International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6581
***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 14 April 2023*

Robust Video Watermarking Algorithm based on DCT-SVD approach and Encryption

Praful Saxena[1], Santosh Kumar[2]
[1]Research Scholar , Computer Science & Engineering
Maharishi University of Information Technology
Lucknow, India
shyam.praful@gmail.com
[2]School of Computing & Engineering
Galgotias University
Greater Noida, India
Sant7783@hotmail.com

Abstract— Sharing of digital media content over the internet is increasing everyday .Digital watermarking is a technique used to protect the intellectual property rights of multimedia content owners. In this paper, we propose a robust video watermarking scheme that utilizes Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) for embedding a watermark into video frames. The proposed method uses encryption to make the watermark more robust against malicious attacks. The encryption key is used to modify the watermark before it is embedded in the video frames. The modified watermark is then embedded in the DCT and SVD coefficients of the video frames. The experimental results show that the proposed method provides better robustness against various attacks such as compression, noise addition, and filtering, while maintaining good perceptual quality of the watermarked video. The proposed method also shows better resistance against geometric attacks such as cropping, rotation, and scaling. Overall, the proposed method provides an effective solution for protecting the intellectual property rights of multimedia content owners in video distribution and transmission scenarios.

Keywords- Watermarking,Discrete Cosine Transform, Singular Valur Decomposition, Encryption.

I. INTRODUCTION

Due to extensive use of multimedia and the Internet, digital content, particularly digital photographs, digital videos has drawn a lot of attention. The Internet and media technologies make it exceedingly simple, inexpensive, and expedient to change, replace, regenerate, and distribute digital images. Data authentication safeguards the integrity of the multimedia component by ensuring its accuracy and consistency. One type of authentication method that has drawn scholars to this area of study is digital image watermarking. This approach creates the watermarked image by embedding a watermark (ownership information) into the host image. Later, the system takes the created watermarked image and extracts the watermark image from it. Digital watermarking is a process of embedding an imperceptible pattern of digital data within a multimedia file, such as an image, video, or audio clip. This pattern serves as a digital signature that can be used to authenticate the content's origin, track its usage, or protect it against unauthorized duplication. The watermark is typically added by altering the least significant bits of the file's pixels or samples, so that the visual or auditory quality of the content is not affected. The watermark may contain information such as the creator's name, copyright notice, or a unique identifier that can be used to link the content to a specific owner or distributor[1].

Digital watermarking has a wide range of applications, including content protection, copyright management, forensic analysis, and multimedia authentication. For example, watermarking can be used to prevent piracy by making it easier to detect and track illegal copies of a file. It can also be used to trace the source of leaked or stolen content, or to prove ownership in case of disputes[2]. However, digital watermarking also raises concerns about privacy, security, and fair use. Critics argue that watermarking can be used to invade users' privacy by tracking their consumption habits or to limit their rights to use or share the content. Therefore, the design and implementation of digital watermarking systems require careful consideration of ethical, legal, and technical issues[3]. A digital image watermarking system has four design features: imperceptibility, resilience, capacity, and security. Nevertheless, these needs cannot be met at the same time due to their limitations and incompatibilities. The application often determines how imperceptibility, robustness, and capacity are balanced. Also, it was found in the literature that spatial domain approaches are less reliable than transform domain methods. Spatial domain techniques directly use the pixel values in the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6581
***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 14 April 2023*

image. So, by modifying these pixel values, the watermark can be integrated into the host image[4]. These spatial domain approaches are only appropriate for images with no noise. Cropping attacks can omit the watermark image, which is a significant disadvantage of spatial domain watermarking[5].

II. METHODOLOGY USED

In this research work the focused areas are Discrete Cosine Transform, Singular Value Decomposition , Motion frame selection and Encryption method for Watermark.

A. Discrete Cosine Transform

The Discrete Cosine Transform (DCT) is a mathematical tool that is commonly used in digital image and video processing, including in digital watermarking. DCT is a technique that converts a spatial signal into its frequency domain representation[6]. It does this by representing the image as a sum of sinusoidal functions of different frequencies and amplitudes, with each sinusoidal function representing a specific frequency component of the image. In watermarking, the DCT can be used to embed the watermark within the image or video by modifying the high-frequency components of the image or video[7]. High-frequency components are typically areas of an image where there is rapid change, such as edges or textures, and they are less sensitive to human perception than low-frequency components, which contain smoother variations in the image. The watermark can be added to the high-frequency coefficients of the DCT by modifying the values of the coefficients in a way that is imperceptible to human vision or hearing. The modification process is carefully designed to minimize the impact on the original image quality, and the changes are usually distributed across several DCT coefficients to make the watermark more robust against common image processing operations, such as cropping or compression. When the watermarked image is received, the DCT coefficients are extracted, and the watermark can be detected by applying a watermark extraction algorithm that looks for the specific pattern or signal that was embedded in the DCT coefficients[8]. Overall, the DCT plays an important role in watermarking by providing a way to embed the watermark into an image or video in a way that is robust, imperceptible, and reversible. Equation 1 shows the DCT coefficient for 8 X 8 blocks size of divided image .

