

Enhancing of coverless image steganography capacity based on image block features

Hadeel Talib Mangi, Suhad A. Ali, Majid Jabbar Jawad

Department of Computer Science, College of Science for women, University of Babylon, Hilla, Iraq

Article Info

Article history:

Received Nov 21, 2022

Revised Nov 29, 2022

Accepted Feb 16, 2023

Keywords:

Block dividing
Coverless steganography
Hashing generation
Hiding capacity
Information hiding

ABSTRACT

The idea of coverless information hiding has seen a great deal of development since it was initially introduced due to its effectiveness in defeating steganalysis tools. However, the capacity for general coverless information hiding methods to conceal information is limited, as well as no previous methods worked at the other requirements such as robustness. In this paper, a coverless image steganography (CIS) method for increasing capacity is proposed while retaining the robustness. The proposed method consists of several steps. Firstly, the secret data is segmented into segments of the n length. Secondly, a suitable image that has features similar to the secret message is selected and divided into non-overlapping blocks. Thirdly, these blocks are transformed into the frequency domain by applying discrete wavelet transform (DWT). Fourthly, building a hash sequence table using a suggested hashing algorithm. Fifthly, to reduce search time an indexing table is built based on the generated hash sequence. Sixthly, match each segment with the generated hash sequences and save the auxiliary information for each matched segment in the image in a file. Lastly, send the stego image and the auxiliary information file to the receiver. The experimental results show that the CIS method produces high capacity compared with previous CIS methods.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Suhad A. Ali

Department of Computer Science, College of Science for women, University of Babylon

Hilla, Iraq

Email: suhad_ali2003@yahoo.com

1. INTRODUCTION

In the modern world, security issues related to information transmission have grown to be a major concern to prevent unanticipated outcomes [1], [2]. Two technologies can be used for saving any particular firm from losing its priceless information namely steganography and cryptography. The issue with cryptography is that security will be compromised after decryption. Steganography is proposed to address the drawback related to cryptography [3]. Steganography is the art or science in which the secret message is embedded undetectably in the carrier so that no one except the sender and receiver will be aware of its existence of it [4]-[6]. Many works have been done in image steganography because images are one of the crucial carriers utilized in multimedia communication [7]. Steganography can be classified into two types namely traditional image steganography and coverless image steganography. Additionally, there are two subcategories of data embedding methods: frequency domain and spatial domain [8], [9]. Spatial domain approaches directly alter the pixels in the image, enabling imperceptibility and hiding more information. The drawback of the spatial domain is that is vulnerable to common attacks [10]. For this reason, the frequency domain is suggested for embedding data. There are several transformation tools such as discrete Fourier transform (DFT) [11], discrete wavelet transform (DWT) [12], and discrete cosine transform (DCT)

[13]. The traditional steganography typically changes the carrier just enough to disguise the information. Unfortunately, the changing of the cover after embedding a secret message can be detected by smart steganalysis techniques. To avoid being discovered, coverless steganography is produced [14]. The objective behind coverless steganography is to choose cover images that have features that indicate secret information [15]. A potent hashing method can be used to map associations between visual features and hidden message parts [16]. The image is divided into numerous blocks and the hash algorithm is used to create one or more hash sequences from it [17]. The current coverless drawback, several stego-images are used to communicate a single hidden message in information hiding strategies based on mapping relationships. Besides, there may be instances where we are unable to locate images that satisfy the requirement.

