Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

Authentication Message and Image for Digital Watermarking and Steganography Technique: A Survey

Varsha Nagle, Dr. Navneet Kaur, Pramod Kumar
Sagar Institute of Research & Technology, Bhopal, M.P., India

Abstract - With the rapid growth of digital communication and multimedia sharing over open networks, ensuring the security, authenticity, and integrity of digital data has become a major concern. Digital watermarking and steganography are widely used techniques for protecting multimedia content by embedding authentication information into digital media such as images, audio, and video. Digital watermarking primarily focuses on copyright protection, ownership verification, and tamper detection, whereas steganography aims at concealing secret messages within digital content to achieve covert communication. This survey presents a comprehensive review of message and image authentication techniques using digital watermarking and steganography. Various spatial-domain and transform-domain approaches, including Least Significant Bit (LSB), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD), are discussed and analyzed. The paper also reviews robustness, imperceptibility, and security aspects of existing methods, along with performance evaluation metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Bit Error Rate (BER). The survey aims to provide insights into current research trends, challenges, and future directions in secure multimedia authentication systems.

Keywords— Discrete Wavelet Transform, Watermarking, Steganography

I. INTRODUCTION

The rapid advancement of digital communication technologies and the widespread use of the internet have led to an exponential increase in the creation, storage, and transmission of digital multimedia content. Images, videos, and text messages are extensively shared across social media platforms, cloud services, and communication networks. While this digital revolution has improved accessibility and information exchange, it has also introduced serious challenges related to data security, authenticity, copyright protection, and unauthorized manipulation. Digital content can be easily copied, altered, or redistributed without the owner's consent, making it difficult to verify originality and integrity. As a result, robust authentication mechanisms for digital messages and images have become a critical requirement in modern multimedia systems [1, 2].

Digital watermarking and steganography have emerged as two prominent techniques for ensuring security and authentication of digital media. Although both belong to the broader domain of information hiding, they serve distinct yet complementary purposes. Digital watermarking focuses on embedding identification or authentication information directly into the host media, such as an image or video, in a manner that is either visible or imperceptible to the human eye. This embedded watermark can be used for copyright protection, ownership verification, content tracking, and tamper detection. In contrast, steganography aims to conceal the very existence of a secret message within a digital object, enabling covert communication between sender and receiver without raising suspicion [3].

Image and message authentication is particularly important in sensitive application domains such as medical imaging, military communication, forensic analysis, legal documentation, and secure online transactions. In medical systems, for example, any unauthorized modification of diagnostic images can lead to incorrect clinical decisions. Similarly, in legal and forensic applications, the authenticity and integrity of digital evidence must be guaranteed to maintain credibility. Watermarking-based authentication techniques can detect even minor alterations in image content, while steganographic approaches can securely transmit authentication codes, hash values, or encrypted messages alongside the multimedia data [4, 5.

Various watermarking and steganography techniques have been proposed in the literature, operating in either the spatial domain or the transform domain. Spatial-domain methods, such as Least Significant Bit (LSB) modification, are simple and offer high embedding capacity but are generally less robust against common image processing attacks. Transform-domain techniques, including Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD), provide improved robustness and imperceptibility by embedding information into frequency components of the image. Hybrid approaches that combine multiple transforms have also gained attention for enhancing security and resilience.

Despite significant research progress, designing an authentication system that simultaneously achieves high robustness, imperceptibility, security, and payload capacity remains a challenging task. There exists an inherent trade-off between embedding strength and visual quality, as well as between robustness and secrecy. Furthermore, emerging threats such as image forgery, deepfake generation, and sophisticated signal processing attacks demand more intelligent and adaptive authentication mechanisms [6, 7].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

In this context, this survey paper provides a comprehensive review of existing digital watermarking and steganography techniques used for message and image authentication. It analyzes their fundamental principles, performance metrics, strengths, and limitations, while highlighting recent research trends and open challenges. The survey aims to serve as a valuable reference for researchers and practitioners seeking to develop secure, reliable, and efficient multimedia authentication systems [8].

