



A NEW NESTED HYBRID DWT-HD-SVD WATERMARKING SCHEME FOR DIGITAL IMAGES

Sara R. Qasim¹, Maryam K. Abboud², Eman H. Jaddoua³

¹ Asst.Lec. Department of Computer Engineering/College of Engineering/Mustansiriyah University, Baghdad, Iraq. Email: Sararaad.cac@uomustansiriyah.edu.iq.

² Lec. Dr. College of Electrical Engineering Technical/Middle Technical University, Baghdad, Iraq. Email: maryam.khalifa@mtu.edu.iq.

³ Asst.Lec. Computer Engineering Department/Ministry of Culture, Baghdad, Iraq. Email: eman.hassony@gmail.com

<https://doi.org/10.30572/2018/KJE/150406>

ABSTRACT

Digital watermarking encrypts private information with the original data to protect the ownership rights of the digital asset. This paper suggests a brand-new nested watermarking technique (two-level watermarking technique) to protect copyrights of digital images. It based on a hybrid discrete wave transformation-Hessenberg decomposition-Singular value decomposition (DWT-HD-SVD). The gray-watermark image is first split into n parts, and each portion goes through two steps of watermarking, using two host images, using hybrid DWT-HD-SVD method and one final level of encryption (based on the Lightweight algorithm, the high-speed cryptographic method). The results of the simulation reveal that the suggested system offers a high level of imperceptibility, reliability and robustness. Also it can be used for both the colored and the grayed images.

KEYWORDS

Digital Image watermarking, DWT, SVD, HD, Copyright protection.



1. INTRODUCTION

Today's world becomes more and more accustomed to internet technology, which is now crucial to the dissemination of multimedia material. Thanks to the unfettered access the internet provides its users, we may easily find the information we need. However, due to how easily available online content is, problems like piracy, intellectual property violation, manipulation, and others commonly occur. The focus of academic study has turned to copyright protection. Watermarking has been one of the most extensively employed protection strategies in various fields of multimedia copyright protection (Cox et al., 1997). A common information embedding technique is watermarking, which protects image, video, and audio data. The earliest successful watermarking technique is produced and demonstrated in 1993. Two techniques were used, the first one was easy and based on bit plane-manipulation of the LSB, whereas the second technique uses, a difficult but more secured, linear-addition of the watermark to the original image (Tirkel et al., 1993).

Through subtle data changes, it incorporates important information into the modalities. Robustness and invisibility are thus two important criteria for assessing the efficacy of watermarking approaches. The three kinds of watermarking techniques: robust, fragile, and semi-fragile (Wu and Shih, 2004) can be generally categorized based on these two qualities. Robust watermarking is essential for the security of image data since it can withstand numerous hacking attempts and doesn't appreciably decrease the watermarked image's aesthetic quality. It is mostly used for ownership verification and copyright protection as a result. Only the image's correctness is guaranteed by fragile watermarking; actual ownership is not established. Even while it can detect any improper modifications or edits to the secret watermarked images, if any change takes place it also invalidates the watermark's completeness (Lu and Li, 2006). Semi-fragile watermarking's objective is to remain resilient against allowed manipulations while spotting unauthorized changes. It combines the advantages of robust and fragile watermarking. According to the robust watermarking approach, the watermark data is frequently embedded directly in the spatial domain (Yuan et al., 2020b), or, to put it another way, the watermark data is integrated into the host image by altering the spatial connections between pixels (Nikolaidis and Pitas, 1998).

2. PREVIOUS WORKS

As a result of computer science's rapid growth, digital watermarking techniques have advanced since 2000. A new framework was developed, and performing a detector was investigated, Discrete Cosine Transform (DCT) domain watermarking techniques in still images were researched on blocks of 8×8 pixels as in the JPEG-algorithm by Hernandez et al. (Hernández

et al., 2000). Barni et al. investigated the processing power of DCT photo watermarks in a full-frame analysis and suggest a method to evaluate the watermark-capacity (Barni et al., 2000). Langelaar and Lagendijk (Langelaar and Lagendijk, 2001) created the best differential energy watermarking possible by encoding images and videos using DCT. A digital video watermarking method that combines Spatio-temporal HVS and DCT was proposed by Cedillo-Hernandez et al. (Cedillo-Hernandez et al., 2014). Suhail and Obaidat (Suhail and Obaidat, 2003) invented digital watermarking by combining the DCT and JPEG concepts. LPSNR as well as a hybrid SVD-DCT digital watermarking strategy were proposed by Huang and Guan (Huang and Guan, 2004). To increase speed, Aslantas et al. (Aslantas et al., 2009) used clever optimization methods in DCT-based fragile watermarking. There are numerous disciplines of study related to digital watermarking. In (Su et al., 2014), a brand-new method for blindly watermarking images using QR-decomposition was presented. This method integrates a color watermark image into a color host image. They were able to successfully encode their watermarking. Paunwala and Patnaik suggested (Paunwala and Patnaik, 2014) digital watermarking using DCT for biometric template security. Hu et al. made a digital audio watermarking study. They made their decision to adopt invisible watermarking using the DWPT-DCT perceptual framework (Hu et al., 2014). Hu et al. in (Hu et al., 2015) have looked at DWT-SVD-DCT characteristics-based robust multiple watermarking using JPEG and JPEG 2000 compression. Additionally, Hu and Hsu offered highly effective, resilient DCT domain transparent audio digital watermarking (Hu and Hsu, 2015). Recent research by Joshi et al. (Joshi et al., 2015) used integer DCT against H.264 encoding to produce real-time video digital watermarking. To create a reliable digital picture watermarking approach that may be utilized to defend against and counter primary geometric attacks, Fazli and Moeini (Fazli and Moeini, 2016) combined DWT, SCT, and SVD. The false positive issue with SVD-based watermarking techniques can be resolved using DCT and DWT with using Particle Swarm Optimization (PSO) method to find the scaling factors (Run et al., 2012). Informed watermarking with extreme learning was used by Rajpal et al. to create a watermark sequence on the host image and developed the watermark sequence using DCT and the host image's informed watermarking method (Rajpal et al., 2017). Alshoura et al. in (Alshoura et al., 2020) proposed a new Chaotic Image Watermarking Scheme based on SVD and IWT. In (Yuan et al., 2020a) a new watermarking method that based on 2D-DCT, Two Dimensional-Discrete Cosine Transform, is produced to protect copyrights for color images. The research's methodology in (Liu et al., 2019) combines DWT, HD and SVD and offers a novel way for watermarking digital images.

