A Novel Blind Watermarking Strategy for Rightful Ownership Validation in Digital Imagery

Pavan A.C.
Assistant Professor, Department of Computer Science and Engineering
PES University
Bengaluru, India

M.T. Somashekara
Associate Professor, Department of Computer Science and Applications
Bangalore University
Bengaluru, India

ABSTRACT
The quick growth of the network has made the protection of digital content a critical concern. Digital Rights Management (DRM) systems aim to safeguard valuable assets and regulate their distribution. Among these, digital watermarking serves as an effective technique to embed ownership information into images for copyright enforcement. This paper presents a novel innovative invisible and blind watermarking scheme that embeds a binary watermark into non-overlapping 2 × 2 blocks of the actual host image. The extraction process requires only the watermarked image, eliminating the need for the original or its features. Experimental results validate the robustness and effectiveness of the proposed approach in defending against digital piracy.

Keywords
Digital Rights Management (DRM); Digital images; Copyright Protection; Digital image watermarking; Blind Scheme; Invisible watermarking.

1. INTRODUCTION
Digital Rights Management (DRM) systems have been extensively used for securing and limiting the distribution and utilization of valuable digital properties. The core requirements of a DRM system are to provide persistent content protection against unauthorized access and restrict access solely to authorized users. Additionally, DRM systems must be robust enough to manage access rights across various types of digital content, such as music files, video streams, digital books, and images, and support multiple platforms like PCs, laptops, PDAs, and mobile phones [3]. In general, a DRM system comprises two components: (1) a collection of technologies including encryption, copy control, digital watermarking, fingerprinting, traitor tracing, authentication, integrity checking, access control, tamper-resistant hardware and software, key management, revocation, and risk management architectures, and (2) a set of technologies used to express copyright permissions using rights expression languages and metadata to make DRM policies machine-readable [4]. Among these, copyright protection plays a vital role in addressing disputes arising from ownership claims in the buying and selling of digital documents. This demands a robust mechanism to authenticate document ownership and verify legitimate buyers [5]. With the evolution of image processing tools, digital images have become increasingly susceptible to illegal replication, modification, and distribution, especially with the widespread reach of the internet. As a result, protecting digital images has become a pressing concern, particularly due to the rising threat of revenue loss through piracy [6]. While DRM technologies offer powerful protection mechanisms, they also raise controversy, as they may interfere with legitimate use of digital content. Forensic techniques, unlike DRM, do not prevent copying but aid in identifying and prosecuting offenders once illegal copies are found, making them relatively less contentious [7]. Despite numerous technological approaches to counter copyright piracy, an ideal and universally accepted solution remains elusive, offering ample scope for innovative research. Recently, digital watermarking has emerged as a crucial technique for copyright protection and ownership verification of digital images. Digital watermarking involves embedding data into multimedia elements like images, audio, or video, enabling the extraction of this data for various purposes including copyright protection, access control, and broadcast monitoring [8]. It can be categorized into image, video, and audio watermarking depending on the application, with most existing methods focused on image and video copyright protection [9]. Acting as a digital signature, the watermark provides authenticity and ownership assurance, and its inseparability from the host content offers an added advantage. Key characteristics of a robust watermark [27-28] include being imperceptible, resilient to distortions and attacks, carrying significant data, coexisting with other watermarks, and requiring minimal computational effort for insertion and detection [10]. Watermarking schemes can be broadly classified into non-blind, semi-blind, and blind categories based on extraction requirements [11][12]. Non-blind schemes need the original host image and its secret keys, semi-blind schemes always require the secret key and watermark sequence, while blind schemes demand only the secret key. Watermarks are also categorized as visible and invisible—visible watermarks are directly perceivable in the image, whereas invisible ones are concealed and can be detected only via software [13]. Robust watermarking is designed to resist attacks like compression, cropping, and scaling, and serves copyright protection purposes, while fragile watermarking detects minor changes and validates content integrity [14]. Among all types, visible watermarks often compromise image quality and are more prone to tampering. Numerous research efforts have been devoted to digital watermarking for copyright protection [15–20], including our previous work [25, 26]. In this study, we propose a novel invisible and blind watermarking scheme aimed at preventing digital image piracy. The scheme does not require the original image or any of its features for watermark extraction, thereby making it blind. A binary watermark image is used for embedding, and each pixel of this watermark is embedded into every 2×2 non-overlapping block of the host image using an embedding strength factor and a signum function. During extraction, the binary watermark is retrieved from the watermarked image using the watermark size and embedding strength. Experimental results confirm the effectiveness of the proposed approach. The rest of this paper is structured as follows: Section 2 reviews recent literature on watermarking for digital image copyright protection, Section 3 describes the proposed invisible and blind watermarking