II. LITERATURE REVIEW

Begum *et al.* (2024) proposed an image watermarking approach based on the joint use of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to enhance imperceptibility and robustness. The watermark is embedded into selected wavelet sub-bands using singular values, which are known to be stable under common signal-processing attacks. Experimental results demonstrate improved PSNR and robustness against compression, noise, and filtering operations. This method is particularly effective for image authentication applications where visual quality preservation is critical while maintaining resistance to malicious modifications.

Wang *et al.* (2023) presented a comprehensive survey that unifies digital watermarking and steganography under a deep-learning-based data hiding framework. The study systematically analyzes encoder–decoder architectures, loss functions, and attack simulation strategies used in modern neural data-hiding systems. The authors highlight how deep learning enables adaptive embedding of authentication messages with improved robustness and reduced detectability. This work provides a strong theoretical foundation for integrating watermarking and steganography for secure image authentication in intelligent multimedia systems.

Qin *et al.* (2024) introduced a print–camera resistant image watermarking scheme using deep noise simulation and constrained learning. The proposed method models real-world print-and-capture distortions during training, enabling reliable watermark extraction even after severe geometric and photometric degradations. This approach is highly relevant for authentication of printed images and physical documents, where traditional watermarking techniques often fail. The results show significant improvements in robustness while maintaining acceptable visual quality.

Plata and Syga (2020) developed a robust spatial-spread deep neural image watermarking technique that leverages neural networks for embedding and extraction processes. Although introduced earlier, this method continues to influence recent works due to its ability to distribute watermark information across spatial regions, enhancing robustness against localized attacks. The study demonstrates resilience to compression, noise, and cropping, making it suitable for authentication and copyright protection in untrusted transmission environments.

Ye *et al.* (2023) proposed DbMark, a DNN-based watermarking framework designed to boost robustness through deep boosting strategies. The method improves resistance against both conventional signal-processing attacks and learning-based removal attacks. By integrating robustness-aware training objectives, the approach strengthens authentication reliability in adversarial environments. This work represents an important advancement toward secure, learning-based watermarking systems.

He *et al.* (2020) presented a high-fidelity reversible image watermarking technique based on effective prediction error-pairs modification. The scheme allows exact recovery of the original image after watermark extraction, which is crucial for sensitive applications such as medical imaging, legal evidence, and forensics. High embedding capacity and low distortion make this approach suitable for embedding authentication messages without permanent alteration of the host image.

Bose and Maity (2018) investigated spread-spectrum image watermark detection on degraded compressed sensing measurements with distortion minimization. The proposed detection framework improves watermark recovery even under severe degradation and undersampling conditions. This method is particularly relevant for secure image authentication in bandwidth-limited or noisy environments, where robustness is prioritized over embedding capacity.

Shukla *et al.* (2018) proposed a secure and high-capacity data-hiding method combining compression, encryption, and optimized pixel value differencing. The integration of encryption enhances confidentiality, while optimized embedding improves payload capacity with minimal visual distortion. This work contributes significantly to steganographic authentication systems where both secrecy and data volume are important.

Loan *et al.* (2018) developed a secure and robust digital image watermarking scheme using coefficient differencing and chaotic encryption. The chaotic encryption stage strengthens security against unauthorized extraction, while coefficient differencing improves robustness against common image processing attacks. The method effectively balances imperceptibility, security, and robustness, making it suitable for authentication and copyright enforcement applications.

Ahmaderaghi *et al.* (2018) proposed a blind image watermark detection algorithm based on the Discrete Shearlet Transform and statistical decision theory. The shearlet domain provides superior directional sensitivity, improving watermark detection under geometric distortions. The blind nature of the scheme eliminates the need for the original image during detection, which is highly desirable for real-world authentication systems.

III. DIGITAL WATERMARKING FEATURES

Joining profoundly metadata in sight and sound substance, advanced water checking systems is valuable despite the fact that, aside from accessibility of substitute components like header of a computerized record which stores meta-data. But since of following highlights the advanced watermarking system is engaging for the addition of unmistakable checks in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

video and pictures which additionally includes data about sound in sound clasp and so on [11, 12].

Imperceptibility
The commendations of media are of the feeling that watermarks couldn't be modified as installed watermarks are committed without error and they are factually. Noticeable relics in still pictures are not made by watermarks. The watermarks don't adjust the bit rate of video or does not permit any capable of being heard frequencies in sound signs.

