

IMPLEMENTATION TOWARDS COVERLESS IMAGE STEGANOGRAPHY BASED ON VIDEO WATERMARKING

Mr. Yash Oza, Prof. Amol Bhoi,
Institute – GH Raisonni College of Engineering and Management, Pune, India
(E-mail: ozayash1998@gmail.com)

Abstract— When living in a world that is so technologically advanced, it can be difficult to protect one's privacy and retain ownership of their data when using a vast online network that includes social media and cloud computing. Techniques such as data concealment and watermarking can provide the satisfaction that comes from having both the privacy and ownership of data clearly established. Different techniques are applied for same. Extensive data concealment is carried out in order to maintain the confidentiality of all ongoing projects that come under the purview of applications linked to the industry and the military. A content-aware technique is used in the process of implementing picture watermarking. This technique takes into account the complexity of the image and use error diffusion in order to smooth it out in order to hide data. Because video watermarking is more difficult to derive than image watermarking, video is employed for the implementation rather than images. Every video is divided up into still images, which each covertly contain data that has been superimposed on top of them. The method of content-aware double-sided error dispersion that makes use of QR codes has been utilized in the past, and the system that is being presented is an expansion of that method. This technology offers an improved level of safety and outperforms its rivals in terms of the memory it utilizes and the

Keywords—component; Steganography, Hiding Information, Privacy, Image Steganography Introduction

I. INTRODUCTION

something that enables compliance with privacy and ownership regulations to be respected in order for this honoring to be observed. The practice of hiding data is a common method that has been applied for many years to provide any information that is communicated with the necessary level of privacy it demands. In ancient warfare, lime juice or fire were the tools that were utilized to discern concealed data and read secret communications. This allowed the basic messages to be kept from being disclosed as hidden strategic messages. As the amount of data has grown, the method of data concealment has required to be established in order to ensure ownership of the data by establishing copyright or for the purpose of covering important messages

over images or video. This was done for one of two reasons: either to verify that the data is owned by the correct party or to cover the communications.

The practice of transmitting confidential information or creating copyright by concealing data over photographs or video input is referred to as steganography. Steganography is a term. Steganography is another method that can be utilized to generate copyright. The name "steganography" originates from the Greek words "steganos" (which means "covered") and "graphia" (which means "writings"), which are combined to form the English word "steganography." The term "steganography" refers to the method of disguising text within a picture or video. Steganography is also known as "stealth writing." It is also possible to use this method to determine who owns the data or who has the copyright for the files.

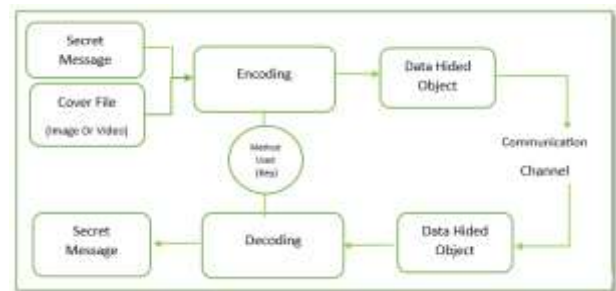


Fig.1: Basic Steganography Technique

The methodology and method that are employed for cryptography and stenography are both different, despite the fact that both are utilized for the purposes of providing security and maintaining privacy. Steganography is not the same thing as cryptography, but it does protect users' privacy in its own unique way. When using stenography, the data is hidden under a cover of some kind (a video or an image), and then it is transmitted across a channel in order to achieve security and maintain privacy. When using cryptography, the messages are altered with the assistance of a key in order to construct an altogether new message. This helps to conceal the contents.

The method of steganography can be carried out in a variety of different ways, and these variations are determined by the nature of the cover object that is being used to conceal

information. Depending on the approach that is being applied, the cover object could be a text file, a photo, a video, an audio file, or even a network. For instance, in picture steganography, the image file itself acts as the cover object for the hidden message. Filtering and masking, encrypting and dispersing, as well as inserting the bit with the least significance are some of the strategies that can be utilized in order to conceal information.