In this area, various researches have been conducted. In Zhou *et al.* [18] proposed one of the first methods of coverless image steganography, which uses an image to represent 8 bits. This method consists of building an image database containing at least 256 different images collected from the internet, then indexing the database according to the 8-bit binary sequence generated by the established mapping rule. In Zhou *et al.* [19] and his research team proposed a coverless image steganography (CIS) based on histograms of oriented gradients (HOGs)-based hashing algorithm. In this method, the original images are split into non-overlapping blocks and find HOG for each block, and generate a hash sequence for each block then the images that have a block where the hash sequence of it is equal to the secret information are selected. However, for improving the capacity of the method introduced in [1]. An effective image hashing algorithm is introduced by Zheng *et al.* [20] and his research team that employs scale-invariant feature transform (SIFT) and creates the hash approach using the SIFT feature points' orientation information to increase the robustness of the image hash. Each carrier image's hash sequence can hold up to 18 bits of hidden data in this approach. However, it still needs to download a large number of images when increasing the length of secret data. In [21] using the DCT and latent Dirichlet allocation (LDA) to categorize an image database according to its topics, this technique uses LDA for clustering the images according to topics; each image in the DCT domain is used to construct the hash sequence. However, 1–15 bits of information can be concealed in a single image. In Bravo *et al.* [22] suggest the generative model-based coverless image information concealment technique. The type of secret data is an image and gives the secret image to the generative model database, which will then produce a meaning-normal and independent image that is distinct from the secret image. The produced image is sent to the receiver and given to the generative model database, producing a new image that is visually identical to the secret image. A coverless steganography technique was recently created in [23] that is based on the "partial_duplicate". It split each image into non-overlapping patches, the technique sends several carrier images from a previously created database that have patches that are identical to the secret image. In Yang *et al.* [24] and her research team developed a CIS technique based on the cover image's most significant bit. The cover image has been divided up into a few fragments. The secret message s converted to binary form. Following that, the mapping between the most significant bit (MSB) of the fragments and the confidential information is established in line with outputs of a mapping flag Kf to the mapping sequence Km . The receiver can extract the secret information from the stego image using Kf and Km . In [25] based on eigen decomposition, the work employed a single cover image to deliver secret information. By creating mapping relationships between the characters of the secret message and the hash codes of the image blocks. Block size, configurations of sub-blocks, and overlapping blocks are three crucial factors in the method. According to the analyses' findings, there must be an overlap between image blocks to produce a large enough number of distinct hash codes to increase capacity. This work presents a block based coverless image steganography strategy employing a single cover image by increasing the capacity of the cover image and retaining the robustness by working on the transform domain.

2. METHOD

Explaining Figure 1 illustrates the proposed CIS, it consists of several steps for two sides (sender and receiver). In the sender side, there are two steps, the first step is for generating the hash sequences process in the Figure 1(a) and the second is the embedding of the secret data process in Figure 1(b). The receiver side will extract the secret data lastly in Figure 1(c). These steps are further explained in the subsequent subsections.

2.1. Sender side

On this side, there are two activities have been performed. The first activity is the hash sequences generation activity which describes the steps that are done for extracting the hash sequences from the cover image. The second activity is the embedding activity of the secret data by the generated hash sequences.

