Ingénierie des Systèmes d'Information
Vol. 29, No. 5, October, 2024, pp. 1991-1997
Journal homepage: http://iieta.org/journals/isi

A Coverless Video Steganography Technique Based on Integer Wavelet Transform

Mohammed Ayad Kadhim[1*], Majid Jabbar Jawad[2]

[1] College of Information Technology, University of Babylon, Babylon 51001, Iraq
[2] Department of Computer Science, University of Babylon, Babylon 51001, Iraq

Corresponding Author Email: Mohamedayad.sw.phd@student.uobabylon.edu.iq

https://doi.org/10.18280/isi.290530

Received: 28 January 2024
Revised: 28 May 2024
Accepted: 31 July 2024
Available online: 24 October 2024

Keywords:
coverless, steganalysis, steganography, coefficients

ABSTRACT

Coverless steganography has received a lot of attention lately because it is a technique that completely defies steganalysis detection by not modifying the carriers. The majority of currently used coverless steganography algorithms, however, use images as their carriers, and there aren't many studies on coverless video steganography. Actually, video is a more trustworthy and educational medium. In addition, most of covert video steganography techniques in use today hide information in a specific video frame. These techniques are insufficiently robust and do not take into account the distinct sequential characteristics of video carriers that set them apart from images. This research proposes a coverless steganography scheme depend on the integer wavelet transform (IWT) of video. At first, a new method is proposed to generate hash sequences based on IWT coefficients. We take each frame in the video and divide it into sub matrices(blocks). After that, the coefficients of each block are converted into a bit sequence. Then, a video index structure was created to expedite the process of finding matching blocks in the video. The procedure of information embedding involves segmenting the confidential info into binary segments (8 bits) and choosing the blocks based on the video index structure whose hash sequence matches the confidential information segment. Finally, all the chosen blocks and ancillary information are transmitted to the recipient. The suggested method outperforms the most recent coverless steganography algorithms in terms of capacity, resilience, and safety, according to experimental findings and analysis.

1. INTRODUCTION

Over the last few decades, the trend has become increasingly to digitize information, as most of the work is done electronically because of its great benefits, including saving time, effort and cost, but on the other hand, this transmitted digital data may face many challenges, including its exposure to piracy or attack from by unauthorized persons because it is done through an unsecure medium which is the Internet. To accomplish hidden correspondence and copyright security, information security has turned into an inevitable problem.

Hence the importance of providing ways to protect this digital data. Information hiding technology has been prioritized for the issues raised above. The very first method that is exploited to preserve media confidentiality is cryptography.

Unfortunately, due to its scrambling nature, it is easily detected and further decoded. Steganography, a method of concealing secret information in host media like audio, digital images, and videos without drawing attention, has been created to better safeguard the security of sensitive data and has become a very important matter in the field of information security [1, 2]. In the traditional steganography algorithm [3-5], researcher's primarily exploit the redundant properties of the media and human visual sensitivity for hiding significant secret messages in it, giving the impression that information is being hidden. Unfortunately, it'll definitely leave modifications behind that can be discovered by steganalysis techniques [6, 7]. Once the attacker discovers the presence of hidden information, he can attack these carriers, even if he cannot decipher the secret information. The explanation behind why the conventional steganography algorithm cannot withstand steganalysis is the alteration brought about by the hiding process.

So as to mainly resist steganalysis, the term of coverless steganography was suggested. "Coverless" does not imply that it does not need the carrier, but using a carrier without making any modifications. With the coverless steganography, the secret message is embedded and extracted through the common mapping rules [8, 9] in order to avoid the carrier modification process. Consequently, this technique will resist steganalysis. In other words, the primary benefits of coverless steganography are that it keeps the original files without increasing their size and limits detectability to outsiders, which was one of the shortcomings of the previous method.

The majority of carriers used in coverless steganography techniques nowadays are images. When compared to images, video sequences include both spatial information and a lot of temporary redundancy.

A little studies on coverless video steganography, nevertheless, have been published.