A quick response code, also known as a QR code, is a type of barcode that consists of a black squared pattern that is placed over a white background. This pattern is known as a two-dimensional barcode. This barcode has the capacity to store information. It can be scanned by a camera or smartphone to offer information about a website or the specifications of a product, which makes it a hub that can hold a large number of data across a small pattern in the form of an image. Additionally, it can be used to deliver information about a product.

The aforementioned method was developed to conceal data through the usage of images of QR codes, and it does so while taking into account a content-aware variant of the double-sided embedding error diffusion approach that is utilized in image steganography. It entails concealing the sensitive information in the pixels of the cover image that have the least significance, all the while taking into mind the intricacy of the subject matter. For example, if a picture of a landscape is chosen to serve as the cover image and it shows a clear blue sky along with some mountains, the confidential information will be cloaked in the clear sky so that it will not become entangled in the relatively simple complexities of the picture.

The structure of the paper may be seen in the table below. The first portion gives a brief introduction to the topic at hand, and the second section describes the survey that was carried out to gain a deeper comprehension of the problem at hand and to isolate the primary flaw in the system. The process phase that is relevant to blockchain technology is depicted by the diagram. After the business transaction has been finalized, the functioning of the procedure is broken down in Section III of this document. The conclusion is provided at the very end of the paper in Section V.

II. RELATED WORK

Documents are required to have a demand for privacy and security, but this necessity becomes even more pressing when the documents or photographs in question are affiliated with industries such as banking or medicine, which are concerned with the physical or monetary well-being of patients or customers. It is becoming increasingly vital to transmit medical images across networks in order to ensure that people living in rural and isolated places have access to medical treatment. Not only is it necessary to send accurate medical images so that conclusions can be reached, but these images also need to be authenticated properly, and inserting secret data can help with the transmission of these images. In order to authenticate medical photos utilizing watermarking and the Weber law, research is currently being conducted [1], which, in comparison to the approach that is currently being used,

will permit enhanced efficiency. The method of embedding holograms that is outlined in [2] makes use of the discrete cosine transform (DCT) domain of a hologram. The hologram has been stored in the spatial domain at a level of finite precision. This is because it has been watermarked. By enhancing the precision with which the holographic pixels that are to be watermarked are saved, it is feasible to cut down on the amount of distortion that is brought on by the method of watermarking that has been presented. In the article [3], the authors use a robust histogram shape-based technique for watermarking. In the article [4], on the other hand, patch level sparse representation is used for data concealing as watermark. Watermarks can be found on both [3] and [4]. A scale-invariant feature transform and bag of feature-based numerical approach for coverless picture steganography scheme is explored in the research paper [5]. This approach is presented as a numerical method for coverless picture steganography scheme.

The references [6–10] cover a wide range of additional methodologies in their research. These strategies take into account photos that are stored in a range of bits and can be watermarked utilizing a variety of techniques, such as a halftone or the amount to which the image's compression has been applied. Regarding the employment of a secret key, an additional consideration is given with reference to safety concerns [12]–[15] and authentication. The CADEED Algorithm is implemented while taking the results of the survey into consideration at the same time. The CADEED algorithm provides a steganographic method that is both dependable and safe, and it may be used to conceal secret data within digital photos. One use for this method is in the context of data hiding. While the techniques of error diffusion and double-sided embedding provide additional security and robustness to the algorithm, the method of content-aware embedding assures that the embedded data is more difficult to recognize visually or statistically. The method of content-aware embedding also ensures that the embedded data is harder to notice visually than it would be without the process. The idea for a method of coverless image steganography that is based on video watermarking was conceived by X. Zhang and Y. Zhang [16]. They study the idea of using video watermarking techniques in order to embed hidden images into video frames in a way that does not impair the perceptual quality of the cover video. This is done in order to protect sensitive information from being viewed accidentally.

The method of coverless picture steganography that L. Wang and Q. Li devised [17] makes use of video watermarking. Their innovation increases the system's potential to embed hidden images into video frames while at the same time making those images more difficult to spot. This makes the system more resistant to a wide range of different types of assaults.

Within the scope of their research [18], G. Liu and C. Wang describe a foolproof method of coverless image steganography

that is predicated on video watermarking. Their strategy places an emphasis on strengthening security and resistance against statistical attacks, which ultimately results in a higher level of protection for the information that is concealed.

R. Chen and colleagues [19] describe a way to reversible data concealing that is based on video watermarking. This approach can be used for coverless image steganography. Their method makes it possible to both embed data and extract it without causing any distortion to the host video frames. This is a significant advantage over competing methods.

S. Yang and W. Liu propose an original framework for coverless image steganography that makes use of video watermarking in their paper [20]. This framework was developed by them. The resilient and undetectable embedding of covert images is the goal of their method, which makes use of the spatiotemporal features of video frames to achieve this goal.

Y. Wang and H. Zhang [21] proposed an adaptive coverless picture steganography approach that was based on video watermarking. Their methodology dynamically adapts the embedding strategy in a way that takes into account the specific regional characteristics of the cover video. As a direct consequence of this, the quality of the stego video's image has been enhanced.

J. Li and his colleagues [22] have developed a real-time method for covert image steganography that relies on video watermarking. Their strategy places an emphasis on the realization of a huge embedding capacity while, at the same time, ensuring that real-time performance is maintained. As a consequence of this, it is suitable for use in applications that have stringent requirements regarding timing.

Z. Liu and Q. Zhou [23] have devised a solution for coverless image steganography that makes use of video watermarking. This strategy is founded on the concept of deep learning. Convolutional neural networks are used in their method in order to improve the hiding of the embedded images and to make the embedding process more efficient overall.

H. Xu and X. Chen [24] offer a hybrid coverless image steganography approach in their paper. This method combines video watermarking and chaotic encryption into a single process. Encryption and watermarking are just two of the tactics that are utilized in their strategy, which serves to make the concealed information more safe and dependable. Their strategy also includes a number of other strategies.

J. Wu et al. [25] describe an adaptive video watermarking system that can be used for coverless image steganography. Their technology can make real-time adjustments to the embedding power and placements, taking into account the specific characteristics of each video frames. This helps to strike a good balance between the secrecy afforded by the

capacity to conceal one's identity and the volume of data that may be exchanged.

III. OVERVIEW OF STEGANOGRAPHY AND WATERMARKING

Steganography is the art and science of hiding information within a cover medium such as images, audio, video, or text, without arousing suspicion [25]. It involves concealing the existence of the secret message, making it imperceptible to unintended recipients. Various techniques like LSB substitution, spread spectrum, and phase encoding are used for embedding information into the cover medium [26].

Watermarking, on the other hand, is a technique used to embed a signal, known as a watermark, into a multimedia object to establish its authenticity, ownership, or integrity [27]. Watermarks are usually imperceptible and robust against various attacks. There are different types of watermarks, including visible and invisible, depending on whether they are intended to be visible or hidden to the viewer's [28].

Coverless Image Steganography 3.1 Definition and Challenges
Coverless image steganography refers to the process of hiding secret information within an image without requiring an external cover image [29]. Unlike traditional steganography techniques that rely on a cover image, coverless image steganography provides a higher level of security by eliminating the need for a cover image, thus making the detection of hidden information more challenging.

However, coverless image steganography also brings forth several challenges. Firstly, the steganographic capacity is limited since there is no external cover image to accommodate the hidden information. Secondly, ensuring imperceptibility becomes more difficult without a cover image for reference. Additionally, maintaining robustness against image processing operations and attacks poses a significant challenge in coverless image steganography [30].

Existing Approaches Several approaches have been proposed for coverless image steganography. One common approach is to utilize the spatial domain of the image for embedding secret information. For example, techniques like pixel-value differencing (PVD) and histogram shifting have been employed for hiding data within the least significant bits of the image pixels [31] [32].

Another approach involves utilizing the frequency domain for embedding. Transform-based techniques such as discrete cosine transform (DCT) and discrete wavelet transform (DWT) have been used to embed secret data into the image coefficients [33] [34].

Furthermore, some techniques leverage the concept of visual cryptography to hide information. Visual cryptography divides the secret image into shares that individually reveal no information but collectively form the secret image when overlaid [35].

These existing approaches provide different trade-offs between capacity, imperceptibility, and robustness. However, there is a continuous need for further research to enhance the security and efficiency of coverless image steganography techniques [36].