$$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{i=0}^{7}\sum_{j=0}^{7} f(i,j) \cos\left(\frac{(2i+1)u\pi}{16}\right) \cos\left(\frac{(2j+1)v\pi}{16}\right) \quad (1)$$

Where F(u,v) is the DCT coefficient of the image.

B. Singular Value Decomposition

The Singular Value Decomposition (SVD) is another mathematical tool that is commonly used in digital watermarking, especially in watermarking of audio signals. SVD is a matrix decomposition technique that decomposes a matrix into three matrices that represent its singular values, left singular vectors, and right singular vectors. In watermarking, SVD can be used to embed the watermark within the audio signal by modifying the singular values of the audio signal's SVD[9]. The singular values represent the amount of energy in the audio signal's frequency components, and modifying them can alter the audio signal's energy distribution in the frequency domain. The watermark can be added to the audio signal's SVD by modifying the singular values in a way that is imperceptible to human hearing.

The modification process is carefully designed to minimize the impact on the original audio quality, and the changes are usually distributed across several singular values to make the watermark more robust against common audio processing operations, such as filtering or compression. When the watermarked signal is received, the SVD is computed, and the watermark can be detected by applying a watermark extraction algorithm that looks for the specific pattern or signal that was embedded in the singular values[10].

Overall, SVD plays an important role in watermarking of digital signals by providing a way to embed the watermark into the audio signal in a way that is robust, imperceptible, and reversible. Suppose there is an image of size M×N that will be watermarked. The image can be presented in a nonzero matrix and made into Equation 2.

$$A = USV^T \quad (2)$$

Where A is denoting as a matrix of image ,S in singular matrix and U and V are the orthogonal matrix .

C. Motion Frame Selection

The host video object's related frames can be found and removed using the scene change detector's functionality. By exploiting a correlation between the video's frames, this is accomplished. Depending on the need for the results to be refined, the procedure can be used up to various degrees. There are many ways to filter similar frames from the video, including linear interpolation, binary search, and histogram. Using a histogram approach, scenes with comparable values are collected in one bin, and an attempt is made to determine the cut-off range for the greatest number of elements[11].

The idea behind this strategy is to measure the signal's distribution across the entire spectrum and use this information for analysis. In this instance, the statistical measure is the difference between the heights of the histograms for the same bins. At the initial stage, a filtering technique that eliminates identical frames is utilized to eliminate comparable frames.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6581
***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 14 April 2023*

The histogram, binary search, and linear interpolation are all used as part of the filtering procedure to remove duplicate frames. The HiBisLI method is the name of this method. The approximate value is calculated using the binary search approach, which is based on sorting arrays. Any function with two values can be approximated using the linear interpolation approach. Either of these techniques can be used to remove comparable frames from the cover video, leaving just the frames that are different from one another.

Extracting motion frames from a video using histograms involves using the changes in pixel intensities between consecutive frames of the video to detect motion. Here are the general steps to extract motion frames using histograms: Use a video reader to read the frames of the video. Convert each frame to grayscale to reduce the computational complexity of the algorithm. Compute the histogram of each frame using a histogram function. The histogram should capture the distribution of pixel intensities in the grayscale image. Compute the difference between the histograms of consecutive frames to detect changes in pixel intensities. Threshold the difference in histograms to identify frames where the changes in pixel intensities are above a certain threshold. This threshold can be set based on the amount of motion required to be detected. Extract the frames where the difference in histograms is above the threshold as the motion frames.