In (Ansari and Pant, 2017), a robust watermark is inserted using DWT, SVD to provide tamper-localization. This insertion is optimized using Artificial Bee Colony (ABC) method. Jane and Elbaşı used a combination of DWT, SVD and LU decomposition to achieve a nonblind watermarking technique (Jane and Elbaşı, 2014).

All the proposed methods mentioned above are based on one level (stage) of watermarking digital images. The proposed methodology in this article is based on two levels (stages) of watermarking (nested watermarking) to provide more security scheme than the previous methods. The results of the performance test show work's significant contributions and how strong and undetectable this strategy is. It is also unrestricted by the limitations imposed by specified watermark sizes.

The paper arranged in the following order. Section (2) discusses related works. The DWT, HD, and SVD concepts are presented in Section (3). A new digital watermarking method is constructed based on hybrid DWT-HD-SVD discussed Section (4). While Section (5) presents the experimental findings and a performance analysis. Conclusion is provided in Section (6).

3. PRELIMINARIES

The three approaches of DWT, HD, and SVD are introduced in this section which were adopted in the suggested watermarking scheme. In order to improve watermarking performance in the face of robustness attacks, DWT uses timescale signal multi-resolution. In the meantime, the resilience gets much better when HD is utilized as the matrix transform. Additionally, the SVD-based watermarking method performs better than competing techniques for defending against geometric attacks (e.g. rescaling attacks). The main concern with SVD-based watermarking, false positives, is addressed in our study by encrypting the SVD parts.

3.1. Discrete Wave Transformation

The robustness of watermarking systems is frequently increased by using the discrete wavelet transform (DWT). The four subbands that DWT creates from the host image are low-high (LH), low-low (LL), high-low (HL), and high-high (HH). After one level of DWT, the LL sub-band contains the majority of the information in the host picture. The wavelet theory permits further breakdown up to the point when the size of the sub-bands meets requirements for a watermark. LL outperforms other sub-bands in assaults like filter and compression attacks, for instance (Barnouti et al., 2018). This feature generates the LL sub-band a top choice to strong watermarking.

3.2. Hessenberg Decomposition

HD is the multiplication of a square matrix A ($n \times n$) by an orthogonal matrix P (Su, 2016). The HD strategy described in Formula (1):

$$PHP^T = HD(X) \quad (1)$$

Where H is an upper Hessenberg matrix and P is an orthogonal matrix. The orthogonal matrix known as the house-holder matrix Q is represented as:

$$Q = \frac{(I_n - 2\mu\mu^T)}{\mu^T\mu} \quad (2)$$

(μ) is a non-zero vector in R_n and I_n is the identity matrix of size n by n. There are n-2 phases in the whole process. In light of this, Hessenberg decomposition is calculated as follows:

$$P = (Q_1 Q_2 \dots Q_{n-2})^T X (Q_1 Q_2 \dots Q_{n-2}) \quad (3)$$

$$\Rightarrow H = P^T X P \quad (4)$$

$$\Rightarrow X = PHP^T \quad (5)$$

HD can find a more exact component of the host image, which improves robustness (Su and Chen, 2017).

3.3. Singular Value Decomposition

In order to separate singular values into diagonal matrices, the SVD divides a symmetric matrix into three sub-matrices (Chang et al., 2005). Under matrix diagonalization, Left singular matrix U, right singular matrix V, and singular matrix S are the three decomposed matrices. The SVD can be determined using the following formula if Y is a symmetric matrix:

$$USV^T = \text{SVD}(Y) \quad (6)$$

Where $USV^T = I_n$ and $VV^T = I_n$. The orthonormal eigenvectors of YY^T are represented by the columns of U, the diagonal matrix S by the square roots of the eigenvalues of U or V in descending order, and the rows of V by the orthonormal eigenvectors of YY^T . If the rank of the matrix Y is r ($r \leq n$), then the diagonal matrix S elements can meet the relation in Eq. 7, and the matrix Y can be expressed as (Formula (8)).

$$\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r \geq \sigma_{r+1} = \sigma_{r+2} = \dots = \sigma_n = 0 \quad (7)$$

$$Y = \sum_{i=1}^r \sigma_i \mu_i v_i \quad (8)$$

Where U and V's ith eigenvectors, μ_i , and, v_i , respectively. σ_i is the ith singular value. In this work, a suitable scaling factor is used to embed the watermark's singular value into the host image using the SVD's singular value S. As the scaling factor is unsuitable, exact performance of the suggested technique needs to be improved. After this operation, the technique of watermarking has essentially reached its full invisibility and robustness. Therefore, additional

optimization of the proposed evaluation function's trade-off between robustness and invisibility is required. U and V^T are two SVD components that, like the other SVD components, would expose geometric information during the extraction process if they were left unprotected. Encrypting U and V^T eliminates this risk for SVD-based watermarking.

4. THE SUGGESTED NESTED-WATERMARKING SCHEME

Watermark embedding and watermark extraction are the two main parts of the method which used to implement the watermarking system. The embedding and extraction of watermark image is based on the combination of DWT, HD and SVD which provides a good reliability and excellent visual performance, as shown in Fig.1. For more security, the new method is proposed; thus there will a tradeoff between visibility, reliability and security.

