

A coverless image steganography based on robust image wavelet hashing

Nadia A. Karim, 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 Mar 17, 2022

Revised Sep 15, 2022

Accepted Sep 25, 2022

Keywords:

Coverless steganography
Discrete wavelet transform
Information hiding
Information security
Steganography

ABSTRACT

Since the concept of coverless information hiding was proposed, it has been greatly developed due to its effectiveness of resisting the steganographic tools. In this paper, a new coverless steganography is presented to hide the secret data in a more secure way and to enhance the robustness against attacks. This method depends on frequency domain. The embedding process consists of several steps. Firstly, the secret data is divided into no overlapping segments. Secondly, a set of images is collected to find appropriate images to be stego images. Thirdly, to build a hash sequence for an image, a powerful hashing algorithm is used. Fourthly, for each image hash sequence, the inverted index structure is created. Fifthly, choose the image which its hash equivalent to the secret data segment. Several tests are done to measure the robustness of the proposed method. The results of the experiments reveal that the proposed strategy is resistant to a variety of image processing attacks such as joint photographic experts group (JPEG) compression, noise, low pass filtering, scaling, rotation and median and mean filter, brightness, and sharpening.

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

Secret communication between a sender and a receiver has become very important due to the extensive usage of multimedia data and advancements in telecommunications such as image, audio and video. So that Information that is sensitive or confidential cannot be accessed by third parties. Information hiding is normally accomplished performed using two well-known methods, steganography and watermarks, both methods directly modify the content of the media file (image, video, and audio) for copyright protection and covert communication or identification of the sender. There are three basic objectives of covert communication: the message cannot be seen by anybody else while it is being transmitted; it is not modified while it is being transmitted; and the sender is who he claims to be. The science of concealing and transferring hidden information is known as steganography [1], [2]. It is a set of techniques for concealing information through the use of multimedia data, such as image, text, audio, video, and network [3]-[5]. Because people utilization of images since they are one of the most widely used media, Image steganography has attracted a lot of interest, steganographic communication has a significant technology in the field of information security today [6], [7].

Image steganography is a component of data security, where images contain sensitive or secret data, such that it is not visible and cannot be identified by the human visual system (HVS) [5]. According to the documentation available, there are two types of steganography techniques for images: image steganography

with data embedding and coverless image steganography. In addition, there are two types of data embedding methods: spatial domain and frequency domain [8]. Although the human visual system does not detect the modification in the carrier image induced by data embed, the disadvantage of spatial domain approaches such as least significant digit (LSD) [5], [9], highly undetectable stego (HUGO) [1], wavelet obtained weights (WOW) [10], and steganographic universal distortion (S-uniward) [10] are that they are not resistant to normal image and steganalysis attacks. As a result, frequency domain algorithms such as the discrete fourier transform (DFT) [11], discrete wavelet transform (DWT) [12], discrete cosine transform (DCT) [13] and integer wavelet transform (IWT) [14] have been presented that use modified coefficients for data embedding. These methods are more resistant to image attacks, but they are more computationally complexity, and the information that can be hidden is limited.

The coverless image steganography framework is a new field of research when compared to previous methods of image steganography. To hide the data, no changes to the image are required. In other words, secret information cannot be transported without a carrier, but it can be hidden by creating a carrier image that is visually identical to the original or by establishing mapping rules between carrier image and secret information [14]. Finding relevant images that already contain the information of the secret data is one technique to hide a secret data in coverless image steganography. Stego images are used to communicate sensitive information and are categorised as such. The biggest issue is locating photos that already contain the required information [15]. The coverless image steganography strategies can resistance image steganalysis tools and considerably increase image security since hiding critical or confidential information does not modify the image and can resist attacks such as contrast change, brightness, noise addition, scaling [16], rotation [17], JPEG compression [18], brightness and noise addition [19].

Several researches have been done in this domain. The first coverless image steganography method is based on the spatial domain, where an image can be represented by 8 bits of information, and uses a hashing algorithm to establish hash sequences equal to a binary bit stream of the secret information. For all hash sequences, including lookup tables, an inverted index structure is created. The approach is tested against several image attacks that are common such as JPEG, contrast, and scaling attack [20]. The bag-of-words (BOW) concept is used for hiding text information. To hide text information in an image, visual words are recovered to represent text information. To extract visual words from an image set, a BOW model is utilized, and a mapping connection is established between keywords in text information and visual terms. After then, each image is separated into many sub-images. For each sub-image, a histogram of visual words is generated, and the borders with the greatest values in the histogram are chosen as the sub-representation of the image. The mapping relation is used to find a group of sub-images with visual words related with text data. For secret communication, stego images are images that include these sub-images. The proposed method has high anti-steganalysis capabilities, robustness towards known attacks, and security, according to the experimental findings and analysis [21]. A method for coverless image steganography is proposed based on histograms of oriented gradients (HOGS) and hashing. Previous image steganography methods normally required the use of a cover image in order for the secret information to be invisibly inserted in it for secret communication. Though using the embedded traces left in the cover image, steganalysis algorithms were able to sufficiently determine the existence of secret information. To resist current steganalysis approaches, a coverless image steganography solution is provided that uses a hashing algorithm based on HOGS. Instead of selecting a cover image for secret information embedding, the original images with hash sequences matching the secret information are extracted direct from a huge database and utilized as stego images for secret communication. This method offers good resistance to existing steganalysis tools, as well as good security and robustness against several attacks such as resampling, brightness and contrast changes, smoothing, and the inclusion of Gaussian noise [22]. A method for coverless hiding based on partial duplicates of a specified secret image as stego images. In this approach, each image in the database is splitting into a number of non-overlapping patches and indexing those images to use the features collected from these patches. Each of which has one or more patches that are visually related to the secret image. Then the searching is done for partial duplicates of the secret image in the database to produce the stego images. In this approach, by utilizing the patches of the stego images, it can be approximate retrieving the secret image at the receiver side. This method offers good resistance to existing steganalysis tools [23]. A coverless image steganography method based on image block matching and dense convolutional network. This method sends a collection of stego images that share one or more visually blocks with the secret image given. Hash sequence corresponding to the secret image is generated based on DCT and DenseNet. The high-level semantic properties of each related block are extracted using DenseNet. DCT produces a strong hash sequence with feature sequence, direct current (DC), and location at the same time. The DCT coefficient and supervised deep learning improve retrieval accuracy and robustness, deep learning can determine the best carrier for real-time image hiding data requirements, and CNN's high-level semantic features are more efficient than low-level features. According to experimental results, this method improves the retrieval accuracy and capacity [24].

2. METHOD

In this section, the proposed coverless image method is explained in details. Figure 1 shows the structure of the proposed method. The proposed method consists of two procedures, namely embedding procedure and extracting procedure.

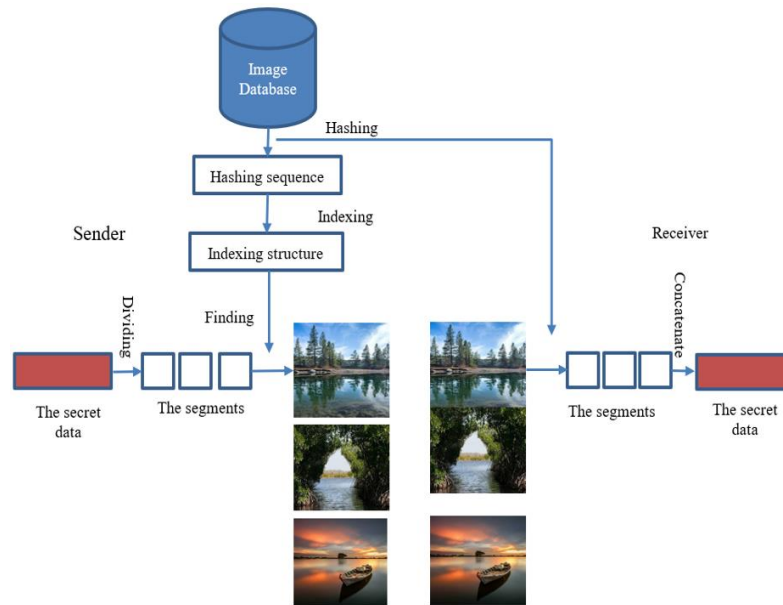


Figure 1. General block diagram of proposed coverless image steganography method

2.1. Embedding procedure

This section is explain the embedding procedure. The embedding procedure is done at the sender side. Several activities are implemented in the embedding procedure such as building image database, hash sequence generation, building the inverted index structural, finding the suitable images, and sending the stego images.

2.1.1. Building image database

This subsection explains the building of database images which will be used for embedding the secret secret data. To hide secret data in coverless image steganography, one way is to find suitable images that already contain the information. Such images are classified as stego images, which are used to communicate sensitive data [25].

2.1.2. Hash sequence generation by robust hashing algorithm

This subsection describes the strong hashing algorithm for generating image hash sequences. Different kind s of attack could be used to modify the stego images during communication. Rescaling, brightness alteration, contrast improvement, joint photographic experts group (JPEG) compression, and noise addition are just a few examples. As a result, the hashing algorithm should be resistant to the majority among those attacks, ensuring that the image hash sequences do not modify during transmission. It means that the secret is sent accurately and reliably, with few errors and changes. As a result, we propose a robust hashing algorithm for production of image hash sequences. Several phases can be completed during the production of a hash sequence using algorithm 1. The above steps are shown in the Figure 2.

2.1.3. Building the inverted index structural by image indexing

To use an image sequence with a binary hash (ImgHash) as the query, it will take a long time to look for all images with hash sequences that match the query in the database if we do an extensive search. To speed up the search, we index all of the images in the database as according their hash sequence. Then, for all of the hash sequences, we make a query table T1, which is an inverted index structure. T1 is a lookup table that contains entries to the greatest extent possible hash sequences of 8 bits. Each value leads to a set of the entire image IXDs that share the same hash sequence. Assume that image A's hash sequence is [1, 1, 1, 0, 0, 1, 1, 1] and that its IXD is IXD(A), and that IXD(A) falls into the list pointed by the entry 1, 1, 1, 0, 0, 1, 1, 1 as shown in Figure 3.

Algorithm 1. Hash sequence generation

Input: O_image//original image

Output: ImgHash//sequence of bits

- Step 1: applying DWT on O_image to obtain four subbands (low low pass (LL), low high pass (LH), high low pass (HL), high high pass (HH)).
- Step 2: dividing the LL subband into 3×3 non-overlapping segment.
- Step 3: computing the average intensity of each segment to obtain 3×3 block average array (BAvg).
- Step 4: converting (BAvg) into vector (VAvg) by scanning the array row by row.
- Step 5: converting VAvG into binary by comparing every two adjacent elements to obtain binary hash image sequence (ImgHash) with length 8 bits.

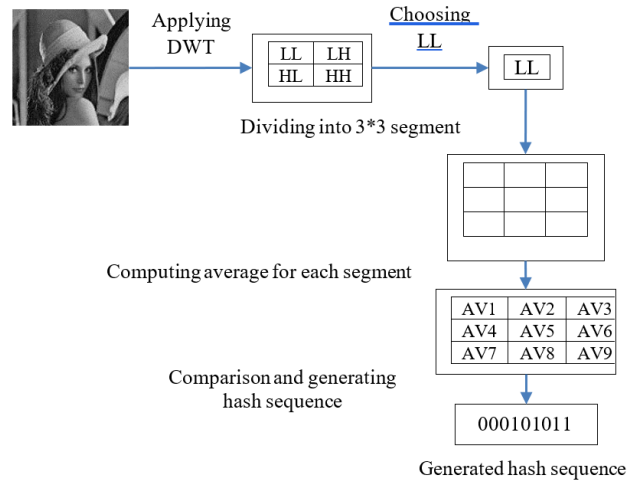


Figure 2. Hash sequence generation

The following equation is used to calculate the binary activity conversion.

$$\begin{cases} h_j = 1; & \text{if } h_j > h_{j+1} \\ h_j = 0; & \text{otherwise} \end{cases} \text{ where } 1 < j < 8 \quad (1)$$

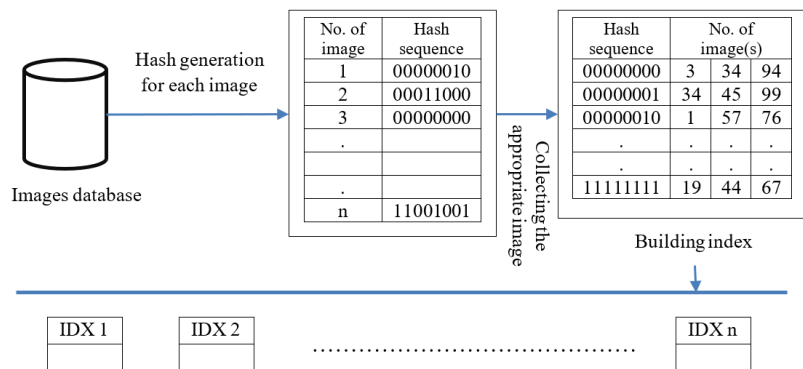


Figure 3. Building index

2.1.4. Using the index structure to find suitable images

This subsection describes finding the appropriate image depending on the secret message. The finding procedure is done as the following steps.

- 1) Transferring the secret message into a bit string that can be sent.
- 2) Dividing the secret message into a number of equal-length segments (8-bit).
- 3) Obtaining images with hash sequences those are the same with the segment to use each segment as a query.
- 4) These found Images that are stego images can be considered.

2.1.5. Sending the stego images

This sub section explains the last activity of the ebedding procedure. After finding the suitable images which have a hash sequence equivalent to the secret message, these images are considered as stego images. Later, the stego images are sent one by one to the receiver at the sender's end.

2.2. Extraction procedure

This section describes extraction the secret message in the receiver side. Herein, the secret data can be recovered without disorder if all stego images are acquired in if all of the stego images are received in order the correct order. Once the receiver has obtained all of the images, the sender uses the same hashing process to generate the hash sequence for each received image. To extract the secret data, the receiver generates a new all of their hash sequences of those images according to the sequence of the received images.

3. RESULTS AND DISCUSSION

This section discusses the results after implementing the proposed method. Several experimental results are obtained after implementing the proposed methods. The performance of the proposed method is tested in te rms of embedding and robustness.

3.1. Tests of embedding and extracting procedures

This sub section describes the embedding and extracting procedures. Let us explaine the two procedures deeply. Suppose that we have a secret message called (computer) and sample images dataset as shown in Figure 4.



Figure 4. Sample of image dataset

The embedding procedure is done (in the sender side) as:

- 1) Take the American standard code for information interchange (ASCII) code for each letter in message and transforming the secret message into bits as shown in Figure 5 and Figure 6.

99	111	109	112	117	116	101	114
----	-----	-----	-----	-----	-----	-----	-----

Figure 5. ASCII code for letters of computer word

0110001101101111011011010111000001110101011101000110010101110010
--

Figure 6. Binary number for the letters of computer word

- 2) As illustrated in Figure 7, dividing the secret message into a number of segments of identical length (8 bits).

01100011	01101111	01101101	01110000	01110101	01110100	01100101	01110010
----------	----------	----------	----------	----------	----------	----------	----------

Figure 7. Segmented secret message

- 3) Generating hash sequence for each image. For example, image1 has hash equal (01100011) and image2 has hash equal (01101111).
- 4) Each segment is used as a query; discover the images that have hash sequences that are like as the segment. For example, the bits of letter c equal to hash of image1 and the bits of letter o equal to hash image2. So, image1 and image2 will be stego image.
- 5) Sending image1 and image2 to the receiver.

The extracting procedure is done (in the receiver side) as:

- 1) Each incoming image's hash set is created by the same hashing algorithm employed by the sender once the receiver has obtained all of those images, (as described in the subsection 2.1.2). To extract the secret data, the receiver generates a new all of their hash sequences of those images according to the ordering of the received images. So, the result will be as shown in the Figure 8.

0110001101101111011011010111000001110101011101000110010101110010
--

Figure 8. Extracted secret message (as bits)

- 2) As illustrated in Figure 9, dividing the recovered secret message into a number of segments of similar length (8 bits).

01100011	01101111	01101101	01110000	01110101	01110100	01100101	01110010
----------	----------	----------	----------	----------	----------	----------	----------

Figure 9. Segmented extracted secret message

- 3) Transforming the bits into ASCII and transform it to letters as shown in Figure 10.

c	o	m	p	u	t	e	r
---	---	---	---	---	---	---	---

Figure 10. Extracted secret message (as letters)

3.2. Robustness measures

To measure the robustness of the proposed algorithms two measures are used these are normalized correlation (NC) and bit error rate (BER). Normalized correlation is used to measure the resemblance among the extracted secret information and the original ones and bit error rate is used for measuring the error rate between the extracted secret information and the original [25]. NC is calculated:

$$NC = \frac{\sum_{i=1}^n w(i)w'(i)}{\sum_{i=1}^n w(i)^2} \quad (2)$$

While BER is calculated:

$$BER = \frac{\sum_{i=1}^n w(i) \otimes w'(i)}{n} \quad (3)$$

Where w is the original image and w' is the extracted secret information.

