International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

Review Paper on Authentication Information In Digital Watermarking and Stenography Technique

Vivek Upadhyay
M. Tech. Scholar
Department of Electronics and Communication
Bhabha Engineering Research Institute, Bhopal

Prof. Suresh S. Gawande
Guide
Department of Electronics and Communication,
Bhabha Engineering Research Institute, Bhopal

Abstract

The rapid expansion of digital communication and multimedia data sharing over open and insecure networks has increased the risk of unauthorized access, data tampering, and copyright violations. Ensuring the authenticity and integrity of digital content has therefore become a critical requirement in modern information security systems. Digital watermarking and steganography are two prominent information hiding techniques widely employed for embedding authentication information into multimedia content such as images, audio, and video. Digital watermarking primarily aims at copyright protection, ownership verification, and tamper detection by embedding robust or fragile authentication marks within the host signal. In contrast, steganography focuses on concealing secret authentication data in an imperceptible manner, enabling covert communication without raising suspicion.

This review paper presents a comprehensive analysis of authentication mechanisms based on digital watermarking and steganography techniques. Various spatial and transform domain approaches, including Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD), are examined with respect to imperceptibility, robustness, and security. Performance evaluation metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), payload capacity, and Bit Error Rate (BER) are discussed to assess authentication effectiveness. Furthermore, recent advancements incorporating cryptographic hashing, hybrid watermarking–steganography frameworks, and machine learning techniques are reviewed. The paper highlights key challenges, including robustness–imperceptibility trade-offs and computational complexity, and outlines future research directions for developing secure and intelligent authentication systems in multimedia applications.

Keywords: - Digital Watermarking, Steganography, Authentication Information, Multimedia Security, Data Integrity, Information Hiding, Copyright Protection, Tamper Detection

1. INTRODUCTION

The rapid advancement of digital technologies and the widespread availability of high-speed communication networks have led to an unprecedented growth in the creation, storage, and transmission of digital multimedia content. Images, audio, and video data are routinely exchanged across open and distributed networks such as the Internet and cloud platforms. While this digital transformation has improved accessibility and efficiency, it has also introduced significant security challenges, including unauthorized copying, data manipulation, identity forgery, and copyright infringement. Ensuring the authenticity and integrity of digital information has therefore become a fundamental requirement in modern multimedia security systems.

Conventional cryptographic techniques are widely used to protect sensitive information during transmission by encrypting the data. However, once the encrypted content is decrypted, cryptography alone cannot prevent illegal duplication, tampering, or misuse of digital media. Moreover, cryptographic methods do not provide inherent mechanisms to verify content ownership or detect post-decryption modifications. To overcome these limitations, information hiding techniques, particularly digital watermarking and steganography, have emerged as effective solutions for embedding authentication information directly into multimedia content [1, 2].

Digital watermarking is a technique in which authentication or ownership information is embedded into a host signal in such a way that it remains permanently associated with the original content. Depending on the application, the watermark may be visible or invisible, robust or fragile. Robust watermarking is commonly used for copyright protection and ownership verification, while fragile and semi-fragile watermarking techniques are designed to detect unauthorized modifications and ensure data integrity. Watermarking methods operate in either the spatial domain or the transform domain, with frequency-domain approaches such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD) offering improved resistance to signal processing attacks [3, 4].

Steganography, on the other hand, focuses on concealing the existence of secret information within digital media. Unlike watermarking, which prioritizes robustness and traceability, steganography emphasizes imperceptibility and secrecy. Authentication data such as hash values, digital signatures, or encrypted credentials can be hidden within multimedia content using steganographic techniques, ensuring that the embedded information remains undetectable to unauthorized users. Any alteration to the cover media can invalidate the hidden authentication data, thereby enabling tamper detection and integrity verification [5, 6].

In recent years, the integration of digital watermarking and steganography has gained increasing attention for developing hybrid authentication frameworks that combine robustness, imperceptibility, and security. Such systems are particularly valuable in sensitive applications including medical image authentication, military communication, forensic analysis, and secure cloud-based data storage. Additionally, advancements in machine learning and deep learning have further enhanced authentication systems by enabling adaptive embedding strategies, intelligent attack detection, and improved robustness against steganalysis and watermark removal attacks [7].