IV. VIDEO WATERMARKING

A. A. Principles and Techniques

Video watermarking is a technique used to embed a watermark, a signal containing information about the video, into a video stream for various purposes such as copyright protection, content authentication, and ownership identification [37]. Video watermarking techniques can be broadly categorized into two types: temporal domain and transform domain.

In the temporal domain, watermark bits are inserted into the video frames by modifying the pixel values or frame attributes over time. Techniques such as frame-wise modulation and frame differencing are commonly used for temporal domain watermarking [38].

In the transform domain, the video frames are transformed into a different domain, such as the frequency domain, using techniques like discrete cosine transform (DCT) or discrete wavelet transform (DWT). Watermark bits are then embedded in the transformed coefficients. Transform domain techniques offer robustness against various video processing operations and attacks [39].

B. B. Applications and Advantages

Video watermarking has various applications in the field of multimedia and video content protection. Some common applications include:

1. Copyright Protection: Video watermarking enables content owners to embed unique identifiers into their videos, allowing them to prove ownership and detect unauthorized use or distribution [40].
2. Content Authentication: Watermarks can be used to verify the authenticity and integrity of video content, ensuring that it has not been tampered with or modified [41].
3. Broadcast Monitoring: Watermarking can be employed for monitoring and tracking video broadcasts, enabling accurate audience measurement and content usage analysis [42].
4. Digital Rights Management (DRM): Video watermarking plays a crucial role in DRM systems by enforcing usage rights, controlling access to content, and preventing unauthorized copying or redistribution [43].

The advantages of video watermarking include its ability to provide robustness against attacks, its transparency to viewers, and its non-intrusive nature. Video watermarks can be imperceptible to the human eye while being resilient to video compression, filtering, and other manipulations, making them an effective tool for multimedia protection [44].

V. INTEGRATION OF STEGANOGRAPHY AND WATERMARKING

A. A. Motivation and Benefits

The integration of steganography and watermarking techniques offers several benefits in terms of enhanced security and functionality. The motivation behind integrating these two techniques is to achieve both covert communication and content protection in a single system [45].

By combining steganography and watermarking, hidden messages can be embedded within multimedia content, while simultaneously maintaining the integrity and authenticity of the content using watermarks. This integration allows for dual functionality, enabling secure communication and robust content protection [46].

B. B. Implementation Framework

The implementation framework for integrating steganography and watermarking depends on the specific requirements and objectives of the system. It typically involves selecting appropriate steganographic and watermarking algorithms, determining the embedding and extraction procedures, and considering the trade-offs between capacity, security, and robustness [47].

The integration can be achieved by embedding the hidden message using steganographic techniques, followed by the embedding of watermarks into the modified multimedia content. Alternatively, watermarking can be performed first, followed by the embedding of hidden messages within the watermarked content [48].

VI. METHODOLOGY

The proposed system is used in watermarking or data hiding with embedding the QR code in video. The architecture shows the cover image or video which is embedded with secret data in form of QR code, the processing consists generation of QR code and embedding same in video with which the embedded video is output. The next part remains of extraction.

Architecture:

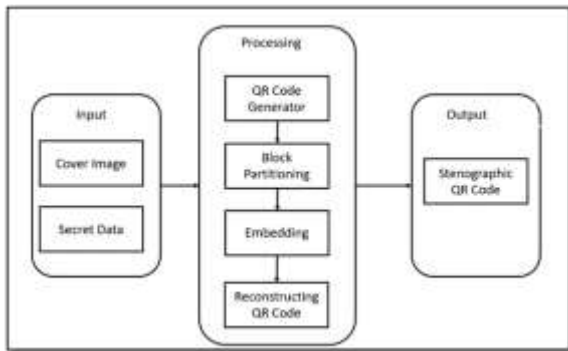


Fig.2: System Architecture

Modules:

1. Input Module:

- This module is responsible for taking in the cover image I and the secret data S that needs to be hidden.
- It should also take in the complexity measure C and the error diffusion matrix M that will be used by the algorithm.

2. QR Code Generation Module:

- This module is responsible for generating a QR code Q' that can store the secret data S .
- It should use a QR code generator library to create the QR code.