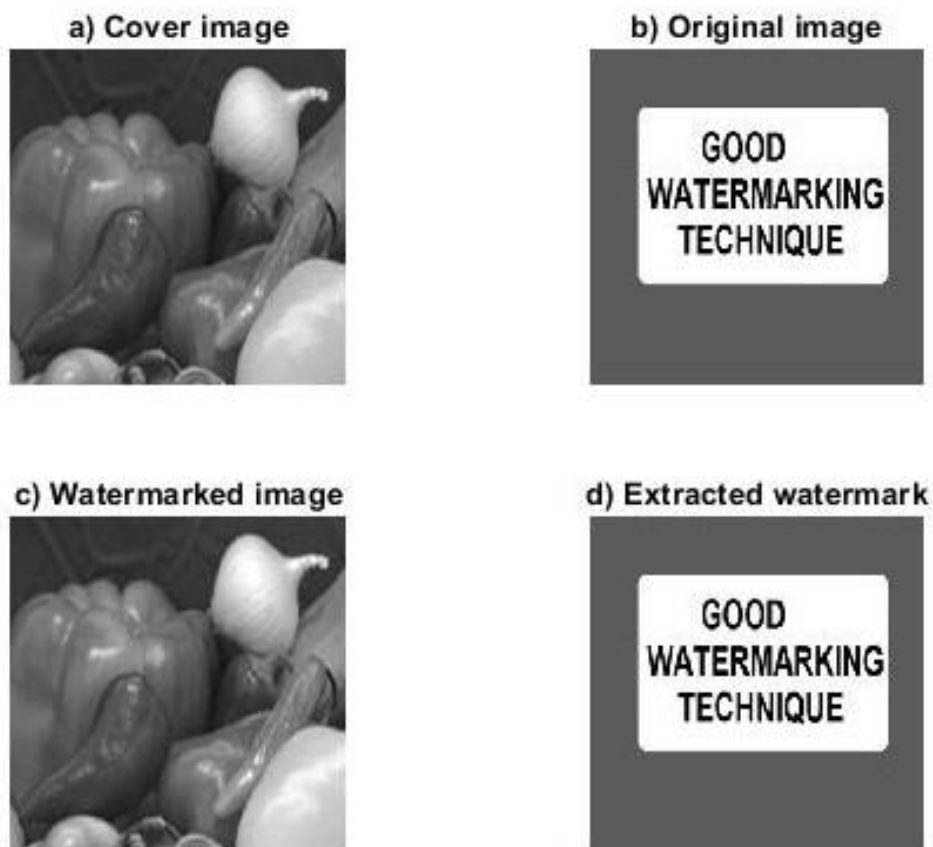


Fig. 1. The DWT-HD-SVD Watermarking Algorithm

In the proposed scheme, an encryption stage is also performed between the watermarking and extraction. The lightweight encryption algorithm (Usman et al., 2017) is adopted for the encryption stage due to its speed, high performance and reliability. The flow chart for the watermarking algorithm is shown in Fig.2.

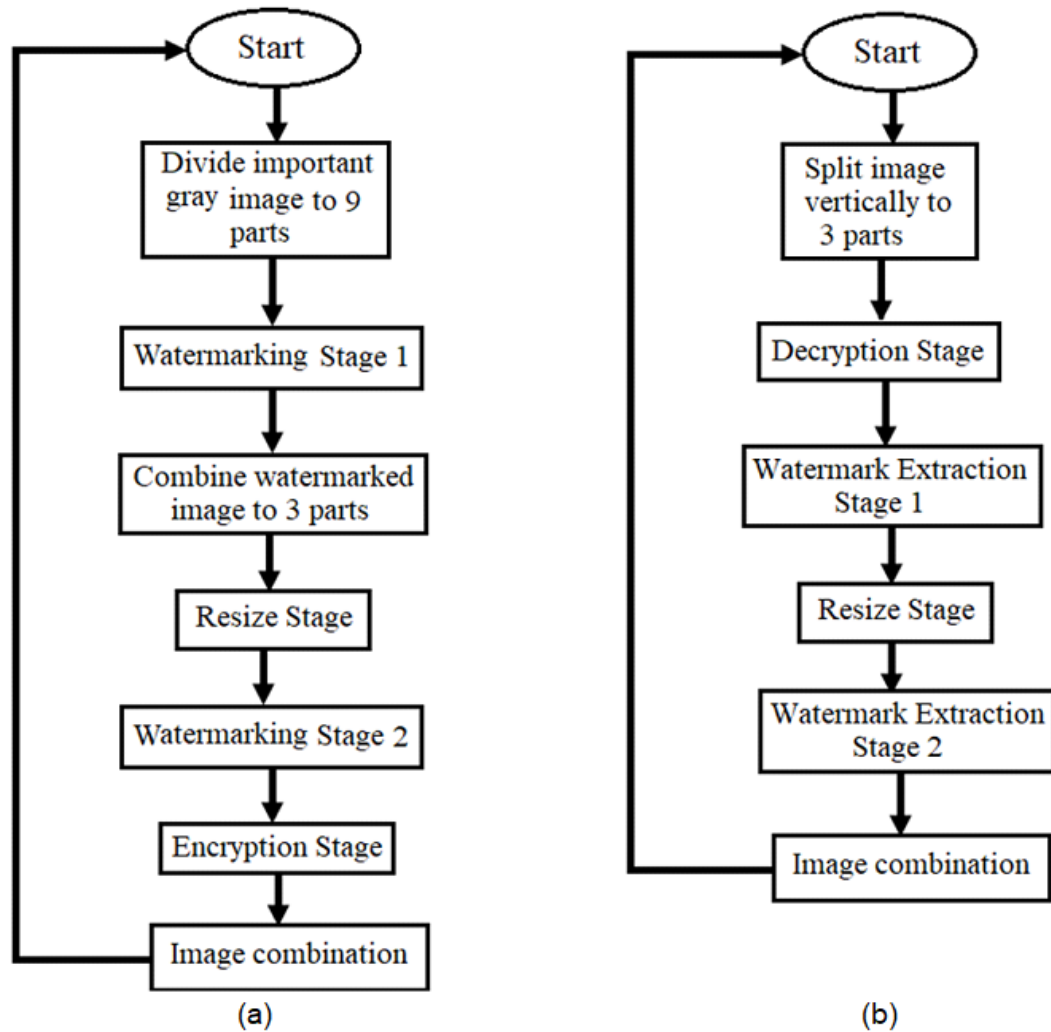


Fig. 2. The New Nested-Watermark Algorithm Flow Chart
(a) Image Watermarking Algorithm. (b) Image Watermarking-Extraction Algorithm.

The detailed steps of the proposed algorithm are listed as follows:

4.1. Image Watermarking Procedure

The following stages represent the watermarking algorithm, Fig. 3 shows the watermarking flow diagram steps.

Step1: Transform the colored image (256×256) (which we want to hide) to gray space then divide it into n -parts (we choose $n=9$ for simplicity) as shown in Fig. 3 (a).

Step2: Embed each part in the same host image (onion image (512×512) is used for this stage) using DWT-HD-SVD method (explained in section 3). This stage represents (watermarking stage 1), as depicted in Fig. 3 (b).

Step3: Combine the first three horizontal parts into one part of size (256×768) (this means that the new image will contain only three parts) as shown in Fig. 3 (c).

