IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 1, May 2025

Impact Factor: 7.67

Enhanced Image-Based Security: Integrating Cryptography, Steganography and Watermarking

Dr. D. Vijaya Lakshmi[1], Baireddy Sai Chandhan[2], Kalvakunta Shriya[3]

[1]Professor & HOD, Mahatma Gandhi Institute of Technology, Hyderabad, India

[2,3]UG Student, Mahatma Gandhi Institute of Technology, Hyderabad, India

Abstract: *The rise of digital communication has brought about major security issues when it comes to keeping sensitive data safe and unchanged during transmission. Regular encryption methods do a good job of hiding messages but don't do much to check if the data has been messed with while it's being sent. In the same way, steganography tricks can hide data in pictures, but they often can't stop someone from changing the data without permission. The big problem is coming up with a safe way to communicate that not protects what's in the messages but also lets us know if someone has tampered with them while they're being sent. To tackle these problems, we want to create a strong safe communication system that brings together AES encryption, LSB steganography using images, and fragile watermarking. This system will make sure the encrypted message is hidden in a picture keeping it secret and making it hard for unauthorized people to find. At the same time, the fragile watermark will act as a way to spot tampering allowing us to check if the image has been changed. This multi-layer approach will deal with both keeping things secret and making sure they stay unchanged offering a complete answer for sending data. The communication system we're suggesting will provide an advanced way to make sure sensitive information is exchanged protecting both unauthorized access and tampering.*

Keywords: Cryptography, Steganography, Watermarking, AES Encryption, Cipher Block Chaining, Least Significant Bit (LSB) Steganography, Fragile Watermarking, Tamper Detection, Confidentiality, Integrity Verification, Secure Communication, Image-Based Security, Stego Image

I. INTRODUCTION

The quick growth of online communication has made participating information easier, but it's also made us more open to online troubles. These include data leaks, people getting in without authorization, and intruding with our information. The usual ways we try to stay safe, like scrabbling our data or hiding it in filmland try to keep effects secret. But they frequently forget about making sure the data stays the same and proving it's real. This design suggests a safe way to communicate that has numerous layers. It combines AES encryption (a way to scramble data), LSB image steganography (hiding word in filmland), and a type of watermarking that changes and is easy to break. AES encryption makes sure that private information stays private. individualities enjoying the correct key have the capability to crack and understand the communication. The system hides translated data in a cover image using LSB steganography taking advantage of how digital images can hide dispatches without drawing attention. To boost security, it adds a changing fragile watermark to the stego image. This watermark breaks or foundations if anyone changes the image, showing possible tampering or unapproved changes. By using these styles together, the system offers full protection keeping the transferred information secret and allowing druggies to check if it's been altered. It aims to fix the weak points of old security systems by creating a secure, secure, and tamper- evidence communication system that can stand up to moment's cyber pitfalls.

II. EXISTING SYSTEM

The SMH- SWE system has the thing to conceal secret dispatches in images without changing the vessel images. This happens through a two- stage frame with an image conflation module and an image mapping module. The system uses inimical networks to produce images and hide secret dispatches in their idle space. It also uses a trained bus- encoder to

DOI: 10.48175/568

separate the image structural and texture features. The system also puts the main part of the secret communication into the created image by switching the structural attributes. The big problem with this conflation system is that the secret communication cannot be rebuilt at the receiver's end indeed without an attack. The conflation module might have birth crimes. To allow full recovery of the secret communication, the system inserts the remaining communication corridor into chosen vessel images through statistical hash matching. The leftover communication part, which holds the birth crimes, takes the form of a statistical hash representation. The system picks seeker vessel images from a database grounded on how analogous their block statistical hashes are to the hash of the compressed leftover communication. The system also assigns the residuals to the named vessel images.

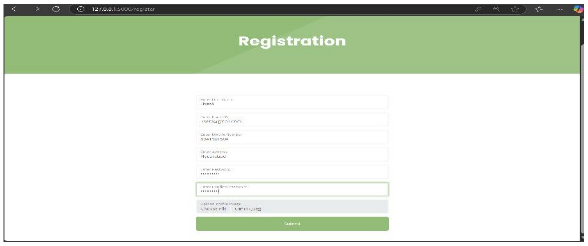
III. LITERATURE SURVEY

In this paper Rong Huang, Chunyan Lian, Zhen Dai, Zhaoying Li, and Ziping Ma propose SMHSWE, a two- stage crossbred frame for steganography without embedding, barring pixel variations and making it vulnerable to traditional steganalysis tools. The frame includes an image emulsion module, using a flinch machine- encoder to render secret dispatches into structural features of synthesized images, and an image mapping module, compressing birth crimes as residuals matched to vessel images. This reduces the number of vessel images demanded while icing full communication recovery. still, SMH- SWE has limitations, including lower sheltered capacity and vulnerability to compression, blurring, and sterilization attacks due to high- frequency element garbling. future advancements involve advanced caching ways and inimical knowledge to enhance robustness and capacity.[1] In this paper, Shahid Rahman, Jamal Uddin, Habib Ullah Khan, Hameed Hussain, Ayaz Ali Khan, and Muhammad Zakarya (2022) propose an enhanced Least Significant Bit (LSB) concession system for coverlet secret dispatches in digital images. The fashion introduces a Magic Matrix and a Modified Least Embedding Algorithm (MLEA) to meliorate the security, embedding capacity, and robustness of the steganographic process, while icing that the stego- image remains visually indistinguishable from the original image. The authors illuminate the strengths of their system, including enhanced data concealment and increased rigidity against unauthorized access. still, they also admit several limitations. The proposed system remains vulnerable to steganalysis attacks and its embedding capacity is constrained by the size and colour depth of the cover image. also, the computational complexity of the fashion may increase when dealing with larger datasets, potentially impacting its effectiveness. likewise, the system's robustness is limited when the stego image undergoes advanced image processing ways, analogous as compression or noise attacks. The authors suggest that future work could concentrate on enhancing the robustness of the fashion and extending its connection to address these limitations. This study provides a precious foundation for developing bettered steganographic styles by balancing security, capacity, and effectiveness in digital image steganography. [2] In this paper, Sunpreet Sharma, Ju Jia Zou, and Gu Fang propose a new multipurpose watermarking scheme designed to address challenges in image authentication and brand protection, particularly in artificial surroundings within the terrain of sedulity 4.0. The proposed system embeds two distinct watermarks a robust watermark for brand protection and a fragile watermark for tamper discovery and localization. The robust watermark is bedded in the frequency sphere using a new mean- predicated measure selection procedure, enhancing imperceptibility and robustness against various watermarking attacks. The fragile watermark, bedded in the spatial sphere through a self-generated halftone system and predicated on least significant bit (LSB) concession, is designed to meliorate the fragility of the watermark, making it effective for detecting and localizing tampering. still, a significant limitation of the proposed scheme is its non- reversible nature, meaning it ca n't restore or recover tampered regions, which may be a disbenefit in operations taking image restoration. This limitation highlights the need for further disquisition to address scripts where recovery of the original image is critical. [3] In this paper Arshiya S. Ansari, Mohammad S. Mohammadi, and Mohammad Tanvir Parvez propose the general Steganography Algorithm (GSA) to address the limitations of being steganography styles that work with only one image format. GSA is a flexible approach that objectifications image factors, allowing harmony across formats like JPEG, Bitmap, TIFF, and PNG. It incorporates capacity pre-estimation, adaptive partitioning, and data spreading to bed data securely while conserving image quality. The algorithm also enhances security by concluding optimal cover formats predicated on data size and respectable distortions, making it adaptable to different use cases. Experimental results demonstrate that GSA improves PSNR values by at least 26, enabling advanced data coverlet with minimal impact on visual quality. still, the authors note the need for further evaluation of its robustness against advanced steganalysis and compression ways. also, GSA's performance with lower common or heavily manipulated images remains unexplored. future work includes refining partition schemes and testing the algorithm with a wider range of formats and complex manipulations to enhance security and versatility. [4] In this paper Jagan Raj Jaya pandiyan, C. Kavitha, and K. Sakthivel propose the enhanced LSB (eLSB) algorithm to meliorate the traditional Least Significant Bit system for image- predicated text steganography. Operating in the spatial sphere, eLSB optimizes coverlet to enhance cover image quality. The algorithm involves two phases coverlet title information about the secret communication and recovering the communication itself using a character sequence- predicated optimization fashion. This approach improves space operation, reduces distortion, and increases embedding capacity. The eLSB algorithm also enhances security by preprocessing the secret communication before embedding. Experimental results show it outperforms the traditional LSB system, achieving advanced PSNR and lower MSE and RMSE values, indicating reduced noise and distortion. Tests with various cover images and communication sizes confirm harmonious advancements in stego image quality, demonstrating eLSB's effectiveness. [5] In this paper Donghui Hu, Liang Wang, Wenjie Jiang, Shuli Zheng, and Bin Li propose a new steganography system using Deep Convolutional Generative Adversarial Networks (DCGANs) under the order of Steganography Without Embedding (SWE). rather of modifying a carrier image, their system generates a stego image directly from a noise vector representing the secret data using a DCGAN creator. A separate extractor network retrieves the sheltered information with high delicacy, enhancing security and making the stego image resistant to advanced steganalysis. Despite its advantages, the system has limitations. Some generated stego images warrant naturalness, risking discovery, and the steganographic capacity is confined due to the small size of generated images. While birth delicacy is high, it's not impeccable, suggesting a need for error- correction canons to meliorate recovery. future work aims to address these issues and enhance robustness and capacity.[6]

