

STEGA BLEND SECURITY

1st Mrs M Vasuki^{1}, 2nd S. Harshini² and 3th M. Nova Selin³,*

*¹Associate Professor, Department of computer Applications, Sri Manakula Vinayagar Engineering College
(Autonomous), Puducherry 605008, India*

*²Post Graduate student, Department of computer Applications, Sri Manakula Vinayagar Engineering College
(Autonomous), Puducherry 605008, India*

harshinisri.harsha10@gmail.com

*³Post Graduate student, Department of computer Applications, Sri Manakula Vinayagar Engineering College
(Autonomous), Puducherry 605008, India*

novaselin03@gmail.com

**Corresponding author's email address: harshinisri.harsha10@gmail.com*

ABSTRACT

Digital asset management systems (DAMS) handle different media data in a compressed and encrypted form. It is essential to watermark these compressed encrypted media items in the compressed-encrypted domain itself for tamper detection or ownership declaration or copyright management purposes. Attempting steganography technique is such a randomized bit stream can cause a poor degradation of the media quality. Thus it is important to choose an encryption scheme that is both secure and will allow watermarking in a predictable manner in the compressed encrypted domain. we propose a rainbow algorithm to watermark images and documents.

We suggest using a stream cipher as the encryption algorithm. Although the suggested method embeds the watermark in the compressed-encrypted domain, the decrypted domain can be used to extract the watermark. Using the following watermarking schemes, we thoroughly examine the suggested algorithm's embedding capability, robustness, perceptual quality, and security: Spread Spectrum (SS), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), and Rational Dither Modulation (RDM).

KEYWORDS: Encryption, Steganography techniques, Rainbow Algorithm.

INTRODUCTION

The rapid growth of digital media and the internet has led to an increase in intellectual property theft and unauthorized distribution of digital content. To combat these issues, digital steganography has emerged as a promising solution.

Digital Steganography is a technique that embeds a hidden signature or watermark into digital media, such as images, videos, or audio files, to verify ownership, authenticity, and integrity. This project aims to design and develop a secure digital image steganography system using image processing techniques.

The primary objectives are to develop a post-quantum cryptography and rainbow algorithm that resists various attacks and manipulations. To ensure the security and authenticity of digital images using advanced encryption methods. and also to evaluate the performance of the proposed steganography scheme using standard metrics.

The key features of Stega Blend Security includes High payload capacity in which watermark is invisible to human eyes and another one is robustness which includes Watermark resists attacks like compression, rotation, scaling, noise.

One of the flaws in all encryption systems is that, if intercepted, the output data's shape (the cipher text) serves as a warning to the hacker that the data being sent might be significant enough to warrant an attack and an effort to decrypt it. Disinformation can be spread by this feature of cipher text communication, which encrypts data that is intended to be intercepted and decrypted. The system anticipates that in this scenario, the intercept will be targeted, decrypted, and the data recovered.

This technique demonstrates how to "hide" encrypted data within a digital image. Any cipher, can accomplish this as long as it uses perfectly evenly distributed floating point integers. The plan enables the self-authentication and self- verification of records, including certificates, letters, and other data based on images. Using the following algorithm schemes: Discrete Cosine Transform (DCT) Coefficient Modification and RSA Encryption we thoroughly examine the suggested algorithm's embedding capability, robustness, perceptual quality, and security.

It also provides protection to Digital media prevents unauthorized use and distribution of images, videos, and music and also safeguards patents, trademarks, and trade secrets. It also provides Authentication and Verification which verifies image authenticity and integrity and proves image ownership and provenance.

