DOI: https://doi.org/10.33103/uot.ijccce.23.3.15

A Comparative Study Between the Fragile and Robust Watermarking Techniques and Proposing New Fragile Watermarking with Embedded Value Technique

Yasmin A. Hassan[1], Abdul Monem S. Rahma[2]
[1]Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq,
[2]Department of Computer Science, Al-Maarif University College, Alanbar, Iraq
[1]yasmin.a@sc.uobaghdad.edu.iq, [2]monem.rahma@uoa.edu.iq

Abstract— *Since the Internet has been more widely used and more people have access to multimedia content, copyright hacking, and piracy have risen. By the use of watermarking techniques, security, asset protection, and authentication have all been made possible. In this paper, a comparison between fragile and robust watermarking techniques has been presented to benefit them in recent studies to increase the level of security of critical media. A new technique has been suggested when adding an embedded value (129) to each pixel of the cover image and representing it as a key to thwart the attacker, increase security, rise imperceptibility, and make the system faster in detecting the tamper from unauthorized users. Using the two watermarking types in the same system reaches better results and increases the power of the system and makes it robust against any attack and revel the modification if any at the same time. PSNR has been used as a performance metric to evaluate the study. The result of the new proposed watermark is 54. It is preferable to utilize both a fragile and a robust watermark simultaneously.*

Index Terms— *Robust Watermarking, Fragile Watermarking, Embedded Value, Imperceptibility, Security.*

I. INTRODUCTION

Image protection is a major topic today. It covers a wide range of concepts, including data hiding, image encryption, watermarking, and more. Each of them is a unique technique for protecting digital images. It is crucial to know how to maintain data integrity and authenticity while preventing unauthorized change and unlawful data copying [1].

A method for including secret information in digital content is watermarking [2]. Users must choose which form of watermarking to employ based on the application since there are two types of watermarking: visible and invisible [3]. Fragile watermarking is a technique for obscuring sensitive data in the host image in the spatial domain using the least significant bit (LSB) technique whereas robust watermarking is a more reliable technique that prevents unauthorized modification and ensures the authenticity and the ownership of the digital media using frequency domain to obtain the coefficient of cover image by using transform techniques such as (DCT, DWT, SVD) [4]. An effective watermark must include various properties like imperceptibility, robustness, security, and recovery. Imperceptibility refers to the watermark image or data not being apparent in the host image or cover image. Robustness is the second property that ensures the power against attacks like noise, filtering, and cropping. Not all watermarking systems include recovery property but sometimes can localize the area of tampering. Therefore it is difficult to ensure all these properties in one system but can make a balance between them. The user will have to choose between these two attributes during design. Spatial

Received 05/March/2023; Accepted 20/April/2023
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.15

domain approaches and domain transfer techniques are the two categories into which all watermarking techniques fall [5].

The most common and significant features of frequency-domain watermarking techniques are better imperceptibility and more robustness against attacks like noise addition, pixel removal, rescaling, rotation, and shearing. This is because frequency coefficients better capture the characteristics of the human visual system (HVS) than spatial coefficients [6].

The remainder of this article is organized as follows: In Section II, the Literature review is briefly described. Watermarking, with its two types (fragile and robust watermarking), and a comparison between them as advantages and disadvantages in section III. The methodology includes embedding of the fragile watermark, robust watermark, and the proposed method in Section IV. Section V presents the experimental results, performance analysis, and discussions. The conclusions are presented at the end of the paper in Section VI.

II. LITERATURE REVIEW

Watermarking for digital video has been a popular research topic. Commercial software has recently made it quite easy to change digital media, increasing the need to verify authenticity.

- Bhattacharya and Palit [7] provide a method for reducing the reference strategy by combining robust picture characteristics with fragile watermarking approaches. The technique does not require any other data other than the input image. The watermark is built from the picture to be sent using robust image characteristics and then placed as a fragile watermark in the image itself. The highest result was reached (SSIM=0.9971).
- Kadian, Arora, and M. Arora [8] present the DWT-SVD and RDWT-SVD blind watermarking methods. Except rotation and cropping, redundant discrete wavelet transform-singular value decomposition (RDWTSVD) has demonstrated greater resilience against geometric and nongeometrical attacks. The highest result reached (SSIM=0.95) and (PSNR=44.22).
- Msallam [9] suggests employing a dynamic stego-key to conceal a message behind an image cover using the least significant bit of the Steganography technique. As stego-key relies on the cover picture to conceal a secret message, the results show increased resilience in steganography. The highest result was reached (PSNR=77.90) because of the use a of text watermark therefore the result was high.
- Salman and Abdulwahab [10] propose a modified dual-tree complex wavelet (DTCWT) transform-based invisible and blind watermark method for 3D video copyright and authenticity protection. The outcomes of the trial demonstrate that the 3D video key extraction technology has provided a high compression ratio (from 4:1 to 5:1) . When varied watermark lengths are embedded in frames with strong imperceptibility and PSNR values between 62 and 64 dB, the payload of the watermark has no impact on the quality of the images.
- ALattar and Rahma [11] Creates a new cryptographic algorithm that is based on the order-five magic square technique with more sophisticated multi-message lengths. The proposed method is superior to the other algorithms because of its good complexity and small speed variation.
- Abdulhussain, AbdulWahab, and Abdulhoseen [12] present a technique to guarantee the security of the system, an encrypted holographic watermark picture was developed employing chaotic technology, which makes use of three different chaos maps: logistic, Arnold, and Baker. The highest result was reached (SSIM=0.9).

III. WATERMARKING

The technology of watermarking is employed to safeguard crucial media from copyright infringement, manipulation, and forging. Several ways for watermarking are dependent on domains, cover media types, and human perceptibility [13] [14].

Received 05/March/2023; Accepted 20/April/2023
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.15

By immediately modifying the pixel values of the host picture or video, the watermark is directly incorporated into the spatial domain [15]. The original signal must be transformed into the frequency domain to extract the frequency component [16]. This transformation must be performed before embedding the watermark and after switching back to the spatial domain. Thus, compared to frequency domain watermarking, spatial domain watermarking is simpler [17]. Two types of watermarking based on human perception (visible and invisible) and the invisible watermarking techniques branch into fragile and robust:

A. Fragile watermarking

A form of watermarking that enables exact authentication is fragile watermarking. Files with embedded watermarks can be compared to check if they are the same watermarked file. Because any alteration to the file, whether intentional or unintentional, would be regarded as a new file, fragile watermarking is seldom utilized in practical settings[18]. Some particular uses for fragile watermarking include monitoring for tampering or alterations to works-in-progress. even if just because of noise [19]. Watermark insertion, tamper detection, and tamper localization make up a fragile watermark [20].

B. Robust watermarking

Robustness and invisibility are the main variables taken into account while developing a watermark technology. The two categories of video watermarking techniques are transform-domain and spatial-domain techniques. The embedding of the watermark in the transform domain approach is accomplished by changing the transform coefficients. In the recent past, the discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT), and singular value decomposition (SVD) have all been frequently used in the transform domain video watermarking technique [21].
Combining many transforms might potentially make up for each transform's shortcomings while also increasing the effectiveness of the watermarking technique [22].

C. Comparison Between the Fragile and Robust Watermarking

The advantages and disadvantages have been considered as a comparison between the two types of watermarking [23] [24] [6]:

Watermarking Type	Advantages	Disadvantages
Fragile Watermarking	1. Provides high security as any alteration to the content will be detected. 2. Can be used to verify the authenticity and integrity of the content.	1. Fragile watermarks can be easily destroyed or removed by malicious attackers. 2. Not suitable for applications where the content may undergo legitimate modifications.
Robust Watermarking	1. Watermark can survive most transformations to the content such as compression, cropping, etc. 2. Can be used for applications where the content may undergo legitimate modifications.	1. Robust watermarks may not be able to detect some malicious attacks such as content replacement. 2. The quality of the content may be degraded due to the presence of the watermark.

Received 05/March/2023; Accepted 20/April/2023
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.15

IV. METHODOLOGY

The embedding of the watermark is based on the cover image and the watermark image embedded in the cover image is a secret image to satisfy the integrity and authenticity, and make sure not to be seen by any unauthorized persons. the embedding of a traditional fragile watermark depends on the Least significant bit (LSB) of the cover image and replace it with the most significant bit of the watermark image. It is a simple and usable method but it is easily to cracked by attackers. Using transform (T) and its inverse (T^{-1}) may increase the security and robustness of this technique because the attacker doesn't know the value of the agreed transform between the parties. The transform matrix has been illustrated in the example below using a matrix multiplication (row by column). *Fig. 1* visually clarifies the process.

In *Fig. 1*, firstly, the cover image and watermark image have been read by the system and analyzed to their components (RGB) and multiplied by the transform matrix. The transform matrix is better to be symmetric and no one knows its values of it except the authorized parties. At this level, a binary of the resulting multiplication can be obtained to easily modify the LSB and embed the watermark image values. The integer values after modification have been obtained and again multiply by the inverse of the transform to get the image with its true components (RGB) that represent the watermarked image.

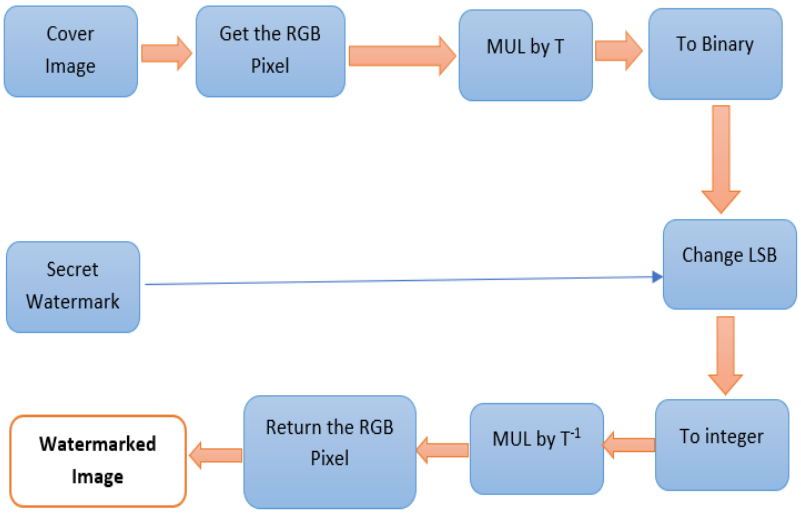

FIG. 1. FLOWCHART THAT ILLUSTRATES THE EMBEDDING OF THE TRADITIONAL FRAGILE WATERMARK.

The robust watermark is more secure and robust to several attacks and is used commonly today. The use of transforms like DCT, DWT, and SVD to get the coefficients of the image and apply the watermark. In *Fig. 2*, after reading the cover image and the watermark image, DCT (Discrete Cosine Transform) has been applied. It converts an image from the spatial domain into the frequency domain by representing it as a sum of cosine functions with different frequencies. After that, the system modifies the values by replacing the LSB of the cover image with the MSB of the watermark image, then after embedding the watermark values, an IDCT (Inverse Discrete Cosine Transform) is applied. IDCT is the inverse operation of the DCT. It converts an image from the frequency domain back to the spatial domain by computing the sum of cosine functions with different frequencies, and reconstructing the watermarked image.

Received 05/March/2023; Accepted 20/April/2023

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.15

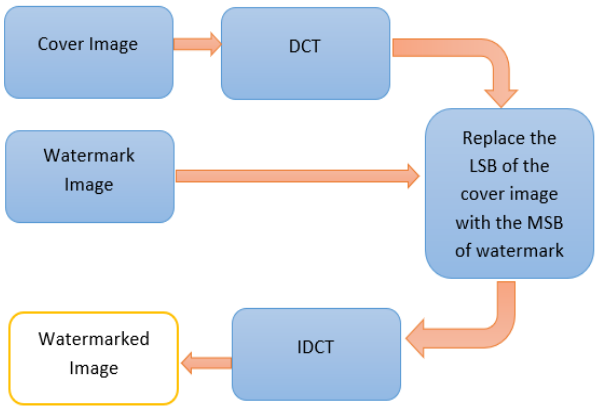

FIG. 2. FLOWCHART THAT ILLUSTRATES THE EMBEDDING OF THE ROBUST WATERMARK.

The proposed new technique suggests improving the fragile watermark by embedding value (129) that is agreed upon ed between both the sender and the receiver. They used it as a key and can change it each period. That will increase security because the unauthorized users don't know the embedded value. The embedding value is added as a fourth dimension in the image and does not affect the appearance of the image for the human therefore, this technique will increase the imperceptibility. As mentioned in *Fig. 3*, the cover and watermark images have been read and then processed the same as adding a traditional fragile watermark but here the embedded value is added in the beginning and removed at the end of the process. All the steps of adding the proposed watermark have been illustrated in detail in the following algorithm and *Fig. 3*.

Algorithm: Adding the FRAGILE watermark with embedded value:
INPUTS: **- cover image** **- watermark image** **- embedded value (129)**
OUTPUTS: **- Watermarked image.**
Begin
1. Load the cover image and watermark image **2. Resize the watermark image to match the size of the cover image** **3. Loop over each pixel in the cover image:** **a. Get the current pixel and its RGB values** **b. Prepare the transform matrix and its inverse** **c. Add the embedded value (129) as the fourth dimension to the pixel** **d. Multiply the pixel by the transform matrix** **e. Convert the result to binary and get the LSB of each channel** **f. Get the corresponding pixel from the watermark image** **g. Modify the LSB of each channel according to the watermark image** **h. Convert the modified pixels to integers** **j. Multiply the modified pixel by the inverse matrix** **k. Set the new RGB values for the pixel** **4. Remove the embedded value from the fourth dimension of each pixel.** **5. Save the watermarked image.**
End

Received 05/March/2023; Accepted 20/April/2023

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.15

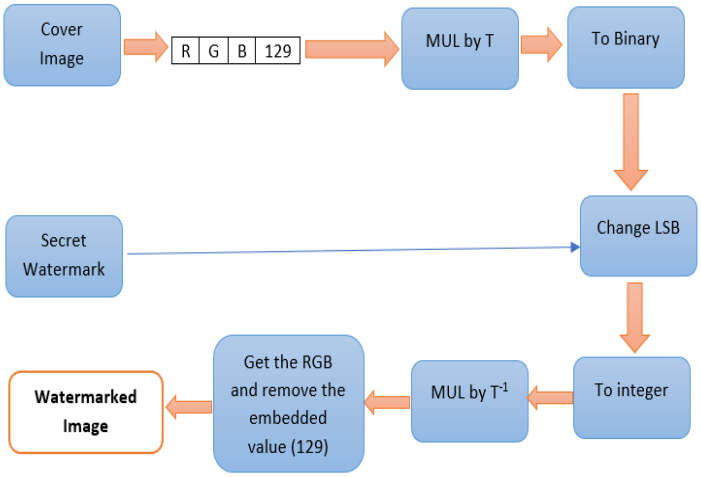

FIG. 3. FLOWCHART THAT ILLUSTRATES THE EMBEDDING OF THE PROPOSED FRAGILE WATERMARK.

The multiplication used in the embedding of the new proposed fragile watermark will be explained as an example. An embedded value (129) has been used for each pixel to thwart the attacker and increase the security of watermarking.

EXAMPLE:

A=[[226 231 134 129] [134 92 55 129] [11 22 33 129] [142 221 99 129]]	T= [[77 114 117 214] [114 77 126 116] [117 126 77 126] [214 116 126 77]]
Mul=[[87020 75399 82120 101977] [54847 44254 47759 56211] [34822 22070 22854 18997] [75317 60643 68337 78431]]	

A Matrix A represents four pixels of the image with three channels red, green, and blue. The embedded value 129 was added as the fourth channel and can treat as a key that can be changed at any time to increase robustness and security. The value (129) came from dividing the maximum value of pixel (256) by two and then adding one to the result (256/2+1=129). The matrices A and T have been multiplied and the result is called the "Mul" matrix.

Convert the multiplied matrices "Mul" to binary and change the LSB 0 → 1 or 1→ 0 according to the watermark image value.

The first value of multiplied matrices was taken and the same process was for the rest values.

Binary of the first value: 10101001111101100

Change the LSB: 10101001111101101

then return the binary matrix to its integer values and multiply it by the inverse of the transform matrix T to get the original matrix A.

Received 05/March/2023; Accepted 20/April/2023

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.15

[[226 231 134 129]
[134 92. 55 129]
[11 22. 33 129]
[142 221 99 129]]

V. EXPERIMENT RESULTS AND DISCUSSIONS

In this study, three standard images have been used each of size 1000*1000 as the cover image (Pepper, Lena, and Parrot), and a watermark image of size 64*64 which was a binary image, and apply two types of watermarking (fragile and robust) after that the newly proposed technique has been implemented using embedded value (129). The peak signal-to-noise ratio (PSNR), signal-to-noise ratio (SNR), structural similarity index (SSIM), and bit error rate (BER) have been used for comparison and to measure the performance of the proposed technique.