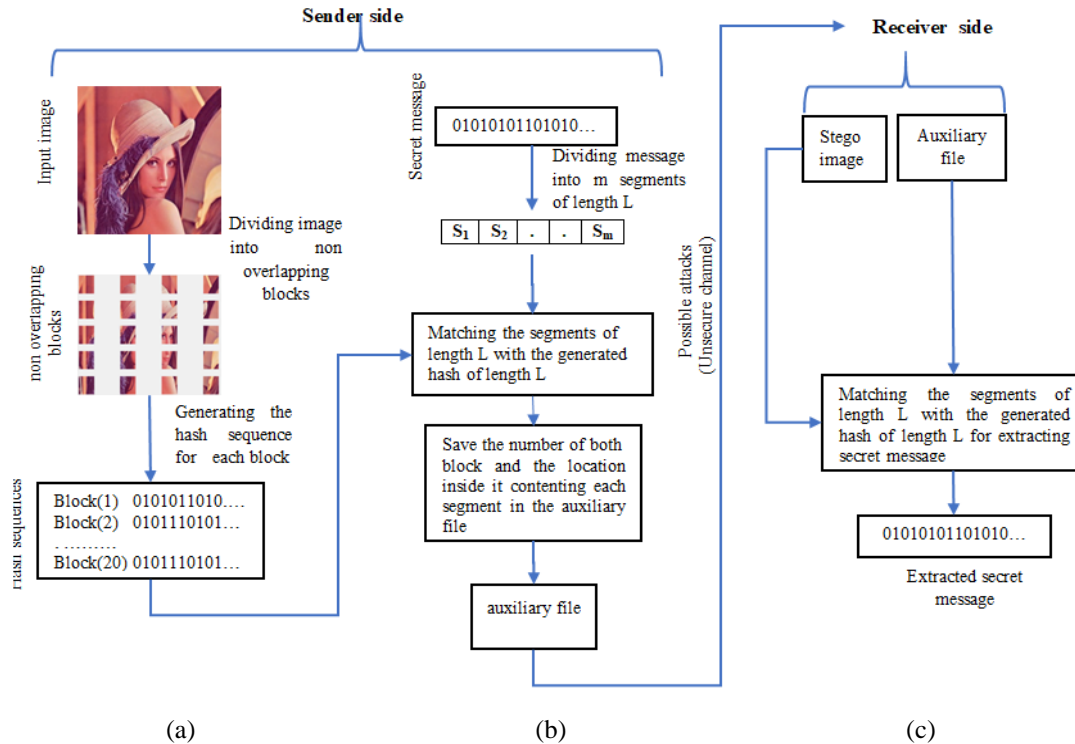


Figure 1. The proposed CIS method: (a) hash sequence generation activity, (b) embedding activity, and (c) extracting activity

2.1.1. Hash sequence generation activity

Hash sequence generation is done in the frequency domain by applying the following steps:

- Step 1: selecting an image for hiding a secret message such that the image must have features similar same as a secret message.
- Step 2: dividing the selected image into non-overlapping blocks with size (8×8) .
- Step 3: hash sequence is created from the coefficient of the image block by implementing the DWT on each block to generate four subbands (low low, low high, high low, and high high).
- Step 4: choosing the low low subband (LL) for each block.
- Step 5: doing quantization by dividing each coefficient in the LL subband by 2 to increase the robustness of the proposed method.
- Step 6: generation of a hash sequence from LL subband coefficients with dimension (8×8) . Then for each row (i) apply the (1) to obtain a hash sequence with length (7).

$$H_{LL(i)} = \begin{cases} 1, & \text{if } LL(i) > LL(i+1) \\ 0, & \text{otherwise} \end{cases} \text{ where } 1 \leq i < 8 \quad (1)$$

The number of rows is (8) and the number of columns is (7) which represents the hash sequence in each row. The total length of the hash sequence obtain from the LL subband for each block is $(8 \times 7 = 56)$ which will be converted into a vector and save as a column in the hash table for block no. which represents the row in the table.

For the selected cover image, a hash table is generated by applying hash sequences activity as shown in (Figure 2). This table is generated for saving the generated hash sequences. This table consists of two columns (block no, and the generated hash sequence corresponding to each block).

2.1.2. Embedding activity

In this activity, the secret message is splitting into segments with length $(n \text{ bits})$ which is mean that hash sequences from $(0 \dots 2^n)$ must be found in the cover image. Then, each segment will be matched with a hash table to find the block that its sequence matched to the sequence of the segment. The matching process is done in an overlapping way. The block number and the location of the matching for each segment are saved in the auxiliary information file. This file will be encrypted and send with a stego image to the receiver. Figure 3 shows the embedding activity with segment length $(n = 4)$.

