An Entropy Based Robust Secured Imperceptible Digital Color Image Watermarking

Renuka V. Mahagaonkar[1], Dr U.D. Shiurkar[2]
[1]*Lecturer, Puranmal Lahoti Government Polytechnic, Latur.*
Email: renuka2209@gmail.com
[2]*Director, Deogiri Institute of Engineering and Management Studies, Aurangabad.*
Email: shiurkar@gmail.com

Abstract - Digital color image watermarking is known as an efficient technique to provide confidentiality, authority, copyright protection, trustworthiness and secrecy. This is a robust, secure and imperceptible color image watermarking process, in which a binary logo is inserted by selecting the maximal entropy blocks. Arnold transform is employed on the logo to get the scrambled version of it, thus the security is increased. Hue, Saturation and Value (HSV) transform do activated on the watermarking image, and then the H channel is considered for 2-level Discrete Wavelet Transform (DWT) decomposition. Maximum entropy blocks are picked and Singular Value Decomposition (SVD) do employed with these blocks. The scrambled DWT transformed watermark is embedded in it with proportionality coefficient α. The designed approach assessed on different signal processing attacks. Robustness and visual qualities are evaluated by Structural Similarity Index Measure (SSIM), Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE) and Normalized Cross-Correlation (NCC). Based on the experimental outcome, this method exhibits intense grade of imperceptible and strong robustness against numerous types of attacks.

Keywords: Digital Color image watermarking, Arnold transform, DWT, SVD, Maximum Entropy, PSNR.

1. Introduction

Digital watermarking is a process well known to conceal multimedia information and is often utilized for purposes like copyright protection, ownership identification, and authentication. There are three classifications of watermark technology based on its anti-attack ability: fragile, semi-fragile, and robust. Robust watermarking is particularly useful as it makes the watermarked image is not only resistant to non-malicious attacks but also to malicious attacks within a certain distortion range [1]. The two primary features of robust digital watermarking are imperceptibility and robustness [2]. Imperceptibility reveals the visual quality of the watermarked image, while robustness indicates the capability of a watermark to be successfully recovered and identified from a watermarked image under different types of attacks. Achieving both imperceptibility and robustness is challenging, as these two characteristics tend to be mutually exclusive [3].

As a result, researchers working on robust watermarking typically aim to meet the proportion among imperceptibility and robustness. Watermarks could be implanted within the spatial or transform domain of the watermarking image. The spatial domain embedding involves concealing a substantial volume of information within the watermarking image, but the robustness of this technique is generally lower than that of transform domain schemes [4]. Transform domain embedding involves converting the watermarking image into a transform domain, inserting the watermark by modifying its coefficients, and then converting it back to the spatial domain. This approach exhibits excellent robustness against geometric attacks such as rotation, scaling, and panning [5]. Digital watermarking typically employs common transform techniques such as discrete Fourier transforms (DFT), discrete wavelet transforms (DWT), and discrete cosine transforms (DCT). Recently, some researchers have explored the possibility of combining multiple transform methods to leverage the strengths of each transform domain and improve overall performance.

Optimizing the watermarking scheme can be a challenging task, particularly in terms of dynamically selecting the appropriate embedding position and strength. In this regard, to compute the uncertainty of image information, entropy of data is commonly utilized to resolve the problem. Higher entropy in an image indicates greater pixel complexity. Therefore, selecting the embedding position from the region with higher information entropy can effectively enhance the imperceptibility of the watermarking scheme [6].

2. Literature Review

Lai, et.al [7], proposed a hybrid approach that incorporates the advantages of both SVD and DWT. Their method involves a two-stage process: first, the watermark logo undergoes 2-level DWT decomposition, and then SVD transform is activated upon two sub-bands of the logo. In the second stage, the watermark logo is implanted in the singular value components of the original image. This technique has shown resilience against various image processing attacks.

Singh et al. [8] launched a fusion watermarking procedure that combines DWT and SVD in the DCT domain. The presented scheme involves using 4x4 blocks of DCT middle coefficients to conceal the watermark, and then SVD transform is activated on it. The technique has shown resilience against various attacks. However, the authors noted that SVD-based watermarking methods may be susceptible to false positives, according to their research findings.

Singh R et al. [9] have established a new watermarking performance that leverages the selection of the highest entropy blocks for improved efficiency. Initially, both the cover and watermark images undergo Arnold transform for shuffling. Next, the encrypted images undergo a 2-level discrete wavelet transform, activated by singular value decomposition. The suggested system has undergone evaluation using standard image datasets, with attacks ranging from geometrical to filtering, noise, and contrast adjustment.

Ahmed et al. [10] have presented a technique which incorporates DWT, SVD and arithmetic optimization algorithm (AOA) for color images. To get the increased robustness, the watermark is inserted in every sub band with scaling factor (α). To determine the prime value of α can be exploited by AOA process.

Roy et al. [11] presented a blind watermarking system built on RDWT-DCT. This approach involves inserting scrambled logos into the horizontal wavelet coefficients of an image to create the watermarked image.

Ernawan et al. [12] conferred a blind watermarking procedure using RDWT. The U matrix and LL sub band is chosen for inserting the scrambled logo.

Based on the findings of the literature survey, it has been suggested that incorporating a hybrid domain technique and using a scrambled watermark can enhance the robustness of an image watermarking scheme while also providing additional security.

3. Proposed Method

A novel process to safeguarding digital images is proposed through a hybrid, imperceptible, secure and robust digital watermarking process that utilizes the maximum entropy and DWT-SVD domains.

DWT-based watermarking systems provide several benefits, including multi-resolution capability, efficient energy compression, and imperceptible visual quality [13].

To enhance the effectiveness of the approach, multiple transformations are applied to the original watermarking image. Additionally, the embedding position and strength are optimized in an adaptive manner to ensure a balance between transparency and robustness.

Hence, the primary contributions of this approach are

(i) This process is an efficient, robust, imperceptible and secure watermarking process designed specifically for color images in the DWT-SVD hybrid domain.
(ii) This process is imperceptible, as maximum entropy blocks are utilized to conceal the watermark, resulting in a reduction in computational costs
(iii) This process is semi-blind, as the original image is not compulsory, only distinct side details are essential for extraction.
(iv) This process is with improved security as the watermark or logo scrambled using Arnold transform.
(v) This process is robust under different geometrical attacks.

3.1 Watermark Embedding Process

This section provides a comprehensive description of the embedding procedure. Arnold transform is applied on watermark to enhance security. The original color watermarking image is first transformed to HSV transform, and H component is considered for 2-level DWT transform. The HH sub-band is then distributed into 8x8 blocks [14]. Maximum entropy blocks are calculated and SVD is applied on these blocks and to insert the scrambled watermark with proportionality coefficient α. Embedding the watermark into maximum entropy blocks with proportionality coefficient α has been found to enhance PSNR and NCC values while reducing computational costs.

1. Consider the original watermarking image and binary logo.
2. Arnold transform is employed on the the watermark logo and 1-level DWT is applied on scrambled logo.
3. HSV transform is employed on the original color image, and the H channel is selectively chosen for inserting the scrambled logo.
4. A 2-level discrete wavelet transform (DWT) is applied to the original image, producing four frequency sub-bands: LL, HL, LH, and HH.
5. The HH sub-band is partitioned into blocks of size 4 × 4.
6. And the entropy of each block is computed. The blocks with the maximum entropy are then selected.
    - First, entropy of every block and average entropy are evaluated.
    - If the block whose entropy is greater than average entropy is considered as the maximum entropy block.
7. Singular value decomposition (SVD) is then accomplished on the certain maximum entropy blocks.
8. Now, insert the scrambled wavelet transformed watermark into the SVD performed maximum entropy blocks with proportionality coefficient α.
9. Apply the Inverse SVD on the watermark embedded block and all the blocks are combined by taking the LL, LH and HH bands from the original watermarking image.
10. The inverse DWT is activated to attain the watermarked H channel image.