Robustness
The utilization of computerized watermarking is by and large for distinguishing proof of possession, so it isn't subjected for any change. The methods of advanced watermarking is fit for supporting distinctive levels of durability against changes assuming any, that can be made to the substance of watermark unconcerned application. The advanced watermarks debased or be demolished because of getting undesirable and hurtful signs and geometric contortions like symmetrical computerized transformation, computerized to simple change, editing, turn, disease, scaling, dithering, a pressure and so on of the substance. Then again in the event that it utilized for the confirmation of the substance. Those ought to effectively break or pulverized at whatever point, the substance is altered for the reason of adjusting the substance which is identified.

Inseparability
It isn't conceivable either to particular or get again into the first position of the watermark after implant with watermark is finished.

Security
Individuals, who are not unapproved, are not permitted to identify and change the watermarks which have been settled immovably in the cover motion by the advanced watermarking method and the keys of watermark guarantee that to distinguish and adjust watermark just approved people are allowed.

IV. STEGANOGRAPHY

Steganography is in practice since ancient time for concealing the existence of a message inside another media. In a modern approach, the concept of contemporary steganography is explained in Figure 1. The secret message, which is to be transmitted, is embedded inside a cover file at sender premise. Digital image, text document, audio file, video file, etc. can be used as a cover file. A key might be related to the concealing procedure. The file obtained as a result of embedding message in a cover file is named as stego file which is communicated to the receiver. A similar method is followed at the receiver site, in reverse order, to extract the hidden message. Key plays the role of controlling parameter for hiding as well as extraction of the message at both the ends. Thus it is crucial for secure communication to make an intelligent choice regarding key selection.

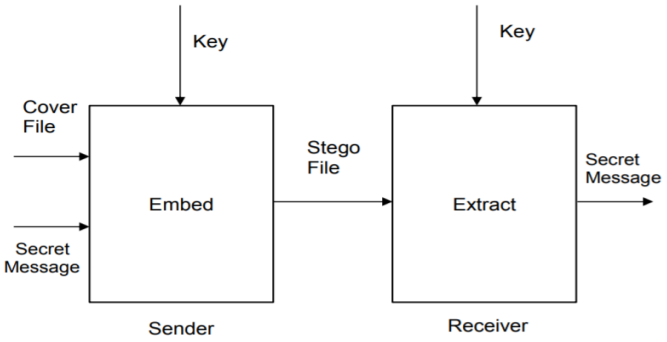

Figure 2: Steganography (Anderson, 1996)

The aforementioned discussion clarifies the goals of steganography. The prime goals of steganography itself act as an inspiration for a researcher to work in this area. It is worth to mention at this point that out of the above stated objectives; it becomes a tradeoff to achieve some of the goals while maintaining others at a satisfactory level.

V. METHODOLOGY

Watermarking Embedding procedure:
The procedure for embedding the watermark that we are following in this project is given as follows:
a. Select the host and the watermark image.
b. Apply DWT transform on both original and the watermark image.
c. Apply SVD on the LL sub band of both original and the watermark image.
d. Apply the watermarking algorithm on the two images and generate the resulting watermarked image.

Algorithm

Step 1: Input Host image, Take cover image (CI).
Step 2: Apply 2-D DWT on CI to decompose it into four subbands.
Step 3: Select sub-band LL2 of CI.
Step 4: Take watermark image (WI)
Step 5: Apply 2-D DWT on WI to decompose into four subbands.

