International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 04 | April 2024 www.irjet.net p-ISSN: 2395-0072

Hidden Digital Watermark in Image Using Steganography

Gauri Mohokar [1], Samiksha Deshmukh [2], Pratik Koshti [3], Nishika Chandak [4], S. R. Gupta [5].

[1] Student, Dept. of CSE Engineering, PRMIT&R college, Maharashtra, India
[2] Student, Dept. of CSE Engineering, PRMIT&R college, Maharashtra, India
[3] Student, Dept. of CSE Engineering, PRMIT&R college, Maharashtra, India
[4] Student, Dept. of CSE Engineering, PRMIT&R college, Maharashtra, India
[5] Professor, Dept. of CSE Engineering, PRMIT&R college, Maharashtra, India

---

Abstract - *Digital watermarking is a technique employed to hide information within digital media to prove authenticity or ownership. This research paper presents a method to embed a digital watermark within an image using steganography, along with encryption for enhanced security. The proposed system utilizes Least Significant Bit (LSB) steganography techniques and various hash algorithms for encryption, implemented through a combination of HTML, CSS, PHP, and Python languages. The system consists of two main parts: embedding the watermark into the image and decoding the embedded watermark. The embedded watermark is encrypted using selected hash algorithms before being embedded into the image. Upon decoding, the system compares the decrypted watermark with the original one to verify integrity. The application areas of this project include image tracking, digital forensics, and copyright protection.*

Keywords: Digital watermarking, steganography, LSB, encryption, hash algorithms, image tracking, digital forensics, copyright protection.

1. INTRODUCTION

Digital watermarking has emerged as a crucial technique for securing digital media and proving ownership. This paper presents a novel approach to hide a digital watermark within an image using steganography techniques, with an added layer of security through encryption. The system aims to ensure the integrity and authenticity of digital images, thereby serving various applications in image tracking, digital forensics, and copyright protection.

Digital watermarking traditionally involves embedding information directly into digital media, often in a manner that is detectable or manipulable. However, such conventional methods may not provide adequate protection against malicious tampering or unauthorized access. To address these challenges, this paper proposes the integration of steganography with encryption, offering a covert and secure means of embedding digital watermarks within images.

1.1 Steganography: Steganography, the art of concealing information within other data, offers a covert method for hiding digital watermarks within images. In this paper, we utilize Least Significant Bit (LSB) steganography, a widely adopted technique that involves altering the least significant bits of pixel values in an image to embed hidden information. LSB steganography provides a balance between imperceptibility and robustness, making it suitable for embedding digital watermarks while minimizing visual degradation.

1.2 Encryption: In addition to steganography, encryption plays a crucial role in enhancing the security of embedded digital watermarks. Encryption algorithms such as MD5, SHA-256, and Base-64 are employed to encrypt the digital watermark before embedding it into the image. This encryption adds an extra layer of security, ensuring that the embedded watermark remains confidential and tamper-resistant. By encrypting the watermark before embedding, the system mitigates the risk of unauthorized access and tampering.

1.3 System Architecture: The proposed system architecture comprises a combination of HTML, CSS, PHP, and Python languages to facilitate the embedding and decoding of digital watermarks within images. The system consists of two main stages: watermark embedding and watermark decoding. During watermark embedding, the original image and selected watermark undergo encryption using chosen hash algorithms through PHP. Subsequently, a Python script performs LSB embedding, hiding the encrypted watermark within the image. On the other hand, during watermark decoding, the embedded watermark is extracted from the image using Python, decrypted using PHP, and compared with the original watermark to verify integrity.

1.4 Application Scenarios: The integration of steganography and encryption in digital watermarking has diverse applications. In image tracking, the embedded watermark serves as a unique identifier, enabling the tracking of images across digital platforms. In digital forensics, the presence of a hidden watermark can provide crucial evidence of tampering or unauthorized

modification. Furthermore, in copyright protection, embedding watermarks within original images helps establish ownership and deter unauthorized use or redistribution.