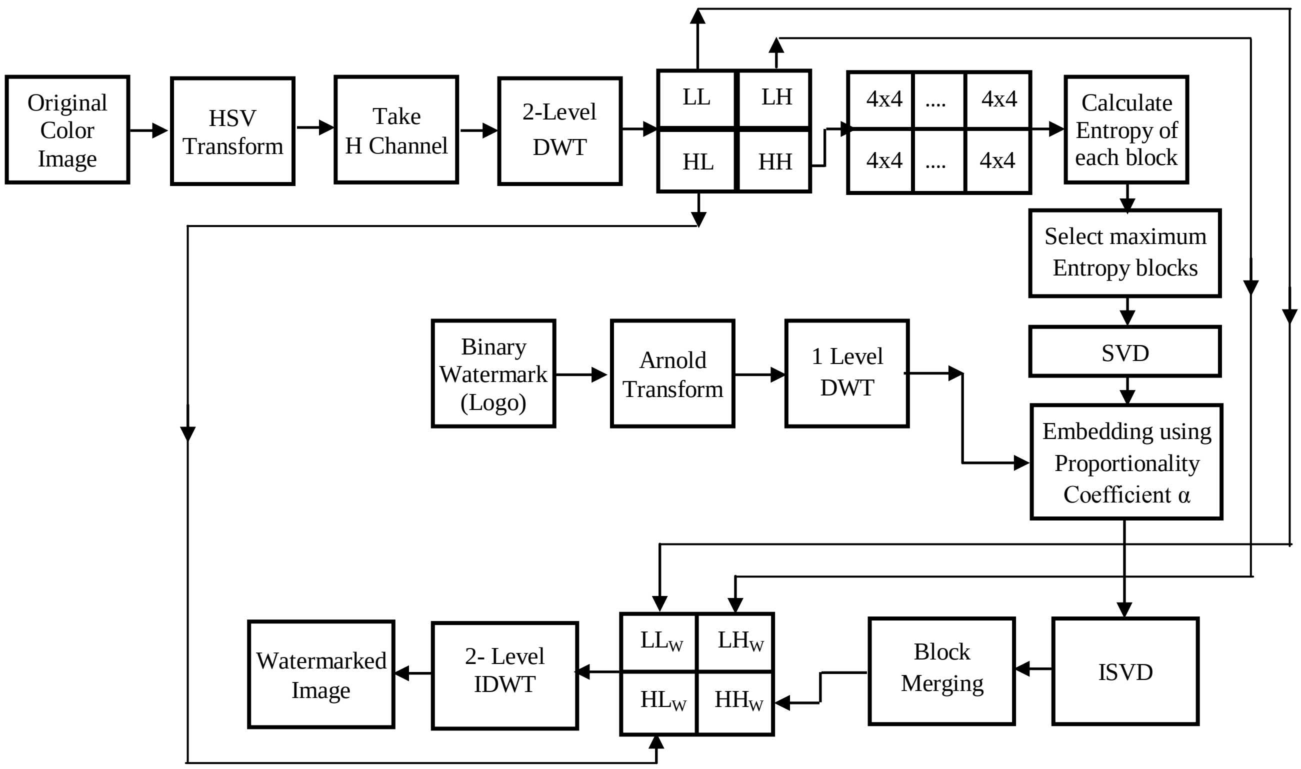

Fig. 1: Block diagram of the logo embedding process

11. To produce a watermarked image, it is necessary to convert the modified HSV color model back to the RGB color model.

One of the crucial contests in enhancing the watermarking process is dynamically choosing the suitable inserting location and energy. To address this issue, this research proposes the use of information entropy, a measure commonly employed to quantify the randomness of image data. The entropy of an image is directly proportional to the complexity of the pixels. Therefore, to enrich the visual quality of this process, we can insert the logo in the area with high information entropy [15].

The proportionality coefficient α performs a significant contribution to decide the visual quality and toughness of the watermarking process. Even a slight rise in the value of α can upgrade the visual appearance of the image, but it may reduce the toughness of the watermarked image. Contrariwise, if the value of α is increased, then toughness may be increased with decreased visual quality (Singh 2022). Therefore, it is necessary to discover the optimal value of α to assault the correct equilibrium between toughness and invisibility.

3.2 Watermark Extraction Process

During the extraction phase, the embedded watermark image is retrieved by applying the reverse operation of the embedding process to the watermarked image. The watermarked image is subjected to a 2-level DWT to divide it into four sub-bands, and the sub-band LL is used for watermark extraction [16].This involves applying the SVD technique to extract the watermark logo.

1. The watermarked color image undergoes HSV transform.
2. The DWT transform is adopted on the H channel of the HSV transformed watermarked image, producing four sub-bands: LL, HL, LH, and HH.
3. The HH sub-bands are then partitioned into blocks of size 4 × 4.
4. The entropy of each block is computed. The blocks with the maximum entropy are then selected.
5. SVD is then performed on the selected maximum entropy blocks.
6. The watermark is extracted by considering the same proportionality coefficient α.
7. Then apply 1-level IDWT and Inverse AT on the watermark.
8. Thus the watermark is extracted.

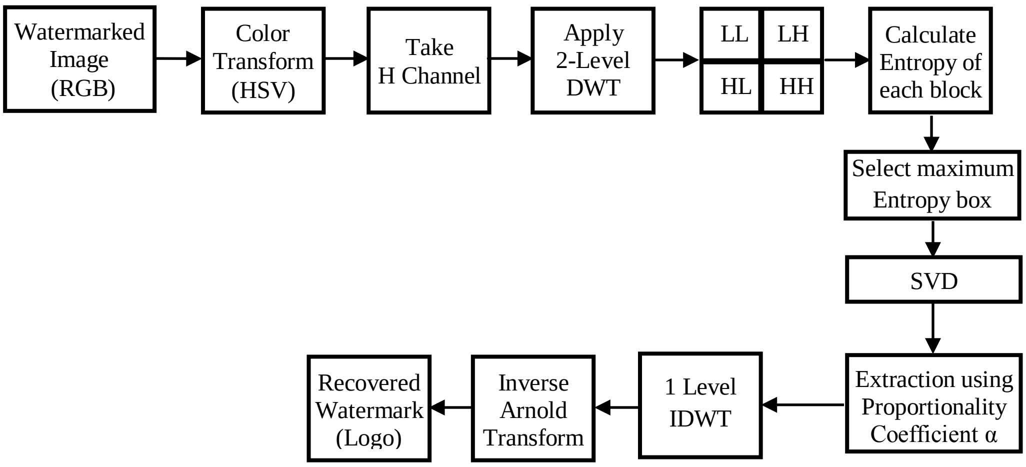

Fig. 2: Block diagram of the logo extraction process

4. Results and Discussion

In order to assess the effectiveness of the presented process, we tested it on various true color image samples with resolutions of 256x256 and 512x512. We accompanied trials on two widely obtainable image databanks, namely CVG-UGR and USC-

SIPI [17, 18]. This section presents a critical assessment of the presented process with regard to its effectiveness in achieving imperceptibility and robustness.

Fig. 3: Results of presented process a) original watermarking image; (b) watermark logo; (c) Watermarked image; (d) Extracted watermark.

Assessing image quality is a critical task for accurate interpretation, but it is also notoriously challenging. To evaluate its imperceptibility, we consider the metrics: the PSNR, MSE, NCC and SSIM. This approach ensures a balance between transparency and robustness, providing a reliable compromise [19].

MSE is a degree of the average of the squares of modifications among the actual (genuine) and predicted (approximated) values. It can be mathematically expressed by Eq. (1).

$$\mathrm{MSE} = \frac{\sum_{p,q}\left[M(p,q) - M^{l}(p,q)\right]^2}{p \times q} \quad (1)$$

Here, $M(p,q)$ is the original watermarking image.

$M^{l}(p,q)$ is the image where the logo is inserted.

$p \times q$ is the dimensions of the image.

PSNR is a measure of the relationship between the maximum possible signal power and the power of interfering noise that affects the quality of an image [20]. PSNR is calculated using MSE, and Eq. (2) provides the formula for calculating PSNR from MSE. PSNR is commonly expressed in decibels (dB).

$$\mathrm{PSNR} = 10\log_{10}\frac{D^2}{\mathrm{MSE}} \quad (2)$$

The variable D represents the maximum deviation that can occur within the primary image data format.

The NCC value is a measure of the toughness between the watermark logo and the recovered watermark logo images against attacks.

