department of Animation and Game Design, TOKO University (Taiwan), during 2011–2018, and an associate professor during 2018–2019. He was an associate professor at the Department of Digital Multimedia, Lee-Ming Institute of Technology (Taiwan) during 2019–2023. Now he is an associate professor at the Department of Information Management, Lunghwa University of Science and Technology (Taiwan) since 2023 and also the director of the eSports Training Centre since 2020. His current research interests include game design, eSports training/management, multimedia processing, multimedia security, data hiding, and privacy-preserving. He published over ten international journal papers (SCI) and conference papers.

M.-S. Hwang received MS in industrial engineering from National Tsing Hua University, Taiwan in 1988, and a Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan, in 1995. He was a distinguished professor and Chairman of the Department of Management Information Systems, NCHU, during 2003–2011. He obtained 1997, 1998, 1999, 2000, and 2001 Excellent Research Awards from the National Science Council (Taiwan). Dr. Hwang was a dean of the College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with the Department of Computer Science and Information Engineering, AU. His current research interests include information security, electronic commerce, database, data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles.