[1]Nitin Kanzariya,

[2]Dr. Dhaval Jadhav,

[3]Dr. Nilesh Maltare,

[4]Dr. Lokesh Gagani

A Coverless Image Steganography Based on Huffman Encoding and Robust Image Wavelet Hashing

JES Journal of Electrical Systems

Abstract: **-** Data hiding approaches are crucial in insecure communication to protect sensi- tive information from illegal access. The robustness of existing coverless image steganogra- phy methods that utilize mapping rules is derived from their ability to extract feature patterns within the spatial domain. In order to protect sensitive data more securely and to increase its durability against attacks, a new coverless steganography is introduced in this study. The me- thod used is based on the frequency domain. A coverless image steganography based on ro- bust image wavelet hashing and Huffman encoding. Initially, the confidential data is encoded through lossless compression using Huffman Encoding, which reduces the payload and en- hances the capacity for embedding. Second, segments of an 8-bit size are created from the compressed secret data. The efficient DWT hashing technique has been employed to generate a hash sequence for an image. An inverted index structure is established, allowing for the se- lection of the image whose hash corresponds to the secret data segment. Subsequently, all chosen images along with supplementary information are transmitted to the recipient. Testing has shown that the proposed method is robust against various image processing attacks, in- cluding scaling, low pass filtering, JPEG compression, rotation, noise introduction, and me- dian/mean filtering. Research findings and analysis indicate that this method enhances the latest coverless steganography algorithms in terms of capacity, resilience, and security.

Keywords: Image Steganography, coverless image steganography, information hiding, in- formation security, discrete cosine transform, discrete wavelet transform.

1 INTRODUCTION:

Electronic multimedia is common in network transmission due to the advancement of media and information technology [1, 3]. However, it also brings an increasing number of informa- tion security issues, including issues with information integrity, copyright protection, and in- formation authenticity [22, 23]. Two technologies are already in use to increase information security: cryptography and information concealing. In cryptography, after the secret informa- tion has been encrypted, a third party cannot read it. However, a third party can quickly ascer- tain whether the carrier is carrying secret information, which results in secret information be- ing intercepted. The idea of information hiding is put out as a solution to this issue. Information hiding technology differs from typical encryption technology in that it is transpa-rent, robust, and secure. It also creates a new type of information discipline in security [3]. Thesecret information is integrated into the carrier by altering the carrier itself in conventional in-formation hiding techniques [16, 18].

[1]Research Scholar, Gujarat Technological University,Gujarat

[2]Vidyabharti Trust College of Master in Computer Application(MCA), Umrakh, Bardoli Gujarat

[3]Government Engineering Colleges, Modasa, Gujarat

[4]LDRP Institutes of Technology and Research, Gujarat

nitinkanzariya5219@gmail.com dhaval.jadhav@vbtmca.ac.in nilesh.maltare@gecmodasa.ac.in gagnani.lokesh@gmail.com

Image steganography has emerged as a significant area within the field of information con- cealment. Conventional techniques can be categorized into spatial domain-based and trans- form domain-based methods. Spatial domain algorithms, such as WOW, LSB matching, pre- diction error, histogram manipulation, and modulo operations, provide benefits in terms of image quality and data capacity, yet they exhibit limitations in robustness. On the other hand, transform domain methods, including discrete cosine transform (DCT), discrete wavelet trans-form (DWT), and discrete Fourier transform (DFT), have also been introduced. Additionally, anew reversible data hiding algorithm utilizing differential compression has been suggested. Nonetheless, these techniques necessitate modifications to the carrier, which can facilitate the detection of concealed information through steganalysis tools.

A solution to the underlying issue was proposed through the concept of "coverless image information hiding." The term "coverless" refers to the establishment of a mapping connectionbetween the secret information and the carriers without any alterations, indicating that a carrieris not necessary for transmission. In contrast to traditional image steganography, coverless in- formation hiding emphasizes the inherent characteristics of the image rather than altering the cover image to convey the secret information. Research in coverless steganography mainly centers on mapping rules and texture synthesis [16]. The resilience of the texture-based tech- nique, which often necessitates a second sample of the picture since it conceals hidden infor- mation throughout the process of synthesis, still has to be enhanced.

