IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

A SECURE DATA SHARING USING DATA HIDING WITH STEGANOGRAPHY APPROACH

[1]K.Silpha, [2]U.Sasikumar, [3]D.Srinivasan, [4]S.Surenthar,[5]R.Rajkumar

[1]Assistant Professor, [2,3,4,5]Student
[1]Computer Science and Engineering,
[1]Sri Ramakrishna College Of Engineering, Perambalur, Tamil Nadu, India

Abstract : Secure data sharing is crucial for many real time applications such as law enforcement agencies, military conversations and medical data sharing, etc., however, sharing sensitive data poses a significant security challenge as it can be intercepted or leaked. To address this challenge, here propose a novel approach that combines steganography and cryptography techniques. The proposed system aims to enhance the security of data transmission by encrypting data using AES encryption and hiding it within an image using Modified Least Significant Bit (LSB) with and image encryption using Elliptic Curve Cryptography (ECC). The first layer of security involves AES encryption, a widely recognized symmetric encryption algorithm known for its robustness and efficiency. This ensures that the plaintext message remains confidential, protected by a strong encryption key. However, take this a step further by embedding the AES-encrypted text within a cover image using a modified Least Significant Bit (LSB) algorithm. This covert embedding ensures that even if the transmission is intercepted, the presence of sensitive information remains hidden within the seemingly innocuous image.

IndexTerms: Secure Data sharing,Stegnography approaches,Data Hiding.

INTRODUCTION

Steganography is the practice of hiding secret messages (hidden text) within every day, seemingly innocuous object (cover text) to produce a stego text. The recipient of a stego text can use his knowledge of the particular method of steganography employed to recover the hidden text from the stego text. The goal of steganography is to allow parties to converse covertly in such a way that an attacker cannot tell whether or not there is hidden meaning to their conversation. This sets steganography apart from cryptography which, although providing for private communication, can arouse suspicion based solely on the fact that it is being used.

Modern steganography was characterized by G J Simmons when he stated the problem in terms of prisoners attempting to communicate covertly in the presence of a warden. Alice and Bob, prisoners, are allowed to communicate, but their channel is through

FEW TYPES IN STEGNOGRAPHY IMAGES:

2.1 LEAST SIGNIFICANT BIT INSERTION

Least Significant Bit (LSB) insertion is most widely known algorithm for image steganography, it involves the modification of LSB layer of image. In this technique, the message is stored in the LSB of the pixels which could be considered as random noise.

2.2 MASKING AND FILTERING

Masking and filtering techniques work better with 24 bit and grey scale images. They hide info in a way similar to watermarks on actual paper and are sometimes used as digital watermarks. Masking the images changes the images. To ensure that changes cannot be detected make the changes in multiple small proportions. Compared to LSB masking is more robust and masked images passes cropping, compression and some image processing. Masking techniques embed information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the "noise" level. This makes it more suitable than LSB with, for instance, lossy JPEG images.

2.3 REDUNDANT PATTERN ENCODONG

Redundant pattern encoding is to some extent similar to spread spectrum technique. In this technique, the message is scattered throughout the image based on algorithm. This technique makes the image ineffective for cropping and rotation. Multiple smaller images with redundancy increase the chance of recovering even when the stegano-image is manipulated.

2.4 ENCRYPT AND SCATTER

Encrypt and Scatter techniques hides the message as white noise and White Noise Storm is an example which uses employs spread spectrum and frequency hopping. Previous window size and data channel are used to generate a random number and within this random number, on the entire eight channels message is scattered throughout the message. Each channel rotates swaps and interlaces with every other channel. Single channel represents one bit and as a result there are many unaffected bits in each channel.

EXISTING SYSTEM

Reversible Data Hiding in cipher media for privacy protection has recently drawn attentions in the community. There are mainly two types of cryptosystems adopted in the existing RDH-EI schemes. The first type is to perform encryption with a stream cipher, which is implemented with low complexity. However, processing in the encrypted domain is hardly allowed with a cipher stream. The second kind of encryption achieves “privacy homomorphism” to enable processing in the encrypted domain by using the cryptosystems.

So a desired plain-text image may be obtained after decrypting the processed cipher image. Data have been hidden in a cipher image; an original plain-text image may be obtained after decrypting the cipher image. Meanwhile, the data hidden in the cipher image can be extracted before or after decryption. As compatibility with processing in the encrypted domain a new preprocessing-free and lossless data hiding method called random element substitution (RES) is proposed for the Paillier cryptosystem. In particular, data embedding is conducted by substituting the to-be-hidden bits for the random element in a cipher value so that the plaintext value is preserved.