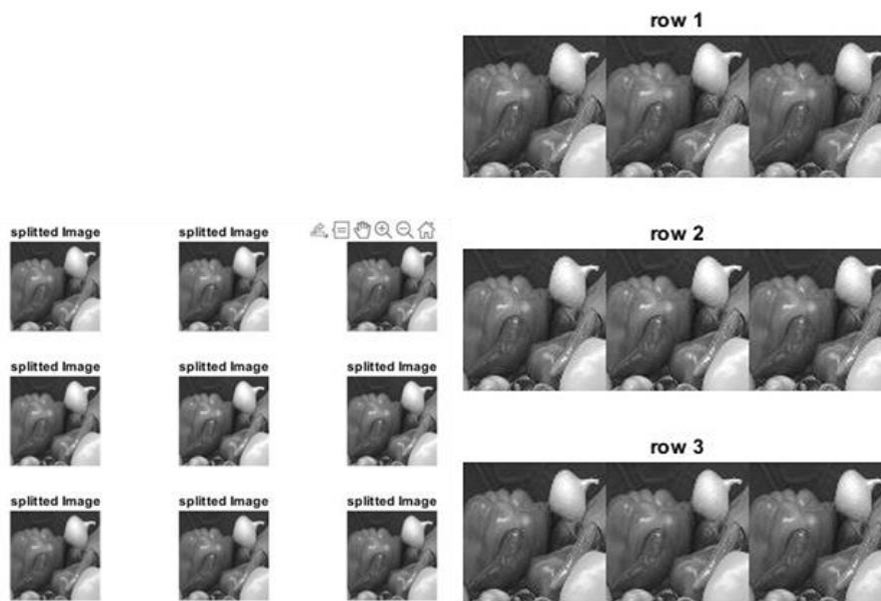
Step4: Resize each part to have a (256×256) image in order to embed it into another host image (cameraman (512×512) is used in this stage). This step represents (watermarking stage 2), as depicted in Fig. 3 (d).

Step5: Encrypt each part using lightweight encryption algorithm. Fig. 3 (e) shows the result of this step.

Step6: Combine the three parts into one final part of size (256x768) as shown in Fig 3 (f).



(a)



(b)

(c)



(d)

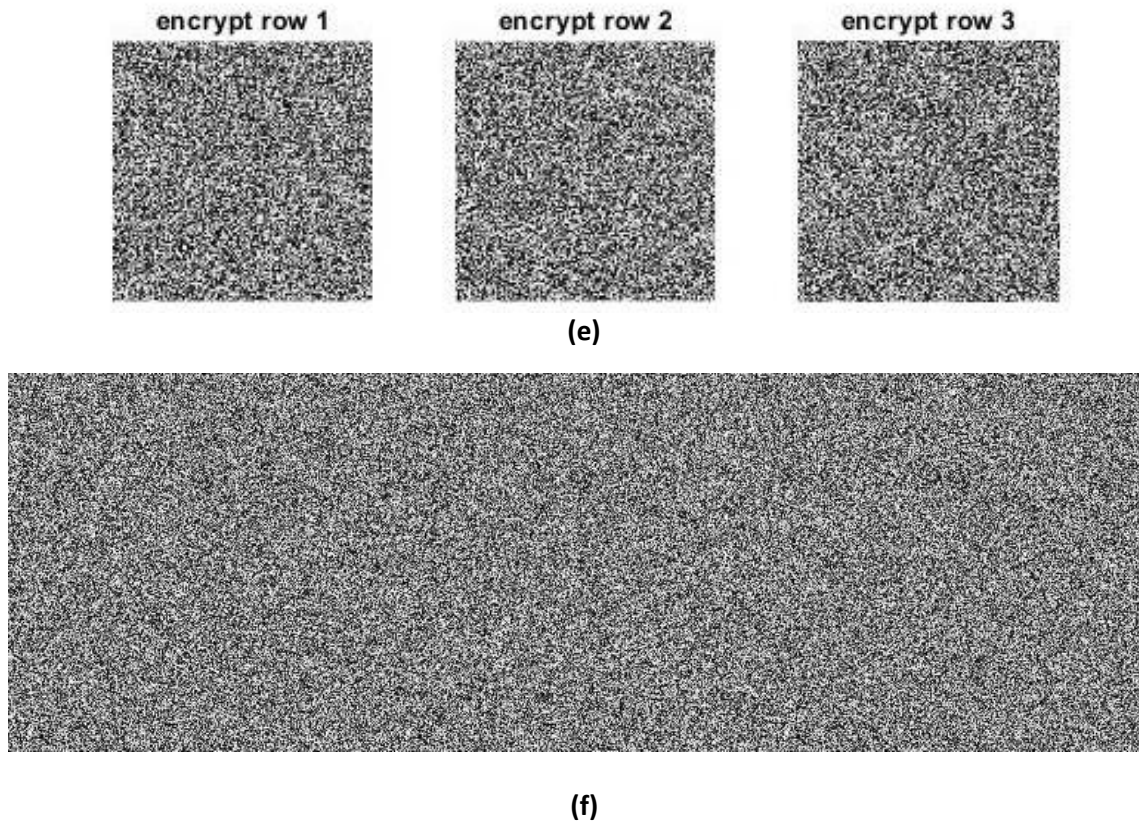


Fig. 3. Image watermarking steps

4.2. Image Watermarking-Extraction Procedure

Watermarking-extraction algorithm can be represented in the following steps; Fig. 4 shows the watermarking-extraction flow diagram steps.

Step1: Split the image vertically to three parts each of size (256×256) as shown in Fig.4 (a).

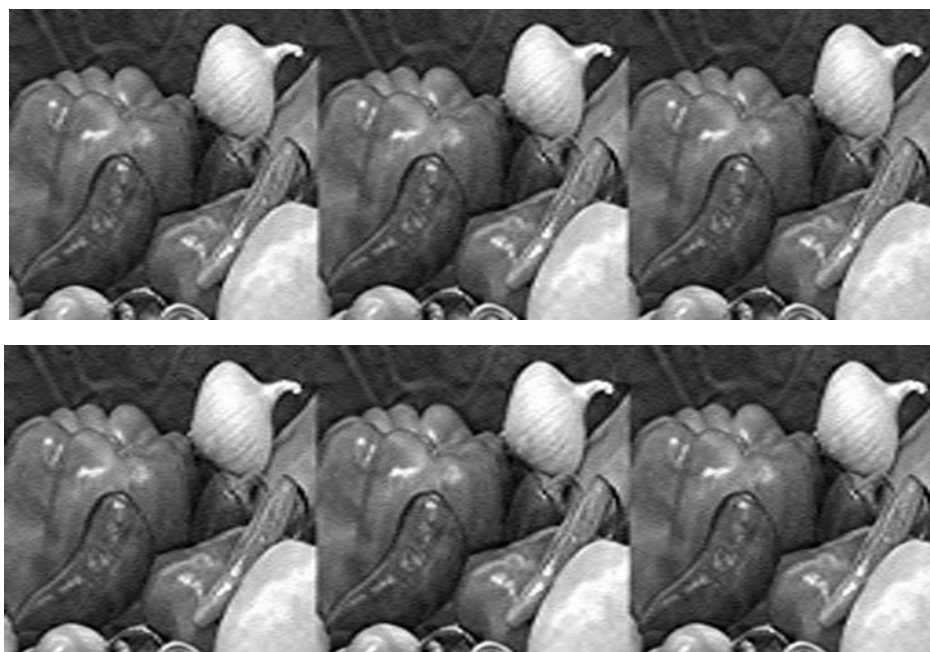
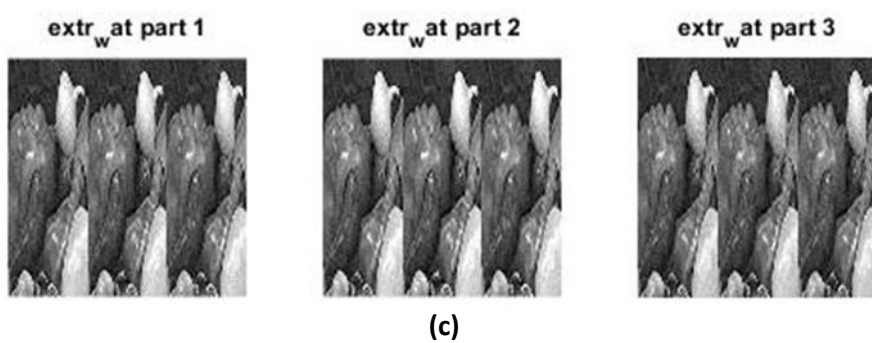
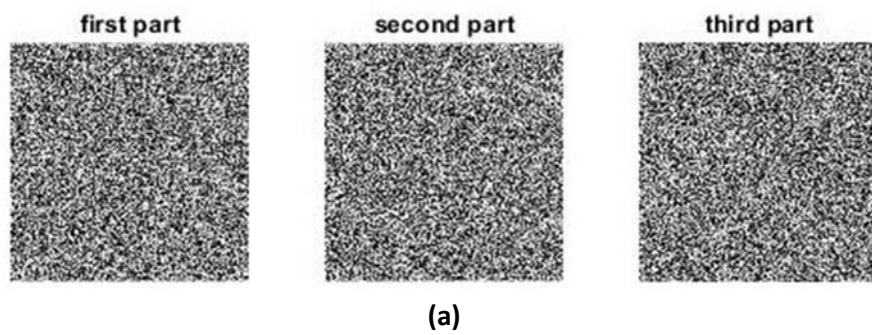
Step2: Decrypt each part using the same method of step 5 (lightweight encryption algorithm). Fig. 4 (b) shows the result of this step.

Step3: Extract each part from the host image (cameraman). This step represents (extraction stage 1), as depicted in Fig.4 (c).

Step4: Stretch each part to its original size (256×768) and split again vertically to three parts each of size (256×256) and obtain 9 parts as shown in Fig. 4 (d) and (e).

Step5: Extract each part from the host image (onion). This step represents (extraction stage 2), as depicted in Fig. 4 (f).

Step6: Combine all the 9 parts into one part as shown in Fig. 4 (g).



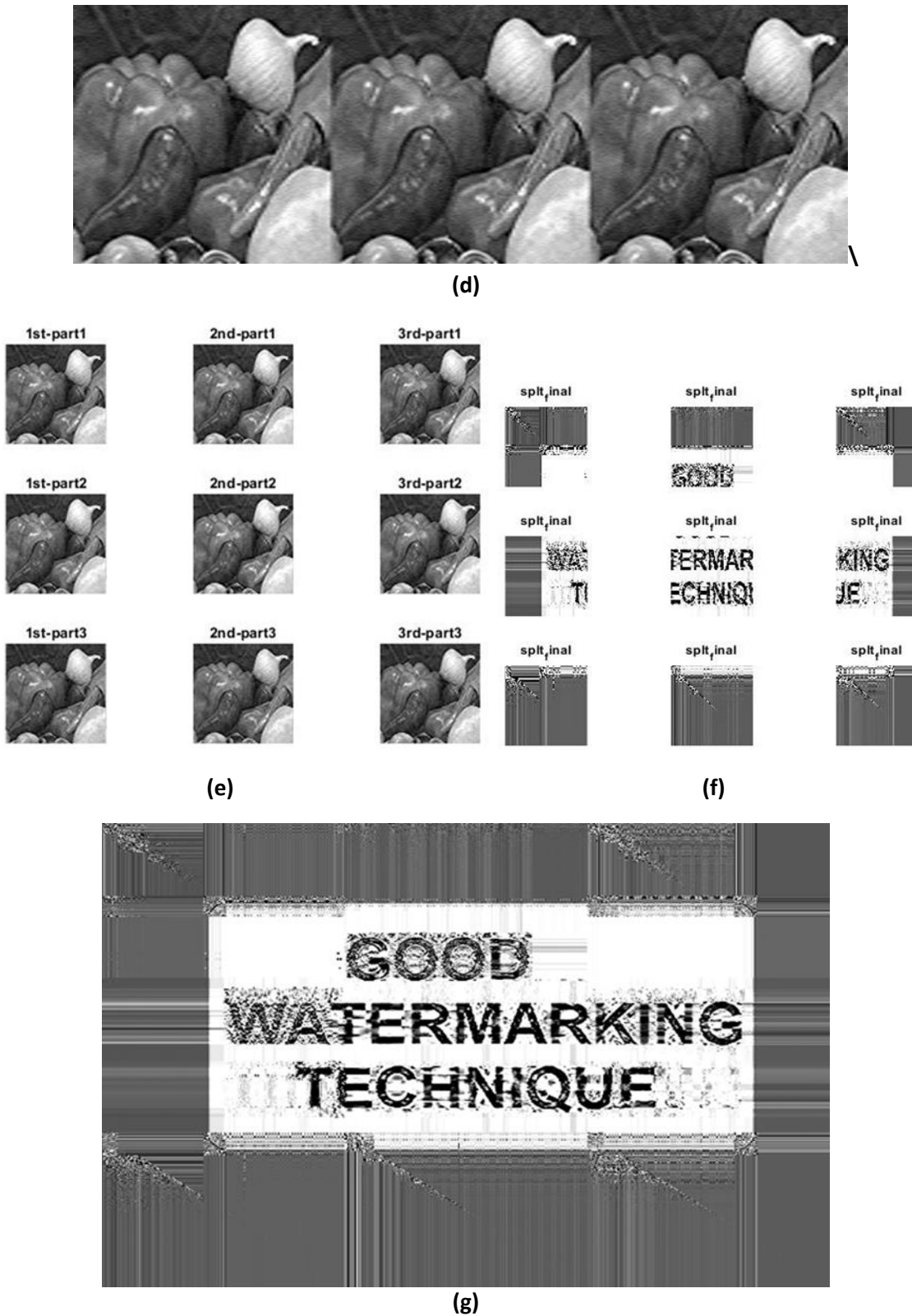


Fig. 4. Image watermarking-extraction steps

5. EXPERIMENTAL RESULTS AND DISCUSSION

The anticipated results of the suggested watermarking technique are described in this section. The effectiveness of picture watermarking technique is typically measured by factors like

invisibility, robustness, computing complexity, and so forth. By means of both objective quantitative analysis and subjective visual observation, the proposed the robustness and invisibility of the approach are determined. Finally, the suggested method's robustness and invisibility are evaluated in comparison to earlier efforts. The host image and watermarked host image are displayed in Fig.5.

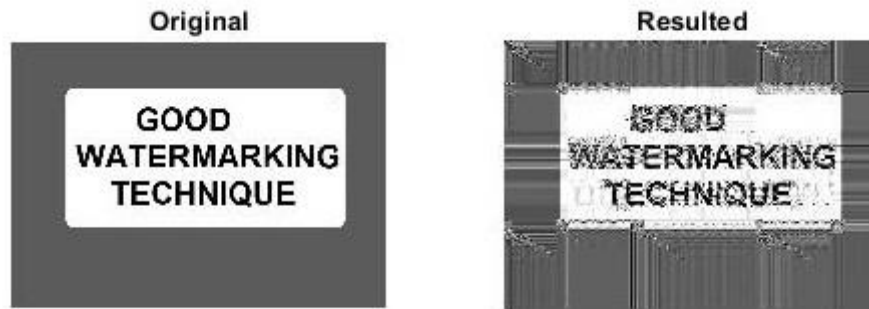


Fig. 5. Original watermark image and the recovered (resulted) image

5.1. Histogram Analysis

The histogram's bins each indicate the number of pixels that have the value they represent. The original image's histogram is shown in Fig. 6 (a), while the recovered (resulted) image's histogram is shown in Fig. 6 (b).

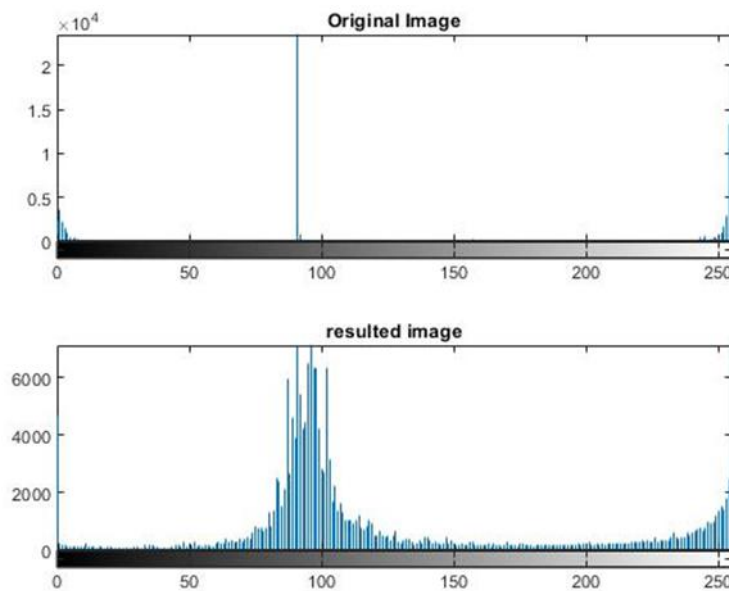


Fig. 6. Histogram difference between original image and resulted image

5.2. Performance Evaluation

The proposed algorithm's performance tested by applying different attacks like- Gaussian, speckle, salt-and-pepper noises, sharpening, average filtering, median filtering, blurring, JPEG Compression and rotation as shown in Table 1 and 2.

PSNR and MSE are objective evaluation indexes. PSNR can compute the degree of similarity between both the carrier image and the watermarked image can be measured by:

$$PSNR = 10 \left(\frac{I_{max}^2}{MSE} \right) \quad (9)$$

Where I_{max} is the image (I) maximum possible pixel value.

MSE stands for mean square error (shown in (Formula (10))). The error lowers as the MSE value lowers.

$$MSE = \frac{1}{M^2} \sum_{i=1}^M \sum_{j=1}^M (C_{i,j} - C_{i,j}^*)^2 \quad (10)$$

Table 1. Comparison of the watermarked image's MSE and PSNR values under various attacks

Type of attack	MSE	PSNR
No attack	24.531	54.233
Median filtering	8.205	58.989
Gaussian noise	25.904	53.997
Salt and pepper noise	0.0316	83.123
Rotation	17.196	55.776
Averaging filtering	7.445	59.411
Sharpening	1.442	66.539
Speckle noise	0.00032	83.052
Blurring	6.940	59.717
JPEG Compression	0.0041	92.0253

Table 2. Comparison of the recovered image's MSE and PSNR values under various attacks

Type of attack	MSE	PSNR
No attack	20.642	54.983
Median filtering	0.645	70.034
Gaussian noise	26.043	53.973
Salt and pepper noise	0.0264	83.920
Rotation	4.560	61.540
Averaging filtering	0.715	69.584
Sharpening	0.216	74.783
Speckle noise	2.8492e-04	83.583
Blurring	0.969	68.263
JPEG Compression	e-058.9174	99.6284

The new algorithm robustness to various attacks and noises may be observed. The verification accuracy performs best under normal conditions, when there is JPEG Compression, and performs least against Gaussian noise. In [Fig. 7](#), the experimental outcomes of the new

watermarking technique under each of the mentioned attacks have been contrasted in terms of PSNR values.