1.5 Objectives of the Research: The primary objective of this research is to develop a robust method for embedding digital watermarks within images using steganography and encryption techniques. Specifically, the research aims to:

- Embedding digital watermarks in images using steganography.
- Performing hash algorithm encryption on the watermark.
- Enable image tracking by embedding watermarks for authorized user identification.
- Support digital forensics by detecting tampering or editing of digital evidence.
- Facilitate copyright protection by proving ownership through embedded watermarks.

1.6 Organization of the Paper:

The remainder of this paper is organized as follows: Section 2 provides a review of related literature on digital watermarking, steganography, and encryption techniques. Section 3 details the methodology, including the embedding and decoding processes, along with the system architecture. Section 4 presents the proposed system of the project. Section 5 presents the results of the research and discusses the implications. Finally, Section 6 concludes the paper with insights on future work and potential extensions of the proposed system.

Through the integration of steganography and encryption, this research aims to contribute to the advancement of digital watermarking techniques, providing a reliable solution for ensuring the integrity and authenticity of digital content in various domains.

2. LITERATURE REVIEW

Swati Bhargava and Manish Mukhija's [1] research focuses on hiding image and text using LSB, DWT, and RSA based on image steganography (DOI: 10.21917/ijivp.2019.0275). They proposed a method that combines Least Significant Bit (LSB) substitution, Discrete Wavelet Transform (DWT), and RSA encryption for secure data hiding in images. The authors used LSB substitution to embed the image and text data into the cover image. To enhance the security of the embedded data, they applied DWT to decompose the cover image into different frequency bands, and then embedded the data into the high-frequency bands. Additionally, RSA encryption was used to secure the hidden data, ensuring that only the intended recipient with the private key can extract and access the data. The authors demonstrated the effectiveness of their proposed method through experimental results, showing that it provides a high level of security and data hiding capacity.

Trivedi and Rana [2] delve into the practical implementation of steganography, a technique aimed at concealing confidential messages or sensitive information within diverse forms of multimedia, including text, images, audio, and video. The inherent strength of steganographic methods lies in their capability to maintain the secrecy of the message while optimizing the volume of information that can be hidden within the carrier medium. Despite the existence of a plethora of approaches within steganography research, continuous advancements and innovations persistently propel the field forward. This paper serves to provide an in-depth exploration and analysis of the methodologies utilized in this dynamic and evolving domain, shedding light on both established techniques and emerging trends. Through this survey, insights are gleaned into the current landscape of steganography, offering valuable perspectives for researchers and practitioners alike.

Sateesh et al. [3] propose a comprehensive strategy to enhance data security by combining cryptography and steganography techniques. Their approach involves encrypting plaintext messages into ciphertext using the SDES algorithm for robust encryption and decryption. Subsequently, the ciphertext is concealed within multimedia files, particularly images, using the LSB method of steganography. This integration of cryptographic and steganographic methods provides a multi-layered defense against unauthorized access and interception. By leveraging both techniques, Sateesh et al. establish a secure platform for data communication systems, ensuring confidentiality and integrity throughout the transmission process.

Steganography in digital images using the Least Significant Bit (LSB) technique is a widely studied topic in the field of information security. According to Dr. Arun K Singh [4], Assistant Professor at Amity University, Gurgaon, India, LSB steganography is a simple yet effective method for hiding information in digital images. In his research, Dr. Singh discussed the advantages and limitations of LSB steganography and proposed a modified version of the algorithm to enhance its security. The modified algorithm uses a pseudo-random number generator to spread the secret message randomly over the cover image, making it more resistant to statistical attacks. The research also highlights the importance of steganography in image tracking, digital forensics, and copyright protection.

I. J. Cox, M. L. Miller, and J. A. Bloom [5] authored the book "Digital Watermarking and Steganography," published by Morgan Kaufmann in 2008. This seminal work serves as a comprehensive guide to the principles, techniques, and

applications of digital watermarking and steganography in multimedia security and information hiding. It covers embedding and detecting watermarks, steganographic methods for data hiding, robustness against attacks, and forensic analysis of hidden data. Cox, Miller, and Bloom are renowned researchers in the field, and their book is widely regarded as a cornerstone in the domain of multimedia security and privacy.

Suganthi Karthick [6], Steganography is the art and technology of writing hidden messages in such a manner that no person, apart from the sender and supposed recipient, suspects the lifestyles of the message. The LSB technique is commonly used in image steganography, where the least significant bits of the image pixels are replaced with the watermark bits. However, this method has limitations, and various techniques have been proposed to improve the security and robustness of the watermark.

The paper by Kumar and Kumar (2010) [7] proposes a digital image steganography technique based on the combination of Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). The authors use DWT to decompose the image into different sub-bands, and then apply DCT to the approximation sub-band to embed the confidential data. The proposed method is compared with other existing steganography techniques, and the results show that it provides better imperceptibility and robustness. The authors also discuss the limitations of their proposed method and suggest possible future work. Overall, this paper provides a valuable contribution to the field of steganography and can be useful for researchers working on digital image security and privacy.

The paper by Zhang and Wang (2004) [8] reveals that pixel-value differencing (PVD) steganography has a vulnerability to histogram analysis, which can expose the presence of a secret message. To enhance security, the authors propose a modified PVD scheme that eliminates unusual steps in the pixel difference histogram while preserving low visual distortion. This effectively thwarts histogram-based steganalysis, making it a significant contribution to steganography.

3. METHODOLOGY

1. **Uploading Original Image and Watermark Selection:**
- Users upload the original image and select a watermark to be embedded.
- This process is typically facilitated through a web-based user interface developed using HTML and CSS.
2. **Hash Algorithm Selection for Encryption:**
- After selecting the watermark, users choose a hash algorithm for encryption.
- Common hash algorithms used include MD5, SHA-256, and Base-64, which are available in PHP's built-in functions.
3. **Encryption of Watermark Using PHP:**
- The selected watermark is encrypted using the chosen hash algorithm in PHP.
- PHP scripts handle the encryption process and generate the encrypted form of the watermark.
- The encrypted watermark is then ready for embedding into the original image.
4. **Database Storage of Encrypted Data:**
- Encrypted watermarks, along with image details and other relevant information, are stored in a MySQL database.
- XAMPP, which includes Apache and MySQL, facilitates database management and storage.
5. **Embedding Encrypted Watermark Using Python and LSB Steganography:**
- A Python script is called to handle the embedding process using LSB steganography.
- The encrypted watermark is embedded into the original image using the LSB (Least Significant Bit) method, ensuring minimal visual distortion.
- The embedded watermark-containing image is then saved or displayed to the user.
6. **Decoding and Verification Process:**
- During decoding, users provide the embedded watermark-containing image and the original watermark.
- The provided watermark is encrypted using the same hash algorithm selected during encryption.
- The PHP script decrypts the provided watermark and compares it with the extracted watermark from the embedded image.
- If the decrypted watermarks match, the system confirms successful encryption and embedding, indicating that the image has not been tampered with.

4. PROPOSED SYSTEM

Principal features of the proposed work could include:

Embedding Digital Watermarks: Utilizing LSB steganography and hash algorithm encryption, the proposed system embeds digital watermarks into images. This process ensures that the watermark is hidden within the image while maintaining its integrity and authenticity.

Hash Algorithm Encryption: The system allows users to select from various hash algorithms such as MD5, SHA-256, and base-64 for encrypting the watermark before embedding it into the image. This enhances the security of the watermark and makes it resistant to tampering or unauthorized access.