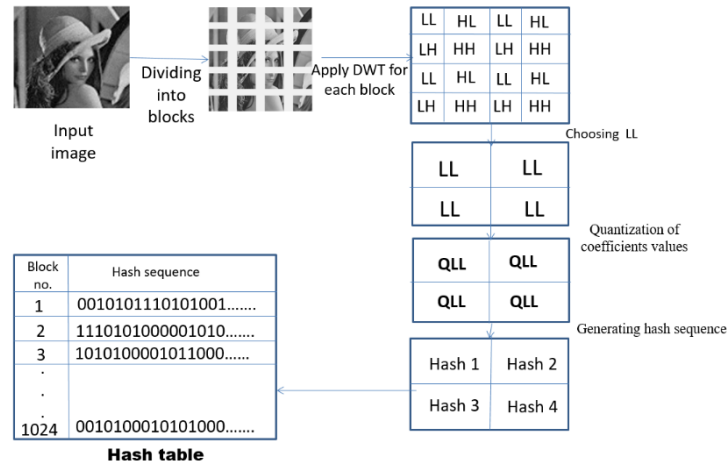


Figure 2. Hash sequence generation

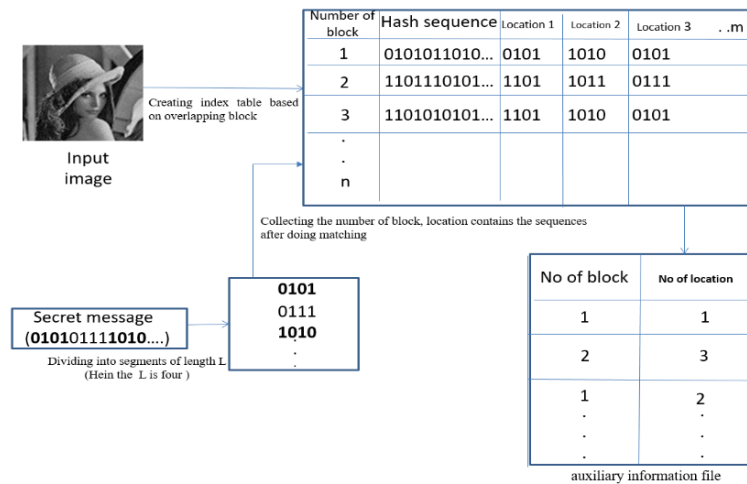


Figure 3. Block diagram of embedding activity

2.2. Receiver side

On this side, the stego image and auxiliary information file are received. The stego image is divided into non-overlapping blocks with size (8×8). Then, the hash sequences table is constructed in the same way that is done by the sender by applying steps in section 3.1. By using the auxiliary information file, the secret message is extracted from the hash sequences table as shown in Figure 1(c).

3. RESULTS AND DISCUSSION

The suggested coverless method's effectiveness is evaluated in terms of embedding, capacity, and robustness. The evaluation of the embedding process is for testing the effectiveness of the proposed system of embedding and extracting processes. The evaluation of the capacity criteria is for testing the gained capacity of the cover image. The robustness criteria is taken also for testing the resistance of the image against attacks.

3.1. Testing the embedding and extracting procedure

For understanding the suggested approach, suppose that we have a secret message (as shown in Figure 4) and a sample of images dataset (as shown in Figure 5). The sample that was taken consists of six images. The results of embedding and extracting processes steps that are done on the taken samples will show in details.

0 0 1 0 1 0 1 0 1 1 1 0 - -

Figure 4. The secret message



Figure 5. Sample of image dataset

On the sender side, the embedding process is carried out as:

- a. Splitting the secret message into s segments of length n (herein $n = 4$). That means the possible probabilities of hash sequences from (0000) to (1111) must be found in the cover image. Figure 6 shows the splitting of the secret message into segments with ($n = 4$).

Segment no.	1	2	3	.	.	S
Bits	0010	1010	1110	.	.	.

Figure 6. The secret message after dividing

- b. Selecting a cover from the dataset of size $I \times I$ (herein $I = 256$), dividing the cover into non-overlapping blocks of size $M \times M$ pixels (herein $M = 8$). So, the number of blocks is 1024.
- c. Generating a hash sequence from each block according to section 3.1. Figure 7 illustrates the result of hash sequences of size 1024×64 .

Block no.	Sequence (bit no.)									
	1	2	3	4	5	6	.	.	.	63
1	1	0	1	1	1	0	.	.	.	0
2	0	0	0	0	0	0	.	.	.	0
3	0	0	0	0	0	0	.	.	.	0
.
1024	0	0	0	0	0	0	.	.	.	0

Figure 7. The generated hash sequences

- d. Mapping each segment of the secret message with a similar hash sequence saved in the hash table. For example, segment no. three is similar to the segment that is found in block no. 1 and location no. 3 as shown in Figure 8.
- e. Saving the results of mapping operating in a file. Figure 9 illustrates the results of the mapping procedure.