The important contributions made by Coverless Information Hiding are listed below:

1. The stego-image won't be modified in any way to carry out secret communication.
2. Since the stego-image was not altered, current steganalysis methods cannot identifyhidden information.

The subsequent sections of this paper are organized as follows: Section 2 reviews related research, including coverless image steganography and steganalysis, along with recent ad- vancements and key challenges. Following this, Section 3 introduces fundamental techniques in coverless image steganography. Section 4 provides an evaluation of performance. Finally, Section 5 concludes the paper and outlines potential future work.

2 BACKGROUND CONTEXT AND RELATED RESEARCH

In order to address the issue that steganalysis activities can easily detect the hidden informa- tion using classic information masking methods. The idea of coverless information conceal- ment was first put forth by zhou et al. in August 2015 at the inaugural international confe- rence on cloud computing and security [1]. Technology that can hide information without a cover cannot imply that it lacks carriers. It directly relies on "secret information" to "gener- ate/obtain" stego carriers, in contrast to typical information concealment technology. Zhou et al. (2015) conducted a study that employs a pixel feature approach. They utilize a robust hashing technique that calculates the average intensity of each block to create a hash se- quence for every image in the database, subsequently inverting all images based on this hash sequence. The indexing structure retrieves the stego image that corresponds to the secret in- formation sequence. These images are then transmitted to the recipient. Upon receipt, the re- cipient generates a hash sequence using the identical hashing method. These hash patterns contain confidential information. The algorithm proposed in this study has a capacity of 8bits.

To enhance the concealed capacity, Zheng et al. [2] refined the hashing algorithm and extended the length of the confidential data, resulting in 18 bits of availability. Yuan et al. (Yuan, Xia, and Sun, 2017) introduced a coverless information hiding technique utilizing SIFT and BOF. In this method, text is employed to convey the confidential information, which is segmented after being converted into binary format. For the image component, SIFT feature extraction and clustering are applied to generate the image hash sequence. This se- quence is then compared with the hash sequence of the confidential information. When a match occurs, the recipient receives the image as a stego image.

Liming Zou proposes an innovative coverless information hiding technique that relies on the average pixel values of sub-images. This method employs a hashing technique to gen- erate hash sequences, which are utilized to conceal secret information through established mapping relationships. Initially, a dictionary and a hash array are constructed. These compo- nents are subsequently mapped according to the defined relationships. Additionally, a multi- level index structure is developed to facilitate the efficient retrieval of the stego-images.

Qiang Liu[8] suggests a brand-new coverless image steganography algorithm that makes use of DWT sequence mapping and DenseNet features. The approach employs super- vised learning to retrieve images, extracts features from image datasets, separates chosen im- ages into 4x4 sub-blocks, computes DWT coefficients, and creates resilient feature se- quences. Images having the same feature sequence as the secret information segment are chosen as carriers once secret information is segmented into separate parts and an

inverted index is created.

Deep learning-based CIS methodology was proposed by Luo et al. [20]. Coverless in- formation hiding has grown increasingly popular and drawn a lot of attention as a result of its continued development. Existing CIS techniques, however, struggle to withstand the content loss. Meanwhile, the growth of deep learning offers us fresh perspectives. When an image undergoes geometric manipulation, the pre-trained deep CNN model is capable of preserving the image's fundamental characteristics. As a result, even in the presence of geometric at- tacks, the hash sequence derived from the CNN features can still be retrieved.

Based on the above analysis, this paper proposed a CIS technique based on Huffman Encoding and DWT, which attempts to increase the embedding capacity and as well as ro- bustness of secret information under geometric attacks, based on the analysis mentioned above.

3 SUGGESTED APPROACH

In this section, a detailed explanation of the proposed coverless image method is provided. Figure 1 illustrates the framework of the proposed approach. The method comprises two main processes: the initial embedding procedure and the extraction procedure.

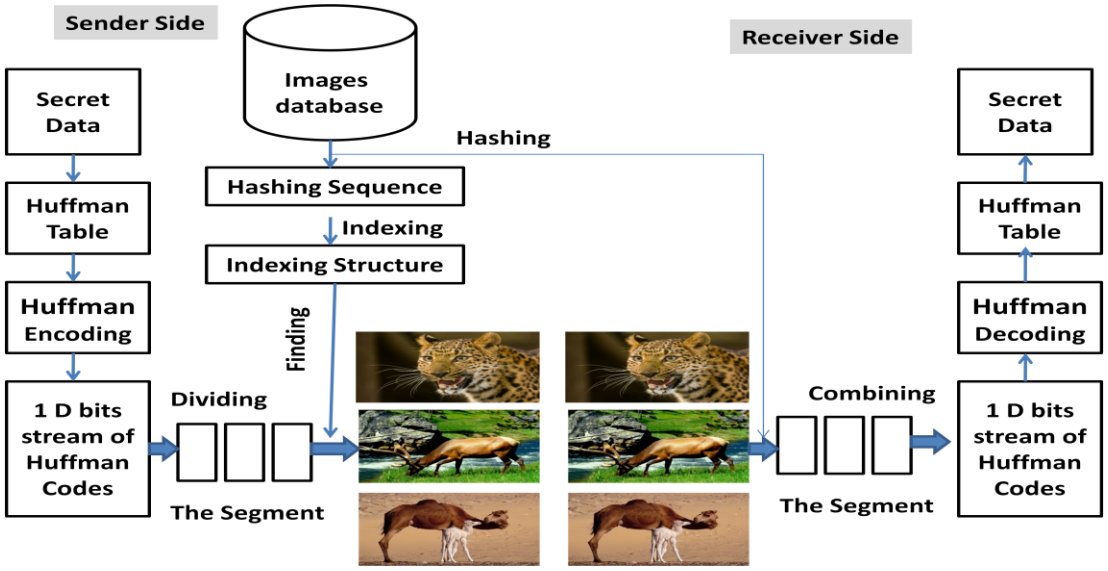


Fig. 1: Proposed block diagram for the coverless image steganography technique.

3.1 Embedding process

The embedding process is detailed in this section. The sending side is where the embedding procedure is completed. The embedding process involves a number of steps, including Huff- man coding, creating an image database, creating hash sequences, creating inverted index structures, locating appropriate images, and delivering stego images.

Fig.1 presents the embedding process' block diagram. First, Huffman coding was used to encode the secret data before embedding. The Huffman code is a prefix and minimum- length code since no other encoding has an average length that is shorter [24]. Bits per pixel are decreased through Huffman encoding and dividing the Huffman code into several, equal- length 8-bit segments.

Secondly, the Discrete Wavelet Transform (DWT) is employed to derive four sub- bands from the cover image: low low pass (LL), low high pass (LH), high low pass (HL), and high pass (HH) [23]. The LL sub- band is then used to generate an 8-bit long, highly secure hash image sequence.

Third, create a strong image hash sequence using the strong hashing technique de- scribed in section below. Finally, using the index structure, collecting images with hash se- quences that are identical to each segment, using each segment as a query, and finding Stego images are sent through a private channel to the destination.

Huffman Encoding

Any item represented in digital form can be compressed using the variable length, lossless Huffman encoding method. First, a secret data is encoded using Huffman coding, and the re- sulting Huffman codes are embedded using the recommended coverless image approach.

Huffman codes are among the most efficient codes since they transform one secret da-ta symbol into one code word [1]. The block diagram of Huffman encoding, which trans- forms secret data into a 1-D bits stream, is shown in Fig. 2. Each symbol of secret data is en- coded by a binary code in a Huffman table (HT) [24]. Both the encoder and decoder sides have to use the same Huffman table. As a result, in addition to the stego image, the Huffman table is needed for the decoding process. Three attributes are often encoded using the Huff- man method:

Lossless compression: This method guarantees that the original data is preserved even aftercompression.

Enhanced Safety: A Huffman-encoded bit stream hides everything because a Huffman tableis necessary to decode it accurately.

Authentication: It offers authentication since the Huffman table cannot decode the data ifeven one bit in the bit stream that was encoded by Huffman changes.

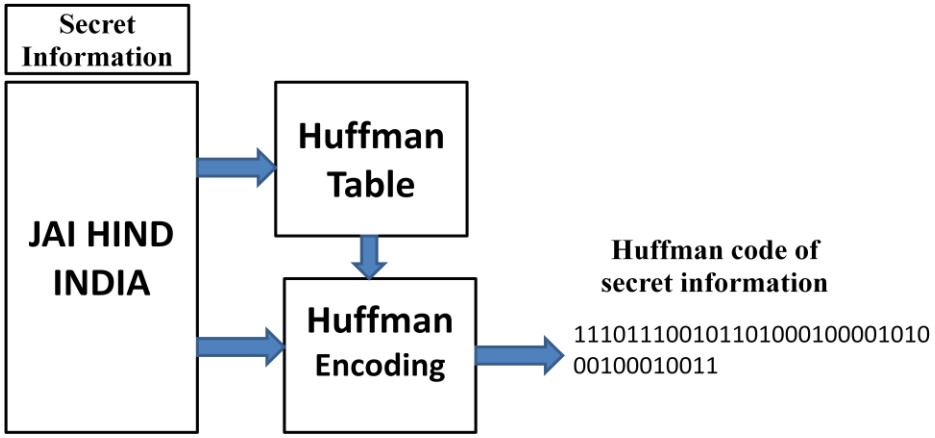


Fig. 2: Block Diagram of Huffman Encoding

Generation of hash sequences using a resilient hashing algorithm.

This subsection outlines the robust hashing algorithm employed to generate image hash se- quences. Various attack types might be adopted to alter the stego images while communicat- ing. Just a few examples are rescaling, brightness modification, raising the contrast, joint photographic experts group (JPEG) compression, and noise addition. The hashing technique must be resilient against such attacks to ensure that the image hash sequences remain un- changed during transmission. This ensures the secure and consistent transmission of confi- dential information. Consequently, we propose a strong hashing algorithm designed for gene- rating image hash sequences. By employing Algorithm 1, multiple steps can be executed to produce a hash sequence, as illustrated in Fig. 3.

Algorithm 1: Hash sequence generation

Step 1: The Discrete Wavelet Transform (DWT) is applied to the cover image to generate four sub-bands: low-low pass (LL), low-high pass (LH), high-low pass (HL), and high pass(HH).

Step 2: Dividing the LL sub-band into non-overlapping segments of 3 by 3.

Step 3: Calculating each segment's average intensity, which is obtained in step 2.

Step 4: Generate a binary hash image sequence of 8 bits by evaluating the average intensitybetween each pair of adjacent elements.

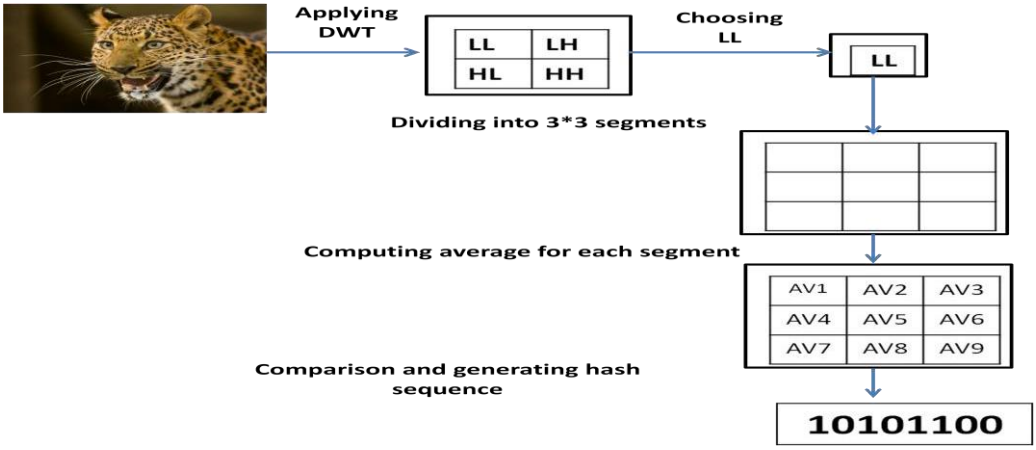


Fig. 3: Hash sequence generation

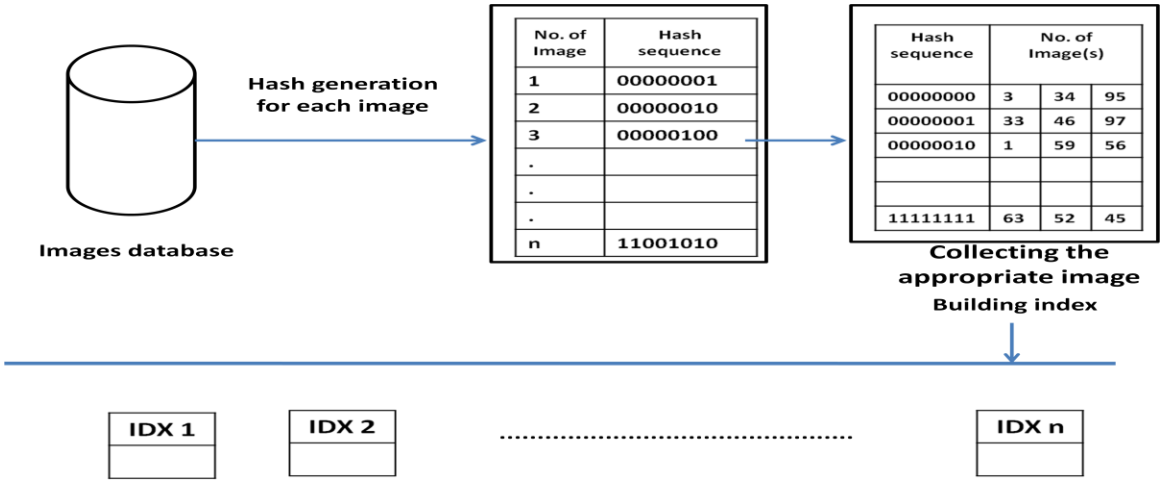
Creating the inverted index structural

Conducting a comprehensive search in the database for all images with hash sequences that correspond to the query, utilizing an image sequence with a binary hash (ImgHash) as the query, can be time-consuming [5]. To enhance the efficiency of the search, we index each image in the database based on its hash sequence [21]. Subsequently, we establish a query ta- ble T1, which serves as an inverted index structure for each hash sequence. T1 functions as a lookup table, accommodating as many 8-bit hash sequences per entry as feasible. Each entry points to a collection of all image IXDs that share the same hash pattern. For instance, if im- age A has an IXD represented as IXD(A) and its hash sequence is [1, 0, 1, 1, 0, 1, 1], then

IXD(A) will be included in the list referenced by the entry 1, 0, 1, 1, 0, 1, 1, 1, as illustrated

in Fig. 4.

Fig 4: Building index



3.2 Extraction procedure

This section explains how to retrieve the hidden message from the receiver side. Sharing the hash method, Huffman Table, and stego image between the sender and the receiver is neces- sary for the recovery operation.

If the stego images are collected in the correct sequence and all of them are success- fully received, the confidential information can be extracted without any issues [21].The re- ceiver generates the hash sequence for each image it receives using the same hashing proce- dure after collecting all of the images. To recover the original secret bits, the retrieved hash code is then decoded using the Huffman table. Once the decoded bits have been received,they must be put in the proper order in order to create the secret data.

4 RESULTS AND DISCUSSION

This section discusses the results obtained from employing the recommended approach. After using the suggested approaches, some experimental findings are achieved. The effectiveness of the suggested strategy is evaluated for embedding and robustness.

4.1 Tests of Huffman Encoding

Huffman coding was used to encode the secret data before embedding. An image's pixel in- tensities, which range from 0-255, are thought of as various symbols. The maximum intensityis 255, while the least intensity is 0. The first stage is to use the hidden data to identify the distinctive symbols and their probability. Then, utilizing distinctive symbols and their corres- ponding probabilities, the Huffman table is retrieved from the secret data. Each symbol's bi- nary code is shown in a Huffman Table along with the matching Huffman Codes. No other encoding has a shorter average length than the Huffman code, making it a prefix and mini- mum-length code [22]. Huffman encoding reduces the number of bits per pixel show in Table1.

For example, The secret data consists of 53 characters, which translates to a require- ment of 424 bits for embedding. Given that each image can accommodate 8 bits of hash code, a total of 53 images would be necessary to convey the secret information. However, by em- ploying Huffman encoding, the embedding requirement is reduced to 164 bits, allowing for the representation of the secret information with only 21 images instead of 53.

Secret Data	**Without Huffman Encoding**			**With Huffman Encoding**		
No of characters	**No. of bits**	**Bits / image**	**Required No of Image**	**No. of bits**	**Bits / image**	**Required No of Image**
21	168	8	21	45	8	6
36	288	8	36	114	8	15
53	424	8	53	164	8	21

Table 1: Number of Bits with and Without Huffman Encoding

4.2. Evaluation of the processes for embedding and extraction.

This subsection outlines the processes for embedding and extracting information. We will delve into each procedure in detail. For illustration, consider a secret message referred to as (JAI HIND INDIA) and a sample dataset of images as depicted in Fig. 5.

Fig 5: sample images dataset

The embedding process is completed on the sender's side as follows:

1. Apply Huffman encoding on secret to reduce no of bits. For ex, before compression , no of bits to embedded is 122 for JAI HIND INDIA secret message, but after compression of secret code, no of bits to embedded is only 38 for JAI HIND INDIA secret message as shown in Fig. 6.

11101110010110100010000101000100010011

Fig 6: Binary bits for JAI HIND INDIA secret message

2. As shown in Fig. 7, the secret message is segmented into multiple parts, each consisting of an equal length of 8 bits.

11101110	01011010	00100001	01000100	01001100

Fig 7: Segmenting binary bits into multiple sections of equal length.

3. Creating a hash sequence for every image. For instance, image1 is assigned a hash of (11101110), while image2 is assigned a hash of (01011010).

4. Each segment functions as a query to identify images with hash sequences similar to that segment. For instance, the bits of the first segment correspond to the hash of image1, while the bits of the second segment match the hash of image2. Consequently, image1 and image2 will be considered stego images.

5. Transmitting image1 and image2 to the recipient.

The extraction process is completed on the receiving end as follows:

1. The hash set for each incoming image is generated using the same hashing algorithm uti- lized by the sender, once the receiver has received all the images (as detailed in subsection 2.1.2). To retrieve the secret data, the receiver creates a new sequence of hashes for these images based on the order in which they were received. The outcome is illustrated in Fig.8.

1110111001011010001000010100010001001100

Fig 8: Retrieved confidential information (in binary form)

2. As shown in Fig. 9, the recovered secret message is segmented into several parts of ap-proximately equal length (8 bits).

11101110	01011010	00100001	01000100	01001100

Fig 9: Segmented extracted secret message

3. Remove padding bit and decode the bit stream of Huffman codes that are extracted in Step-2 using the Huffman table.

4. Received data in step 3 is our secret data which is JAI HIND INDIA.5.End

4.3 Robustness measures

To evaluate the effectiveness of any proposed technique, the Bit Error Rate is assessed. This metric represents the comparison between the received message and the original message, and it is calculated as follows.

$$BER=e/n,\ e=\sum pi \oplus qi;\ \text{Where } i=1:n \quad (1)$$

In this context, e denotes the count of errors detected, n represents the overall number of bits, p refers to the original vector of secret bits prior to the attack, and q signifies the vector of secret bits following the attack [21].

If the Bit Error Rate (BER) is 0, it indicates that no errors were detected, and the secret bits have been successfully and accurately retrieved, demonstrating that the method is fully resistant to this type of attack. Conversely, if the BER is greater than 0, it signifies the pres- ence of an error rate, suggesting that some of the secret bits have been modified or corrupted during the attack, which implies that the technique is not completely impervious to this threat.

Correlation Coefficient (CC).

Equation is used by CC to calculate how similar the cover image and stego image are to one another.

$$CC=\frac{\sum(Xi-Xm)(Yi-Ym)}{\sqrt{\sum(Xi-Xm)2\sqrt{\sum(Yi-Ym)2}}} \quad (2)$$

In this context, Xi represents the intensity of the ith pixel in the cover image, while Xm de- notes the average intensity of the cover image. Similarly, Yi indicates the intensity of the ith pixel in the Stego image, and Ym refers to the average intensity of the Stego image [22].

The correlation coefficient is equal to one when the two images are perfectly similar,zero when they are totally uncorrelated, and one when they are totally anti-correlated.

It is not feasible to completely eliminate all forms of content degradation during commu- nication, such as image noise, JPEG compression, rescaling, alterations in brightness, and shifts in contrast, among others. Such attacks can target any stego image selected from the database to convey the secret data segment. It is essential for these variables to maintain resi- lience against the data extracted from the image. In essence, the hash algorithm must be safe- guarded against these types of threats.

Robust the proposed system against JPEG compression.

The suggested method's resistance to JPEG compression is covered in this subsection. To represent the secret data segment, each stego image chosen from the database is treated to JPEG compression with varying quality factors [17, 18, and 19]. The data presented in Table 1 indicates that the proposed method demonstrates significant resilience to JPEG compres- sion attacks, achieving satisfactory levels for both CC and BER.

Table 2: NC and BER metrics in the context of JPEG compression attacks.

Quality factors (Q)	CC	BER
15	1	1
35	1	1
45	1	1
55	1	1

Robustness against noise attacks.

The resistance of the suggested technique against noise attacks is covered in this subsection. In the noise attack evaluation, various types of noise attacks, such as salt-and-pepper, speckle, and Gaussian noises with different noise densities, are introduced to a stego image [10, 13, 21, and 22].Different noise attack types are displayed in Table 2.

Table 3: NC and BER metrics across various noise attack density levels.

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

Robustness against filtering attack

This subsection addresses the resilience of the proposed technique against filtering attacks. The stego images underwent filtering through low-pass (Gaussian) filtering, mean filtering, median filtering, and a range of filter kernel window widths. The values of NC and BER in the context of filtering attacks are presented in Table 3.

Table 4: NC and BER values under different filter attacks

Attack type	Size	CC	BER
Median filter	1 X 1	1	1
	2 X 2	1	1
	3 X 3	1	1
Mean filter	1 X 1	1	1
	2 X 2	1	1
	3 X 3	1	1
Gaussian filter	1 X 1	1	1
	2 X 2	1	1
	3 X 3	1	1

Robustness against Rotation geometric attacks.

The resistance of the suggested technique against geometrical attacks is covered in this sub- section. Attacks that rotate are tests [6, 8]. The proposed method demonstrated effective per- formance against resizing and rotation attacks across a range of rotation angles. The results are presented in Table 4.

Table 5: NC and BER values under different filter attacks

Attack type	Angle	CC	BER
Rotation	0.180	1	1
	0.280	1	1
	0.350	1	1

CONCLUSION AND FUTURE WORK

This study introduces a novel concept for coverless image steganography utilizing efficient image wavelet hashing and Huffman encoding techniques. The original cover image remains intact throughout the embedding process. As a result, the stego images exhibit no visible alte-rations, allowing for the selection of suitable cover images that incorporate information cor- responding to the concealed data. The use of Huffman encoding facilitates a high capacity forembedding. Furthermore, our method is resilient against various image processing attacks, including JPEG compression, rotation, scaling, and noise, thanks to the robust hashing algo- rithm employed. This algorithm significantly enhances both the security and quality of the stego images. The findings indicate that the proposed method outperforms existing tech- niques, with the retrieved secret data from the stego image perfectly matching the original da- ta. Consequently, the resulting stego images demonstrate resilience against communication loss. However, it is important to note that our approach allows for the concealment of only 8- bit information within each primary image. Future investigations will aim to identify strate- gies to increase the capacity for hiding data without compromising the effectiveness of the steganography.

References

[1] 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.

[2] 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.

[3] Yi Cao, Zhili Zhou, Q. M. Jonathan Wu, Chengsheng Yuan and Xingming Sun,‖ Coverless information hid- ing based on the generation of anime characters‖. EURASIP Journal on Image and Video Processing (2020).

[4] Anqi Qiu, Xianyi Chen,Xingming Sun,‖ Coverless Image Steganography Method Based on Feature Selection

[5] ‖. Tech Science Press JIHPP, vol.1, no.2, pp.49-60, 2019.

[6] Al Hussien Seddik Saad, M. S. Mohamed and E. H. Hafez ,‖ Coverless Image Steganography Based on Jig- saw Puzzle Image Generation ‖. Tech Science Press 10 December 2020.

[7] ZHILI ZHOU, (Member, IEEE), YI CAO,‖ Faster-RCNN Based Robust Coverless Information Hiding Sys- tem in Cloud Environment‖. ‖.IEEE, December 23, 2019.