In this paper, we provide an IWT-based coverless information hiding algorithm. The following are the primary contributions of this paper:

- The proposed schema can withstand all known steganalysis techniques because we don't require the defined cover to conceal confidential data and hence no signs of change would remain.
- Furthermore, because of the strong hashing algorithm, this method is robust against common image attacks like rescaling, brightness modification, filtering, JPEG compression, and noise addition.
- We use the Haar wavelet transform since it is quick to compute due to its integer nature. Another benefit is that it accepts 2k bits as input and returns 2k bits as output. This simplifies the computations.
- The limitations of the current methods, such as high capacity, security and strength against attacks, were taken into consideration in the proposed system.

2. RELATED WORK

In this section, detailed literature-reviewed schemes related to coverless steganography methods are listed. These schemes are recorded as follows:

In the study of Meng et al. [10] authors present a method for coverless video steganography. First, each single frame is separated into blocks of (n*n), and each block is further divided into sub-blocks before the DCT is performed on each sub-block to retrieve DC coefficients. To construct hash sequences, every coefficient is contrasted against the largest DC coefficient in a sub-block. Next, the secret message is segmented and a video index database is formed. Finally, by examining the constructed video index database, the relevant video that's hash sequence is identical to the private data section will have been picked as the carrier for each chunk. The findings reveal that the suggested strategy performs well in terms of capacity and strength in the face of certain assaults, such as video compression, but performs poorly against others, such as frame rate alterations.

In the study of Pan et al. [11] authors offer a video information masking strategy depend on semantic segmentation. In this technology, a video database on various subjects is established and preserved on the cloud platform. To provide a statistical histogram, the frames of each video are separated by utilizing the convolutional neural network (MobilenetV2). The histogram feature is used to build the video index database as well as the hash sequence. . Each bit set in the secret information may be translated to a semantic information network histogram. The data is separated into parts. The appropriate video is considered as the carrier after scanning the video index library. The secret message may be retrieved by the recipient by picking the carrier and video frame depending on the auxiliary information supplied by the recipient. The results demonstrated that the suggested approach is resistant to video data compression attacks. The suggested system's shortcoming is that it is not resistant to certain noises and other threats. The second issue is that the training data set does not include all scenarios from everyday life. As a result, the test data set's segmentation is less precise and robust.

In the study of Liu et al. [12] authors describe a coverless steganography system based on the DWT transform and image retrieval of DenseNet features in 2020. First, the characteristics of image datasets are retrieved using the DenseNet convolutional neural network model in this technique. For image retrieval, supervised learning is applied, and the results of the retrieval might be used as a carrier. Next, the picked images will be separated into sub-blocks and the DWT will be applied on each one of sub blocks. Then, to construct robust feature sequences, a Zigzag scan is utilized to scan coefficients between blocks. Lastly, the confidential information is separated into segments that are roughly the same length as the feature sequence. The image with a sequence of characteristics identical to the segments is picked as the carrier. The results indicated that the suggested technique has strong resistance to most picture assaults, but it is weak against geometric attacks and has a large amount of auxiliary information transmitted.

Tan et al. [13] describe a coverless video information concealing strategy depend on video motion analysis. In this concept, a video database covering a variety of topics is generated, these videos are saved on the cloud platform. Each video in the library has its robust histograms of oriented optical flow (RHOOF) computed. The procedure is divided into three stages: The hash creation procedure is divided into three stages: collecting two consecutive frames from the video, turning them into grayscale, after that a median filter is applied to them, and then computing the pixel differences between both of those two frames. The confidential data is translated to binary representation, separated into parts, and then matched to RHOOF hash sequences. When compared to previous image-based approaches, the suggested system obtains lower data transfer overhead and greater hiding success rate, but the time cost is higher owing to the complexity of hierarchical optical flow computation, and this method be unsuccessful when the movement is large between two adjacent frames.