III. LITERATURE REVIEW

The performance of the transform domain algorithms is superior to the spatial domain methods. Maintaining a trade-off between the design needs at the same time is crucial. The right domain to retain this trade-off by integrating two or more transform domain algorithms is the hybrid domain approaches. The DWT-based technique is effective in both the temporal and frequency domains, yet DWT occasionally produces subpar results. A hybrid method based on lifting wavelet transform (LWT), DCT, and SVD is developed to get over the conventional restrictions of the wavelet-based watermarking algorithm. The Canny edge detector is now utilized to choose the ideal place for putting the binary watermark. Multiple scaling factor (MSF) has been employed during watermark embedding to preserve the trade-off between imperceptibility and resilience, and particle swarm optimization (PSO) has been used to achieve optimum MSF. However, the technique is not resistant to hybrid, resynchronization, and print/scan attacks. The method doesn't take the watermark image's security into account. Moreover, it is not calculated how many watermarks can be included. DCT is a popular technique used in image and video compression, and it has also been used in video watermarking. DCT-based watermarking works by embedding the watermark in the DCT coefficients of the video frames. The watermark is embedded in the high-frequency coefficients of the DCT matrix because they are less visible to the human eye[12]. The watermark is also spread across multiple frames of the video to increase its robustness.

Several studies have explored the effectiveness of DCT-based video watermarking techniques. The proposed DCT-based video watermarking technique that uses a non-blind method to embed the watermark. The technique was found to be robust against common video processing attacks such as frame averaging, frame dropping, and frame flipping[13]. The authors proposed a DCT-based video watermarking technique that uses a singular value decomposition (SVD) pre-processing step to enhance the robustness of the watermark. The results showed that the technique was robust against a variety of attacks, including noise addition, compression, and geometric transformations[14].

Several studies have explored the effectiveness of SVD-based video watermarking techniques. The proposed an SVD-based video watermarking technique that uses a chaotic map to enhance the security of the watermark. The results showed that the technique was robust against a variety of attacks, including cropping, filtering, and compression[15]. The proposed an SVD-based video watermarking technique that uses a non-negative matrix factorization (NMF) pre-processing step to enhance the robustness of the watermark. The results showed that the technique was robust against a variety of attacks, including geometric transformations, filtering, and compression. In the case of content authentication, the high frequency components (HH) of IDWT are employed to embed the logo information as a delicate watermark onto the host image. Imperceptibility, robustness, and capacity are three competing and constrained objectives, and an optimization process called artificial bee colony (ABC) is utilized to achieve the best possible balance between them. Another method applies different DWT levels to the cover (or host) image before merging DCT and DWT. Here, a spread transform quadrature index modulation (QIM) technique is utilized to insert the watermark. It uses an orthogonal matching pursuit compression reconstruction approach to boost the watermarking system's efficiency[16]. The frequency domain and spatial domain are the two domains used in watermarking for the message insertion procedure. Since computation in the spatial domain is faster, simple data are frequently inserted there. The frequency domain is more assault resistant and takes longer to process than the spatial domain, which excels in speed but is not immune to attacks during picture processing[17] . One technique used in image processing for the compression of images is the discrete cosine transform (DCT). DCT's two primary advantages for compressing images and videos are as follows- Concentrate the energy of the image into a few coefficients (energy compaction). Reduce coefficient interdependence as much as possible

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6581
***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 14 April 2023*

IV. PROPOSED METHOD

The initial process is to extract the motion frames the host video . The extraction can be done by using the define process in the previous section . The proposed method is divided into three section watermark encryption , watermark embedding and watermark extraction.

A. Watermark Encryption

Initial step involves reading in the binary image as an array of pixel values. Each pixel can have a value of 0 or 1. The secret key is a binary string that will be used to determine the order in which pixels are swapped. Next step involves generating a random permutation of the pixel indices in the image. This permutation will be used to determine the order in which pixels are swapped. This step involves using the secret key to determine a starting position in the permutation. The starting position should be a value between 0 and the length of the permutation. Traverse the permutation from the starting position, swapping the pixels at each pair of indices with the same XOR value as the secret key. Repeat until the end of the permutation is reached. This step involves outputting the scrambled image as an array of pixel values. The scrambled image should be visually different from the original binary image, but still maintain the same overall structure. Fig. 1 shows the original watermark and Fig. 2 shows the encrypted watermarked after applying the encryption.