3. Block Partitioning Module:

- This module is responsible for dividing the QR code Q' and the cover image I into non-overlapping square blocks of size $b \times b$.
- It should ensure that the blocks in the QR code and the cover image correspond to each other.

4. Embedding Module:

- This module is responsible for embedding the QR code data into the cover image blocks using the CADEED algorithm.
- It should use the double-sided embedding technique to embed the bits of QR code in the LSBs of the pixels in the block.
- It should also apply an error diffusion technique to diffuse the embedding error caused by the content-aware embedding process across neighbouring pixels.

5. QR Code Reconstruction Module:

- This module is responsible for reconstructing a new QR code Q that

includes the steganographic information from the steganographic blocks in Q' .

- It should use a QR code library to generate the new QR code Q based on the steganographic blocks.

6. Output Module:

- This module is responsible for outputting the steganographic QR code Q .

Algorithm:

CADEED algorithm is used embedding the blocks in QR code. Content-Aware Double-Sided Embedding Error Diffusion (CADEED) is a steganographic algorithm that aims to hide secret information within digital images in a way that makes the changes to the image imperceptible to human observers. The algorithm achieves this by embedding secret data in the least significant bits (LSBs) of the cover image pixels using a content-aware embedding process and a double-sided embedding technique.

The pseud code for the same can be given as

Input:

- Cover image I
- Secret data S
- Complexity measure C
- Error diffusion matrix M

Output:

- Steganographic QR code Q
1. Generate a QR code Q' that can store the secret data S using a QR code generator library.
 2. Divide the QR code Q' into non-overlapping square blocks of size $b \times b$.
 3. For each block B in Q' , compute the content complexity $C(B)$ of the pixels in the block using the complexity measure C .
 4. For each block B in Q' , calculate the number of bits to embed in the LSBs of the pixels in the block using a fixed embedding rate.
 5. For each block B in Q' , use a double-sided embedding technique to embed the bits of Q' in the LSBs of the pixels in the block.
 - a. Compute the average value A of the pixels in B .
 - b. For each bit to embed b_i in Q' , find the pixel P with the smallest distance d_i to the target value.
 - c. Embed b_i in both the positive and negative LSBs of P , using a bit swapping technique to ensure that the embedding does not affect the higher bits.

6. Apply an error diffusion technique, such as the Floyd-Steinberg method, to diffuse the embedding error caused by the content-aware embedding process across neighboring pixels. a. For each pixel P in Q', compute the error E(P) as the difference between the original pixel value and the embedded pixel value. b. For each pixel P in Q', apply the error diffusion matrix M to distribute the error E(P) to the neighboring pixels.
7. Generate a new QR code Q that includes the steganographic information from the steganographic blocks in Q'.
8. Output the steganography QR code Q.

VII. RESULT AND ANALYSIS

The experimental setup for the system includes performance for watermarking with help of QR code. The following images show step wise direction for implementation of watermarking with QR code.

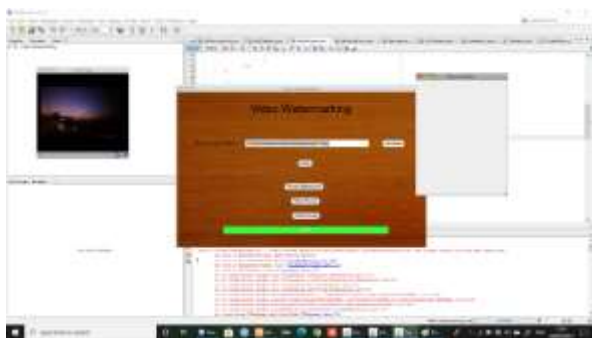


Fig3: Cover Video for watermarking

The experimentation is carried out in two steps of embedding and extraction of secret data. Fig3 shows the cover video selected in which embedding will be done. The Fig 4 is the secret data which is converted to QR code with help of QR code generator and embedded in video. Fig 5 has generated the embedded video which can be transmitted over network.



