UDC 004.8

**M. B. Marchuk**

**V. V. Lukichov**

# THE EVALUATION OF THE EFFECTIVENESS OF DEEP LEARNING BASED IMAGE WATERMARKING

Vinnytsia National Technical University

***Анотація***

*В даній роботі було проаналізовано загальноприйняті критерії оцінювання водних знаків зображень, створених з використанням методів глибинного навчання. Досліджено ключові метрики непомітності, стійкості та пропускної здатності водних знаків. Вивчення цих показників дає комплексне розуміння того, наскільки добре працюють сучасні методи нанесення водних знаків за різних умов і обмежень.*

**Ключові слова**: водяні знаки, глибоке навчання, захист зображень, метрики, оцінка.

***Abstract***

*The commonly adopted evaluation criteria for deep-learning based image watermarking was analyzed. Key metrics for imperceptibility, robustness and capacity of watermarks are explored. By examining these metrics, this study provides a comprehensive understanding of how well modern watermarking techniques perform under various conditions and constraints.*

**Keywords**: watermarking, deep learning, image protection, metrics, evaluation.

## Introduction

In an era where digital content is increasingly vulnerable to unauthorized usage, tampering, and distribution, image watermarking has emerged as a vital technique for ensuring the integrity and ownership of visual data. Deep learning-based watermarking approaches have gained significant attention due to their adaptability, efficiency, and potential to balance imperceptibility, robustness, and capacity. The effectiveness of such systems must be rigorously evaluated using a set of quantitative metrics that reflect their practical reliability and security.

## Watermarking effectiveness evaluation

According to Malanowska. A., Mazurczyk. W., Araghi. T. K. and Megías. D. Imperceptibility refers to the perceptual resemblance of the watermarked and original data. The imperceptibility helps ensure that the watermark does not interfere with the quality of the image. The watermark should be hardly noticeable, such that the end user cannot perceive any visual or audio effect from the watermarked content. Although the watermark is not supposed to degrade the quality of the content, a small amount of degradation is acceptable. The reason for this is to achieve high robustness or low cost in some applications [1].

One most frequently applied evaluation metric is the peak signal-to-noise ratio (PSNR). PSNR evaluates the difference between original and protected images based on pixel-wise intensity differences:

$$PSNR = 10 \times \log_{10}\left(\frac{\max(c)^2}{\frac{1}{RC}\sum_{i=1}^{R}\sum_{j=1}^{C}\left(c_{ij} - m_{ij}\right)^2}\right), \quad (1)$$

where max(c) is the largest possible pixel value for the cover image c which is 255 if we use 8 bits for each grayscale value, and R and C denote the height and width of the images c and m [2].

Notably, apart from the extensively utilized PSNR, the structural similarity index measure (SSIM) is also commonly employed to assess imperceptibility, incorporating evaluations of luminance, contrast, and structural disparities. SSIM evaluates structural discrepancy between original and protected images based on loss of correlation, luminance distortion and contrast distortion. An essential augmentation to visual imperceptibility is security. This entails ensuring that the embedded watermark is not only invisible to the human eye but also resistant to detection through computational analysis, a criterion of paramount importance in secure watermarking applications, exemplified in domains like smart city planning and digital forensics.

SSIM can be computed using next formula:

$$SSIM(x,y) = \frac{\left(2\mu_x 2\mu_y + c_1\right)\left(2\delta_{xy} + c_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\delta_x^2 + \delta_y^2 + c_2\right)}, \quad (2)$$

$$c_x = \left(k_x L\right)^2, \quad (3)$$

$$\mu_x = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad (4)$$

Where μ is a mean intensity of image, which represented as set of pixels x, L is dynamic range of pixel values, K is small constant (less than 1) [3].

Robustness means that the watermarked content should be robust, meaning that, despite the public principle of the watermarking algorithm, it should be impossible to remove and should resist a wide range of attacks [1]. Watermarking robustness metrics include correlation coefficient, similarity measure, bit error rate and accuracy ratio.