scheme, Section 4 will present the experimentational results, and Section 5 would conclude the paper.

2. REVIEW OF RELATED RESEARCH

Our work is inspired by a substantial body of literature that explores the use of digital image watermarking for copyright protection. Below is a brief overview of some recent and significant research contributions in this domain.

Shih-Hao Wang and Yuan-Pei Lin [15] introduced a wavelet-based watermarking technique that employs the quantization of super trees for copyright protection. Each watermark bit is embedded across different frequency bands and distributed over extensive spatial regions, enhancing the technique's robustness to attacks in both frequency and time domains. Experimental results demonstrated resistance to high-pass band removal during low-pass filtering, high-pass detail removal in JPEG compression, as well as pixel shifting and rotation. The scheme also supports data hiding and image authentication, beyond copyright protection.

To address the limitations of symmetric watermarking methods, Jengnan Tzeng et al. [16] proposed an asymmetric watermarking approach based on the zero-knowledge principle. They enhanced their prior symmetric scheme with a watermark space concept, improving robustness. The watermark is closely tied to the original image, making it nearly impossible to extract without introducing visible distortions, thus improving security.

Ching-Sheng Hsu and Young-Chang Hou [17] proposed a copyright protection scheme based on visual cryptography and image statistics. They utilized the Sampling Distribution of Means (SDM) to ensure robustness and distinctiveness, making it difficult for common attacks—like lightening and darkening—to alter statistical image properties. Notably, their approach does not modify the host image and does not require the actual original image for verification, making it particularly suitable for sensitive applications like medical image protection.

Xu Zhou et al. [18] developed a novel watermarking method for embedding data into the angular parameters of polygonal lines or curves in contour maps. This method, applicable to GIS and vector graphics, uses a likelihood ratio test-based hypothesis detection instead of traditional correlation-based techniques. Its geometric nature makes it resilient against common geometric transformations. However, the approach struggles with vertex removal or addition, which compromises robustness unless the original data is referenced—potentially weakening data security.

Ming-Chiang Hu et al. [19] introduced a two-phase watermarking system that extracts both grayscale and binary watermarks from protected images. Initially, a grayscale watermark is constructed using the original image's pixel values. In the second phase, a binary watermark is derived from the permuted grayscale watermark. Their lossless embedding technique ensures that protected images remain visually identical to the originals. The authentication process typically does not require the original image, and only the legitimate owner can retrieve the embedded watermarks using secret keys. The method excels in transparency, robustness, and security.

Shang-Lin Hsieh et al. [20] proposed a watermarking scheme for copyright protection in color images that meets essential requirements such as imperceptibility and robustness. Experimental evaluations revealed strong resistance against various attacks including cropping, editing, scaling, and JPEG image compression. Additionally, the scheme can extract unique features for different images—crucial for reliable feature extraction—and automatically compute the embedding scaling factor, unlike many schemes that rely on manual tuning.

Zeng et al. [21] discussed scenarios where traditional watermarking schemes fail to resolve image ownership disputes. Their scheme protects the watermark itself rather than establishing rightful ownership, as it does not require the original image for detection. Consequently, attackers could fabricate fake originals and falsely claim ownership, highlighting the importance of designing watermarking systems that validate both watermark integrity and content ownership.

Lu et al. [22] introduced a multipurpose watermarking algorithm based on mean-removed vector quantization (VQ), addressing key digital concerns such as copyright enforcement, copy protection, and content authentication.

Finally, Ming-Shi Wang and Wei-Che Chen [23] proposed a digital image copyright protection approach that combines visual cryptography (VC) and singular value decomposition (SVD). The method applies SVD to generate a master share from the host image and embeds the secret image without altering the host, ensuring both integrity and invisibility of the watermark.

3. PROPOSED BLIND WATERMARKING SCHEME FOR PROTECTING RIGHTFUL OWNERSHIP

This section introduces a novel invisible and blind watermarking technique designed to safeguard the copyright of digital images. Since the watermark extraction process does not rely on the original image or any of its features, the scheme qualifies as blind. A binary image serves as the watermark, with its pixel values imperceptibly embedded into the host image to enforce copyright protection. The subsequent subsections detail the procedures used for embedding and retrieving the watermark.

3.1 Watermark Embedding

This sub-section outlines the method used to embed a binary watermark image into a host image. The host image selected is of dyadic dimensions (i.e., $2n\times2n$), and the watermark is a binary image consisting of 0s and 1s. Initially, the host image is divided into non-overlapping 2×2 blocks. Each pixel from the binary watermark is embedded into a corresponding block of the host image.

The embedding process comprises three main steps: calculating the mean of each block, selecting an embedding strength parameter (γ), and applying a signum-based transformation. Each 2x2 block is flattened into a vector, its mean is computed, and the result is scaled using the embedding strength.

Since the watermark consists of binary values, the embedding logic splits into two cases—one for embedding a '1' and another for embedding a '0'. Distinct mathematical operations are applied based on the value of the watermark pixel. A block diagram depicting the overall watermark embedding procedure is provided in Figure 1.

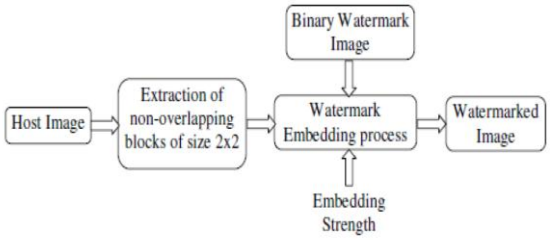


Figure 1. Watermark Embedding Process

Watermark Embedding Steps:

Input: Actual Host Image (I), Binary Watermark Imaging (W), strength of it Embedding (γ)

Output: Watermarked Image (I_W)

1. The binary watermarked image (W) sized n x n is composed of n^2 no. of pixels. n^2 no. of 2x2 non- overlapping pixel blocks are extracted from the actual image and dumped in a vector B.

$$B = [b^1, b^2, b^3, ..., b_n]; \; where\, 0 < N \leq n^2 \tag{1}$$

2. Each and every matrix part in the vector B is changed into a vector V_B.

$$VB = [x1, x2, x3, x4] \tag{2}$$

3. The overall mean value of all the changed vectors V_B is then calculated.

$$\bar{V}_B = \frac{(\Sigma\, from\; i = 1\; to\; k\; of\; V_{Bk})}{k} \; ; \; where\, 0 < k \leq 4 \tag{3}$$

4. A value Q is computed by dividing the overall mean value V_B of all vector by strength of embedding γ.

$$Q = \bar{V}_B / \gamma \; ; \; where\, \gamma = 2 \tag{4}$$

5. Using a predetermined Q value and strength of embedding γ, the binary embedded watermarked image pixels are embedded into the blocks in vector B:

(i) The signum function of all block in vector B is then calculated and dumped in another vector X. The signum function is the real valued function defined for real *x* as follows [24]

$$sign(x) = \{ \\ -1\; if\; x < 0 \\ 0\; if\; x = 0 \\ 1\; if\; x > 0 \\ \} \quad .... (5)$$

(ii) For pixel value '0', perform the following mathematical operation:

$$t = ((round(Q * 0.5) * 2) * \gamma) \tag{6}$$

(iii) For each pixel value of '1', the following mathematical required operation is carried out: Q = (Q −1).

$$t = ((round(Q1 * 0.5) * 3) * \gamma) \tag{7}$$

(iv) All blocks in vector X is then multiplied by the neatly calculated value t wrt watermark pixel and dumped in a vector B.

$$B << (X_i .* t) \; ; \; where\, 0 < i \leq k \tag{8}$$

6. The modified blocks in the vector B are mapped back to its original position in host image I to attain the watermarked image I_W.

3.2 Watermark Extraction

This sub-section explains the procedure for retrieving the binary watermark from the watermarked image. Since the proposed approach is blind, the extraction process requires only the watermarked image, the dimensions of the original watermark, and the embedding strength parameter (γ); it does not rely on the original image or any of its features.

To begin, the watermarked image is divided into non-overlapping 2×2 blocks. The total number of blocks corresponds to the size of the embedded watermark. These blocks are then reshaped into vectors for further processing.

Next, each block is individually converted into a vector, and its mean value is calculated. These mean values are then divided by the embedding strength to aid in the recovery of the watermark information.

Finally, a matrix matching the dimensions of the watermark image is constructed, and the extracted pixel values are inserted into their respective positions to reconstruct the watermark. A schematic representation of this extraction process is provided in Figure 2.

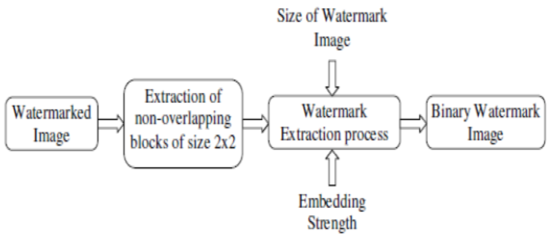


Figure 2. Watermark Extraction Process

Watermark Extraction Steps:

Input: Watermarked Image (I_W), watermarked image size (W), strength of Embedding (γ)

Output: Watermark Image (W)

1. Non-overlapping blocks of size 2x2 are extracted from the watermarked image (W_I). The number of extracted blocks will be identical to the size of the watermark image. The extracted blocks are stored in a vector BV.

$$BV = [b^1, b^2, b^3, ..., b_n]; \; where\, 0 < N \leq n^2 \tag{9}$$

2. All the blocks in the vector BV are changed into a vector V_B.

$$VB = [x1, x2, x3, x4] \tag{10}$$

3. The mean of the value is calculated for all the changed vectors V_B.

$$\bar{V}_B = \frac{(\Sigma \; from \; i = 1 \; to \; k \; of \; V_{Bk})}{k} \; ;$$

$$where \; 0 < k \leq 4 \qquad (11)$$

4. The calculated value of mean V_B of all vectors is sub-divided by the embedding strength γ. The value due to which obtained is represented as Y.

$$Q = \frac{\bar{V}_B}{\gamma} \; ; \; where \; \gamma = 2 \qquad (12)$$

5. The following required mathematical operation is then performed and the result of which is dumper in a vector W_p.

$$W_p \ll (Y[i] \; mod \; 2); \quad 0 \leq i \leq |W| \qquad (13)$$

A given matrix of the size of that of a watermark image is created and the extraction of pixel values (W_p) which is done are placed in it, to get back the watermark image (W).