3. PRELIMINARIES

The Haar Wavelet Transform (HWT) has a significant impact on our methodology. In the interval [0, 1], the Haar Wavelet is expressed as an orthonormal system of square integrable functions. The Haar wavelet is determined by Eq. (1).

$$\Psi_t = \begin{cases} 1. \text{ if } 0 \le t \le \frac{1}{2} \\ -1. \text{ if } \frac{1}{2} \le t \le 1 \\ 0. \text{ otherwise} \end{cases} \quad (1)$$

Its scaling function is given in Eq. (2), where the value is '1' for all values ranging from 0 to 1 and '0' for all other values.

$$\Phi_t = \begin{cases} 1. \text{ if } 0 \le t \le 1 \\ 0. \text{ otherwise} \end{cases} \quad (2)$$

Using the formula in Eq. (3), the mother wavelet may now be utilized to produce the child wavelets, where a and b are location coordinates.

$$\Psi_{a.b}(t) = \frac{1}{\sqrt{a}} \Psi\left(\frac{t-b}{a}\right) \quad (3)$$

We chose the HWT because it has properties that are useful for our steganography approach. The Haar Wavelet Transform is quick to compute because of its integer nature. The main

advantage of employing the HWT is that it only produces integer coefficients [14]. The coefficients may be represented in hardware description languages as fixed-point numbers, giving our project additional flexibility. This simplifies the computations for the following step, which is turning the outputs into binary.

4. THE PROPOSED METHOD

This part describes the suggested coverless video steganography system.

Figure 1 represents the block diagram of the proposed method.

The suggested method includes two sides namely, sender side and receiver side. Each one has several activities as follows.

4.1 Sender side

In this side several activities are be done.