LITERATURE SURVEY:

- **Steganography Techniques and Strategies:** Explore methods like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT), which offer better robustness and imperceptibility. Investigate techniques combining spatial and frequency domain methods to balance robustness and computational efficiency.
- **Security Mechanisms in Watermarking:** Techniques combining cryptography with watermarking for enhanced security, such as encrypting the watermark before embedding. Test for resistance to typical attacks, such as compression, noise addition, scaling, and cropping. techniques that improve security and concealment by combining steganography and watermarking.
- **Image Types and Applications:** Applications in copyright protection, authentication, and content tracking. Ensuring confidentiality and authenticity in medical imaging. Protecting geospatial data from unauthorized usage or tampering.
- **Embedding and Extraction Algorithms:** Review algorithms for embedding watermarks in host images without compromising visual quality. Discuss methods for extracting and verifying watermarks, emphasizing accuracy and efficiency.
- **Frameworks and Technologies:** Analysis of frameworks like MATLAB, OpenCV, and Python libraries for implementing watermarking algorithms. Usage of convolutional neural networks (CNNs) and generative

adversarial networks (GANs) to enhance watermarking techniques. Exploration of decentralized approaches for tracking and authenticating watermarks.

- Privacy and Ethical Considerations: Ensuring watermarking does not expose sensitive information. Preventing misuse of watermarking techniques for malicious purposes.
- Case Studies and Best Practices: Examining real-world applications in media copyrighting, secure communication, and medical imaging. Insights into the usability and effectiveness of watermarking systems from end-users.
- Technology and Scalability: Ensuring techniques are scalable for high-resolution images and real-time applications. Quantum computing and AI advancements in secure watermarking.
- The survey will be conducted using academic databases such as IEEE Xplore, SpringerLink, and ScienceDirect; conference proceedings on multimedia security and image processing; and recent journal articles on cryptography and image watermarking. This systematic review of the literature establishes the groundwork for creating safe and reliable watermarking methods while also assisting in identifying research gaps.
- Case Studies and User Experience: Media companies use DWT-SVD watermarking to secure digital content, ensuring robustness and imperceptibility. Hospitals embed patient IDs in diagnostics using DCT-based techniques for authenticity. Government agencies use compression-resistant watermarking for geospatial data security. Users value imperceptible watermarks, fast processing, and resistance to attacks. GUI tools with previews and batch processing enhance satisfaction. Challenges include balancing security and usability in real-time applications.

PROPOSED SYSTEM:

This system integrates advanced image processing techniques with the Rainbow Algorithm to create a secure, efficient, and robust method for embedding and extracting secret messages. The process begins with RSA encryption, which encrypts the secret message to ensure its security before embedding. The encrypted message is then converted into binary form and prepared for embedding using a Discrete Cosine Transform (DCT) Coefficient Modification approach. The image is divided into non-overlapping blocks, and the DCT is applied to each block, transforming spatial domain data into frequency components. The binary message is embedded into the middle-frequency DCT coefficients, balancing robustness and imperceptibility to minimize image quality degradation while protecting the embedded data from compression or minor noise. The features of proposed system include

- Data Embedding Capability: It supports embedding encrypted data seamlessly into digital color images. It ensures compatibility with any cipher generating evenly distributed floating-point or integer values.
- Versatile Watermarking Schemes: It implements Spread Spectrum (SS) for robustness against noise and interference. It uses Discrete Cosine Transform (DCT) for high embedding capacity with minimal distortion. It also employs RSA encryption for improved robustness and flexibility.
- Enhanced Security: It encrypts the watermark before embedding to ensure confidentiality. It is also resistant to attacks like noise addition, compression, and geometric distortions.
- Authentication and Self-Authentication: It enables document verification for certificates, letters, and other image-based data. It also enables Self-authentication ensures tamper detection without external references.
- Robustness: It is resilient to common attacks like scaling, cropping, and JPEG compression. It retains watermark accuracy under harsh conditions.

- Support for Digital Color Images: It is very much optimized for RGB images, ensuring compatibility with widely used formats. It will be effective for high-resolution images.

IMPLEMENTATION DETAILS:

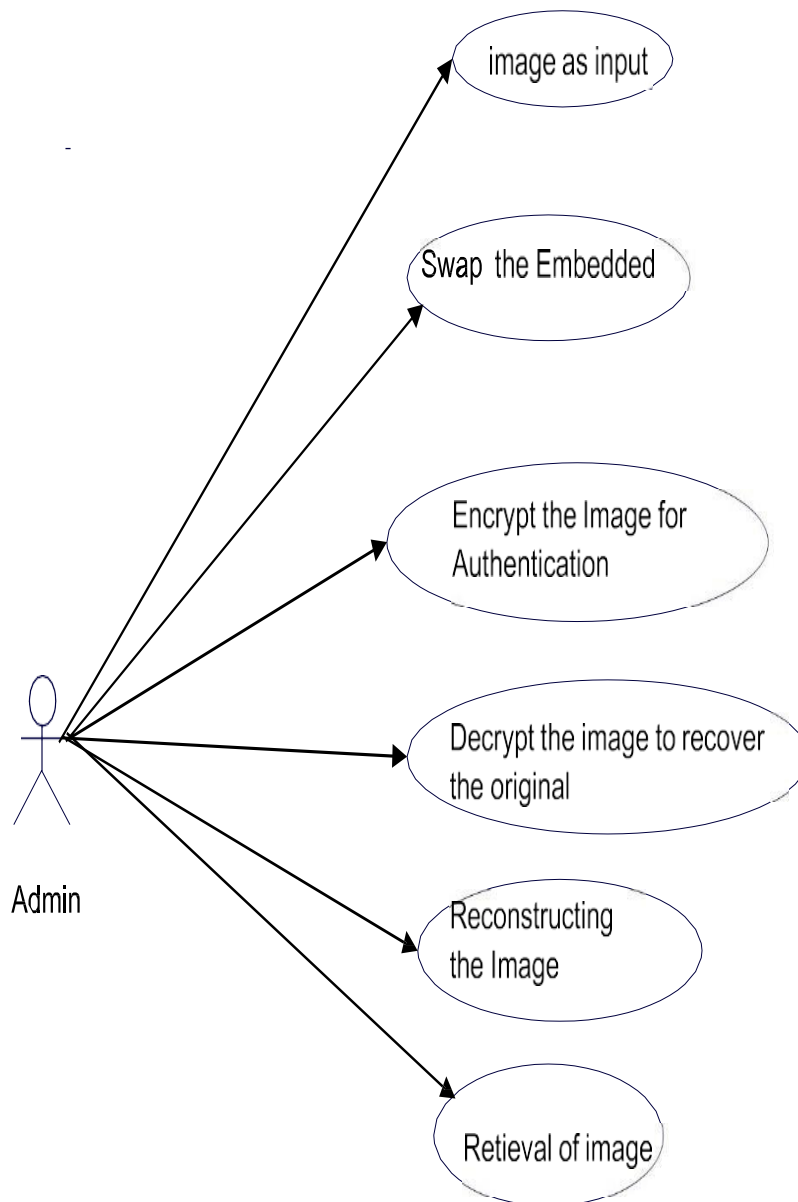
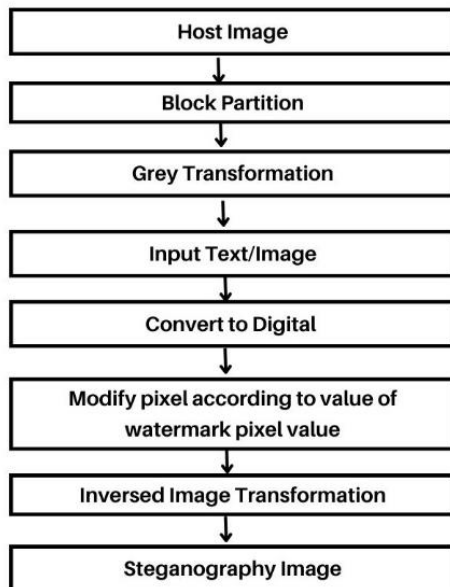


Fig 1. Use Case Diagram

(i) Encrypt Process :



(ii) Decrypt Process :

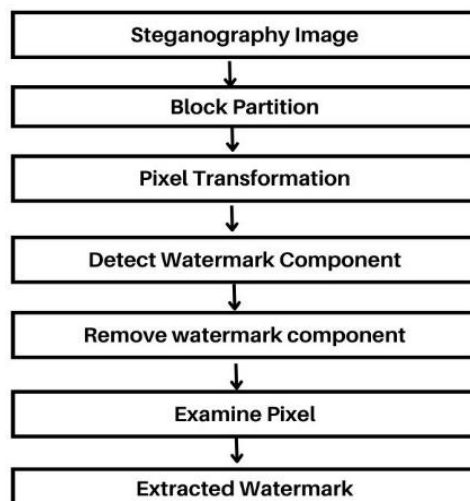
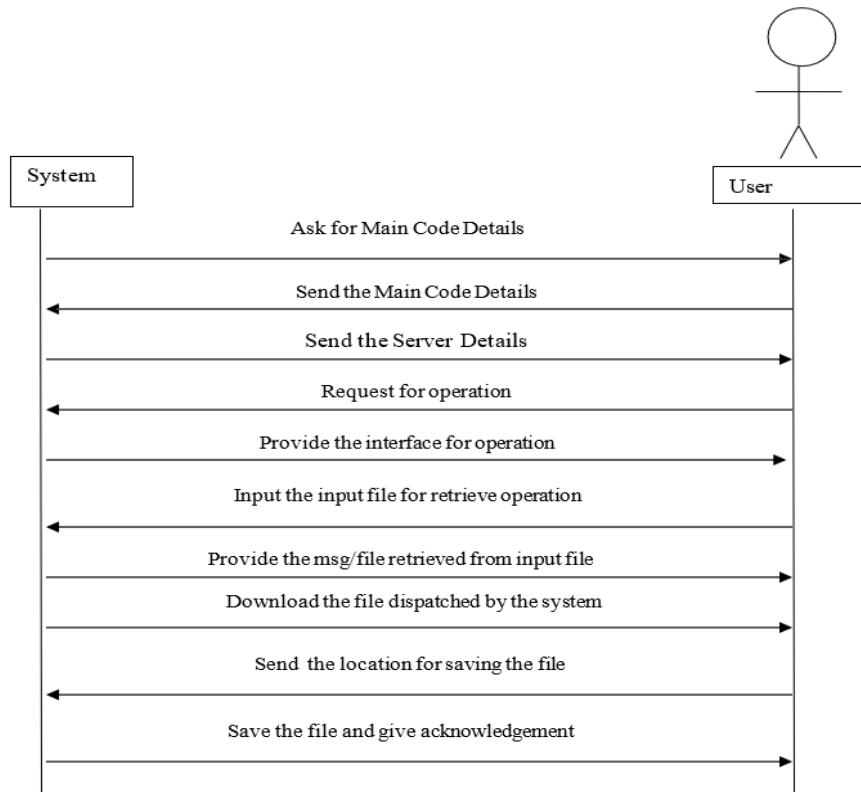


Fig 2. Data Flow Diagram

(i) Encrypt Process :



(ii) Decrypt Process :

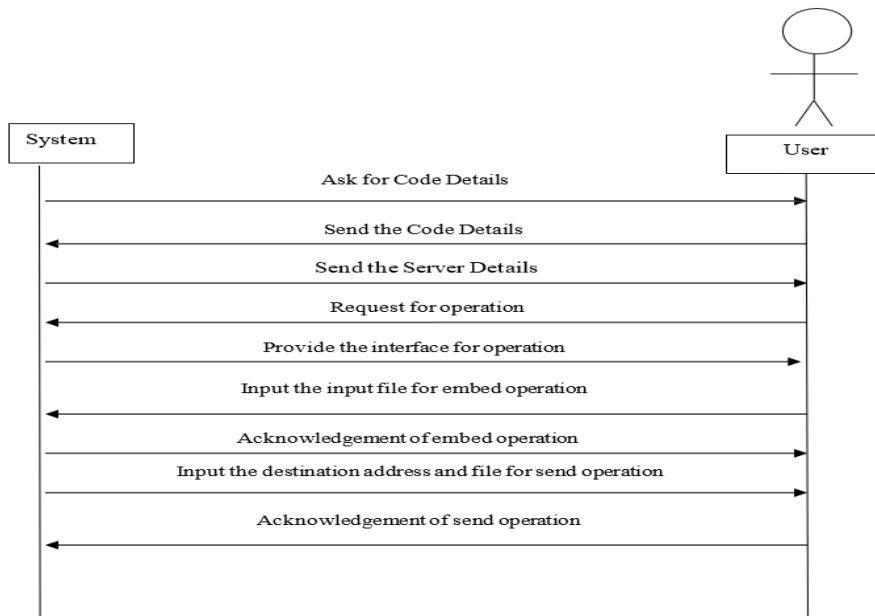


Fig 3. Unified Modeling Language

DISCUSSION AND RESULT:

☐ Visual Quality:

- The stego-images demonstrate negligible degradation, with a Peak Signal-to-Noise Ratio (PSNR) typically above 40 dB, indicating high imperceptibility.