Figure 1. Original Watermark

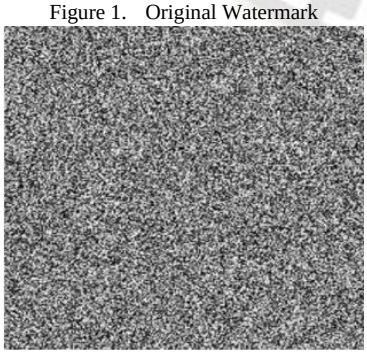

Figure 2. Encrypted Watermark

B. Watermark Embedding

- Extract the motion frames from the host video to identify the frames in which watermark is to be embedded .
- DCT is applied on the frame with the aim of splitting the frame into 8X8 pixel block.
- Apply SVD on the blocks placed prior to DCT to obtain the orthogonal and singular matrix of the frame .

$$I = U \times S \times V \quad (3)$$

- Now apply the SVD method on the watermark image to be embedded . This will results orthogonal and singular matrix of the watermark .

$$W = U_W \times S_W \times V_W \quad (4)$$

- Now to exchange the singular matrix S with the matrix S_W

$$I_{wat} = U \times S_W \times V^T \quad (5)$$

- Apply Inverse SVD to I_{wat}
- Apply the Inverse DCT and this will result the watermarked frame.
- Repeat the process on selected frames so that the complete video will be watermarked .
- Fig. 3 shows the block diagram of this complete process.

C. Watermark Extraction

- Extract the motion frames from the watermarked host video .
- Apply DCT process on the watermarked frame . Divide the image into 8 x 8 block.
- Apply the SVD process on the watermarked frame to obtain the singular values S_{ew} of it.
- Apply the SVD process to get all three values U_w , S_w and V_w .

$$W = U_W \times S_W \times V_W \quad (6)$$

- Apply SVD on the original watermark image to get the orthogonal and singular matrix .

$$I_w = U_{ew} \times S_{ew} \times V_{ew} \quad (7)$$

- Apply Inverse SVD to the U_W , V_W from the original watermark and S_{ew} from the watermarked image which will result the final extracted watermark image.
- In a similar way the watermark can be extracted from other different motion frames .

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6581
***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 14 April 2023*

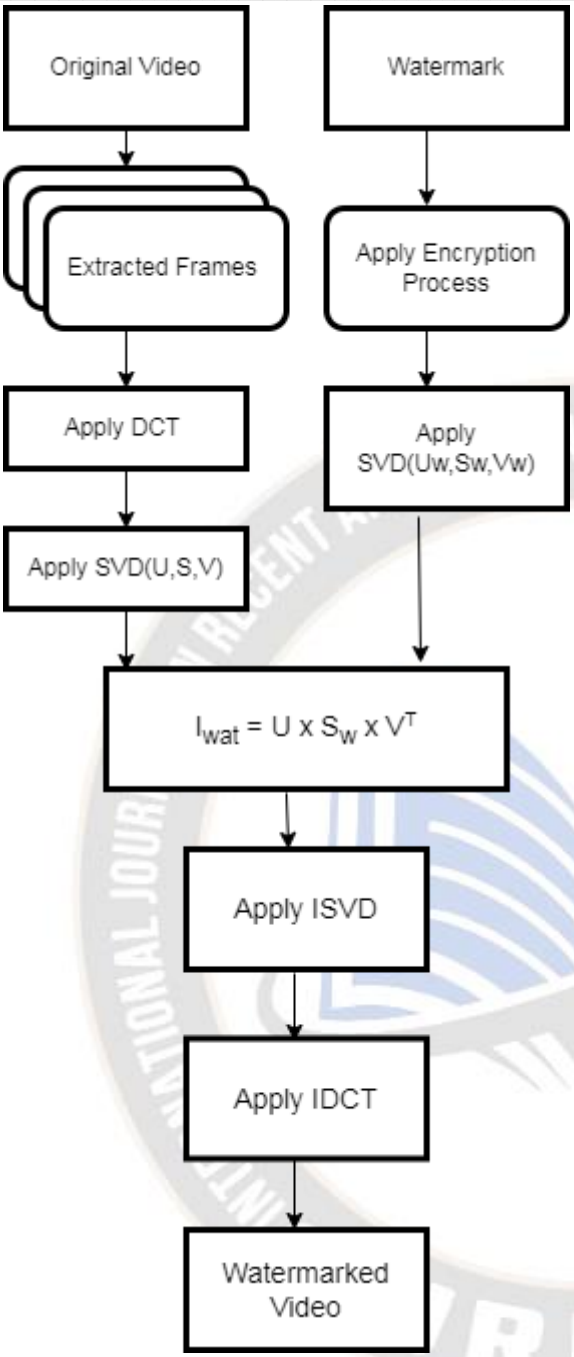

Figure 3. Watermark Embedding Process

V. RESULTS AND DISCUSSION

The proposed algorithm is implemented on two videos "foreman.avi" and "akiyo.avi" . This section contains the three parts the extraction of motion frames, Watermarked embedding process and the results discussion after performing various attacks on watermarked video.