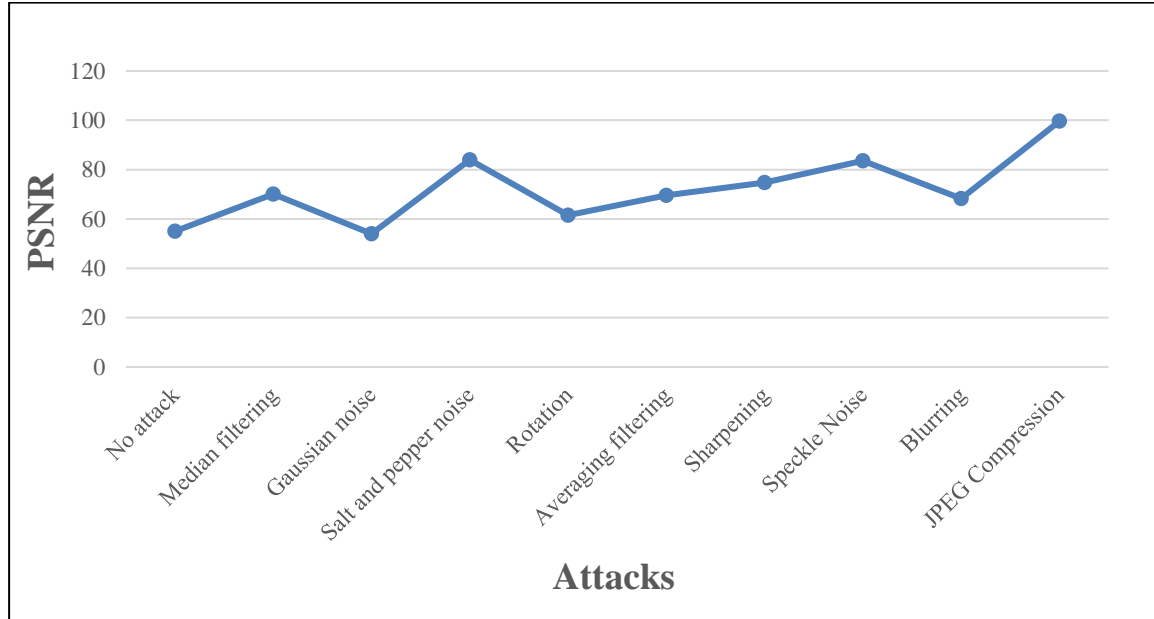


Fig. 7. The experiment results comparison of the new method in terms of PSNR value

The performance of the proposed nested-watermarking method also compared to existing one-level watermarking methods in term of PSNR under different attacks as shown in [Table 3](#).

Table 3. Comparison of the proposed methodology and the previous methods in term of PSNR value under various attacks

Attack	(Rathord and Rai, 2021)	(Mohan et al., 2021)	(Islam et al., 2019)	(Takore et al., 2018)	(Khare and Srivastava, 2021)	The proposed method
No attack	54.2	54.9706	56.43	45.5017	56.4652	54.983
Median filtering	54.2	54.9706	62.0186	42.8188	42.5022	70.034
Gaussian noise	54.2	54.9706	96.8756	43.6644	37.2123	53.973
Salt and pepper noise	-	54.9706	-	42.2495	27.8760	83.920
Rotation	-	-	56.9024	44.5376	11.8908	61.540
Averaging filtering	54.2	-	-	42.4154	34.6001	69.584
Sharpening	-	54.9706	-	-	40.2043	74.783
Speckle Noise	-	54.9706	-	-	22.7281	83.583
Blurring	54.2	-	-	-	-	68.263
JPEG Compression	-	-	-	-	58.2130	99.6284

6. CONCLUSIONS

This proposed paper is suggested to use a novel layered nested-watermarking method, based on hybrid DWT-HD-SVD transformations, and implemented using the DWT, HD and SVD domain. The new algorithm can be applied and used to gray-scale and RGB-images. Numerical simulation experiments are used to analyze this method's robustness and reliability to various attacks ([YouTube, 2024](#)). The outcomes demonstrate that the recovered and watermarked images have excellent reliability, PSNR and MSE. The proposed scheme is also straightforward and of modest complexity. A number of simulation results show that the given watermarking scheme meets the robustness requirement and performs well, making it appropriate for copyright protection of digital images. The performance of the proposed methodology is also compared with the existing one-level methods in term of PSNR under the different attacks. It can be observed that the proposed methodology gives more robust performance and produces higher PSNR value under different attacks than other methods.

In future works, the proposed nested-watermarking method can be extended and applied for Color-Stereo images (CSI), CSI is two-color views named left and right-view ([Yamni et al., 2020a](#); [Yamni et al., 2020b](#)). Also other applications, based on QRFrCMs (Quaternion Radial Fractional-Charlier Moments), can be defined and addressed such as classification and reconstruction of color images.

7. REFERENCES

- Alshoura W H, Zainol Z, The J S and Alawida M. (2020) 'A New Chaotic Image Watermarking Scheme Based on SVD and IWT', *IEEE Access* 8: 43391–43406.
- Ansari I A and Pant M. (2017) 'Multipurpose image watermarking in the domain of DWT based on SVD and ABC', *Pattern Recognition Letters* 94: 228–236.
- Aslantas V, Ozer S, and Ozturk S. (2009) 'Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms', *Optics Communications* 282: 2806–2817.
- Barni M, Bartolini F, De Rosa A and Piva A. (2000) 'Capacity of full frame DCT image watermarks', *IEEE Transactions on Image Processing* 9(8): 1450–1455.
- Barnouti N H, Sabri Z S and Hameed K L (2018) 'Digital Watermarking Based on DWT (Discrete Wavelet Transform) and DCT (Discrete Cosine Transform)', *International Journal of Engineering & Technology* 7(4): 4825-4829.