All types of content damage, such as image noise, JPEG compression, rescaling, brightness change, and contrast shift, are unavoidable during the transmission process and so on. Each stego image selected from the database to represent the secret data segment is subject to these attacks. These variables must be able to withstand the information collected from the image. To put it another way, the hash algorithm is resistant to these types of attacks.

3.2.1. Robust the proposed system against JPEG compression

This sub section discusses robustness of the proposed method against JPEG compression. Each stego image selected from the database to represent the secret data segment is subject to JPEG compression with various quality factors. According Table 1, the proposed system gives a good robustness against JPEG compression attack, where the value of NC and BER is of acceptable.

Table 1. NC and BER values under JPEG compression attacks

Quality factors (Q)	NC	BER
10	0	1
30	0	1
40	0	1
50	0	1

3.2.2. Robustness against noise attacks

This sub section discusses robustness of the proposed method against noise attacks. In noise attack test, a stego image is attacked with several noise attacks namely, salt and pepper, speckle and Gaussian noises with different noise density. Table 2 shows different types of noise attack.

Table 2. NC and BER values under different density levels of noise attacks

Attack type	Density of noise	NC	BER
Salt and pepper	0.001	0	1
	0.01	0	1
	0.02	0	1
	0.03	0	1
Speckle noise	0.01	0	1
	0.02	0	1
	0.001	0	1
Gaussian noise	0.01	0	1
	0.02	0	1
	0.001	0	1
Poisson noise		0	1

3.2.3. Robustness against filtering attack

This sub section discusses robustness of the proposed method against filtering attack. The stego images were filtered with a low pass filtering (gaussian filter), mean filter and a median filter with window size different sizes of filter kernel. Table 3 illustrates NC and BER values under filtering attack.

Table 3. NC and BER values under filtering attack

Attack type		BER	NC
Median filter	1×1	0	1
	2×2	0.0179	0.9860
	3×3	0.0197	0.9860
Mean filter	1×1	0	1
	2×2	0.0179	0.9860
	3×3	0	1
Gaussian filter	1×1	0	1
	2×2	0.0179	0.9860
	3×3	0	1

3.2.4. Robustness against geometric attacks

This sub section discusses robustness of the proposed method against geometric attacks. Rotation and resizing attacks are tests. The proposed method achieved good results in resizing and rotation attack with different rotation degrees. Table 4 shows the results.

Table 4. NC and BER values under geometric attack

Attack type	Angle	BER	NC
Rotation	0.180	0	1
	0.270	0	1
	0.360	0	1
Resize (1024×1024)		0	1

3.2.5. Robustness against brightness and sharpening attacks

This sub section discusses robustness of the proposed method against brightness and sharpening attacks. The stego images were tested against increasing the brightness image with factor its values (10, 20). Also, the stego images are attacked with developing the sharpening of image. Table 5 illustrates the results.

Table 5. NC and BER values brightness and sharpening attack

Attack type	Factor	BER	NC
Brightness	+10	0	1
	+20	0	1
Sharpen		0	1

4. CONCLUSION

In this paper, a coverless image steganography framework based on efficient image wavelet hashing is proposed. The embedding process is done without any modification on cover image. It finds the proper cover images as stego-images that contain information that matches to the secret data because no evidence of change will be left in the stego images. Moreover, due to the suggested strong hashing method, our approach can handle image processing processes such as JPEG compression, image rotation, image scaling, and noise. As a result, the stego images that are formed are robust to signal loss. However, using our technology, only 8-bit info may be hidden in each main image. The goal of future study will be to find techniques to increase hiding capacity without reducing steganography performance.