Block no	Location no.										
	1	2	3	.	5	.	7	.	29	.	56
1	1011	0111	1110	.	.	.	1010
2	0000	0000	0000
3	0000	0000	0000
4	0000	0000	0000	0010	.	.
.
1024	0000	0000	0000

Figure 8. Mapping process

- f. Sending the stego image and the auxiliary information file to the receiver. On the receiver side, the extracting process is carried out as:
- Receiving the stego image and auxiliary information file.
 - Generating the hash table from the stego image (as described on the sender side).
 - Extracting the secret message by the auxiliary information file and hash sequence.
- Figure 10 illustrates the extracted message.

Block no.	Location no.
4	29
1	3
.	.
1	7
.	.
.	.

Figure 9. Auxiliary information file

Segment no.	1	2	3	.	.	s
Bits	0010	1010	1110	.	.	.

Figure 10. extracted message

3.2. The information hiding capacity

The suggested approach can store non-specific bits of information in each image block depending on the size of the image and the size of the blocks. The mapping process is an overlapping way that increases the hiding capacity. The hiding capacity in each block with size $(L \times L)$ depends on the overlapping ratio.

In general, for the overlap ratio equal to (1) the block capacity (B_C) is calculated:

$$B_C = L \times (L - 1) \quad (2)$$

For an image of size $(M \times N)$ that divides into a block of size $(L \times L)$ with an overlap ratio equal to (1) the capacity (C) can be calculated:

$$C = \frac{M}{L} \times \frac{N}{L} \times B_C \quad (3)$$

However, each block can store ($B_C = 56$ bits) of data when the size of the image is 256×256 pixels and the size of each block is 8×8 pixels. Therefore, the hiding capacity is $1024 \times 56 = 57,344$ bits per cover image and when increasing the image size, the number of blocks also increases therefore, embedding capacity also increases. Consider a 512×512 grayscale image. The proposed method's hiding capacity is computed in Table 1. The ability of various strategies to conceal information is seen in the Table 1. It can be shown that our method has a greater hiding capacity compared with the literature's other methods in comparison applied to embed.

Table 1. The hiding capacity of different information hiding approaches

Method	Capacity (bits/image)
HOGs [19]	8
SIFT+BOF [16]	8
SIFT [20]	18
DCT+LDA [21]	1–15
(non-overlapping) [25]	6272
(overlapping) [25]	55,112
The proposed method	229,376

3.3. Robustness measures

Two metrics are used for measuring the robustness of the proposed method namely, normalized correlation (NC) and bit error rate (BER). The similarity between the extracted secret message and the original one is measured using NC, and BER is used to calculate the error rate between the original and extracted secret message [1]. They can be calculated:

$$NC = \frac{\sum_{i=1}^x \sum_{j=1}^y (W_{orgij} \times w_{recij})}{\sum_{i=1}^x \sum_{j=1}^y (W_{orgij} \times w_{orgij})} \quad (4)$$

$$BER = \frac{\sum_{i=1}^x \sum_{j=1}^y (W_{orgij} \otimes w_{recij})}{n} \quad (5)$$

Where W_{org} and W_{rec} are the original secret message and the extracted secret message and n is the total number of secret information bits.

During the transmission process, it is impossible to avoid any kind of content harm, including image noise, JPEG compression, rescaling, brightness alteration, and contrast shift. So forth, these attacks can be made against the stego image that represents the secret data. These variables need to be resilient to the data gathered from the image. In other words, the hash algorithm is protected against these kinds of attacks. Now we use these variables for examining using three different segment lengths (4 bits, 5 bits, and 6 bits) with secret message lengths (16 bits, 32 bits, and 64 bits) respectively.

3.3.1. Robustness suggested system against JPEG compression

The chosen stego image is compressed using JPEG with different quality levels. Table 2 shows that the proposed method provides strong resistance against JPEG compression attacks. The table shows that the proposed method gained acceptable values for NC and BER.