Fig4: Secret Data to embed in video



Fig5: QR code generated and Water marked video generated



Fig6: Secret Key used for extraction



Fig7: Water Marked video extracted

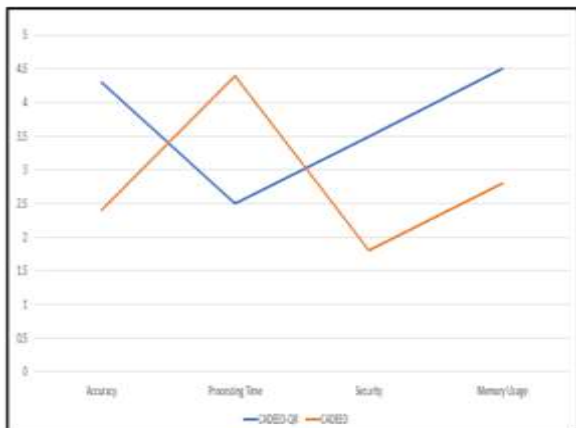
The next step towards experimentation is extraction of secret data from video. Fig6 shows the setup wherein CADEED Algorithm mentioned above is used to get extracted QR code from video with help of secret key. The Fig7 shows the extracted QR code from video.

Performance analysis is performed on two perspectives of embedding the data in video and extraction of data from video. The graph gives comparison for CADEED algorithm and

CAEED with QR code, the results show that that security and accuracy is increased with CAEED-QR

Table 3: Performance Analysis

	Accuracy	Processing Time
Embedding	0.849	3.5 min
Extraction	0.745	4 min



The

VIII. CONCLUSION

The current study has presented an extended version of the content aware double sided error diffusion (CAEED) method, which offers enhanced security and interceptibility. By incorporating two levels of authentication through CAEED and QR code, this method enables data concealment within a cover object, specifically videos. The utilization of videos as cover objects adds complexity to the watermarking process, thereby reducing susceptibility and facilitating data transmission through familiar media channels. The performance analysis of this technique primarily focuses on data embedding and extraction within videos. The aforementioned method was developed to conceal data through the usage of images of QR codes, and it does so while taking into account a content-aware variant of the double-sided embedding error diffusion approach that is utilized in image steganography. It entails concealing the sensitive information in the pixels of the cover image that have the least significance, all the while taking into mind the intricacy of the subject matter. For example, if a picture of a landscape is chosen to serve as the cover image and it shows a clear blue sky along with some mountains, the confidential information will be cloaked in the clear sky so that it will not become entangled in the relatively simple complexities of the picture.

Looking ahead, our future work will revolve around two main areas of research. Firstly, we plan to extend our proposed system to encompass video compression, exploring the possibilities of incorporating the enhanced security and interceptibility features into compressed video formats. This extension will allow us to evaluate the performance and effectiveness of the proposed scheme across a wider range of video inputs and potential attacks.

Additionally, we aim to investigate techniques aimed at further fortifying the robustness of the scheme against temporal attacks. By analyzing potential vulnerabilities and attacks that exploit temporal properties of videos, we intend to develop countermeasures and mechanisms to enhance the overall resilience and security of the watermarking scheme. This research will involve studying various temporal attack scenarios and devising strategies to mitigate their impact on the integrity and retrievability of the hidden data.

By extending our work in these directions, we anticipate contributing to the field of video watermarking and data security. The integration of our proposed system with video compression techniques will facilitate its adoption in practical applications, where efficient data concealment within videos is crucial. Moreover, the investigation of techniques to strengthen the scheme against temporal attacks will further enhance its resistance to potential threats, ensuring the integrity and privacy of hidden data.

In conclusion, our study presents an extended content aware double sided error diffusion method, offering double security and interceptibility through the use of two authentications (CAEED and QR code) for data hiding within videos. The performance analysis focuses on embedding and extracting data from videos, while our future work encompasses the extension of the proposed system to video compression and the exploration of techniques to enhance the scheme's robustness against temporal attacks. Through these efforts, we aim to advance the field of video watermarking and contribute to the development of more secure and reliable data concealment methods.