4. EXPERIMENTAL RESULTS

This section evaluates the performance of the proposed invisible and blind watermarking scheme through a series of experiments. All simulations were conducted using MATLAB 7.4 on standard grayscale images including Lena, Baboon, Pepper, and Cameraman. The watermark used was a binary image of size 64×64. Performance was assessed based on Peak Signal-to-Noise Ratio (PSNR), robustness against attacks, and fidelity of watermark extraction using Normalized Correlation (NC).

A. Visual Quality Assessment

The watermarked images exhibit minimal perceptual distortion from the original host images, confirmed by PSNR values exceeding 44 dB in most cases. Table 1 presents PSNR values for different host images in both unperturbed and attack scenarios.

B. Robustness Analysis

To assess robustness, the watermarked images were subjected to common image processing attacks, including:

- JPEG Compression at 70% quality.
- Additive Gaussian Noise with zero mean and variance 0.001.

Despite these distortions, watermark extraction remained accurate, with NC values close to 1.0, indicating high robustness.

Table 1: Experimental Results of the Proposed Scheme

Host Image	PSNR (No Attack)	PSNR (JPEG 70%)	PSNR (Gaussian Noise)	NC (Extracted WM)
Lena	45.45 dB	38.76 dB	37.52 dB	0.99
Baboon	44.03 dB	39.11 dB	36.70 dB	0.98
Pepper	48.06 dB	41.25 dB	40.88 dB	0.97
Cameraman	46.10 dB	40.55 dB	39.90 dB	0.98

C. Graphical Illustration

The bar chart in **Figure-3** illustrates the PSNR variation across different attacks for each host image. This visualization emphasizes the minimal degradation introduced by watermark embedding and the scheme's resilience under adverse conditions.

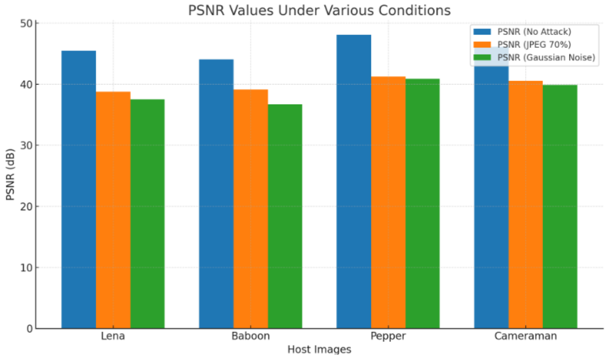
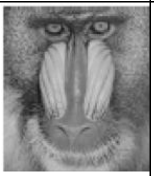
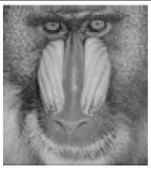


Figure-3: PSNR comparison chart under various conditions (No Attack, JPEG compression, and Gaussian Noise) for different host images.

Host Image	Watermark Image	Watermarked Image	PSNR (dB)
			45.4458
			46.0987
			50.5257
			40.7011

			56.08 92
			52.12 70
			48.06 33
			44.03 13

5. CONCLUSION

With the rapid growth of e-commerce platforms and online services, concerns over unauthorized copying and distribution of copyrighted content have intensified among service providers. The widespread accessibility of the internet has amplified the need for robust protection of digital images. In this work, we have introduced a novel invisible and blind digital watermarking technique aimed at safeguarding image copyrights. The method employs a binary image as the watermark, embedding each pixel into non-overlapping 2×2 blocks of the host image. The watermark is later extracted from the watermarked image using the defined extraction process. Experimental results confirm that the watermarked images maintain high visual quality and yield favorable PSNR values, validating the effectiveness of the proposed watermarking approach.

Looking ahead, this work opens up several avenues for future research. One potential direction is to enhance the robustness of the proposed method against geometric attacks such as rotation, scaling, and translation. The integration of transform domain techniques (e.g., DWT or DCT) with the current spatial domain approach could also be explored to strengthen imperceptibility and resistance to compression. Additionally, adaptive embedding strategies based on content sensitivity may further improve performance. Extending the technique to color images and video sequences would increase its applicability across diverse multimedia platforms. Finally, incorporating cryptographic elements and blockchain-based tracking mechanisms could provide a comprehensive framework for secure digital rights management.