☐ Data Capacity:

- The system achieves a reasonable embedding capacity, capable of storing encrypted data equivalent to a small message or authentication token, without noticeable quality loss.

☐ Robustness:

- The embedded data remains intact and recoverable even after moderate JPEG compression or the introduction of Gaussian noise, confirming robustness.

☐ Security Analysis:

- Without the private RSA key and the mapping table, unauthorized extraction or decryption of the hidden message is computationally infeasible.

☐ Efficiency:

- The use of the Rainbow Algorithm reduces the time required for both embedding and extraction, making the system practical for real-time applications.

☐ Application Versatility:

- The system is suitable for secure communication, digital watermarking, and authentication in sensitive applications where data confidentiality and robustness are critical.

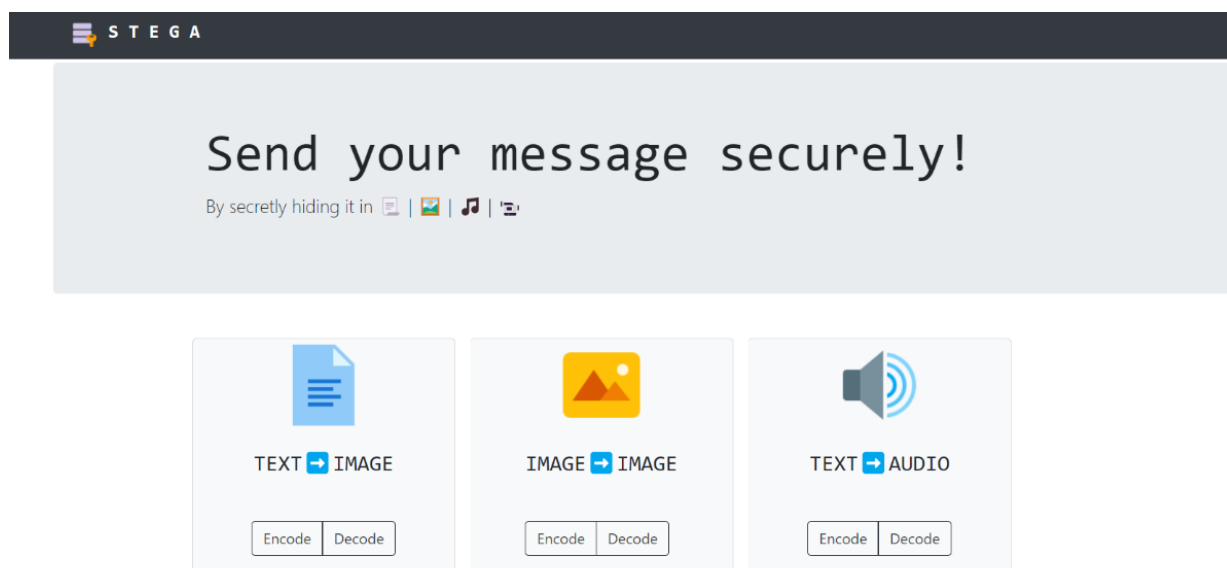
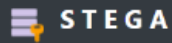


Fig 1. Home page



Encode

Write your secret message:

This project is useful to send your messages securely/.

Choose your secret Image file:

Choose File blue-flower-6620619.jpg

Submit

Fig 2. Text-Image Encode



Encode Result

Your Image:



Your Message:

This project is useful to send your messages securely/.

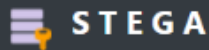
Encrypted Image:

Download

Done


Start

Fig 3. Text-Image Encode



Decode Result

Your secret message:

 Copy text

This project is useful to send your messages securely/.