Table I explains the results after embedding the fragile watermark into the cover images. Table II Explains the results of embedding the robust watermark and Table III Explains the results of embedding the newly proposed technique.

TABLE I. PERFORMANCE EVALUATION OF EMBEDDING THE FRAGILE WATERMARK

Cover Image	Watermark	Watermarked Image using Fragile Watermark	PSNR	SNR	SSIM	BER
			45.98	18.25	0.9977	0.005818
			46.86	18.99	0.9981	0.006957
			47.22	19.37	0.9979	0.006972

Received 05/March/2023; Accepted 20/April/2023

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.15

TABLE II. PERFORMANCE EVALUATION OF EMBEDDING THE ROBUST WATERMARK

Cover Image	Watermark	Watermarked Image using Robust Watermark	PSNR	SNR	SSIM	BER
			46.53	18.80	0.9977	0.004516
			49.09	24.22	0.9976	0.001906
			48.19	20.35	0.9983	0.005658

Received 05/March/2023; Accepted 20/April/2023

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.15

TABLE III. PERFORMANCE EVALUATION OF EMBEDDING THE FRAGILE WATERMARK WITH EMBEDDED VALUE 129

Cover Image	Watermark	Watermarked Image using Embedded Value (129)	PSNR	SNR	SSIM	BER
			54.45	26.72	0.9979	0.001286
			54.51	26.64	0.9981	0.001526
			54.88	27.04	0.9979	0.001351

From the above results, the fragile watermark is simpler and easy to crack than the robust watermark but its benefit is for detection of the modification in the cover image faster than the robust watermark. The robust watermark is more reliable and robust against geometric attacks. The proposed method satisfies good results compared to other techniques. The high PSNR refers to the small changes (LSB) in a large amount of numbers (whole image) therefore the differences between the original cover image and the watermarked image were few compared to the whole image. It is better to use the fragile and robust watermark at the same time to increase invisibility, robustness, security, and tamper detection.

VI. CONCLUSIONS

In this study, two types of watermarking have been presented (robust and fragile). The Discrete Cosine Transform (DCT) expresses data in frequency space rather than time. When compared to spatial domain approaches, DCT-based watermarking techniques are more reliable. The fragile watermark is simple and easy to crack by the unauthorized attacker but it is very important in tamper detection and localization. The embedded value (129) has been used with fragile watermarking to thwart the attacker and used as a key for increasing the security of the proposed technique and increasing the imperceptibility and detecting any tinny modification. PSNR has been used as a performance metric to

Received 05/March/2023; Accepted 20/April/2023

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.15

evaluate the study. The result of using the new proposed technique is 54. In order to maximize invisibility, robustness, security, and tamper detection, it is preferable to utilize both a fragile and a robust watermark simultaneously.

REFERENCES

[1] A. M. Ra'ad and B. S. Mahdi, "Survey: Recent Techniques of Image Fragile Watermarking," *IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING,* vol. 22, no. 2, 2022.

[2] A. Kapse, S. Belokar, Y. Gorde, R. Rane, and S. Yewtkar, "Digital image security using digital watermarking," *International Research Journal of Engineering and Technology,* vol. 5, no. 3, pp. 163-166, 2018.

[3] S. Ramakrishnan, T. Sumathi, and S. Sasidharan, "Resolving ownership rights of video data using visible and invisible watermarking in DWT-SVD domain," in *Journal of Physics: Conference Series*, 2021, vol. 1767, no. 1: IOP Publishing, p. 012053.

[4] R. Ahuja, S. Ahuja, D. Gupta, and M. J. Haque, "Compressed domain based robust digital video watermarking scheme to protect the copyright," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 21, no. 2, pp. 1160-1167, 2021.

[5] M. S. Islam, M. A. Ullah, and J. P. Dhar, "An imperceptible & robust digital image watermarking scheme based on DWT, entropy and neural network," *Karbala International Journal of Modern Science,* vol. 5, no. 1, p. 6, 2019.