- Cedillo-Hernandez A, Cedillo-Hernandez M, Garcia-Vazquez M, Nakano-Miyatake M, Perez-Meana H and Ramirez-Acosta A. (2014) 'Transcoding resilient video watermarking scheme based on spatio-temporal HVS and DCT', *Signal Processing* 97: 40–54.
- Chang C C, Tsai P and Lin C C (2005) 'SVD- based digital image watermarking scheme', *Pattern Recognition Letters* 26(10): 1577-1586.
- Cox, Ingemar J., Joe Kilian, F. Thomson Leighton, and Talal Shamoan. (1997) 'Secure Spread Spectrum Watermarking for Multimedia', *IEEE Transactions on Image Processing* 6 (12): 1673–87. doi:10.1109/83.650120.
- Fazli S and Moeini M. (2016) 'A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks', *Optik* 127: 964–972.
- Hernández J R, Amado M and Pérez-González F. 2000. 'DCT-domain watermarking techniques for still images detector performance analysis and a new structure', *IEEE Transactions on Image Processing* 9: 55–68.
- Hu H T and Hsu L Y. (2015) 'Robust, transparent and high-capacity audio watermarking in DCT domain', *Signal Processing* 109: 226–235.
- Hu H T, Hsu L Y and Chou H H. (2014) 'Perceptual-based DWPT-DCT framework for selective blind audio watermarking', *Signal Processing* 105: 316–327.
- Hu H T, Hsu L Y and Garcia-Alfaro J. (2015) 'Exploring DWT-SVD-DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression', *Computers and Electrical Engineering* 41: 52–63.
- Huang F and Guan Z H. (2004) 'A hybrid SVD-DCT watermarking method based on LPSNR', *Pattern Recognition Letters* 25: 1769–1775.
- Islam M S, Ullah M A and Dhar J P. (2019) 'An imperceptible & robust digital image watermarking scheme based on DWT, entropy and neural network', *Karbala International Journal of Modern Science* 5(1): Article 6.
- Jane O and Elbaşı E. (2014) 'A new approach of nonblind watermarking methods based on DWT and SVD via LU decomposition', *Turkish Journal of Electrical Engineering and Computer Sciences* 22: 1354–1366.
- Joshi A M, Mishra V and Patrikar R M. (2015) 'Design of real-time video watermarking based on Integer DCT for H.264 encoder', *International Journal of Electronics* 102: 141–155.

- Khare P and Srivastava V K. (2021) 'A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT', *Journal of Intelligent System* 30(1): 297-311.
- Langelaar C G and Lagendijk R L. (2001) 'Optimal differential energy watermarking of DCT encoded images and video', *IEEE Transactions on Image Processing* 10: 148–158.
- Liu J, Huang J, Luo Y, Cao L, Yang S, Wei D and Zhou R. (2019) 'An Optimized Image Watermarking Method Based on HD and SVD in DWT Domain', *IEEE Access* 7: 80849–80860.
- Lu Z and Li S. 2006. 'Multipurpose watermarking algorithm for secret communication', *Chinese Journal of Electronics* 15: 79–84.
- Mohan A, Anand A, Singh A K, Dwivedi R and Kumar B. (2021) 'Selective encryption and optimization based watermarking for robust transmission of landslide images', *Computers and Electrical Engineering* 95: 107385.
- Nikolaidis N and Pitas I. (1998) 'Robust image watermarking in the spatial domain', *Signal Processing* 66: 385–403.
- Paunwala M and Patnaik S. (2014) 'Biometric template protection with DCT-based watermarking', *Machine Vision and Applications* 25: 263–275.
- Rajpal A, Mishra A and Bala R. (2017) 'Fast digital watermarking of uncompressed colored images using bidirectional extreme learning machine', In *Proceedings of the International Joint Conference on Neural Networks (IJCNN)*, Anchorage, AK, USA, pp.1361–1366.
- Rathord S S and Rai M. (2021) 'Adaptive Colour Space based Robust Image Watermarking Using Serial DWT-HD-SVD domain', *International Journal of Engineering and Innovative Technology (IJEIT)* 10(9): 1-5.
- Run R S, Horng S J, Lai J L, Kao T W and Chen R J. (2012) 'An improved SVD-based watermarking technique for copyright protection', *Expert Systems with Applications* 39(1): 673–689.
- Su Q and Chen B. (2017) 'A novel blind color image watermarking using upper Hessenberg matrix', *AEU - International Journal of Electronics and Communications* 78: 64-71.
- Su Q, Niu Y, Wang G, Jia S and Yue J. (2014) 'Color image blind watermarking scheme based on QR decomposition', *Signal Processing* 94: 219–235.

Su Q. (2016) 'Novel blind colour image watermarking technique using Hessenberg decomposition', *IET Image Processing* 10(11): 817–829.

Suhail M A and Obaidat M S. (2003) 'Digital watermarking-based DCT and JPEG model', *IEEE Transactions on Instrumentation and Measurement* 52: 1640–1647.

Takore T T, Kumar P R and Lavanya Devi G. (2018) 'A new robust and imperceptible image watermarking scheme based on hybrid transform and PSO', *International Journal of Intelligent Systems and Applications* 10(11): 50–63.

The proposed algorithm programs available: <https://youtu.be/TeAriNfh4gI>

Tirkel, A Z, G A Rankin, R M Van Schyndel, W J Ho, N R A Mee, and C F Osborne. (1993) 'Electronic Watermark', *Digital Image Computing, Technology and Applications (DICTA'93)*, 666–73.

Usman M, Ahmed I, Aslam M I, Khan S and Shah U A. (2017) 'SIT: A Lightweight Encryption Algorithm for Secure Internet of Things', *International Journal of Advanced Computer Science and Applications* 8: 402–411.

Wu Y T and Shih F Y. (2004) 'An adjusted-purpose digital watermarking technique', *Pattern Recognition*, Elsevier Ltd., 37 (12): 2349-2359.

Yamni M, Karmouni H, Sayyouri M and Qjidaa H. (2020a) 'Color stereo image zero-watermarking using quaternion radial Tchebichef Moments', *International Conference on Intelligent Systems and Computer Vision (ISCV)*: 1–7.

Yamni M, Karmouni H, Sayyouri M, Qjidaa H and Flusser J. (2020b) 'Novel octonion moments for color stereo image analysis', *Digital Signal Processing*: 102878.

Yuan Z, Liu D, Zhang X and Su Q. (2020a) 'New image blind watermarking method based on two-dimensional discrete cosine transform', *Optik* 204: 164152.

Yuan Z, Su Q, Liu D, Zhang X and Yao T. (2020b) 'Fast and robust image watermarking method in the spatial domain', *IET Image Processing* 14: 3829–3838.