This review paper aims to provide a comprehensive overview of authentication information embedding using digital watermarking and steganography techniques. It examines fundamental concepts, classification methods, performance evaluation metrics, recent research trends, and existing challenges. By highlighting current advancements and future research directions, this paper seeks to contribute to the development of secure and efficient multimedia authentication systems [8, 9].

2. LITERATURE REVIEW

Mahbuba Begum et al. (2024) proposed an image watermarking technique based on the combined use of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to achieve enhanced imperceptibility and robustness. The watermark is embedded in selected wavelet sub-bands using singular values, which are less sensitive to common image processing attacks. Experimental results demonstrated high PSNR values and strong resistance against noise addition, compression, filtering, and geometric attacks. The study highlights the suitability of DWT–SVD-based watermarking for authentication and copyright protection applications where both visual quality and robustness are critical.

Qin et al. (2024) introduced a print–camera resistant image watermarking framework using deep noise simulation and constrained learning. The proposed deep learning-based approach simulates real-world print–capture distortions during training, enabling the watermark to survive severe physical attacks. The system employs a constrained optimization strategy to balance robustness and imperceptibility. Results reported in IEEE Transactions on Multimedia show significant improvements over traditional watermarking techniques, making the method highly effective for authentication in document security and offline–online media transfer scenarios.

Wang et al. (2023) presented a comprehensive survey on data hiding techniques using deep learning, unifying the concepts of digital watermarking and steganography. The authors systematically reviewed CNN-based, autoencoder-based, and adversarial learning approaches for information hiding, focusing on robustness, capacity, and security. The survey highlights how deep learning bridges the gap between watermarking and steganography for authentication purposes, offering adaptive embedding and extraction mechanisms. This work serves as a valuable reference for understanding modern intelligent authentication frameworks.

Ye et al. (2023) proposed Dbmark, a deep boosting framework designed to enhance the robustness of DNN-based image watermarking systems. The method improves watermark survivability under strong attacks by iteratively strengthening weak robustness components during training. Experimental evaluation demonstrated superior performance against compression, noise, and cropping attacks. The study emphasizes the role of deep boosting strategies in developing resilient authentication watermarking systems.

He et al. (2020) developed a high-fidelity reversible image watermarking scheme based on effective prediction error-pairs modification. The proposed method allows complete recovery of the original image after watermark extraction, making it suitable for sensitive applications such as medical and military imaging. The technique achieves high embedding capacity while maintaining excellent image quality, demonstrating its effectiveness for authentication scenarios where data integrity and reversibility are essential.

Loan et al. (2018) proposed a secure and robust digital image watermarking approach using coefficient differencing combined with chaotic encryption. The watermark is encrypted using chaotic maps before embedding, enhancing security against unauthorized extraction. Experimental results indicated strong robustness against common attacks such as compression, noise, and filtering. This work highlights the importance of integrating cryptographic techniques with watermarking for secure authentication systems.

Hussain et al. (2018) introduced a recursive information hiding scheme combining Least Significant Bit (LSB), Pixel Value Differencing (PVD) shift, and Modulus Pixel Embedding (MPE). The hybrid approach improves embedding capacity while preserving imperceptibility. The scheme is particularly relevant for steganographic authentication, as it enables efficient hidden transmission of authentication data with minimal visual distortion.

Shukla et al. (2018) presented a secure and high-capacity data hiding technique that integrates compression, encryption, and optimized pixel value differencing. The proposed method achieves improved payload capacity and enhanced security by encrypting the hidden data prior to embedding. The results demonstrate robustness against steganalysis attacks, making the method suitable for covert authentication and secure communication applications.

Bose and Maity (2018) proposed a spread spectrum image watermark detection technique for degraded compressed sensing measurements with distortion minimization. The method enhances watermark detection accuracy even under severe degradation caused by compression and noise. The approach is particularly useful for authentication in resource-constrained environments where compressed sensing is employed.

Baharak et al. (2018) developed a blind image watermark detection algorithm based on the Discrete Shearlet Transform and statistical decision theory. The method does not require the original image for watermark extraction, making it suitable for practical authentication systems. Experimental results showed improved detection performance under various signal processing attacks, demonstrating the effectiveness of shearlet-domain watermarking for robust authentication.

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

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. 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.

4. 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.