Correlation Coefficient (CRC) - this metric is calculated to find compatibility present between original and extracted watermark. Value of CRC should lie between 0 and 1 [4]:

$$CRC = \frac{\sum_i \sum_j W_t(i,j) W_t'(i,j)}{\sqrt{\sum_i \sum_j W_t(i,j)^2 \times \sum_i \sum_j W_t'(i,j)^2}}, \quad (5)$$

Where $W_t$ is original image, $W_t$' is watermarked image.

Similarity Measure (SIM) is computed for assessment of extraction fidelity. It shows the similarity between extracted and embedded watermark [4]:

$$SIM\left(W_t, W_t'\right) = \frac{\sum_i \sum_j W_t(i,j) W_t'(i,j)}{\sum_i \sum_j W_t(i,j)^2}, \quad (6)$$

Where $W_t$ is original image, $W_t$' is watermarked image.

Bit Error Rate (BER) is used for representing the probability of wrongly detected binary patterns [4].

$$BER = \frac{DB}{TB}, \tag{7}$$

Where DB shows number of incorrectly decoded bits and TB shows total number of bits.

Accuracy Ratio (AR) is useful in calculating resemblance between original watermark and extracted watermark. It is computed as the ratio between number of correct bits between original and extracted watermark and total number of bits in original watermark [4].

$$AR = \frac{CB}{TB}, \tag{8}$$

Where CB shows number of correct bits and TB shows total number of bits of original watermark.

Capacity, or data payload, in a watermarking system refers to the amount of information that is embedded into the host and the number of bits that are encoded by the watermark. Depending on the application, the payload will be specified to be sufficient and facilitate the envisioned application [1]. Capacity can be measured by bits-per-pixel (BPP) metric.

## Conclusions

This work has outlined the core evaluation metrics that define the effectiveness of deep learning-based image watermarking systems. Through the analysis of imperceptibility, robustness, and capacity, it has been demonstrated that a reliable watermarking scheme must strike a careful balance between maintaining visual quality and ensuring resistance to attacks and tampering. Metrics like PSNR and SSIM quantify perceptual fidelity, while measures such as correlation coefficient, bit error rate, and accuracy ratio assess the system's robustness under distortion and extraction scenarios.

Understanding and applying these metrics is essential for advancing watermarking technologies in practical domains such as digital forensics, copyright protection, and smart infrastructure. As deep learning models evolve, the methods by which they are evaluated—ensuring that image watermarking remains a dependable component in the broader effort to secure digital media.

## REFERENCES


1. A. Malanowska, W. Mazurczyk, T. K. Araghi, D. Megías and M. Kuribayashi, "Digital Watermarking—A Meta-Survey and Techniques for Fake News Detection," in IEEE Access, vol. 12, pp. 36311-36345, 2024, doi: 10.1109/ACCESS.2024.3374201.
2. Zhong, X.; Das, A.; Alrasheedi, F.; Tanvir, A. A Brief, In-Depth Survey of Deep Learning-Based Image Watermarking. Appl. Sci. 2023, 13, 11852. https://doi.org/10.3390/app132111852
3. Zhou Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," in IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, April 2004, doi: 10.1109/TIP.2003.819861.
4. Anuja Dixit, Rahul Dixit,"A Review on Digital Image Watermarking Techniques", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.9, No.4, pp.56-66, 2017. DOI: 10.5815/ijigsp.2017.04.07



***Марчук Михайло Борисович*** - аспірант кафедри захисту інформації ВНТУ, e-mail: dzgamech@gmail.com.

***Лукічов Віталій Володимирович*** - кандидат технічних наук, доцент кафедри захисту інформації ВНТУ, e-mail: lukichov.vitalyi@vntu.edu.ua.

***Marchuk Mykhailo B.*** – Post-Graduate Student of The Department of Information Security, e-mail: dzgamech@gmail.com.

***Lukichov Vitalii V.*** - Cand. Sc. (Eng.), Associate Professor of The Department of Information Security, e-mail: lukichov.vitalyi@vntu.edu.ua.