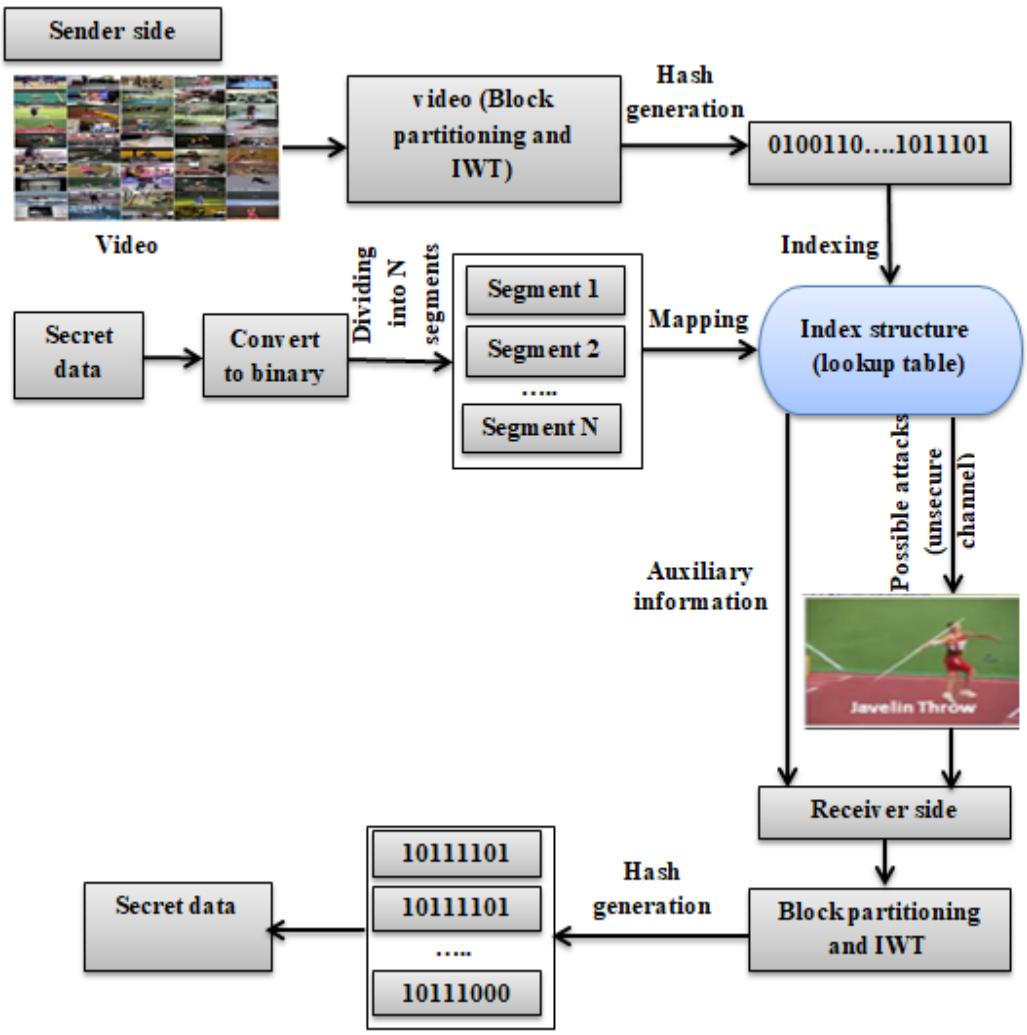

Figure 1. The proposed system

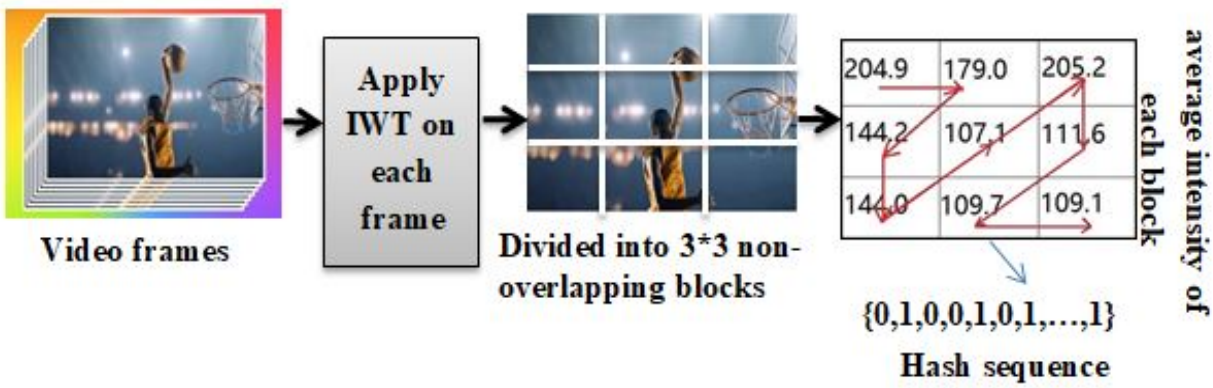

Figure 2. The process of creating the hash sequence

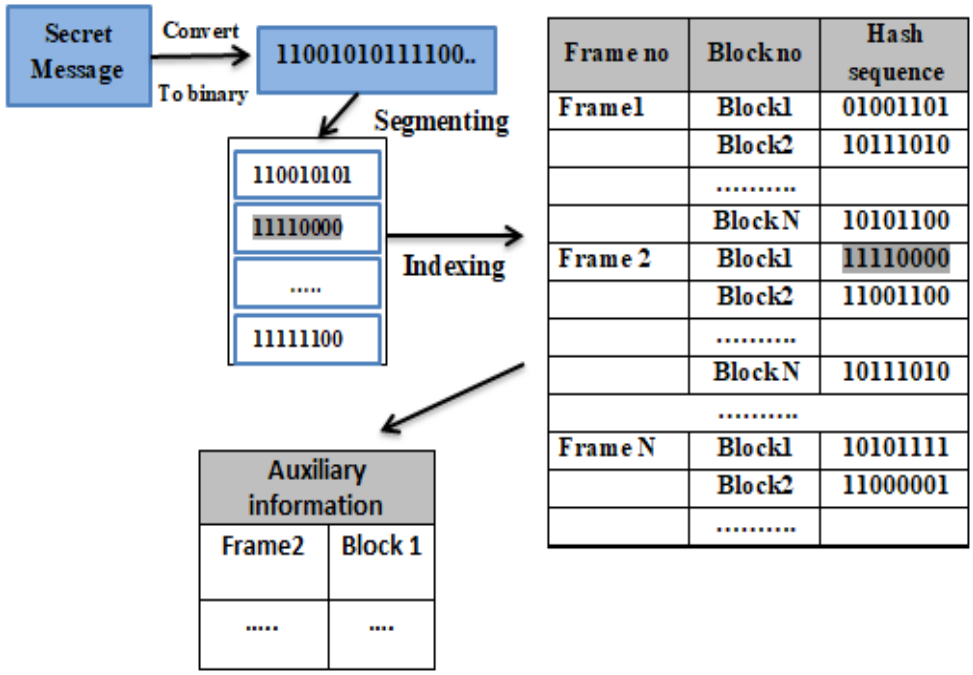

Figure 3. The mapping the secret information

4.1.1 Generation of hash sequence algorithm

This subsection describes the resilient hashing algorithm used to generate video hash sequences. As is well known, the stego-video may be attacked during transmission by several common processing such as rescaling, compression, and noise addition.