IV. PROPOSED SYSTEM

The new system tackles key issues in safe communication, like stopping unwanted access, keeping messages private, preventing image changes, and checking if things are real. Current systems often don't do a good job of making sure messages are safe and spotting when images have been messed with. They try to hide messages but don't check if images have been changed, which means someone could alter them without anyone knowing. Also old methods can't tell you how much an image has been changed so it's hard to know when something's not right. The new system fixes these problems by using AES encryption in CBC mode to keep messages secret Least Significant Bit (LSB) steganography to hide encrypted messages in images, and a special watermark to spot changes. This watermark is put into the image using LSB, so if anyone changes the image, it messes up the watermark, and you can tell something's wrong. The system also makes sure the right people can send and get messages. It checks if an image is real by looking at the watermark and comparing it to the original, which shows how much it's been changed. By putting together AES encryption for safety, LSB steganography to hide things, and the special watermark to check if things are real, the new system gives a complete answer for sending messages transmission, tamper detection, and integrity verification.

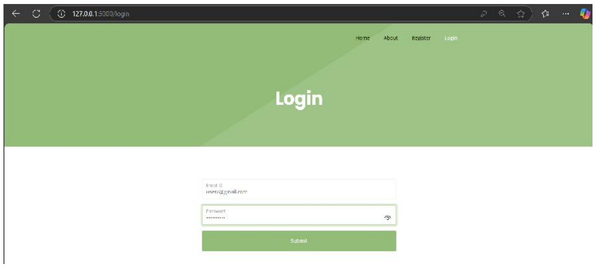
V. RESULTS



Enter User Name
UserA
Enter Email ID
usera@gmail.com
Enter Mobile Number
8341501504
Enter Address
Hyderabad
Enter Password
••••••••••
Enter Confirm Password
••••••••••
Upload Profile Image
Choose File OIP (1).jpeg

Fig. 1 User Registration by providing valid Name, Email, Address, Password, Confirm Password and Profile image.

DOI: 10.48175/568

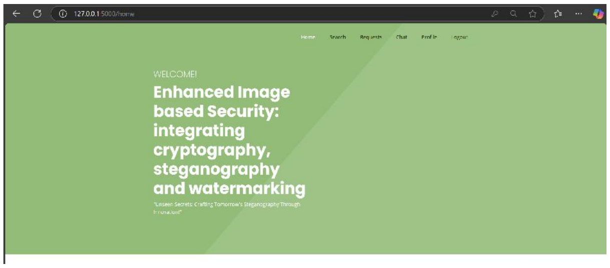


Login

Email ID
usera@gmail.com

Password
••••••••••

Fig.2 User A login by providing valid Email and Password.

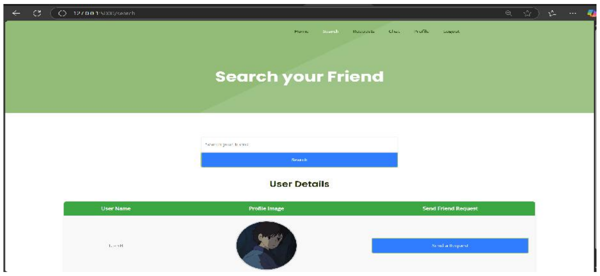


WELCOME!