6. ACKNOWLEDGMENTS

I would like to express my sincere gratitude to Dr. M. T. Somashekara, Associate Professor, Department of Computer Science and Applications, Bangalore University, for his invaluable mentorship and guidance throughout this work, in addition to his contributions as a co-author. We also extend our thanks to the Department of Computer Science and Applications, Bangalore University, and Department of Computer Science and Engineering, PES University, for their academic support and infrastructure that enabled the successful completion of this work.

7. REFERENCES

[1] Claudine Conrado, Milan Petkovic, Michiel van der Veen and Wytse van der Velde "Controlled Sharing of Personal Content Using Digital Rights Management", Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006.

[2] L. C. Anderson, J. B. Lotspiech, “Rights Management and Security in the Electronic Library,” Bulletin of the American Society for Information Science, Vol. 22, No.1, pp.21-3, October-November 1995.

[3] Qiong Liu, Reihaneh Safavi-Naini and Nicholas Paul Sheppard, "Digital Rights Management for Content Distribution", Proceedings of the Australasian information security workshop conference on ACSW frontiers, Adelaide, Australia, Vol. 21, pp. 49 - 58, 2003.

[4] Ian Kerr, "Hacking@privacy: Why We Need Protection from the Technologies That Protect Copyright", In proc. of Conference on privacy and identity, 2007.

[5] Piva, F. Bartolini, and M. Barni, “Managing copyright in open networks,” IEEE Trans. Internet Computing, vol. 6, no. 3, pp. 18–26, May–Jun. 2002.

[6] Shang-Lin Hsieh, Lung-Yao Hsu, and I-Ju Tsai, “A Copyright Protection Scheme for Color Images using Secret Sharing and Wavelet Transform”, proceedings of World Academy of Science, Engineering And Technology, Vol. 10, December 2005.

[7] Hans Georg Schaathun, "On watermarking/fingerprinting for copyright protection", First International Conference on Innovative Computing, Information and Control, ICICIC '06, Beijing, Vol. 3, pp. 50-53, Aug. 30 2006-Sept. 1 2006.

[8] Emir Ganic, Ahmet M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies", International Multimedia Conference, Magdeburg, Germany, pp. 166 - 174, 2004.

[9] Xiang-Yang Wang and Hong Zhao, "A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT", IEEE Transactions On Signal Processing, Vol. 54, No. 12, December 2006.

[10] Miller, M.; Cox, I.J.; Linnartz, J.P.M.G.; Kalker, T., “A review of watermarking principles and practices,” In Digital Signal Processing in Multimedia Systems, Edit. K. K. Parhi and T. Nishitani, Marcell Dekker Inc., pp. 461-485, 1999.

[11] P. Tao and A. M. Eskicioglu, “A Robust Multiple Watermarking Scheme in the DWT Domain,” Optics East 2004 Symposium, Internet Multimedia Management Systems V Conference, Philadelphia, PA, pp. 133-144, October 25-28, 2004.

[12] Ersin Elbasi and Ahmet M. Eskicioglu, “A Semi-Blind Watermarking Scheme for Color Images Using a Tree Structure," in proc. of IEEE Sarnoff Symposium, March, 2006.

[13] Yeung, M. & Minzter, F., “An Invisible Watermarking technique for image verification,” Proceeding on the IEEE International Conference on Image Processing, pp: 680-683, 1997.

[14] Shaowei Weng, Yao Zhao and Jeng-Shyang Pan, “A Novel Reversible Data Hiding Scheme,” International Journal of Innovative Computing, Information and Control, Vol. 4, No. 2, pp. 351-358, 2008.