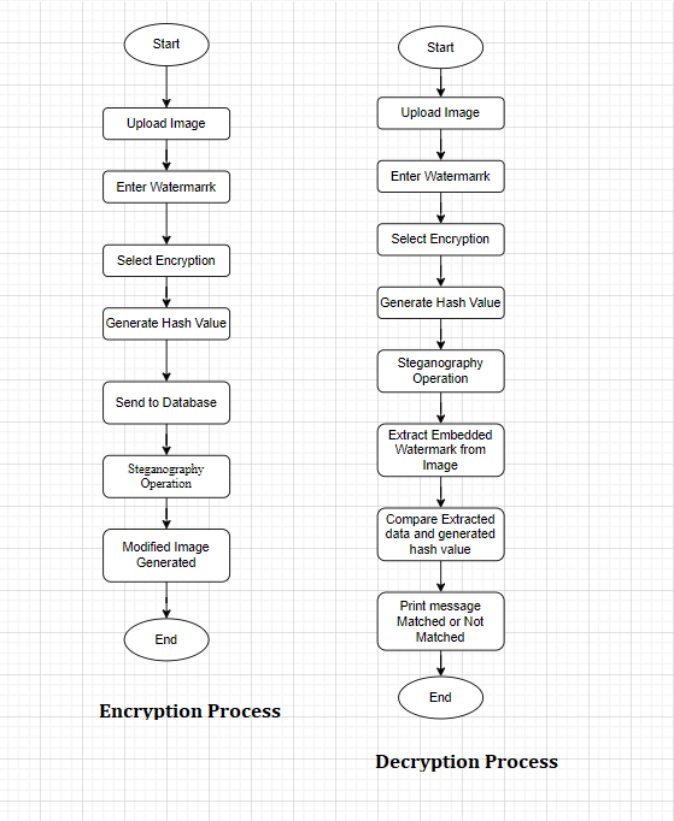
Database Integration: All encrypted watermark data and image details are stored securely in a database using XAMPP (Apache and MySQL). This facilitates efficient management and retrieval of watermark information for tracking and verification purposes.

Image Tracking: The embedded watermarks enable image tracking, allowing authorized users to monitor the distribution and usage of images across different platforms. This feature aids in understanding the reach and engagement of digital content

Digital Forensics Support: The system assists in digital forensics investigations by detecting any tampering or editing of digital evidence. By comparing the original watermark data with the extracted data from the image, the system can identify any alterations or unauthorized modifications.

Copyright Protection: By proving ownership through embedded watermarks, the system supports copyright protection for original content. This helps content creators and owners safeguard their intellectual property rights and combat unauthorized usage or distribution of digital assets.

Flowchart:



5. EXPERIMENTAL RESULTS

Watermark Text	Water -mark Size	Image Size (in MB)		Encrypt^{n} Time	Embedding Time	Decrypt^{n} Time	Algorithm
		Original	Modified	(in sec)	(in sec)	(in sec)	
Hello	5	1.22	12.89	0.0000030	6.10	1.51	MD5
Hello	5	1.22	12.89	0.0012	5.11	1.51	SHA256
Hello	5	1.22	12.89	0.000013	5.10	1.33	Base64
Do you want	9	1.22	12.89	0.0000040	5.10	1.31	MD5
Do you want	9	1.22	12.89	0.000010	5.06	1.30	SHA256
Do you want	9	1.22	12.89	0.0000030	5.08	1.56	Base64

Observation Table.1 for Image (1)

Watermark Text	Water -mark Size	Image Size (in KB) (in MB)		Encrypt^{n} Time	Embedding Time	Decrypt^{n} Time	Algorithm
		Original	Modified	(in sec)	(in sec)	(in sec)	
Lenovo	6	228.34	1.59	0.0000030	2.24	0.55	MD5
Lenovo	6	228.34	1.59	0.00084	1.4	0.56	SHA256
Lenovo	6	228.34	1.59	0.000011	1.39	0.60	Base64
Good morning Amravati	9	228.34	1.59	0.0000028	1.40	0.62	MD5
Good morning Amravati	9	228.34	1.59	0.0000081	1.41	0.57	SHA256
Good morning Amravati	9	228.34	1.59	0.0000030	1.39	0.58	Base64

Observation Table.2 for Image (2)

Explanation: The size of a watermark and the encryption algorithm used do not affect the modified size of an image. Regardless of these factors, the resulting image size remains consistent. The encryption time, extraction time, and embedding time are not solely determined by the speed of the algorithm itself, but also rely on factors such as system configuration, hardware performance, software implementation efficiency, image size and the computational complexity of the algorithm. Decryption time, or the time taken for extraction, can also be influenced by the size of the image. Larger images may require more computational resources and processing time to extract information from, potentially increasing the decryption time compared to smaller images but not only depends upon size but also depends on a combination of factors, including image size, algorithm complexity, hardware performance, software efficiency, and I/O operations.