Because of this, the hashing technique must resist most of these assaults, guaranteeing that the video's hash sequence is not altered throughout the communication. This guarantees that the confidential message is dependably and accurately transferred with little losses and variations. To that aim, we present a strong hashing technique for generating video hash sequences.

The hashing algorithm consists of several major phases.

- Firstly, we convert the video to grayscale
- Secondly, the video is divided into frames
- Thirdly, Haar IWT is applied one on each frame in order to acquire LL, LH, HL, HH coefficients as described in section 3 and selecting LL Coefficients.
- Thirdly, the LL coefficients are divided into n*n nonoverlapping blocks labelled as $\{fb_{11}; fb_{12}; ...; fb_{ij}; ...; fb_{33}\}$.
- Fourthly, after calculating each block's average intensity, intensity values are obtained.
- Lastly, the intensity values are zigzaggedly concatenated to form a vector designated as $\{I_1; I_2; ...; I_9\}$ and each intensity value I_i is compared to its neighboring I_{i+1} by Eq. (4) to obtain the image hash sequence $\{fh_1; fh_2; ...; fh_8\}$.

$$fh_i = \begin{cases} 1. & \text{if } I_i \geq I_i + 1 \\ 0. & \text{otherwise} \end{cases} . \text{where } 1 \leq i \leq 8 \qquad (4)$$

Figure 2 depicts the robust hashing algorithm's technique for generating hash sequences.

4.1.2 Mapping the secret information

To simplify the transfer of the confidential data, the transmitter first converts the confidential data to a bitstream and then splits it into segments of the same length, typically 8-bit. It should be noted that if the length of the bitstream is not a multiple of 8 bits, numerous zeros are appended to the end. Then, using every segment as a separate query, all blocks of the video whose hash sequences match the segment are collected and indexed as auxiliary information as shown in Figure 3.

For instance, assume that the hash sequence of the first segment is {11110000} identical to the first block of the first frame, which is {11110000}, so it will be selected and added to the auxiliary information table.

4.1.3 Embedding operation

This sub section explains how hidden information is embedded which can be done as following steps:

- The secret information is turned into binary sequence S. S is then subdivided into 8-bit segments. Namely S= {S1, S2, Si, and Sn}. If Si is less than eight bits, zeros will be inserted to bring it up to 8 bits. The insertion will be done to the end of that segment.
- The video's hash sequence is generated using the hash sequence generating method suggested in subsection 4.1.1, and a lookup table is constructed.
- The segments of secret information are mapped and matched as stated in subsection 4.1.2, after which the matching carrier is chosen noted as the essential data.
- Step3 should be repeated until all the segments of secret information has been matched and merged to create auxiliary information.
- The video and the auxiliary information are forwarded to the recipient.

Algorithm 1 illustrates the embedding of secret information process.

Algorithm 1: Embedding procedure
Input: Video V, secret information S.
Output: auxiliary information AI = $\{ind_1, ind_2, ..., ind_N\}$.
1: Padding bits to the secret information: Padding(S)= S' $\{S_1, S_2, ..., S_m\}$

2: Decompose video to frames: f = VideoToFrame(V_k)
3: For i=1 into k
4: Generating hash sequences H_i
5: End for
6: Segment S' into N segment:
7: For i=1 to N do
8: Match S_i with H_i
9: Register the index and establish auxiliary information AI = {indN}
10: End for
11: Transmit auxiliary information AI to the recipient

4.2 Receiver side

On the receiving end, the extracting activity will be done.

4.2.1 Information extraction

In this subsection, after receiving the auxiliary information and the video from the sender, the hidden information is restored in the following order.