[8] Yuanjing Luo · Jiaohua Qin · Xuyu Xiang ,‖ Coverless real-time image information hiding based on image block matching and dense convolution network‖. Springer, December 2019.

[9] Qiang Liu, Xuyu Xiang ∗, Jiaohua Qin‖ Coverless steganography based on image retrieval of DenseNet fea-tures and DWT sequence mapping‖ Elsevier December 2019.

[10] M.-M. Liu, M.-Q. Zhang, J. Liu, Y. Zhang, and Y. Ke, __Coverless information hiding based on generative adversarial networks,‘‘ J. Appl. Sci., vol. 36, pp. 371–382, Mar. 2018.

[11] X. Zhang, F. Peng, and M. Long, __Robust coverless image steganography based on DCT and LDA topic classification,‘‘ IEEE Trans. Multimedia, vol. 20, no. 12, pp. 3223–3238, Dec. 2018.

[12] Zhou, Z., Sun, H., Harit, R., Chen, X., Sun, X.: Coverless image steganography without embedding. In: Huang, Z., Sun, X., Luo, J., Wang, J. (eds.) ICCCS 2015. LNCS, vol. 9483, pp. 123–132. Springer, Cham (2015).

[13] 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.

[14] Shuli Zheng1, Liang Wang1, Baohong Ling2, and Donghui Hu1,‖ Coverless Information Hiding Based on Robust Image Hashing Springer , June 2017.

[15] Z.-L. Zhou, Y. Cao, and X.-M. Sun, __Coverless information hiding based on bag-of-words model of im- age,‘‘ J. Appl. Sci. Electron. Inf. Eng., vol. 34, no. 5, pp. 527–536, Sep. 2016.

[16] Z. Zhou, Y. Mu, and Q. J. Wu, __Coverless image steganography using partial-duplicate image retrieval,‘‘ Soft Comput., pp. 1–12, Mar. 2018.

[17] Z. Zhou, Q. M. J. Wu, C. -N. Yang, X. Sun, and Z. Pan, ―Coverless Image Steganography Using Histogramsof Oriented Gradients-Based Hashing Algorithm,‖ Journal of Internet Technology, vol. 18, pp. 1177-1184, 2017, doi: 10.6138/JIT.2017.18.5.20160815b.

[18] M. Y. Valandar, M. J. Barani, P. Ayubi, and M. Aghazadeh, __An integer wavelet transform image stegano- graphy method based on 3D sine chaotic map,‘‘ Multimedia Tools Appl., vol. 78, no. 8, pp. 9971–9989,Apr. 2019.

[19] W. Liang, J. Long, A. Cui, and L. Peng, __A new robust dual intel- lectual property watermarking algo- rithm based on field programmable gate array,‘‘ J. Comput. Theor. Nanosci., vol. 12, no. 10, pp. 3959–3962, Oct. 2015.

[20] J. A. Hartigan and M. A. Wong, __A K-means clustering algorithm,‘‘ Appl. Statist., pp. 100–108, Jun. 2013.

[21] Xintao Duan1, *, Haoxian Song1, Chuan Qin2 and Muhammad Khurram Khan3 ‖Coverless Image Informa- tion Hiding Based On Generative Model‖,Tech Science Press 2018.

[22] Kanzariya Nitin, Dhaval Jadhav, Gaurang Lakhani, Uttam Chauchan, and Lokesh Gagani. "Coverless In- formation Hiding: A Review." In Proceedings of International Conference on Computational Intelligence: ICCI 2021, pp. 109-135. Singapore: Springer Nature Singapore, 2022.

[23] Gagnani, Lokesh P. "Multi Objective Association Rule Mining with Soft Computing Approach." In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), pp. 968-971. IEEE, 2020.

[24] Gagnani, Lokesh, and Kalpesh Wandra. "Data Mining Task Optimization with Soft Computing Approach." In Proceedings of the Third International Conference on Computational Intelligence and Informatics: ICCII 2018, pp. 567-577. Springer Singapore, 2020.

[25] Kanzariya, Nitin, Ashish Nimavat, and Hardik Patel. "Security of digital images using steganography tech- niques based on LSB, DCT and Huffman encoding." In Proceeding of international conference on advances in signal processing and communication-elsevier. 2013.