SSIM is mathematically expressed as Eq. (3).

$$\mathrm{SSIM}(m,l) = \frac{(2\mu_m\mu_l + k_1)(2\rho_m\rho_l + k_2)}{(\mu_m^2 + \mu_l^2 + k_1)(\rho_m^2 + \rho_l^2 + k_2)} \quad (3)$$

Where, μ_m = Mean of the original watermarking image

μ_l = Mean of the watermarked image

ρ_m = Standard deviation of the original watermarking image

ρ_l = Standard deviation of the watermarked image

k_1, k_2 = Constants

Table 1: Measured study for different images with resolution of 256x256

Image	PSNR	SSIM	MSE	NCC
Airplane	39.52	0.957	9.7*10-4	0.968
Barbara	41.81	0.986	5.9*10-4	0.998
Lena	38.47	0.997	4.53*10-4	0.995
Baboon	40.45	0.968	8.72*10-4	0.998
Parrot	43.95	0.991	3.64*10-4	0.995
Average	40.84	0.9798	64.95*10-4	0.9908

Table 2: Measured study for different images with resolution of 512x512

Image	PSNR	SSIM	MSE	NCC
Airplane	35.59	0.987	4.09*10-4	0.989
Barbara	33.86	0.976	7.68*10-4	0.992
Lena	38.72	0.993	2.65*10-4	0.998
Baboon	36.63	0.968	3.96*10-4	0.988
Parrot	41.02	0.991	3.04*10-4	0.997
Average	39.34	0.979	3.36*10-4	0.994

Tables 1 and 2 reveal the metric study of the presented process for various specimens with distinct dimensions. These values specify that the presented process continues the quality of the image and maintains the novelty of the image, as evaluated by PSNR, SSIM, MSE and NCC.

Table 3: Measured study for different images with the resolution of 512x512 beneath Gaussian Noise strike

IMAGE	ATTACK	PSNR	SSIM	MSE	NCC
Airplane	Gaussian Noise (Var=0.01)	25.65	0.55	0.098	0.896
Barbara		21.48	0.67	0.013	0.894
Lena		22.38	0.89	0.019	0.896
Baboon		20.99	0.843	0.042	0.895
Parrot		24.42	0.766	0.097	0.990

Table 4: Measured study for different images with the resolution of 512x512 beneath Salt & Pepper Noise strike

IMAGE	ATTACK	PSNR	SSIM	MSE	NCC
Airplane	Salt & pepper Noise (Var=0.01)	26.15	0.819	0.0037	0.954
Barbara		27.92	0.918	0.0039	0.935
Lena		25.92	0.981	0.0029	0.945
Baboon		28.05	0.898	0.0036	0.919
Parrot		27.27	0.898	0.0031	0.983

Table 5: Measured study for different images with the resolution of 512x512 beneath Scaling Noise strike

IMAGE	ATTACK	PSNR	SSIM	MSE	NCC
Airplane	Scaling Factor=1.2	18.36	0.970	0.019	0.965
Barbara		22.01	0.972	0.008	0.949
Lena		20.96	0.984	0.015	0.996
Baboon		21.95	0.964	0.014	0.994
Parrot		23.19	0.959	0.009	0.997

Table 6: Measured study for different images with the resolution of 512x512 beneath JPEG compression attack

IMAGE	ATTACK	PSNR	SSIM	MSE	NCC
Airplane	JPEG Compression Q=30	37.02	0.97	6.0*10-4	0.998
Barbara		34.79	0.997	0.0013	0.997
Lena		36.43	0.998	6.47*10-4	0.992
Baboon		33.89	0.975	9.64*10-4	0.989
Parrot		39.34	0.996	2.03*10-4	0.996

Tables 3, 4 and 5 reveal the metric study of the presented process for various specimens beneath distinct strikes like Gaussian Noise strike, Salt & Pepper Noise strike and JPEG compression attack.

The tabulated values reveal that, the proposed process has demonstrated sound to achieve the toughness and imperceptibility.

5. Conclusions

With the expansion of online information technology, color images have become increasingly common among people. And necessity copyright protection issues. This work presents an approach that is highly secured by scrambling the watermark. By inserting the logo in high entropy blocks high imperceptivity is obtained. The recompense between imperceptibility and robustness is achieved by selecting the optimal proportionality coefficient α. This method is examined on the database of standard color images by PSNR, SSM, SSIM and NCC parameters under various watermarking attacks.

References

[1] Singh N., Jain M., Sharma S. (2013). A survey of digital watermarking techniques. International Journal of Modern Communication Technologies and Research, 1(6), 265852.