ACKNOWLEDGEMENTS

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





REFERENCES

- [1] 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. [Online]. Available: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.22.7911&rep=rep1&type=pdf>
- [2] A. Arya and S. Soni, "A literature review on various recent steganography techniques," *International Journal on Future Revolution in Computer Science & Communication Engineering*, vol. 4, no. 1, pp. 143-149, 2018. [Online]. Available: http://www.ijfrcsce.org/download/conferences/ICATET_2018/ICATET_2018_Track/1517647667_03-02-2018.pdf
- [3] 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.
- [4] S. Deepikaa, and R. Saravanan, "VoIP steganography methods, a survey," *Cybernetics and Information Technologies*, vol. 19, pp. 73-87, 2019, doi: 10.2478/cait-2019-0004.
- [5] 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.
- [6] 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.
- [7] A. A. E. -Latif, B. A. -E. -Atty, and S. E. V. -Andraca, "A novel image steganography technique based on quantum substitution boxes," *Optics & Laser Technology*, vol. 116, pp. 92-102, 2019, doi: 10.1016/j.optlastec.2019.03.005.
- [8] Y. Cao, Z. Zhou, Q. M. J. Wu, C. Yuan, and X. Sun, "Coverless information hiding based on the generation of anime characters," *EURASIP Journal on Image and Video Processing*, 2020, doi: 10.1186/s13640-020-00524-4.
- [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] T. Pevný, T. Filler, and P. Bas, "Using High-Dimensional Image Models to Perform Highly Undetectable Steganography", *Berlin, Germany: Springer*, vol. 6387, pp. 161–177, 2010, doi: 10.1007/978-3-642-16435-4_13.
- [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*, 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] 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, pp. 878-889, 2021, doi: 10.1016/j.jksuci.2018.06.001.
- [15] S. Zheng, L. Wang, B. Ling, and D. Hu, "Coverless Information Hiding Based on Robust Image Hashing," *ICIC 2017: Intelligent Computing Methodologies*, 2017, vol. 10363, doi: 10.1007/978-3-319-63315-2_47.
- [16] A. Shapi'i, R. Sulaiman, M. K. Hasan, A. Y. Kassim, and S. Abdullah, "Scaling Technique for Digital Implant in Medical Images Using Pixel Density Algorithm," *European Journal of Scientific Research*, vol. 47, no. 1, pp. 24-32, 2010. [Online]. Available: https://www.researchgate.net/publication/242014301_Scaling_Technique_for_Digital_Implant_in_Medical_Images_Using_Pixel_Density_Algorithm
- [17] D. Khovratovich, I. Nikolić, and C. Rechberger, "Rotational Rebound Attacks on Reduced Skein," *International Conference on the Theory and Application of Cryptology and Information Security*, 2010, vol. 6477, pp. 1-19, doi: 10.1007/978-3-642-17373-8_1.
- [18] 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.
- [19] J. Zhou and Z. Wang, "Security Clustering Algorithm Based on Integrated Trust Value for Unmanned Aerial Vehicles Network," *KSII Transactions on Internet and Information Systems*, vol. 14, no.4, pp. 1773-1795, 2020, doi: 10.3837/tiis.2020.04.020.





- [20] Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun, "Coverless Image Steganography Without Embedding," *International Conference on Cloud Computing and Security*, 2015, vol. 9483, pp. 123-132, doi: 10.1007/978-3-319-27051-7_11.
- [21] X. Duan, B. Li, D. Guo, K. Jia, E. Zhang, and C. Qin, "Coverless Information Hiding Based on WGAN-GP Model," *International Journal of Digital Crime and Forensics*, vol. 13, no. 4, pp. 57-70, 2021, doi: 10.4018/IJDCF.20210701.0a5.
- [22] 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, pp. 1177-1184, 2017, doi: 10.6138/JIT.2017.18.5.20160815b.
- [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] Y. Luo, J. Qin, X. Xiang, Y. Tan, Q. Liu, and L. Xiang, "Coverless real-time image information hiding based on image block matching and dense convolutional network," *Journal of Real-Time Image Processing*, vol. 17, pp. 125-135, 2020, doi: 10.1007/s11554-019-00917-3.
- [25] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K. -H. Jung, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication*, vol. 65, pp. 46-66, 2018, doi: 10.1016/j.image.2018.03.012.

BIOGRAPHIES OF AUTHORS







Nadia A. Karim     currently, Nadia is a Master student in Computer Science Department, Science College for Women, University of Babylon, Iraq. She received the B.Sc. degree in computer science on 2007 from Department of Computer Science, Babylon University. His research interests include image processing, digital watermarking. She can be contacted at email: nonaak4@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 University of Technology-Computer Science Dept., 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.