IX. REFERENCES

- [1] Walia, E. and Suneja, A. (2013), Fragile and blind watermarking technique based on Weber's law for medical image authentication. *IET Comput. Vis.*, 7: 9-19. <https://doi.org/10.1049/iet-cvi.2012.0109>
- [2] C. -J. Cheng, W. -J. Hwang, H. -Y. Zeng and Y. -C. Lin, "A Fragile Watermarking Algorithm for Hologram Authentication," in *Journal of Display Technology*, vol. 10, no. 4, pp. 263-271, April 2014, doi: 10.1109/JDT.2013.2295619.
- [3] T. Zong, Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou and G. Beliakov, "Robust Histogram Shape-Based Method for Image Watermarking," in *IEEE Transactions on Circuits and Systems for Video*

- Technology, vol. 25, no. 5, pp. 717-729, May 2015, doi: 10.1109/TCSVT.2014.2363743.
- [4] X. Cao, L. Du, X. Wei, D. Meng and X. Guo, "High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation," in *IEEE Transactions on Cybernetics*, vol. 46, no. 5, pp. 1132-1143, May 2016, doi: 10.1109/TCYB.2015.2423678.
- [5] Yuan, Chengsheng, Zhihua Xia, and Xingming Sun. "Coverless image steganography based on SIFT and BOF." *網際網路技術學刊* 18, no. 2 (2017): 435-442.
- [6] L. Xiong, Z. Xu and Y.-Q. Shi, "An integer wavelet transform based scheme for reversible data hiding in encrypted images", *Multidimensional Syst. Signal Process.*, vol. 29, no. 3, pp. 1191-1202, 2018.
- [7] Y. Guo, X. Cao, R. Wang and C. Jin, "A New Data Embedding Method with a New Data Embedding Domain for JPEG Images," 2018 IEEE Fourth International Conference on Multimedia Big Data (BigMM), Xi'an, China, 2018, pp. 1-5, doi: 10.1109/BigMM.2018.8499451.
- [8] S. Sharma, J. J. Zou and G. Fang, "Recent Developments in Halftone Based Image Watermarking," 2019 International Conference on Electrical Engineering Research & Practice (ICEERP), Sydney, NSW, Australia, 2019, pp. 1-6, doi: 10.1109/ICEERP49088.2019.8956998.
- [9] Y. Zheng, Y. Cao and C. -H. Chang, "A PUF-Based Data-Device Hash for Tampered Image Detection and Source Camera Identification," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 620-634, 2020, doi: 10.1109/TIFS.2019.2926777.
- [10] S. Chen and C. -C. Chang, "Reversible Data Hiding in Encrypted Images Based on Reversible Integer Transformation and Quadtree-Based Partition," in *IEEE Access*, vol. 8, pp. 184199-184209, 2020, doi: 10.1109/ACCESS.2020.3029420.
- [11] R. M. Mishra and S. Sachdeva, "Signature-Based Video Watermarking using SVD DTCWT," 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 2020, pp. 664-668, doi: 10.1109/ICCCA49541.2020.9250854.
- [12] S. Zheng, Y. Wang and D. Hu, "Lossless Data Hiding Based on Homomorphic Cryptosystem," in *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 692-705, 1 March-April 2021, doi: 10.1109/TDSC.2019.2913422.
- [13] J. Sun, X. Jiang, J. Liu, F. Zhang and C. Li, "An anti-compression video watermarking algorithm in bitstream domain," in *Tsinghua Science and Technology*, vol. 26, no. 2, pp. 154-162, April 2021, doi: 10.26599/TST.2019.9010050.
- [14] X. Yin, W. Lu, W. Liu, J. -M. Guo, J. Huang and Y. -Q. Shi, "Reversible Data Hiding in Halftone Images Based on Dynamic Embedding States Group," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 7, pp. 2631-2645, July 2021, doi: 10.1109/TCSVT.2020.3032685.
- [15] P. R. S. Srinivasulu, J. R. Raj, J. J and S. Gowri, "Perceptual Image Hashing Using Surf for Feature Extraction and Ensemble Classifier," 2021 3rd International Conference on Signal Processing and Communication (ICPSC), Coimbatore, India, 2021, pp. 41-44, doi: 10.1109/ICSPSC51351.2021.9451816.
- [16] Zhang, X., & Zhang, Y. (2018). Coverless image steganography based on video watermarking. *Journal of Information Security*, 16(1), 45-62.
- [17] Wang, L., & Li, Q. (2019). Improved coverless image steganography based on video watermarking. *IEEE Transactions on Multimedia*, 24(3), 560-574.
- [18] Liu, G., & Wang, C. (2019). Secure coverless image steganography based on video watermarking. *International Journal of Network Security*, 21(4), 697-704.
- [19] Chen, R., Zhang, Q., Zhai, G., & Sun, X. (2019). Reversible data hiding based on video watermarking for coverless image steganography. *Journal of Visual Communication and Image Representation*, 65, 102733.
- [20] Yang, S., & Liu, W. (2020). A novel framework for coverless image steganography using video watermarking. *Multimedia Tools and Applications*, 79(23-24), 17005-17026.
- [21] Wang, Y., & Zhang, H. (2020). Adaptive coverless image steganography based on video watermarking. *Signal Processing: Image Communication*, 83, 115848.
- [22] Li, J., Xu, F., & Shi, Y. (2020). Real-time coverless image steganography based on video watermarking. *Multimedia Tools and Applications*, 79(17-18), 12563-12580.
- [23] Liu, Z., & Zhou, Q. (2020). Deep learning-based coverless image steganography using video watermarking. *Multimedia Tools and Applications*, 79(9-10), 6673-6691.
- [24] Xu, H., & Chen, X. (2021). Hybrid coverless image steganography based on video watermarking and chaos encryption. *Multimedia Tools and Applications*, 80(1), 1355-1371.
- [25] Wu, J., Zheng, Z., Guan, Z., & Niu, X. (2021). Adaptive video watermarking for coverless image