Table 2. JPEG compression attack values for NC and BER

Quality factors (Q)	4 bits		5 bits		6 bits	
	BER	NC	BER	NC	BER	NC
30	0.3529	0.7247	0.3846	0.5676	0.4091	0.4595
60	0.1176	0.8919	0.2615	0.7027	0.2273	0.7027
80	0.1471	0.9459	0.2923	0.6486	0.2121	0.6757
90	0.1029	0.9189	0.2923	0.6757	0.2424	0.7297

3.3.2. Robustness to noise attacks

A stego image is subjected to noise attacks in a noise attack test, including salt and pepper, speckle, and Gaussian noises. All these attacks are taken with different noise densities. Table 3 shows the results of these noise attacks types.

3.3.3. Robustness to filtering attacks

Additionally, the stego image was filtered using different types of filtering attacks. These are a low pass (Gaussian) filter, a mean filter, and a median filter with various filter kernel window sizes. NC and BER values under filtering attack are shown in Table 4.

3.3.4. Resistance to attacks involving brightness and sharpness

The brightness of the stego image was examined in comparison to its values. We took two angles in tests, there are (10, 20). Additionally, as demonstrated in Table 5, the stego image is assaulted when developing the image sharpening.

In our previous tests, we observed a clear trend: when the length of the secret message segment increases, the value of NC decreases while the value of BER increases. Conversely, when the length decreases, the opposite effect occurs. This relationship between the length of the secret message segment and the values of NC and BER is consistently evident in our findings.

Table 3. NC and BER values under various noise densities

Attack type	Density of noise	6 bits		5 bits		4 bits	
		NC	BER	NC	BER	NC	BER
Salt and pepper	0.001	0	1	0	1	0	1
	0.01	0.0882	0.8919	0.0462	0.9459	0	1
	0.02	0.1176	0.8919	0.1692	0.8378	0	1
	0.03	0.2794	0.7027	0.1846	0.7568	0	1
Speckle noise	0.001	0.1029	0.8649	0.1538	0.8378	0.1212	0.8378
	0.01	0.1912	0.8649	0.3077	0.6216	0.2424	0.7027
	0.02	0.2500	0.8108	0.3538	0.7027	0.3182	0.6757
Gaussian noise	0.001	0.1618	0.8108	0.3231	0.6757	0.3030	0.6486
	0.02	0.2941	0.7568	0.3692	0.5946	0.3788	0.6486
	0.4	0.3676	0.7297	0.4000	0.5405	0.3939	0.6216
Poisson noise	0.1912	0.8108	0.1846	0.7838	0.1970	0.7568	

Table 4. NC and BER values under filtering attack

Attack type	Window size	6 bits		5 bits		4 bits	
		BER	NC	BER	NC	BER	NC
Median filter	1×1	0	1	0	1	0	1
	2×2	0.2059	0.8378	0.2462	0.6757	0.3182	0.5676
	3×3	0.2941	0.6757	0.4154	0.5405	0.4242	0.4595
Mean filter	1×1	0	1	0	1	0	1
	2×2	0.1765	0.8919	0.2308	0.7297	0.2424	0.7027
	3×3	0.5147	0.4324	0.3846	0.5946	0.3636	0.5676
Gaussian filter	1×1	0	1	0	1	0	1
	2×2	0.2059	0.8649	0.2769	0.7297	0.2879	0.6757
	3×3	0.5000	0.4595	0.3231	0.5946	0.3030	0.6486

Table 5. NC and BER values under brightness and sharpen attacks referred

Attack type	Angle	6 bits		5 bits		4 bits	
		BER	NC	BER	NC	BER	NC
Brightness	+10	0	1	0	1	0	1
	+20	0	1	0	1	0	1
Sharpen		0.0147	0.9730	0.0923	0.9189	0.0909	0.8919

4. CONCLUSION

The paper presents a framework that increases the capacity of coverless image steganography. It allows for hiding the complete secret message in one cover image. The cover image should contain all the features of the secret message. For hiding, the cover image is segmented into non overlapping blocks, transform each block to the frequency domain, generates a hash sequence for each block, and by mapping relationships between the segments of the message and the generated hash sequences, saves the auxiliary information in a file of indexes of sequences and send both the file and stego image to the receiver. Because of the block dividing and the proposed approach for generation hash sequences, the approach has a higher capacity than other previous methods and the suggested methodology is more resistant to some image processing assaults and detection tools since it acts in the transform domain and because the mechanism hasn't yet been changed. In the future, we will focus on improving security by using encryption for the information file.

