JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

HIDING TEXT INFORMATION IN ENCRYPTED IMAGE WITH DISTRIBUTED SOURCE ENCODING

Abhishek M Y +
Dept. of CSE, MCA Program
Visvesvaraya Technological University
"Jnana Sangama", Belagavi-590018
Karnataka

Dr.Ravish G K
Asst.Professor
Dept. of CSE, MCA Program
Visvesvaraya Technological University
"Jnana Sangama", Belagavi-590018

Abstract:

In the digital age, ensuring information security and privacy has become a critical concern during communication and data exchange. Steganography, a technique that conceals vital information within innocent-looking cover media like photographs, has emerged as an effective solution to address these challenges. The objective of this project is to develop a comprehensive steganography tool capable of securely hiding any type of data file within an image, bolstered by multiple layers of protection.The proposed system offers a user-friendly interface, allowing users to select a destination image, specify the storage location, and customize the image's division into numerous parts. The user's information is then divided into random chunks and discreetly written into various storage locations within the image. To further conceal classified info, the image consolidated with a cover image.

To maintain confidentiality, the final image is encrypted using a robust encryption technique and a randomly generated key.The encrypted image can be easily shared with the intended recipients through cloud storage. To ensure only authorized access, the linked key is sent via encrypted email, accessible only to those who are meant to receive the secret data. Upon receiving the image and key, the recipient can use the key to unlock the concealed information and verify their ownership.

Which give individuals a flexible and powerful solution for safeguarding their data during transmission, integrating the capabilities of steganography, encryption, and secure key exchange. The system's ability to hide sensitive information within image files significantly reduces the hazard of info breaches and unauthorized access. Ultimately, this initiative aims to enhance the safety and security of critical info in digital era.

Introduction:

In our interconnected world, securing data transmission has become of utmost importance. With the widespread use of digital communication and data exchange, ensuring the confidentiality and integrity of information has become a critical concern for both individuals and organizations. Addressing this challenge, steganography has emerged as a powerful technique for concealing sensitive data within seemingly innocuous cover media.

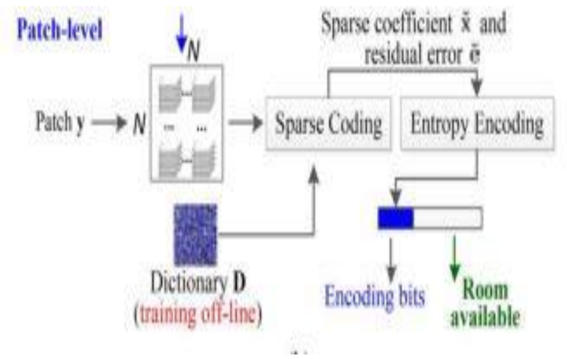
Unlike cryptography, which primarily deals with encrypting and obfuscating data, steganography works differently. It involves the hiding of data within a carrier medium, making it virtually undetectable to casual observers. By embedding information discreetly in images, audio files, or other digital media, steganography offers an extra layer of protection to sensitive data during transmission.

Overall, steganography provides an innovative approach to data security, complementing the traditional encryption methods employed in cryptography. This combined use of techniques ensures that data remains safe from prying eyes and unauthorized access, thus bolstering the overall security landscape in our digital age.

Literature Survey:

This study delves into a comprehensive exploration of various picture steganography techniques. It thoroughly examines fundamental concepts and discusses the advantages and limitations of prominent methods, including the LSB (Least Significant Bit), DCT (Discrete Cosine Transform), and F5 algorithm. Additionally, the review encompasses recent advancements in steganography, such as geographic domain, transform domain, and statistical domain approaches. Performance and security analyses of different picture steganography methods are carried out, offering valuable insights for researchers and practitioners seekingadeeper understanding of image steganography.

System Architecture:



- The system architecture is designed to illustrate the process of concealing data inside an imagees by Patch-level Sparse encoding method. The flow begins with the info owner selecting an image, which undergoes encryption. During this stage, the image properties are collected and compressed to prepare it for further processing.

- Once encrypted, the image is ready for sparse encoding. The sparse encoding technique is then applied to embed user data into the image. This process creates a significant amount of additional space within the image to accommodate the hidden data securely.

- The architecture diagram visually represents the steps involved in this data concealment process, showcasing how the image is transformed to allow for the seamless integration of user data without compromising the integrity or appearance of the primary images. This innovative approach ensures efficient data hiding while preserving the image's quality and providing a robust solution for safeguarding sensitive information.