[2] Alzahrani A. (2022). Enhanced invisibility and robustness of digital image watermarking based on DWT-SVD. *Applied Bionics and Biomechanics*, *2022*. https://doi.org/10.1155/2022/5271600

[3] Thulasidharan P. P., Nair M. S. (2015). QR code based blind digital image watermarking with attack detection code. *AEU-International Journal of Electronics and Communications*, *69*(7), 1074-1084. https://doi.org/10.1016/j.aeue.2015.03.007

[4] Singh A. K., Dave, M., Mohan, A. (2016). Hybrid technique for robust and imperceptible multiple watermarking using medical images. *Multimedia Tools and Applications*, *75*, 8381-8401. https://doi.org/10.1007/s11042-015-2754-7

[5] Makbol N. M., Khoo, B. E. (2013). Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *AEU-International Journal of Electronics and Communications*, *67*(2), 102-112. https://doi.org/10.1016/j.aeue.2012.06.008

[6] Zhuang Y., Zhou X., Liu, S. (2020). An entropy-based image watermarking scheme by improving robustness in shearlet and wavelet domain. https://doi.org/10.21203/rs.3.rs-63616/v1

[7] Lai C. C., Tsai C. C. (2010). Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on instrumentation and measurement*, *59*(11), 3060-3063. https://doi.org/10.1109/tim.2010.2066770

[8] Singh D., Singh S. K. (2017). DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimedia Tools and Applications*, *76*(11), 13001-13024. https://doi.org/10.1007/s11042-016-3706-6

[9] Singh R., Izhar L. I., Elamvazuthi I., Ashok A., Aole S., Sharma N. (2022). Efficient Watermarking Method Based on Maximum Entropy Blocks Selection in Frequency Domain for Color Images. *IEEE Access*, *10*, 52712-52723. https://doi.org/10.1109/access.2022.3174964

[10] Ahmed B, Mohammed T, Mohamed A T, Hicham K, Mohammed A, Mohammed Q J, Hassan Q, Mhamed S (2023) Optimal Color Image Watermarking Based on DWT-SVD Using an Arithmetic Optimization Algorithm Inter. Conf. on Digital Technologies and Applications (ICDTA-2023), Springer. 669, 441-450. https://doi.org/10.1007/978-3-031-29860-8_45

[11] Roy S., Pa A. K. (2017). A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling. *Multimedia Tools and Applications*, *76*(3), 3577-3616. https://doi.org/10.1007/s11042-016-3902-4

[12] Ernawan F., M. N. Kabir, (2020) A block-based RDWT-SVD image watermarking method using human visual system characteristics. Visual Computers, 36(1), 19–37. https://doi.org/10.1007/s00371-018-1567-x

[13] Makbol N. M., Khoo B. E., Rassem, T. H. (2016). Block‐ based discrete wavelet transform‐ singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image processing*, *10*(1), 34-52. https://doi.org/10.1049/iet-ipr.2014.0965

[14] Zainol Z., Teh J. S., Alawida M., Alabdulatif A. (2021). Hybrid SVD-based image watermarking schemes: a review. *IEEE Access*, *9*, 32931-32968. https://doi.org/10.1109/access.2021.3060861

[15] Singh, G., & Goel, N. (2016, March). Entropy based image watermarking using discrete wavelet transform and singular value decomposition. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 2700-2704). IEEE.

[16] Yadav J, Sehra K 2018 Large scale dual tree complex wavelet transform based robust features in PCA and SVD subspace for digital image watermarking. Proc. Comput. Sci. 132: 863-872. https://doi.org/10.1016/j.procs.2018.05.098

[17] University of Granada. Computer Vision Group. CVG-UGR Image Database. Accessed: 2022. [Online]. Available: *http://decsai.ugr.es/cvg/dbimagenes/*

[18] University of Southern California. Signal and Image Processing Institute. USC-SIPI Image Database. Accessed: 2022. [Online]. Available: *http://sipi.usc.edu/database*

[19] Bose A.,Maity S. P. (2022). Secure sparse watermarking on DWT-SVD for digital images. *Journal of Information Security and Applications*, *68*, 103255. https://doi.org/10.1016/j.jisa.2022.103255

[20] Wang B.,Zhao P. (2020). An adaptive image watermarking method combining SVD and Wang-Landau sampling in DWT domain. *Mathematics*, *8*(5), 691. https://doi.org/10.3390/math8050691