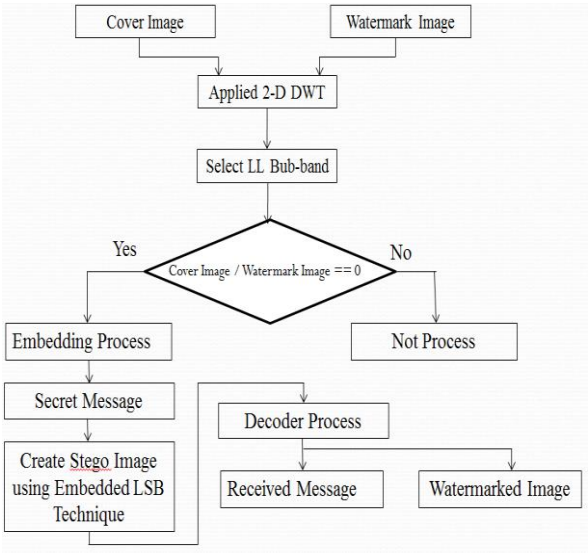

Figure 3: Flow Chart of Proposed Methodology

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

Step 6: Select sub-band LL2 of WI.
Step 7: Embedding Process
Step 8: Enter Secrete Massage
Step 9: Applied LSB technique for Encoder
Step 10: Find Stego Image
Step 11: Applied Decoder Process
Step 12: Finally get secrete message and watermarked image

DCT: The most well-known DCT meaning of a 1-D grouping of length N is given in Equation

$$F(u) = \alpha(u)\sum_{x=0}^{N-1} f(x)\cos[\frac{\pi(2x+1)u}{2N}] \quad (1)$$

The backwards discrete cosine change is the reverse of the DCT work and recreates a succession from its DCT coefficients. For u=0, 1, 2… N-1. Also, the reverse change is characterized as

$$f(x) = \sum_{u=0}^{N-1} \alpha(u)F(x)\cos[\frac{\pi(2x+1)u}{2N}] \quad (2)$$

For x=0, 1, 2… N-1. In the two conditions (1) and (2) is characterized as

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}} & for\ u = 0 \\ \sqrt{\frac{2}{N}} & for\ u = 0 \end{cases}$$

It is clear from (1) that for u=0, $c(u=0) = \sqrt{\frac{1}{N}}\sum_{x=0}^{N-1} f(x)$. Hence, the first change coefficient is the normal estimation of the example succession. In writing, this worth is alluded to as the DC Coefficient. All other change coefficients are known as the AC Coefficients. To fix thoughts, overlook the f(x) and α(u) part.

DWT

The discrete wavelet arrangement is only a tested form of Continuous Wavelet Transform (CWT) and its calculation may devour noteworthy measure of time and assets, contingent upon the goal required. The DWT which depends on sub-band coding is found to yield a quick calculation of wavelet change. It is anything but difficult to execute and decreases the calculation time and assets required. In 1983, a procedure like sub-band coding was created which was named pyramidal coding. Later numerous upgrades were made to these coding plans which brought about productive multi-goal investigation plans.
In CWT, the signs are investigated utilizing a lot of essential capacities which relate each other by straightforward scaling and interpretation. On account of DWT, a timescale portrayal of the computerized signal is gotten utilizing advanced separating procedures. The sign to be broke down is gone through channels with various cut-off frequencies at various scales.

Wavelet change can be applied to any flag with limited vitality, that is, a sign f(x) can be deteriorated by utilizing the wavelets as the premise work $\psi(t)$ as given in Eq. 3.

$$C_{a,b}(f) = \int_{\infty}^{\infty} \psi_{a,b}(t)\, f(t)dt \quad (3)$$

Where $\psi_{a,b}(t)$ is the wavelet work, got through enlargement and interpretation of the mother wavelet as given in Eq. 4.

$$\psi_{a,b}(t) = |a|^{1/2}\, \psi(at-b) \quad (4)$$

VI. CONCLUSION

This survey presented a comprehensive review of authentication message and image-based techniques in digital watermarking and steganography, highlighting their roles in ensuring data integrity, ownership protection, and secure communication. Traditional signal-processing-based methods such as DWT, SVD, DCT, and shearlet transform-based watermarking have demonstrated strong performance in terms of imperceptibility and robustness against common attacks like compression, noise addition, and filtering. Reversible watermarking approaches further enable exact recovery of original images, making them particularly suitable for sensitive applications such as medical imaging, legal forensics, and military communication.
Recent advances in deep learning have significantly transformed the landscape of information hiding. Neural-network-based watermarking and steganography frameworks enable adaptive embedding of authentication messages while improving robustness against complex distortions, including print–camera attacks and geometric transformations. The integration of attack simulation and adversarial training has enhanced the survivability of embedded information in hostile environments. However, these learning-based approaches often face challenges related to computational complexity, generalization across unseen attacks, and explainability.