ACKNOWLEDGEMENTS

This work was supported by the Department of Computer Science, College of Science for Women, Babylon University, Babylon, Iraq.




REFERENCES

- [1] J. Wu, Y. Liu, Z. Dai, Z. Kang, S. Rahbar, and Y. Jia, "A Coverless Information Hiding Algorithm Based on Grayscale Gradient Co-occurrence Matrix," *IETE Technical Review*, vol. 35, pp. 23-33, 2018, doi: 10.1080/02564602.2018.1531735.
- [2] C. F. Osborne, A. Z. Tirkel, and T. E. Hall, "Image and Watermark Registration for Monochrome and Coloured Images," *Digital Image Computing, Technology, and Applications*, pp. 59-64, 1997.
- [3] A. Kumar and K. Pooja, "Steganography- A Data Hiding Technique," *International Journal of Computer Applications*, vol. 9, no. 7, pp. 19-23, 2010, doi: 10.5120/1398-1887.
- [4] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, "A Review on Text Steganography Techniques," *Mathematics*, vol. 9, no. 21, 2021, doi: 10.3390/math9212829.
- [5] S. Deepikaa, and R. Saravanan, "VoIP steganography methods, a survey," *Cybernetics and Information Technologies*, vol. 19, no. 1, pp. 73-87, 2019, doi: 10.2478/cait-2019-0004.
- [6] J. Chaharlang, M. Mosleh, and S. R. Heikalabad, "A novel quantum audio steganography–steganalysis approach using LSFQ-based embedding and QKNN-based classifier," *Circuits, Systems, and Signal Processing*, vol. 39, pp. 3925-3957, 2020, doi: 10.1007/s00034-020-01345-6.
- [7] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727-752, 2010, doi: 10.1016/j.sigpro.2009.08.010.
- [8] Z. Zhou, Y. Cao, M. Wang, E. Fan, and Q. M. J. Wu, "Faster-RCNN Based Robust Coverless Information Hiding System in Cloud Environment," in *IEEE Access*, vol. 7, pp. 179891-179897, 2019, doi: 10.1109/ACCESS.2019.2955990.
- [9] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proceedings of the first ACM workshop on Information hiding and multimedia security*, 2013, pp. 59–68, doi: 10.1145/2482513.2482514.
- [10] A. Shaik and V. Thanikaiselvan, "Comparative analysis of integer wavelet transforms in reversible data hiding using threshold based histogram modification," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 7, pp. 878-889, 2021, doi: 10.1016/j.jksuci.2018.06.001.
- [11] R. T. McKeon, "Strange fourier steganography in movies," *2007 IEEE International Conference on Electro/Information Technology*, 2007, pp. 178-182, doi: 10.1109/EIT.2007.4374540.
- [12] P. C. Tay and J. P. Havlicek, "Frequency implementation of discrete wavelet transforms," *6th IEEE Southwest Symposium on Image Analysis and Interpretation*, 2004, pp. 167-171, doi: 10.1109/IAI.2004.1300967.
- [13] T. Rabie and I. Kamel, "On the embedding limits of the discrete cosine transform," *Multimedia Tools and Applications*, vol. 75,