Enhanced Image based Security: integrating cryptography, steganography and watermarking

"Unseen Secrets: Crafting Tomorrow's Steganography Through Innovation!"

Fig.3 Home page displays after successful login.

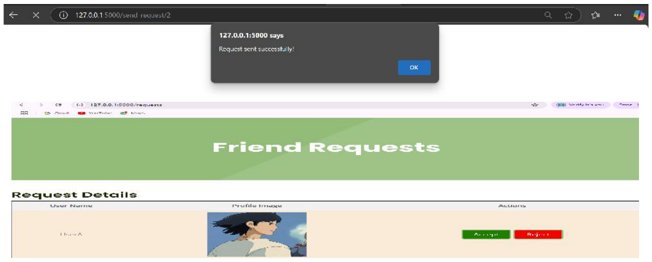


Search your Friend

User Details

User Name	Profile Image	Send Friend Request
User B		Send a Request

Fig. 4 User A searching other users of the application



127.0.0.1:5000 says

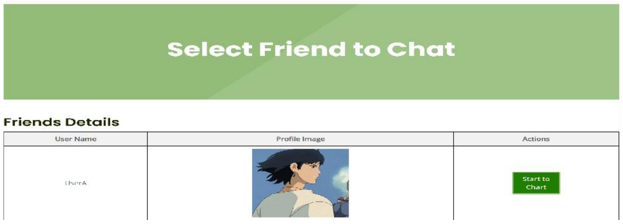
Request sent successfully!

Friend Requests

Request Details

User Name	Profile Image	Actions
User A		Accept Reject

Fig. 5 User A sending request to User B.



Select Friend to Chat

Friends Details

User Name	Profile Image	Actions
UserA		Start to Chart

Fig. 6 User B accepts request from User A. Later, User A is added to friends list of User B and vice versa.

DOI: 10.48175/568

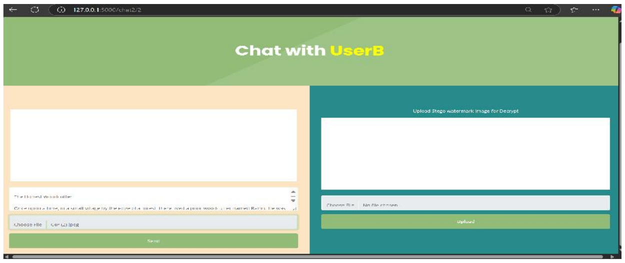


Fig. 7 User A sending message to User B by entering text and uploading the image.

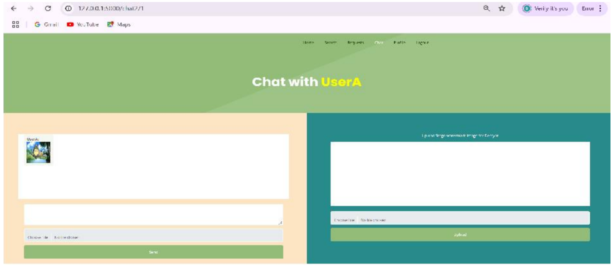


Fig. 8 User B receiving the image sent by the User A

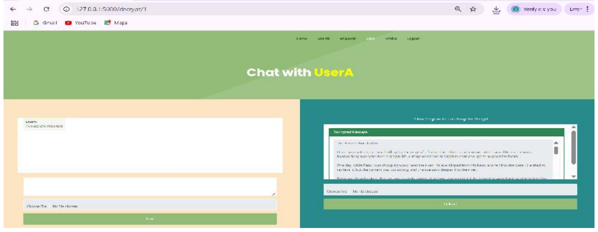


Fig. 9 User B uploading the image sent by the User A for accessing the message content in the image.