Algorithm 2: Extraction procedure

Input: Video V, auxiliary information AI= {ind_1, ind_2, …, ind_N}.
Output: The secret information bit bitstream is S= {S_1, S_2, …, S_d}
1: Decompose video to frames: f = VideoToFrame(V_k)
2: For i = 1: n
3: Get FrameID, blockID from Index item AI of auxiliary information
4: Generating hash sequences H_i= Hashcal($H_{block\ ID}$)
5: End for
6: Join all of the segments as {$hash_1$, $hash_2$, …, $hash_n$}
7: Remove the padding bits to recover the secret information bitstream: S = {S_1, S_2, . . ., S_d}

- Corresponding frames and blocks can be located by the receiver based on the received auxiliary information.
- The hash sequence of the corresponding blocks is generated using the hash sequence generating method described in subsection 4.1.1.
- Repeat the step2 until all hash sequences are extracted.

After linking the hash sequences and deleting the inserted bits from the end, the bitstream containing hidden data is retrieved effectively.

The extraction process of secret data is illustrated by algorithm 2.

5. EXPERIMENTS

The experimental findings suggest that the secret information can be successfully retrieved. Furthermore, we will evaluate our method's resistance to Common attacks, security, the capacity of information hiding, and compare with previous steganography approaches.

5.1 The robustness to typical attacks

Robustness is a rational steganography algorithm assessment that represents the algorithm's capacity to resist adversary attacks [15, 16]. The failure of the steganography technique during the transmission process is caused by typical assaults such as JPEG compression, noise, filtering, cropping etc.

The Bit Error Rate (BER) is used to assess the resilience of an algorithm throughout the communication procedure [15]. If O={o_1, o_2,.. , o_n} represents the binary vector of the original picture and A = {a_1, a_2,.. a_n} implements the binary vector of the frame after it has been attacked, the BER is then calculated as follows:

$$\mathrm{BER} = \frac{\mathrm{e}}{\mathrm{n}} \tag{5}$$

$$\mathrm{e} = \sum_{i=1}^{n} (Oi + \mathrm{A}i) \tag{6}$$

5.1.1 JPEG compression

JPEG is the most widely used and fundamental compression format for continuous-tone still image. It a lossy compression method that permits information loss due to a certain frequency at which human eyesight is insensitive, and is done on digital images before transmission across digital devices [15]. As a result, if this type of compression is used, the cover video is likely to be destroyed during transmission. The BER is used to assess the resilience of the suggested method to JPEG compression attack.

Table 1 compares the BER of four methods as well as our algorithm when attacked by JPEG compression. The findings demonstrate that the recommended strategy outperforms others by having the lowest BER at the same compression quality value.

Table 1. Comparison of the capabilities of Ref. [17], Ref. [18], Ref. [13], Ref. [11] and the proposed method to withstand JPEG compression assault

Quality (σ)	Ref. [17]	Ref. [13]	Ref. [18]	Ref. [11]	The Proposed Method
90	0.8833	0.9439	0.9935	0.8542	0
70	0.7717	0.9149	0.9912	0.8476	0

5.1.2 Noise attack

The robustness of the signal pulse causes salt and pepper noise, likewise referred to as double pulse noise. This noise is divided into two categories: high grayscale noise (salt noise) and low grayscale noise (pepper noise). In most cases, these forms of noise arise simultaneously [10, 15]. The suggested approach is analyzed for salt and pepper noise, that has a density varies from 0 to 0.1 with an increment of 0.01.

A fundamental interference model, additive white Gaussian noise (AWGN), degrades the signal by linear added white noise. While the power spectral density has a uniform distribution, the AWGN amplitude has a Gaussian distribution. AWGN has two parameters: mean and variance σ2 [15, 17].

If the original bit stream {b_1, b_2, ..., b_m} and the extracted bit stream {b_1', b_2'... b_m'}, the accuracy rate is determined using:

$$\mathrm{ACC} = \frac{\sum_{i=1}^{m} \mathrm{f(i)}}{\mathrm{m}} \tag{7}$$

where,

$$\mathrm{f(i)} = \begin{cases} 1.\ \mathrm{if}\ \mathrm{HS_i} = \mathrm{HS_i'} \\ 0.\ \mathrm{if}\ \mathrm{HS_i} \neq \mathrm{HS_i'} \end{cases} \tag{8}$$

This research examines the strength of retrieving single-bit confidential information in Table 2. When compared to existing video coverless information concealing algorithms, the suggested approach performs well in single-bit robustness. In terms of image-type assaults, the algorithm's extraction precision of a single bit is preserves at or above 90%, and the strength is good and well-balanced.