Drawback of the Existing System:

- information is encrypted in pixel level, so large amount of data cannot be added.
- The hash key generated is attached to the image itself, so intruder can easily encrypt the hash key.
- After hiding the info in the images the image is still in original form and visible to the intruder.
- Lack of safety to the user data.

Proposed System:

The proposed system for data concealment in images employs the Patch-level Sparse encoding method, a departure from traditional steganography techniques. Utilizing sparse encoding enables us to create ample space within the image, allowing users to hide a substantial amount of data effectively, The primary objective of these apprroaches is to guarantee the precise retrieval of two encrypted classified info and the primary images without any loss of data. This method offers enhanced capacity for data hiding, ensuring seamless retrieval of the embedded info & pristine appearance of primary images for the user's convenience and security.

THE BENEFITS OF THE INTENDED SYSTEM

- In proposed system info is encrypted by sparse encoding technique, providing more space to store any large data in an image.
- The system provides a way to add any data and divides the data into different parts using the split& merge technique**.**
- Using the sparse encoding technique the parts of the image is pushed and created a space for the data to be hidden.
- The SHA-256 hash key algorithm is used.
- A secrete key and data is sent to the requested user.
- The SHA-256 hash key generated is sent to receiver's secured E-mail address.

Implementation modules:

- Sender
- Receiver

Sender

The data owner uploads the images with info and the data is sparse encoded in the image. Now the hash key is generated.

Receiver

The receiver registers himself and logged in and view the inbox for the sender file. The receiver gets the details of the new received file and the name of the sender with the subject. The receiver receives the encoded image in the inbox, and the hash key in the email. The receiver enters the hash key and the reverse data hiding takes place and the original data is retrieved by the receiver.

Conclusion:

the image steganography project aims to provide a secure and efficient means of hiding information within image files. By utilizing steganography techniques, the project allows users to embed any type of data file into an image, ensuring the confidentiality and integrity of the hidden information. The project incorporates various functionalities such as data splitting, merging, encryption, and key generation to enhance protection against unauthorized access.

Through the executiontion off steganography tools, users can securely transmit sensitive data through cloud-based platforms without the fear of data breaches or hacking. The project splits the image into user-defined pieces, stores the data within these parts, and randomly merges and combines them. Additionally, primary image added to further conceal the hidden data. The resulting images are encrypted, and a key is generated for secure transmission.

The recipient of the encrypted image can then use the supplied hash key to reveal the concealed information. The system verifies the hash key with the one embedded within the image, ensuring the authenticity of the receiver. This process allows the receiver to access the hidden data while maintaining the integrity and security of the transmitted information.

By implementing this image steganography project, users can confidently transmit sensitive data through cloud platforms, safeguarding their information from potential unauthorized access or hacking attempts. The project includes several levels of protection for the concealed information. These include encryption, information breaking down, and key authentication.

In conclusion, the image steganography project provides an effective and secure solution for hiding information within image files, offering users peace of mind when transmitting.

Refrences:

- MU. Celiik,G. Shawrma,& A.M.Tekaalp, "Losses generalized- info embeding," IEE Trans. Image Process., volumes. 14, no.02, pp. 253–265, Febrauary. 2005.
- H. J. Kimm, V. Saachnev, Y.Q. Shii, J. Nam, and H.G.Chhoo, For reverseble info embedding, a unique difference expansion transform," IEE Trans. Info. Forensecs protection, volume number. 03, number. 03, pp. 456–466, Sept. 2008.
- D.Coltuc, "Improve embedding for anticipation based reverseble watermark," IEEE Trans. Info. Forensics protection, volume. 06, number. 03, p. 873–882, September. 2011.
- Xli. B. Yingg, and Zengg, "anticipatting adoptive forecast-erorr expansion & pixel selection, this method allows efficient reversible watermarking."," IEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.
- YHu, H.K. Leee, . Cheen, and JLi, "The method titled "Differense Expansion-Based encryption of info Using Dual Embedding Directions" focuse on encryption and employes two embeding directons.IEE Trans.media,volume. 10, number. 8, pp. 1500–1511, December. 2008.
- W LTai, CM. Yeah, & CC. Changg, "data encrypting upon histoogram modifications of pixel differenses," IEE Trans. Circuits Sys. Video Tech.,. 19, number. 6, p. 906–910, Jun. 2009.
- CC. Lin, WL. Tai, and CC. Chang, "is centered around modifying difference images within the histogram to achieve its objectives.Pattern Recognition., volumee.fourty one, number. 12, p. 3582–3591, Dec. 2008.