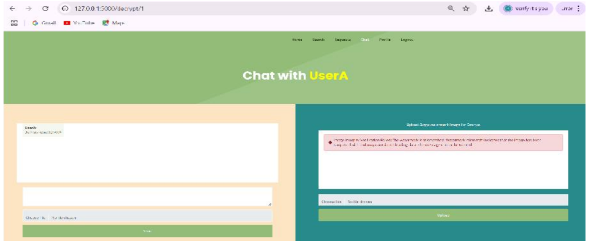


Fig. 10 User B uploading the tampered or manipulated image sent by the User A.

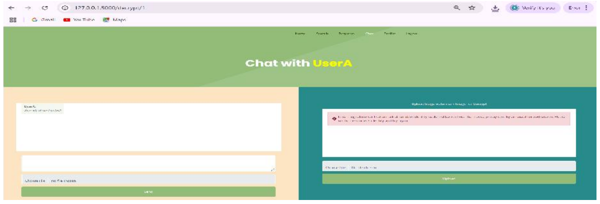
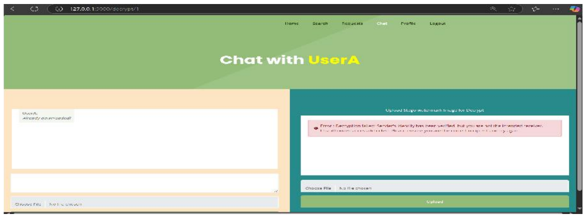


Fig. 11 User B Uploading Image Received from an Impersonator Posing as User A (Image was actually User C to the User B)



Chat with UserA

UserA:
Already downloaded!

Upload Stego watermark Image for Decrypt

Error : Decryption failed: Sender's identity has been verified, but you are not the intended receiver. [illegible]

Fig. 12 User B Unauthorizedly Accessing an Image Sent by User A to User C.

VI. CONCLUSION

The system successfully utilizes AES encryption, LSB image steganography, and fragile dynamic watermarking to satisfy the basic need for secure and tamper-evident communication. The system uses the three methods in combination to keep sensitive data private against illegal use as well as to authenticate its integrity. AES encryption offers maximum confidentiality by transforming plaintext messages into unreadable ciphertext, only feasible to be decrypted by legitimate receivers. The LSB method inserts the encrypted message into a cover image in such a way that the communication is done in a covert manner without arousing suspicion. In addition, the vulnerable dynamic watermarking helps in enhanced tamper detection so that unauthorized tampering inside the stego image can be detected. The multi-level security system not only hides the presence of data but also safeguards the message against alteration while being transmitted. The system is thus extremely effective where integrity, authenticity, and confidentiality are needed most, such as in secure messaging, digital document protection, and confidential data transfer. The entire project succeeds in fulfilling its aim of offering a secure, dependable, and tamper-evident communication system.

ACKNOWLEDGEMENT

We would like to take this opportunity to sincerely thank everyone who contributed to the successful completion of this project. The continuous guidance, valuable suggestions, and constructive feedback we received played a significant role in shaping our work. We're grateful for the supportive environment, access to resources, and opportunities for learning that helped us overcome challenges along the way. A heartfelt thank you goes out to our friends and families for their unwavering encouragement, patience, and belief in us throughout this journey. This project stands as a reflection of the collective effort and support we were fortunate to receive.

REFERENCES

[1] Rong Huang 1, Chunyan Lian, Zhen Dai1, Zhaoying Li, And Ziping Ma, "A Novel Hybrid Image Synthesis-Mapping Framework for Steganography Without Embedding", Journal, 2023.
[2] Shahid Rahman, Jamal Uddin, Habib Ullah Khan, Hameed Hussain, Ayaz Ali Khan, Muhammad Zakarya, "A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method", Journal, 2022.
[3] Sunpreet Sharma, Ju Jia Zou, Gu Fang, "A Novel Multipurpose Watermarking Scheme Capable of Protecting and Authenticating Images With Tamper Detection and Localization Abilities", Journal, 2022.
[4] Arshiya S. Ansari, Mohammad S. Mohammadi, Mohammad Tanvir Parvez, "A MultipleFormat Steganography Algorithm for Color Images", Journal, 2020.
[5] Jagan Raj Jayapandiyan, C. Kavitha, K. Sakthivel," Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization", Journal, 2020. [6] Donghui Hu, Liang Wang, Wenjie Jiang, Shuli Zheng, Bin Li, "A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks", Journal, 2018