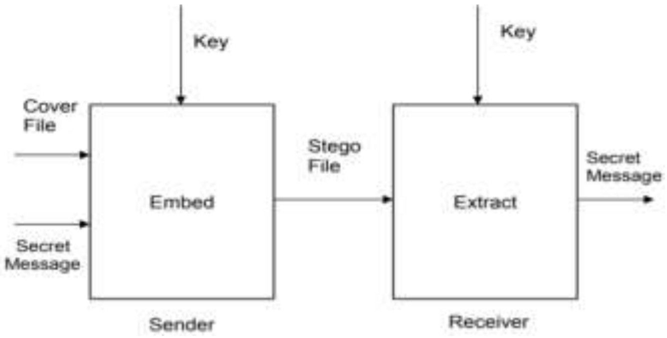

Figure 1: Steganography

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 abovestated objectives; it becomes a tradeoff to achieve some of the goals while maintaining others at a satisfactory level.

5. MRI IMAGE

MRIs employ powerful magnets which produce a strong magnetic field that forces protons in the body to align with that field. At the point when a radiofrequency current is then beat through the patient, the protons are animated, and turn out of balance, stressing against the draw of the attractive field.

At the point when the radiofrequency field is killed, the MRI sensors can identify the vitality discharged as the protons realign with the attractive field.

Attractive polarization .Very solid uniform magnet excitation .Very capable rf transmitter Acquisition, Location is encoded by angle attractive fields .Very effective audi amps Polarization, Proton have an attractive minute proton have turns like pivoting magnets Body has a great deal of protons.

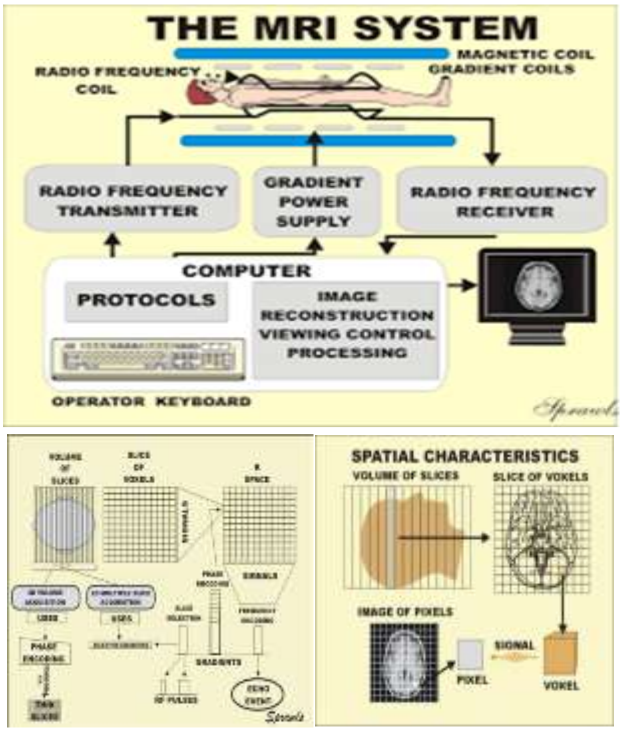

Figure 3: Working of MRI Image

6. CONCLUSION

This review paper presented a comprehensive analysis of authentication information embedding using digital watermarking and steganography techniques for securing digital multimedia content. With the increasing reliance on digital communication and multimedia data exchange, ensuring authenticity, integrity, and protection against unauthorized modification has become a critical requirement. Digital watermarking provides effective mechanisms for copyright protection, ownership verification, and tamper detection by embedding authentication data directly into the host media, while steganography enables covert transmission of authentication information with high imperceptibility. Both techniques play complementary roles in modern multimedia security systems.

The review highlighted various spatial and transform domain approaches, emphasizing that transform domain techniques such as DCT, DWT, and SVD generally offer superior robustness against common signal processing and geometric attacks compared to spatial domain methods. Performance evaluation metrics including PSNR, SSIM, BER, payload capacity, and robustness were discussed as essential criteria for assessing the effectiveness of authentication schemes. Furthermore, hybrid watermarking–steganography frameworks were identified as promising solutions that balance robustness, security, and invisibility.

Recent advancements incorporating cryptographic techniques and machine learning models have significantly enhanced authentication performance by enabling adaptive embedding strategies, intelligent attack detection, and improved resistance to steganalysis and watermark removal attacks. Despite these advances, challenges such as robustness–imperceptibility trade-offs, limited embedding capacity, computational complexity, and lack of standard evaluation benchmarks remain open research issues.