REFRENCES

[1] Mahbuba Begum, Sumaita Binte Shorif, Mohammad Shorif Uddin , Jannatul Ferdush, Tony Jan, Alistair Barros 5 and Md Whaiduzzaman, “Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition for Enhanced Imperceptibility and Robustness”, MDPI 2024.
[2] Z. Wang, O. Byrnes, H. Wang, R. Sun, C. Ma, H. Chen, Q. Wu, and M. Xue, “Data Hiding With Deep Learning: A Survey Unifying Digital Watermarking and Steganography,” *IEEE Trans. Comput. Social Syst.*, vol. 10, no. 6, pp. 2985–2999, Dec. 2023.
[3] C. Qin, X. Li, Z. Zhang, F. Li, X. Zhang, and G. Feng, “Print-Camera Resistant Image Watermarking With Deep Noise Simulation and Constrained Learning,” *IEEE Trans. Multimedia*, vol. 26, pp. 2164–2177, 2024.
[4] M. Plata and P. Syga, “Robust Spatial-Spread Deep Neural Image Watermarking,” in *Proc. 2020 IEEE 19th Int. Conf. Trust, Security and Privacy in Comput. Commun.*, TrustCom 2020, 2020, pp. 62–70. *(Though originally 2020 this technique is widely cited in recent works in 2023-24)*
[5] G. Ye, J. Gao, B. Yin, W. Xie, and X. Wei, “Deep Boosting Robustness of DNN-Based Image Watermarking via Dbmark,”

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

in *Proc. 2023 Int. Conf. Culture-Oriented Science and Tech.*, CoST 2023, 2023, pp. 186–191.

[6] Wenguang He, Zhanchuan Cai and Yaomin Wang, "High-fidelity Reversible Image Watermarking Based on Effective Prediction Error-Pairs Modification", IEEE Transactions on Multimedia, IEEE 2020.

[7] A. Bose and S. P. Maity, ''Spread spectrum image watermark detection on degraded compressed sensing measurements with distortion minimization,'' Multimedia Tools Appl., vol. 77, no. 16, pp. 20783–20808, Aug. 2018.

[8] Awdhesh K. Shukla, Akanksha Singh, Balvinder Singh and Amod Kumar, "A Secure and High-Capacity Data-Hiding Method using Compression, Encryption and Optimized Pixel Value Differencing", IEEE Access, October 8, 2018.

[9] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh, and G. Mohiuddin Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption", Received January 4, 2018, accepted February 7, 2018, date of publication March 16, 2018, date of current version April 25, 2018.

[10] Baharak Ahmaderaghi ; Fatih Kurugollu ; Jesus Martinez Del Rincon ; Ahmed Bouridane, "Blind Image Watermark Detection Algorithm based on Discrete Shearlet Transform Using Statistical Decision Theory", IEEE Transactions on Computational Imaging, Volume: 4 , Issue: 1, Page s: 46 – 59, IEEE 2018.

[11] S. P. Maity and S. Maity, ''On detection improvement in MC-CDMA image watermarking on fading channel,'' Wireless Pers. Commun., vol. 100, no. 2, pp. 587–609, May 2018.

[12] X. Xie, Z. Xu, and H. Xie, ''Channel capacity analysis of spread spectrum watermarking in radio frequency signals,'' IEEE Access, vol. 5, pp. 14749–14756, Oct. 2017.

[13] Q. Zhou, G. Zang, and H. Song, ''DSSS signal detection method based on cyclic Spectrum,'' Commun. Technol., vol. 50, no. 11, pp. 2419–2425, Nov. 2017.

[14] H. Xing, X. Kang, K.-K. Wong, and A. Nallanathan, ''Optimizing DF cognitive radio networks with full-duplex-enabled energy access points,'' IEEE Trans. Wireless Commun., vol. 16, no. 7, pp. 4683–4697, Jul. 2017.

[15] Etti Mathur and Manish Mathuria, "Unbreakable Digital Watermarking using combination of LSB and DCT", International Conference on Electronics, Communication and Aerospace Technology ICECA 2017