- pp. 5939-5957, 2016, doi: 10.1007/s11042-015-2557-x.
- [14] N. A. Karim, S. A. Ali, and M. J. Jawad, "A coverless image steganography based on robust image wavelet hashing," *TELKOMNIKA*, vol. 20, no. 6, pp. 1317-1325, 2022, doi: 10.12928/TELKOMNIKA.v20i6.23596.
- [15] M. Liu, M. Zhang, J. Liu, P. Gao, and Y. Zhang, "Coverless Information Hiding Based on Generative Adversarial Networks," *Yingyong Kexue Xuebao/ Journal of Applied Sciences*, vol. 36, no. 2, pp. 371-382, 2018, doi: 10.3969/j.issn.0255-8297.2018.02.015.
- [16] C. Yuan, Z. Xia, and X. Sun, "Coverless image steganography based on SIFT and BOF," *Journal of Internet Technology*, vol. 18, no. 2, pp. 435-442, 2017, doi: 10.6138/JIT.2017.18.2.20160624c.
- [17] A. Qiu, X. Chen, X. Sun, S. Wang, and G. Wei, "Coverless Image Steganography Method Based on Feature Selection," *Journal of Information Hiding and Privacy Protection*, vol. 1, no. 2, pp. 49-60, 2019, doi: 10.32604/jihpp.2019.05881.
- [18] Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun, "Coverless Image Steganography Without Embedding," *International Conference on Cloud Computing and Security*, 2016, vol. 9483, pp. 123-132, doi: 10.1007/978-3-319-27051-7_11.
- [19] Z. Zhou, Q. M. J. Wu, C. -N. Yang, X. Sun, and Z. Pan, "Coverless Image Steganography Using Histograms of Oriented Gradients-Based Hashing Algorithm," *Journal of Internet Technology*, vol. 18 no. 5, pp. 1177-1184, 2017, doi: 10.6138/JIT.2017.18.5.20160815b.
- [20] S. Zheng, L. Wang, B. Ling, and D. Hu, "Coverless Information Hiding Based on Robust Image Hashing," *International Conference on Intelligent Computing (ICIC 2017): Intelligent Computing Methodologies*, 2017, vol. 10363, pp. 536-547, doi: 10.1007/978-3-319-63315-2_47.
- [21] X. Zhang, F. Peng, and M. Long, "Robust Coverless Image Steganography Based on DCT and LDA Topic Classification," in *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223-3238, 2018, doi: 10.1109/TMM.2018.2838334.
- [22] L. A. S. -Bravo, V. I. Ponomaryov, R. R. -Reyes, and C. C. -Ramos, "Coverless image steganography framework using distance local binary pattern and convolutional neural network," *Proceedings of the SPIE*, 2020, vol. 11401, doi: 10.1117/12.2556310.
- [23] Z. Zhou, Y. Mu, and Q. M. J. Wu, "Coverless image steganography using partial-duplicate image retrieval," *Soft Computing*, vol. 23, pp. 4927-4938, 2019, doi: 10.1007/s00500-018-3151-8.
- [24] L. Yang, H. Deng, and X. Dang, "A Novel Coverless Information Hiding Method Based on the Most Significant Bit of the Cover Image," in *IEEE Access*, vol. 8, pp. 108579-108591, 2020, doi: 10.1109/ACCESS.2020.3000993.
- [25] F. S. Abdulsattar, "Towards a high capacity coverless information hiding approach," *Multimedia Tools and Applications*, vol. 80, pp. 18821-18837, 2021, doi: 10.1007/s11042-021-10608-6.

BIOGRAPHIES OF AUTHORS






Hadeel Talib Mangi    Currently, Hadeel is a Master's student in the Computer Science Department, Science College for Women, University of Babylon, Iraq. She received the B.Sc. degree in computer science in 2014 from the Department of Computer Science, Al-Nahrain University. His research interests include image processing and digital watermarking. She can be contacted at email: hadeeltalib1992@gmail.com.



Suhad A. Ali    She is working as Professor in Computer Science Department, Science College for Women, University of Babylon, Iraq. She received M.S. and Ph.D. degrees from Department of Computer Science, Babylon University in 2002 and 2014, respectively. Her areas of interest are digital image and video processing, pattern recognition, and information hiding. She can be contacted at email: suhad_ali2003@yahoo.com.



Majid Jabbar Jawad    He is received the B.Sc. degree in computer science on 1989 from the Department of Computer Science, University of Technology, Iraq. He received the M.Sc. degree in Steganography on 2003 from the same university. He received the Ph.D. degree in Digital Watermarking and GIS on 2013 from the University of Babylon, Iraq. Currently, he is Professor in the University of Babylon. His research interests include steganography, digital watermarking, processing of raster and vector image and applying the information hiding techniques in GIS (geographical information system). He can be contacted at email: wsci.majid.jabbar@uobabylon.edu.iq.