In conclusion, digital watermarking and steganography continue to be vital technologies for authentication and multimedia security. Future research should focus on AI-driven adaptive methods, lightweight authentication for resource-constrained environments, and application-specific solutions such as medical and cloud-based data authentication to develop more secure, efficient, and intelligent authentication systems.

REFERENCES

[1] Mahbuba Begum, Sumaita Binte Shorif, Mohammad Shorif Uddin, Jannatul Ferdush, Tony Jan, Alistair Barros, and Md. Whaiduzzaman, “Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition for Enhanced Imperceptibility and Robustness,” MDPI, 2024.

[2] Chao Qin, Xiaoyan Li, Zhen Zhang, Fang Li, Xiaoming Zhang, and Guang Feng, “Print-Camera Resistant Image Watermarking With Deep Noise Simulation and Constrained Learning,” IEEE Transactions on Multimedia, vol. 26, pp. 2164–2177, 2024.

[3] Zhongliang Wang, Owen Byrnes, Hao Wang, Rui Sun, Chao Ma, Hao Chen, Qiang Wu, and Min Xue, “Data Hiding With Deep Learning: A Survey Unifying Digital Watermarking and Steganography,” *IEEE Transactions on Computational Social Systems*, vol. 10, no. 6, pp. 2985–2999, Dec. 2023.

[4] Guanghui Ye, Junchao Gao, Bo Yin, Wen Xie, and Xianfeng Wei, “Deep Boosting Robustness of DNN-Based Image Watermarking via Dbmark,” in *Proc. International Conference on Culture-Oriented Science and Technology (CoST)*, 2023, pp. 186–191.

[5] Wenguang He, Zhanchuan Cai, and Yaomin Wang, “High-Fidelity Reversible Image Watermarking Based on Effective Prediction Error-Pairs Modification,” *IEEE Transactions on Multimedia*, 2020.

[6] Nazir Ahmad Loan, Nasir Nazir Hurrah, Shabir Ahmad Parah, Jong Weon Lee, Javaid Ahmad Sheikh, and Ghulam Mohiuddin Bhat, “Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption,” *IEEE Access*, 2018.

[7] Mohammad Hussain, A. W. Abdul Wahab, N. Javed, and Ki-Hyun Jung, “Recursive Information Hiding Scheme Through LSB, PVD Shift, and MPE,” *IETE Technical Review*, vol. 35, no. 1, pp. 53–63, 2018.

[8] Awdhesh Kumar 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*, 2018.

[9] Anindya Bose and S. P. Maity, “Spread Spectrum Image Watermark Detection on Degraded Compressed Sensing Measurements With Distortion Minimization,” *Multimedia Tools and Applications*, vol. 77, no. 16, pp. 20783–20808, 2018.

[10] Baharak A., Fatih K., Jesus Martinez Del Rincon, and Ahmed B., “Blind Image Watermark Detection Algorithm Based on Discrete Shearlet Transform Using Statistical Decision Theory,” *IEEE Transactions on Computational Imaging*, vol. 4, no. 1, pp. 46–59, 2018.

[11] Etti Mathur and Manish Mathuria, "Unbreakable Digital Watermarking Using Combination of LSB and DCT," in *Proc. IEEE ICECA*, 2017.

[12] Aleksei Zhuvikin, "Selective Image Authentication Using Shearlet Coefficients Tolerant to JPEG Compression," in *Proc. IEEE Conference*, pp. 681–688, 2017.

[13] N. Senthil Kumaran and S. Abinaya, "Comparison Analysis of Digital Image Watermarking Using DWT and LSB Technique," in *Proc. ICCSP*, IEEE, 2016.

[14] Morteza Heidari, Nader Karimi, and Shadrokh Samavi, "A Hybrid DCT-SVD Based Image Watermarking Algorithm," in *Proc. Iranian Conference on Electrical Engineering (ICEE)*, IEEE, 2016.

[15] Ajay Kumar Singh, Mayank Dave, and Anil Mohan, "Multilevel Encrypted Text Watermarking on Medical Images Using Spread-Spectrum in DWT Domain," *Wireless Personal Communications*, vol. 83, no. 3, pp. 2133–2150, 2015.