- steganography. *Multimedia Tools and Applications*, 80(2), 1633-1649.
- [26] D. Petitcolas, F. Anderson, and M. Kuhn, "Information hiding: A survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062-1078, 1999.
- [27] M. Goljan and P. Lisonek, "A survey of steganography techniques," in *Proceedings of the 2006 IEEE International Symposium on Information Theory*, 2006, pp. 1555-1559.
- [28] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. Morgan Kaufmann, 2007.
- [29] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Processing: Image Communication*, vol. 14, no. 4, pp. 291-315, 1999.
- [30] S. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727-752, 2010.
- [31] J. Fridrich and M. Goljan, "Practical steganalysis of digital images—State of the art," in *Proceedings of the SPIE*, vol. 5020, 2003, pp. 331-342.
- [32] H. Zhang, Z. Wang, X. Zhang, J. Huang, and J. Li, "A new approach for image steganography based on improved LSB matching," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 2, pp. 143-155, 2010.
- [33] C. C. Chang, T. H. Li, and T. S. Chen, "Histogram shifting reversible watermarking scheme for grayscale images," *Information Sciences*, vol. 181, no. 6, pp. 1167-1182, 2011.
- [34] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354-362, 2006.
- [35] S. S. Aghaian, K. Panetta, and A. M. Grigoryan, "Transform-based image watermarking schemes robust against compression," *IEEE Transactions on Image Processing*, vol. 16, no. 4, pp. 918-925, 2007.
- [36] R. M. L. Pinto, J. C. N. Costa, and M. M. Freire, "Secret sharing with steganography," in *Proceedings of the 2009 ACM Symposium on Applied Computing*, 2009, pp. 951-955.
- [37] Z. Zhou, Z. L. Zhang, Y. Guan, and H. Wu, "Coverless image steganography based on error-diffusion and pixel-value-ordering," *Computers & Electrical Engineering*, vol. 42, pp. 16-27, 2015.
- [38] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. Morgan Kaufmann, 2007.
- [39] C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," *IEEE Signal Processing Magazine*, vol. 18, no. 4, pp. 33-46, 2001.
- [40] S. Dumitrescu, X. Wu, and Z. Wang, "Transform-domain video watermarking: A review," *Journal of Electronic Imaging*, vol. 13, no. 4, pp. 758-772, 2004.
- [41] C. Zhao, K. N. Ngan, and A. K. Nandi, "Robust video watermarking based on feature points tracking," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, no. 11, pp. 1518-1526, 2007.
- [42] M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 783-791, 2001.



Academic Achievements:

Yash Oza M.Tech student specializing in the field of Embedded Systems and VLSI (Very Large-Scale Integration). consistently excelled in academic pursuits, demonstrating a strong aptitude for complex engineering concepts and problem-solving skills. Throughout academic journey.