[6] M. Begum and M. S. Uddin, "Digital image watermarking techniques: a review," *Information,* vol. 11, no. 2, p. 110, 2020.

[7] A. Bhattacharya and S. Palit, "Blind quality assessment of image and video based on fragile watermarking and robust features," *Multidimensional Systems and Signal Processing,* vol. 29, no. 4, pp. 1679-1709, 2018.

[8] P. Kadian, N. Arora, and S. M. Arora, "Performance evaluation of robust watermarking using DWT-SVD and RDWT-SVD," in *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, 2019: IEEE, pp. 987-991.

[9] M. M. Msallam, "A development of least significant bit steganography technique," *IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING,* vol. 20, no. 1, pp. 31-39, 2020.

[10] A. D. Salman and H. B. Abdulwahab, "Proposed copyright protection systems for 3D video based on key frames," *IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING,* vol. 20, no. 3, pp. 1-15, 2020.

[11] I. M. ALattar and A. M. S. Rahma, "A Comparative Study of Researches Based on Magic Square in Encryption with Proposing a New Technology," *IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING,* vol. 21, no. 2, 2021.

[12] D. Y. Abdulhussain, H. B. AbdulWahab, and A. jaber Abdulhoseen, "Holographic Digital Image Watermarking Based on Chaos Techniques," *IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING,* vol. 22, no. 1, 2022.

[13] R. Hamza and H. Pradana, "A Survey of Intellectual Property Rights Protection in Big Data Applications," *Algorithms,* vol. 15, no. 11, p. 418, 2022.

[14] K. Sreenivas and V. Kamkshi Prasad, "Fragile watermarking schemes for image authentication: a survey," *International Journal of Machine Learning and Cybernetics,* vol. 9, no. 7, pp. 1193-1218, 2018.

[15] C. Sharma, B. Amandeep, R. Sobti, T. K. Lohani, and M. Shabaz, "A secured frame selection based video watermarking technique to address quality loss of data: combining graph based transform, singular valued decomposition, and hyperchaotic encryption," *Security and Communication Networks,* vol. 2021, pp. 1-19, 2021.

[16] F. Y. Shih and S. Y. Wu, "Combinational image watermarking in the spatial and frequency domains," *Pattern Recognition,* vol. 36, no. 4, pp. 969-975, 2003.

[17] K. Zhang, "Blind Digital Watermark Based on Discrete Fourier Transformation," *Highlights in Science, Engineering and Technology,* vol. 1, pp. 441-452, 2022.

[18] A. A.-A. Gutub, "Adopting counting-based secret-sharing for e-Video Watermarking allowing Fractional Invalidation," *Multimedia Tools and Applications,* vol. 81, no. 7, pp. 9527-9547, 2022.

[19] N. Akhtar, M. Saddique, K. Asghar, U. I. Bajwa, M. Hussain, and Z. Habib, "Digital video tampering detection and localization: review, representations, challenges and algorithm," *Mathematics,* vol. 10, no. 2, p. 168, 2022.

[20] L. Rakhmawati, W. Wirawan, and S. Suwadi, "A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability," *EURASIP Journal on Image and Video Processing,* vol. 2019, pp. 1-22, 2019.

[21] M. Begum, J. Ferdush, and M. S. Uddin, "A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition," *Journal of King Saud University-Computer and Information Sciences,* vol. 34, no. 8, pp. 5856-5867, 2022.

Received 05/March/2023; Accepted 20/April/2023
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.23.3.15

[22] S. B. Latha, D. V. Reddy, and A. Damodaram, "Robust Video Watermarking using Secret Sharing and Cuckoo Search Algorithm," *International Journal of Innovative Technology and Exploring Engineering,* vol. 8, no. 11, 2019.

[23] N. N. Hurrah, S. A. Parah, N. A. Loan, J. A. Sheikh, M. Elhoseny, and K. Muhammad, "Dual watermarking framework for privacy protection and content authentication of multimedia," *Future generation computer Systems,* vol. 94, pp. 654-673, 2019.

[24] N. Sivasubramanian and G. Konganathan, "A novel semi fragile watermarking technique for tamper detection and recovery using IWT and DCT," *Computing*, vol. 102, no. 6, pp. 1365-1384, 2020.

Received 05/March/2023; Accepted 20/April/2023
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*