A. Motion Frames Extraction

The method of extracting the motion frames from video is defined in the previous section . The proposed method is implemented using MATLAB and the sample video of "foreman.avi" is used . After the implementation there were total 300 frames out of which 114 are motion frames . In Fig. 4 some of the sample motion frames are shown .

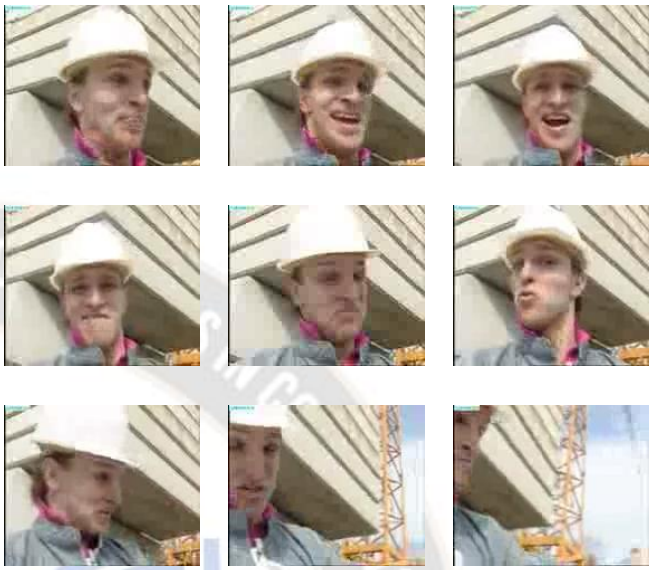

Figure 4. Extracted Motion Frames

B. Watermark Embedding

The method for embedding the watermark in the video is defined in the previous section . The proposed algorithm is implemented on two sample videos . Fig. 5 shows the original video and the Fig.6 shows video after embedding the watermark.

Figure 5. Original Video

Figure 6. Watermarked Video

C. Robustness Analysis

This section includes the robustness of proposed algorithm .The strategy to check the robustness of algorithm is to apply the various types of attacks on the watermarked video and then

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6581
***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 14 April 2023*

extract the watermark . The similarity between the extracted watermark and the original watermark shows how much the proposed algorithm is robust against the various attacks. To check the similarity two metrics are used commonly called Structural Similarity Index (SSIM) and Normalized Correlation(NC). SSIM is frequently used to measure the similarity between two images .NC parameter used for the robustness of Watermarking method. Several watermarking attacks, such as JPEG compression, noise addition, filtering, geometric assaults, and multiple types of common attacks are used to applied on the watermarked video as part of robustness studies. There are three different kinds of filtering attacks: mean, median, and Gaussian Low Pass Filter (LPF). Cropping, rotation, and flipping are the geometric attacks used. To calculate the robustness of the proposed algorithm some of the above stated attacks are selected . Table 1 and Table 2 shows the results of SSIM and NC against the performed attacks on the watermarked videos..

TABLE I. ROBUSTNESS ANALYSS(FOREMAN.AVI)

S.No	Attack Performed	SSIM	NC
1	Speckle Noise	0.9912	0.851
2	Frame Deletion (around 15%)	0.8891	0.878
3	Rotation(45 degree)	0.9001	0.993
4	Gaussian Low Pass Filter	0.9087	0.812
5	Cropping(left)	0.8879	0.898
6	Salt and Pepper	0.8874	0.882
7	JPEG Compression	0.8003	0.863

TABLE II. ROBUSTNESS ANALYSS(AKIYO.AVI)

S.No	Attack Performed	SSIM	NC
1	Speckle Noise	0.8702	0.902
2	Frame Deletion (around 10%)	0.9018	0.807
3	Rotation(60 degree)	0.8957	0.893
4	Gaussian Low Pass Filter	0.9007	0.957
5	Cropping(left)	0.8977	0.943
6	Salt and Pepper	0.9112	0.921
7	JPEG Compression	0.8801	0.872

VI. CONCLUSION

The paper proposes a robust video watermarking scheme that utilizes Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) for embedding a watermark into video frames. The proposed method uses encryption to make the watermark more robust against malicious attacks, and the experimental results show that the proposed method provides better robustness against various attacks such as compression, noise addition, and filtering, while maintaining good perceptual quality of the watermarked video. The maximum value of SSIM (Structural Similarity Index) is 0.99, which indicates that the watermarked video maintains a high level of structural similarity with the original video. The value of NC (Normalized Correlation) is 0.9500, which suggests that the watermark is well-correlated with the original watermark, indicating good embedding and extraction accuracy. Overall, the proposed method provides an effective solution for protecting the intellectual property rights of multimedia content owners in video distribution and transmission scenarios. However, it's important to note that the effectiveness of any watermarking scheme also depends on the specific application and the potential attacks it may face. In future the proposed method can be extended by using other methods such as DFT , Hybrid approach of DWT-DCT or FDCuT

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” *Signal Processing*, vol. 90, no. 3. 2010, doi: 10.1016/j.sigpro.2009.08.010.