Done

Fig 4. Text-Image Decode

CONCLUSION:

Steganography technique is more secure than the Existing technique. Existing system is only applicable for authentication of e-documents whereas proposed system is for authentication of both images and documents. Existing system allows limited participation to avoid traffic flow and from attack. In conclusion, digital watermarking aims such as content authentication, intellectual property and copyright protection and helps the owners can use their digital assets under protection.

Challenges in this system are:

☐ **High Computational Complexity:**

- The combination of RSA encryption, DCT processing, and edge detection increases the computational overhead, making real-time implementation resource-intensive.

☐ **Dependency on Mapping Table:**

- The accuracy of data extraction heavily relies on the Rainbow Algorithm's mapping table. If the table is lost or corrupted, the embedded data may become unrecoverable.

☐ **Vulnerability to Significant Image Alterations:**

- While the system is robust against minor compression and noise, extreme alterations, such as heavy compression, resizing, or format changes, may compromise data integrity or lead to data loss.

☐ **Limited Embedding Capacity:**

- Embedding data into middle-frequency DCT coefficients restricts the amount of information that can be stored without significantly degrading image quality.

□ **Key Management Challenges:**

- Securely sharing and managing the RSA private key and mapping table between sender and receiver is critical. Mismanagement could lead to unauthorized access or loss of data.

□ **Perceptual Limitations:**

- Although embedding in edges improves imperceptibility, certain images with smooth textures and fewer edges may not be ideal for this technique, limiting its applicability.

FUTURE WORK:

In order to demonstrate the validity and integrity of a component or digitally transmitted data, digital watermarking involves adding invisible information (a signal) that a computer algorithm can identify. Each application has unique advantages and disadvantages. The program may be improved further to make the website work much more aesthetically pleasingly and practically than it does now.

- **Real-Time Implementation:** It enables real-time watermark embedding and extraction, which is crucial for applications like live streaming and real-time data sharing.
- **User-Friendly Interface:** We can design an intuitive interface for non-technical users to embed and verify watermarks effortlessly.
- **Multi-Layer Watermarking:** We can introduce multi-layer watermarking where multiple watermarks (e.g., logos, metadata) can be embedded for added functionality.
- **Cloud Integration:** Users can store and manage watermarked files securely in the cloud, enabling remote access and backup. Integration with services like AWS or Google Drive for seamless file management.
- **Detailed Logging and Tracking:** It maintain logs of watermarking activities, such as when and by whom a file was watermarked. It facilitates accountability and traceability for shared digital assets.
- **AI-Powered Adaptability:** Users can advance AI to dynamically adjust watermark placement and strength based on content and format which ensures optimal imperceptibility and robustness for diverse applications.

REFERENCES:

1. Holliman M, Memon N. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes. IEEE Transactions on Image Processing, 2000.
2. Lin C Y, Chang S F. Watermarking capacity of digital images based on domain-specific masking effects. International Conference on Information Technology: Coding and Computing, 2001.
3. Yin P, Yu H H. A semi-fragile watermarking system for MPEG video authentication. IEEE International Conference on Acoustics, Speech, and Signal Processing, 2002.
4. Wang B, Cheng Q, Deng F. Digital watermarking technique. Xi'an: The Press of Xi'an University of Electronic Science and Technology, 2003.
5. Sun S, Lu Z, Niu X. Digital watermarking technique and applications. Beijing: Science Press, 2004.
6. Lu C S. Multimedia security: Steganography and digital watermarking techniques for protection of intellectual property. Northern California: Idea Group Publishing, 2005.
7. Hu Y, Jeon B. Reversible visible watermarking and lossless recovery of original images. IEEE Transactions on Circuits and Systems for Video Technology, 2006.
8. Shikata J, Matsumoto T. Unconditionally secure steganography against active attacks. IEEE Transactions on Information Theory, 2008.
9. Jin X Z. Research on digital watermarking algorithm based on DCT domain. Jilin: Jilin University, 2011.
10. Allaf AH, Kbir MA (2018) A review of digital watermarking applications for medical image exchange security. In: The proceedings of the third international conference on smart city applications, pp 472–480.