[15] Shih-Hao Wang and Yuan-Pei Lin, "Wavelet Tree Quantization for Copyright Protection Watermarking", IEEE Transactions on Image Processing, Vol. 13, No. 2, February 2004.

[16] Jengnan Tzeng, Wen-Liang Hwang, and I-Liang Chern, "An Asymmetric Subspace Watermarking Method for Copyright Protection", IEEE Transactions on Signal Processing, Vol. 53, No. 2, February 2005.

[17] Ching-Sheng Hsu, Young-Chang Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods", Optical Engineering, Vol. 44, No. 7, July 2005.

[18] Xu Zhou, Yu Ren, and Xuezeng Pan, "Watermark Embedded in Polygonal Line for Copyright Protection of Contour Map", IJCSNS International Journal of Computer Science and Network Security, Vol.6 No.7B, pp. 202-205, July 2006.

[19] Ming-Chiang Hu, Der-Chyuan Lou and Ming-Chang Chang, "Dual wrapped digital watermarking scheme for image copyright protection," Computers & Security, Vol. 26, No. 4, pp. 319-330,2007.

[20] Shang-Lin Hsieh, I-Ju Tsai, Bin-Yuan Huang and Jh-Jie Jian, "Protecting Copyrights of Color Images using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform", Journal Of Multimedia, vol. 3, no. 4, October 2008.

[21] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images", IEEE Transactions on Image Processing, Vol. 8, No. 11, pp. 1534-1548, 1999.

[22] Zhe-Ming Lu, Wei-Min Zheng, Jeng-Shyang Pan and Zhen Sun, "Multipurpose Image Watermarking Method Based on Mean-removed Vector Quantization", Journal of Information Assurance and Security, Vol. 1, pp. 33-42, 2006.

[23] Ming-Shi Wang and Wei-Che Chen, "Digital image copyright protection scheme based on visual cryptography and singular value decomposition", Optical Engineering, Vol. 46, No. 6, 2007.

[24] Stefean Porubsky, "Signum Function", Retrieved 2009/4/30 from Interactive Information Portal for Algorithmic Mathematics, Institute of Computer Science of the Czech Academy of Science, Prague, Czech Republic, Web-page http://www.cs.cas.cz/portal/AlgoMath/MathematicalAnalysis/SpecialFunctions/SignumFunction.htm.

[25] M. A. Dorairangaswamy, “A Novel Invisible and Blind Watermarking Scheme for Copyright Protection of Digital Images,” International Journal of Computer Science and Network Security (IJCSNS), Vol. 9, No. 4, pp. 71-78, 2009.

[26] M. A. Dorairangaswamy, “A Robust Blind Image Watermarking Scheme in Spatial Domain for Copyright Protection,” International Journal of Engineering and Technology (IJET), Vol. 1, No.3, pp. 249 - 255, August 2009.

[27] A. C. Pavan and M. T. Somashekara, "Two-order wavelet transform-based dual-tamper detection and self-restoration," in Proceedings of the 2024 IEEE International Conference on Communication, Computing and Signal Processing (IICCCS), 2024, doi: 10.1109/IICCCS61609.2024.10763854.

[28] A. C. Pavan and M. T. Somashekar, "An approach for detecting and restoring tampering in digital image watermarking," in Cognitive Computing and Information Processing, Springer, Cham, 2024, pp. 176–187. doi: 10.1007/978-3-031-60725-7_14

[29] A. C. Pavan, S. Lakshmi, and M. T. Somashekara, "An improved method for reconstruction and enhancing dark images based on CLAHE," International Research Journal on Advanced Science Hub, vol. 5, no. 2, Feb. 2023. doi: 10.47392/irjash.2023.011

[30] A. C. Pavan and M. T. Somashekara, "An overview on research trends, challenges, applications and future direction in digital image watermarking," International Research Journal on Advanced Science Hub, vol. 5, no. 1, pp. 8–14, Jan. 2023. doi: 10.47392/irjash.2023.002.