[2] X. Chang, W. Wang, J. Zhao, and L. Zhang, “A survey of digital video watermarking,” in *Proceedings - 2011 7th International Conference on Natural Computation, ICNC 2011*, 2011, vol. 1, doi: 10.1109/ICNC.2011.6022111.

[3] S. K. Praful Saxena, “Hybrid Approach based Video Watermarking Technique by using Scene Detection,” *IJRTCSIT*, vol. 12, no. 1, p. 10, 2021.

[4] T. Sathies Kumar and C. Arun, “A review of robust video watermarking technique,” *Journal of Advanced Research in Dynamical and Control Systems*, vol. 2017, no. Special Issue 2. 2017.

[5] S. B. Rakesh Ahuja, “All Aspects of Digital Video Watermarking Under an Umbrella,” *Int. J. Image, Graph. Signal Process.*, vol. 7, no. 12, p. 54, 2015.

[6] F. Ernawan, D. Ariatmanto, and A. Firdaus, “An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients,” *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3067245.

[7] N. Deshpande, A. Rajurkar, and R. R. Mathalkar, “Robust Dual Watermarking Scheme for Video Derived from Strategy Fusion,” *Int. J. Image, Graph. Signal Process.*, vol. 6, no. 5, 2014, doi: 10.5815/ijigsp.2014.05.03.

[8] N. Chawla and V. Singh, “A novel video watermarking scheme based on DWT and PCA,” *Int. J. Eng. Adv. Technol.*, vol. 7, no. 5, 2018.

[9] L. Chen and J. Zhao, “Adaptive digital watermarking using RDWT and SVD,” 2015, doi: 10.1109/HAVE.2015.7359451.

[10] S. K. Praful Saxena, “Robust Video Watermarking scheme based on DWT and SVD approach using Multiple frequency bands,” *Parishodh*, vol. 8, no. 9, p. 74, 2019.

[11] L. Agilandeeswari and K. Ganesan, “A robust color video watermarking scheme based on hybrid embedding

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6581
***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 14 April 2023*

techniques," *Multimed. Tools Appl.*, vol. 75, no. 14, 2016, doi: 10.1007/s11042-015-2789-9.

[12] A. K. Abdulrahman and S. Ozturk, "A novel hybrid DCT and DWT based robust watermarking algorithm for color images," *Multimed. Tools Appl.*, vol. 78, no. 12, 2019, doi: 10.1007/s11042-018-7085-z.

[13] Y. Yang, Y. Zhao, J. Zhang, J. Huang, and Y. Gao, "Recent Development of Theory and Application on Homomorphic Encryption," *Dianzi Yu Xinxi Xuebao/Journal Electron. Inf. Technol.*, vol. 43, no. 2, 2021, doi: 10.11999/JEIT191019.

[14] A. Kanhe and A. Gnanasekaran, "Security of electronic patient record using imperceptible DCT-SVD based audio watermarking technique," *Int. J. Electron. Telecommun.*, vol. 65, no. 1, 2019, doi: 10.24425/123560.

[15] A. A. Mohammed, B. A. Jebur, and K. M. Younus, "Hybrid DCT-SVD Based Digital Watermarking Scheme with Chaotic Encryption for Medical Images," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1152, no. 1, 2021, doi: 10.1088/1757-899x/1152/1/012025.

[16] A. Chopra, S. Gupta, and S. Dhall, "Analysis of frequency domain watermarking techniques in presence of geometric and simple attacks," *Multimed. Tools Appl.*, vol. 79, no. 1–2, 2020, doi: 10.1007/s11042-019-08087-x.

[17] S. S. Jamal, T. Shah, S. Farwa, and M. U. Khan, "A new technique of frequency domain watermarking based on a local ring," *Wirel. Networks*, vol. 25, no. 4, 2019, doi: 10.1007/s11276-017-1606-y.