Table 2. Single byte accuracy with various attacks

Attack	Ref. [11]	Ref. [18]	Ref. [16]	The Proposed Method
Salt and pepper (σ = 0.002)	84.6%	--	81.5%	100%
Salt and pepper (σ = 0.005)	62,1%	--	74.8%	99.9%
Gauss (σ = 0.001)	31%	51%	70.9%	99.9%
Gauss (σ = 0.006)	30.1%	51.7%	71.4%	99.8%

5.1.3 Filtering attacks

The stego-video was filtered using a mean filter, a median filter, and a sharpening filter, each with various kernel window sizes. Table 3, shows the robustness of the proposed system against some filtering attacks.

Table 3. The results of some filtering attacks

Attack Type	Density of Noise	BER %	SSIM
Median filter	1*1	0	1
Median filter	2*2	0.19	0.9
Median filter	3*3	0.15	0.93
Mean filter	1*1	0.1	0.92
Mean filter	2*2	0.21	0.8
Mean filter	3*3	0.19	0.9
Sharpening filter	1*1	0.5	0.86
Sharpening filter	2*2	0.7	0.85
Sharpening filter	3*3	0.7	0.85

5.2 Capacity analysis

This part investigates the program's capacity. The ability to hide information is determined by the length of the hash sequences. In this study's experiment, we produce more than an 80-bit hash sequence for hiding the confidential information in each frame. As demonstrated in Table 4, our suggested coverless information concealing approach has a substantially better.

Table 4. Capacity comparison

Method	Ref. [16]	Ref. [19]	Ref. [20]	Ref. [13]	Ref. [18]	The Proposed Method
Capacity (bits/ carrier)	8	8	16	32	8	256

6. CONCLUSIONS

The coverless steganography approach based on wavelet transform is suggested in this research as a novel solution for video security. The algorithm is characterized by strong hash generation due to the fact that it uses Haar IWT, which is characterized by being computationally fast due to its integer nature as it only produces integer coefficients. Investigations and comparisons with currently used methods have been made regarding the capacity analysis and robustness to common attacks, JPEG compress, filtering and noise attacks. Based on the investigations and comparisons that were mentioned before, the experimental results and analyses demonstrate that the suggested algorithm outperforms the contemporary methods. This is because the algorithm achieved a higher capacity rate than its counterparts from the proposed methods and has the ability to withstand the majority of attacks.

REFERENCES

[1] Meng, L., Jiang, X., Zhang, Z., Li, Z., Sun, T. (2022). A robust coverless image steganography based on an end-to-end hash generation model. IEEE Transactions on Circuits and Systems for Video Technology, 33(7): 3542-3558. https://doi.org/10.1109/TCSVT.2022.3232790

[2] Kadhim, M.A., Jawad, M.J. (2022). A coverless video steganography: A survey. In 2022 5th International Conference on Engineering Technology and its Applications (IICETA), Al-Najaf, Iraq, pp. 522-527. https://doi.org/10.1109/IICETA54559.2022.9888744

[3] Liu, Y., Liu, S., Wang, Y., Zhao, H., Liu, S. (2019). Video steganography: A review. Neurocomputing, 335: 238-250. https://doi.org/10.1016/j.neucom.2018.09.091

[4] Yao, Y., Yu, N. (2021). Motion vector modification distortion analysis-based payload allocation for video steganography. Journal of Visual Communication and Image Representation, 74: 102986. https://doi.org/10.1016/j.jvcir.2020.102986

[5] Nguyen, D.C., Nguyen, T.S., Hsu, F.R., Hsien, H.Y. (2019). A novel steganography scheme for video H. 264/AVC without distortion drift. Multimedia Tools and Applications, 78: 16033-16052. https://doi.org/10.1007/s11042-018-6976-3

[6] Feng, G., Zhang, X., Ren, Y., Qian, Z., Li, S. (2019). Diversity-based cascade filters for JPEG steganalysis. IEEE Transactions on Circuits and Systems for Video Technology, 30(2): 376-386. https://doi.org/10.1109/TCSVT.2019.2891778