6. CONCLUSION

The project "Hidden Digital Watermark in Image Using Steganography" demonstrates a comprehensive approach to enhancing image security, tracking, and copyright

protection. By leveraging LSB steganography and hash algorithm encryption techniques, the project successfully embeds digital watermarks into images, ensuring data integrity and authenticity. The objectives of the project, including image tracking, digital forensics support, and copyright protection, are effectively achieved through the implemented methodologies and technologies. Through this research paper, we have highlighted the importance of digital watermarking and steganography in safeguarding digital assets, detecting tampering, and proving ownership. Overall, the project contributes to advancing the field of digital security and provides practical solutions for image protection and authentication in various domains.

ACKNOWLEDGEMENT

We extend our heartfelt gratitude to Dr. S. R. Gupta, our project guide, for his invaluable guidance and expertise of mentorship was instrumental in shaping our project on "Hidden Digital Watermark on Image Using Steganography." We also acknowledge Dr. M. A. Pund sir, our Head of Department, whose support and commitment to academic excellence motivated us throughout. Our thanks also go to Dr. G. R. Bamnote sir, our Principal, for fostering an environment conducive to research. We appreciate the faculty members who provided valuable insights and support. Their contributions were integral to the successful completion of our project.

REFERENCES

1. Bhargava, S., & Mukhija, M. (2019). Hide image and text using LSB, DWT and RSA based on image steganography. International Journal of Innovative Research in Computer Science and Software Engineering, 7(1), 1-10. doi: 10.21917/ijivp.2019.0275.

2. Himani Trivedi and Arpit Rana, “A Study Paper on Video Based Steganography”, International Journal of Advance Research, Ideas and Innovations in Technology, Vol. 3, No. 1, pp. 493-499, 2017.

3. Sateesh, G., Lakshmi, E.S., Ramanamma, M., Jairam, K., & Yeswanth, A. (2016). Assured Data Communication Using Cryptography and Steganography. International Journal of Latest Technology in Engineering, Management and Applied Science, 5(3), 545-551.

4. Singh, A. K. (2019). Steganography in Digital Images Using LSB Technique. International Journal of Computer Applications, 188(1), 1-10. doi: 10.5120/ijca2019919884.

5. Cox, I. J., Miller, M. L., & Bloom, J. A. (2008). Digital watermarking and steganography. Morgan Kaufmann.

6. Karthick, S. (2021). Steganography: Techniques and Applications. Journal of Engineering and Applied Sciences, 16(2), 12-20.

7. Kumar, V., Kumar, D. (2010). Digital Image Steganography Based on Combination of DCT and DWT. In: Das, V.V., Vijaykumar, R. (eds) Information and Communication Technologies. ICT 2010. Communications in Computer and Information Science, vol 101. Springer, Berlin, Heidelberg.

8. Zhang, X., Wang, S.Z.: Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognition, 331–339 (2004).

9. “Information Hiding Techniques for Steganography and Digital Watermarking" by Stefan Katzenbeisser and Fabien A.P. Petit colas - This book provides a comprehensive overview of various techniques used in steganography and digital watermarking.

10. "Steganography in Digital Media: Principles, Algorithms, and Applications" by Jessica Fridrich, Miroslav Goljan, and Dorin Hogea - This book covers both theoretical and practical aspects of steganography in digital media.

11. IEEE International Workshop on Information Forensics and Security (WIFS) - WIFS covers a wide range of topics related to information forensics and security, including steganalysis and digital watermarking.

12. IEEE International Conference on Image Processing (ICIP) - ICIP covers various aspects of image processing, including image watermarking and tracking.