The RES method can be applied in or after the process of encryption, while the decrypted plaintext value is needed to extract the hidden data from the cipher value. To achieve data extraction before decryption as well, it is combined with the self-blinding (SB) method so that two lossless data hiding schemes are generated for encrypted images.In addition, the data hidden in the encrypted image can be correctly extracted before processing in the encrypted domain,

PROPOSED SYSTEM

The need for secure and efficient methods for managing and sharing data is paramount in today's society. With the advancement of technology, it has become possible to encrypt the secret data and hide sensitive information within images. Here implement a text encryption process using symmetric encryption process.

The encryption and decryption process of secret text will be done using Advanced Encryption Standard. AES is employed as the chief encryption primitive. It is an encryption technique which uses the substitution and permutation method. The encryption is done in specified number of rounds. This makes the data secure. Then hide the encrypted sensitive information in cover image using Modified LSB Technique. In Modified LSB, the cover image is divided into non-overlapping pixel blocks of 3x3 pixel blocks. Block levels are based cardinality of the cover image.

The encrypted information is hidden within cover image for secure transmission. Using the data extraction key the users will be able to access the relevant data only. Then the stegnographic image can be encrypted using ECC based asymmetric encryption algorithm. Asymmetric cryptography based image encryption is a promising technique for securing data, which involves encrypting images into unpredictable form and distributing them to the authorized receiver. Encrypted image was shown useless, but when secret key of the image was find, the original image can be decrypted.In this context, the encrypted text data hidden within cover images can be secured using Modified LSB Data hiding and ECC based image encryption.

This technique ensures that the data is protected, and only authorized individuals can access it. This proposed data hiding with image encryption is a promising technique for securing sensitive information. Its use can enhance the effectiveness of secure communication systems while ensuring the privacy and security of the data.

IV. MODULE DESCRIPTION

4.1 USER ENROLMENT

This module facilitates the registration process for users who intend to engage in data sharing within the system. It involves collecting and validating user information, such as username, email address, and password. During enrollment, users may also generate encryption keys required for data encryption and decryption processes. This module ensures that only authorized users can access the system and participate in secure data sharing activities.

4.2 USER AUTHENTICATION

Upon registration, users must authenticate themselves before gaining access to the system's features. This module verifies the identity of users through credentials provided during enrollment, such as username and password. Advanced authentication mechanisms, such as multi-factor authentication, may also be implemented to enhance security. Once authenticated, users are granted access to the system's functionalities.

4.3 DATA SHARING

This module enables users to securely share sensitive information with other authorized users. Users can initiate data sharing by selecting the data to be transmitted and specifying the recipients. The module ensures that data transmission occurs securely by encrypting the information using AES encryption before embedding it into an image for transmission. This ensures confidentiality and integrity during data sharing activities, safeguarding sensitive information from unauthorized access.

4.4 DATA ENCRYPTION USING AES

This module is responsible for encrypting sensitive data before it is shared or transmitted within the system. AES encryption, a symmetric encryption algorithm, is utilized to encrypt the data securely. Users may specify encryption keys during data sharing to ensure that only authorized recipients can decrypt and access the information. This module ensures that sensitive data remains protected against unauthorized access or interception during transmission.

CONCLUSION:

This paper proposed a new steganographic algorithm for hiding text files in images. Here provide an overview of steganography and introduce some techniques of steganography which help to embed the data. These techniques are more useful for detecting the stegno images as well as the image media relating to security of images and embed the data for complex image area and can easily estimate the high embedding rate by using the quantitative steganalysis technique. Developed a system with help of efficient cryptography and data hiding algorithm. Hence this new steganographic approach is robust and very efficient for hiding text data in images.In conclusion, the implementation of a secure data sharing system using a data hiding approach with steganography offers several advantages in safeguarding sensitive information while enabling efficient communication and collaboration. By embedding confidential data within innocuous carrier files, such as images or audio files, steganography provides a covert means of transmission that conceals the existence of the hidden data from unauthorized users. This method offers an additional layer of security beyond encryption, making it harder for adversaries to detect or intercept sensitive information during transmission.