[7] Boroumand, M., Chen, M., Fridrich, J. (2018). Deep residual network for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 14(5): 1181-1193. https://doi.org/10.1109/TIFS.2018.2871749

[8] Liu, Q., Xiang, X., Qin, J., Tan, Y., Zhang, Q. (2021). A robust coverless steganography scheme using camouflage image. IEEE Transactions on Circuits and Systems for Video Technology, 32(6): 4038-4051. https://doi.org/10.1109/TCSVT.2021.3108772

[9] Zhou, Z., Sun, H., Harit, R., Chen, X., Sun, X. (2015). Coverless image steganography without embedding. In Cloud Computing and Security: First International Conference, ICCCS 2015, Nanjing, China, pp. 123-132. https://doi.org/10.1007/978-3-319-27051-7_11

[10] Meng, L., Jiang, X., Zhang, Z., Li, Z., Sun, T. (2020). Coverless video steganography based on maximum DC coefficients. arXiv preprint arXiv:2012.06809. https://doi.org/10.48550/arXiv.2012.06809

[11] Pan, N., Qin, J., Tan, Y., Xiang, X., Hou, G. (2020). A

video coverless information hiding algorithm based on semantic segmentation. EURASIP Journal on Image and Video Processing, 2020(1): 1-18. https://doi.org/10.1186/s13640-020-00512-8

[12] Liu, Q., Xiang, X., Qin, J., Tan, Y., Tan, J., Luo, Y. (2020). Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping. Knowledge-Based Systems, 192: 105375. https://doi.org/10.1016/j.knosys.2019.105375

[13] Tan, Y., Qin, J., Xiang, X., Zhang, C., Wang, Z. (2021). Coverless steganography based on motion analysis of video. Security and Communication Networks, 2021(1): 1-16. https://doi.org/10.1155/2021/5554058

[14] Govindasamy, V., Sharma, A., Thanikaiselvan, V. (2020). Coverless image steganography using Haar integer wavelet transform. In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, pp. 885-890. https://doi.org/10.1109/ICCMC48092.2020.ICCMC-000164

[15] Wu, J., Liu, Y., Dai, Z., Kang, Z., Rahbar, S., Jia, Y. (2018). A coverless information hiding algorithm based on grayscale gradient co-occurrence matrix. IETE Technical Review, 35(1): 23-33. https://doi.org/10.1080/02564602.2018.1531735

[16] Li, R., Qin, J., Tan, Y., Xiong, N.N. (2022). Coverless video steganography based on frame sequence perceptual distance mapping. Computers, Materials & Continua, 73(1): 1571-1583. https://doi.org/10.32604/cmc.2022.029378

[17] Bi, R. (2022). The communication process of digital binary pulse-position modulation with additive white Gaussian noise. In International Conference on Neural Networks, Information, and Communication Engineering (NNICE), 12258: 496-504. https://doi.org/10.1117/12.2640680

[18] Zou, L., Wan, W., Wei, B., Sun, J. (2021). Coverless video steganography based on inter frame combination. In Geometry and Vision: First International Symposium, ISGV 2021, Auckland, New Zealand, pp. 134-141. https://doi.org/10.1007/978-3-030-72073-5_11

[19] Yuan, C., Xia, Z., Sun, X. (2017). Coverless image steganography based on SIFT and BOF. Journal of Internet Technology, 18(2): 435-442. https://doi.org/10.6138/JIT.2017.18.2.20160624c

[20] Zheng, S., Wang, L., Ling, B., Hu, D. (2017). Coverless information hiding based on robust image hashing. In Intelligent Computing Methodologies: 13th International Conference, ICIC 2017, Liverpool, UK, pp. 536-547. https://doi.org/10.1007/978-3-319-63315-2_47

NOMENCLATURE

IWT	integer wavelet transform
DWT	discrete wavelet transform
HWT	Haar wavelet transform
RHOOF	robust histograms of oriented optical flow
DCT	discrete cosine transform
AWGN	additive white Gaussian noise
JPEG	Joint Photographic Experts Group
BER	Bit Error Rate
α	Scaling factor
Ψ	Haar wavelet's mother wavelet function
Φ	scaling function