REFERENCES

[1] Al-Hadhrami, A. A., & Khan, M. K. (2018). "A novel secure and high-capacity data hiding technique based on pixel-value differencing". Multimedia Tools and Applications, 77(2), 2827-2855

[2] Al-Qershi, O. M., & Khoo, B. E. (2019). "A novel secure data hiding approach using dynamic steganography with enhanced security and capacity". Multimedia Tools and Applications, 78(7), 8955-8990.

[3] Avcı, E. (2017). "A Novel Secure Data Hiding Method with an Application in Healthcare". Journal of Medical Systems, 41(1), 10.

[4] Bender, W., Gruhl, D., Morimoto, N. & Lu, A. (1996). "Techniques for data hiding". IBM Systems Journal, 35(3.4), 313-336.

[5] Chen, Fan, Yuan Yuan, Hongjie He, Miao Tian, and Heng-Ming Tai. "Multi-MSB compression based reversible data hiding scheme in encrypted images." IEEE Transactions on Circuits and Systems for Video Technology 31, no. 3 (2020): 905-916.

[6] Chen, Bing, Wei Lu, Jiwu Huang, Jian Weng, and Yicong Zhou. "Secret sharing based reversible data hiding in encrypted images with multiple data-hiders." IEEE Transactions on Dependable and Secure Computing 19, no. 2 (2020): 978-991.

[7] Du, Yang, Zhaoxia Yin, and Xinpeng Zhang. "High capacity lossless data hiding in JPEG bitstream based on general VLC mapping." IEEE Transactions on Dependable and Secure Computing 19, no. 2 (2020): 1420-1433.

[8] Fridrich, J., Goljan, M., & Du, R. (2001). "Reliable Detection of LSB Steganography in Color and Grayscale Images". Proceedings of ACM Workshop on Multimedia and Security.

[9] He, Junhui, Junxi Chen, Weiqi Luo, Shaohua Tang, and Jiwu Huang. "A novel high-capacity reversible data hiding scheme for encrypted JPEG bitstreams." IEEE Transactions on Circuits and Systems for Video Technology 29, no. 12 (2018): 3501

[10] Hossain, M. S., & Mansoor, N. (2020). "A novel data hiding technique using block-based image steganography". Multimedia Tools and Applications, 79(13-14), 9315-9338.

[11] Hua, Zhongyun, Yanxiang Wang, Shuang Yi, Yicong Zhou, and Xiaohua Jia. "Reversible data hiding in encrypted images using cipher-feedback secret sharing." IEEE Transactions on Circuits and Systems for Video Technology 32, no. 8 (2022): 4968-4982.

[12] Li, B., & Wang, W. (2017). "A novel steganography algorithm for high payload based on LSB matching scheme".

[13] Liu, Sheng, Chengqing Li, and Qiao Hu. "Cryptanalyzing two image encryption algorithms based on a first-order time-delay system." IEEE MultiMedia 29, no. 1 (2021): 74-84.

[14] Lu, Wei, Junjia Chen, Junhong Zhang, Jiwu Huang, Jian Weng, and Yicong Zhou. "Secure halftone image steganography based on feature space and layer embedding." IEEE Transactions on Cybernetics 52, no. 6 (2020): 5001-5014.

[15] Luo, W., Huang, J., & Fan, X. (2017). "A novel reversible data hiding algorithm based on side match". Multimedia Tools and Applications, 76(19), 20263-20282.

[16] Ou, Bo, and Yao Zhao. "High capacity reversible data hiding based on multiple histograms modification." IEEE Transactions on Circuits and Systems for Video Technology 30, no. 8 (2019): 2329-2342.

[17] Rajput, M., & Grewal, A. S. (2020). "A novel approach for secure data hiding in images using hybrid steganography". Multimedia Tools and Applications, 79(5-6), 4031-4057.

[18] Singh, P., & Kaur, H. (2018). "A novel steganography approach for secure data hiding in image". Multimedia Tools and Applications, 77(3), 3215-3241.

[19] Wu, Hao-Tian, Yiu-ming Cheung, Zhiyuan Yang, and Shaohua Tang. "A high- capacity reversible data hiding method for homomorphic encrypted images." Journal of Visual Communication and Image Representation 62 (2019): 87-96.

[20] Xiao, Di, Fei Li, Mengdi Wang, and Hongying Zheng. "A novel high-capacity data hiding in encrypted images based on compressive sensing progressive recovery." IEEE Signal Processing Letters 27 (2020): 296-300