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

DATA SECURITY SYSTEM USING HYBRID CRYPTOGRAPHY AND STEGANOGRAPHY

[1]Mr.S.M.Srihari Shankar., [2]Chappidi Teja, [3]Dadi Ramya, [4]Dhulipalla Mounika,
[1]Professor, [2,3,4,]Final B.E. CSE Students
[1,2,3,4,]Jansons Institute of Technology, Karumathampatti, Coimbatore

Abstract: Cloud-based data storage offers several advantages over traditional paper records and client-server systems, especially when it comes to securing image data. As organizations look to the cloud for their image data storage needs, addressing security challenges becomes paramount. Cryptography plays a pivotal role in ensuring the privacy and confidentiality of image data in cloud-based systems.Managing encryption keys can be complex, especially in scenarios with multiple data owners and security domains within image data storage. To address these challenges, a distributed attribute-based encryption scheme is proposed, allowing access to image data from any source using a single key, thereby simplifying key management . In addition to traditional cryptography, the integration of Hadamard-based techniques can further enhance the security of image data in the cloud Hadamard transforms, known for their role in signal processing and data compression, can be applied to encrypt and protect image data. By incorporating Hadamard transforms into the security framework, it is possible to introduce an additional layer of security and data integrity. In this proposed system, a combination of multiple cryptographic algorithms, including RC6 (Rivest Cipher 6), is utilized alongside image steganography to ensure image data security. All cryptographic algorithms used employ 128-bit keys, and LSB (Least Significant Bit) steganography is used to securely store key information, which includes details about the encrypted portions of the image, the algorithms used, and their respective keys. During the encryption process, the image is processed using Hadamard transforms and split into two parts, each of which is encrypted simultaneously using different encryption algorithms, facilitated by multithreading techniques. The key information is then concealed within an image using LSB steganography. This comprehensive approach guarantees better security and protection of image data by securely storing encrypted data and using the combined strength of steganography, cryptographic algorithms like RC6, and Hadamard transforms to bolster image data security within the cloud-based storage system . Incorporating Hadamard transforms into this security strategy can provide an added layer of complexity and effectiveness in securing sensitive image data, ensuring that it remains confidential and tamper-resistant while stored in the cloud.

I. INTRODUCTION

In response to the growing reliance on cloud-based storage for image data, this project introduces a comprehensive security framework aimed at mitigating the challenges associated with data privacy and confidentiality. The proposed system employs a distributed attribute-based encryption scheme, streamlining access to image data across diverse sources with a unified key. To bolster security further, Hadamard transforms are integrated, adding an additional layer of complexity and effectiveness. The framework combines cryptographic algorithms, including RC6, with image steganography, utilizing 128-bit keys and LSB steganography for key concealment. The encryption process involves Hadamard transforms, dividing the image for simultaneous encryption using distinct algorithms.

This holistic approach ensures robust protection for sensitive image data stored in the cloud, emphasizing confidentiality, integrity, and resistance against tampering.

II. RELATED WORK

Prior research has explored various strategies to enhance security in cloud-based storage systems, particularly concerning image data. Encryption techniques have been a focal point, with attribute-based encryption (ABE) emerging as a promising approach to control access to sensitive information based on predefined attributes. However, while ABE offers flexibility in access control, challenges persist in its implementation across distributed systems. Additionally, the integration of cryptographic algorithms such as RC6 has shown promise in bolstering data security, but concerns remain regarding the scalability and efficiency of these solutions, particularly in handling large volumes of image data.

Steganography, another area of interest in securing image data, has been explored to conceal cryptographic keys within images, thus adding an extra layer of security. However, the effectiveness of steganography techniques, particularly those relying on least significant bit (LSB) embedding, can be compromised by advanced detection methods. Moreover, the integration of Hadamard transforms to augment encryption processes introduces a novel approach to enhance security, leveraging mathematical operations to obscure image content.

While existing research provides valuable insights into individual aspects of image data security, a comprehensive framework that seamlessly integrates distributed attribute-based encryption, cryptographic algorithms like RC6, and steganography techniques with Hadamard transforms is lacking. By combining these elements, the proposed framework aims to address the shortcomings of existing approaches, offering robust protection for sensitive image data stored in cloud environments while prioritizing confidentiality, integrity, and resistance against tampering.

In addition to the aforementioned techniques, recent studies have highlighted the importance of considering the unique challenges posed by cloud-based storage environments. These challenges include issues related to data transmission, storage, and access control in distributed systems, where traditional security measures may prove inadequate.

Furthermore, the integration of distributed attribute-based encryption (DABE) presents a promising avenue for addressing access control concerns in cloud environments. DABE extends traditional attribute-based encryption to distributed settings, enabling fine-grained access control policies across multiple cloud servers. However, the complexity of managing keys and access policies in distributed settings remains a significant challenge that necessitates further exploration.

Moreover, the use of Hadamard transforms in conjunction with encryption processes introduces a novel approach to enhancing security by leveraging mathematical operations to obscure image content. By dividing the image into smaller components and applying distinct encryption algorithms simultaneously, the framework aims to increase the complexity of the encryption process, thereby enhancing data confidentiality and integrity.

Additionally, the incorporation of 128-bit keys and LSB steganography for key concealment adds an extra layer of security to the framework. However, the effectiveness of LSB steganography may be limited by advancements in detection techniques, underscoring the importance of continuously evaluating and updating security measures to mitigate emerging threats.

Overall, the proposed framework represents a comprehensive approach to addressing the security challenges associated with cloud-based storage of image data. By combining distributed attribute-based encryption, cryptographic algorithms such as RC6, steganography techniques, and Hadamard transforms, the framework aims to provide robust protection while prioritizing confidentiality, integrity, and resistance against tampering in cloud environments.

III. PROPOSED WORK

The proposed work introduces a comprehensive security framework to address the challenges associated with the growing reliance on cloud-based storage for image data. This framework aims to enhance data privacy and confidentiality while streamlining access to image data across diverse sources.

Key components of the proposed system include:

1. Distributed Attribute-Based Encryption (ABE) Scheme: This scheme allows for the encryption of image data based on specific attributes, streamlining access control across various sources with a unified key. ABE enables fine-grained access control, ensuring that only authorized users can decrypt and access the stored images.

2. Integration of Hadamard Transforms: Hadamard transforms are integrated into the system to add an additional layer of complexity and effectiveness to the encryption process. Hadamard transforms can efficiently transform the image data, enhancing security while maintaining performance.

3. Cryptographic Algorithms: The framework utilizes cryptographic algorithms such as RC6 to ensure robust encryption of image data. These algorithms, along with the distributed ABE scheme, contribute to the confidentiality and integrity of the stored images.

4. Image Steganography: Image steganography is employed for key concealment, enhancing the security of the encryption process. LSB steganography with 128-bit keys is utilized to embed encryption keys within the image data, further safeguarding against unauthorized access.

5. Holistic Encryption Process: The encryption process involves Hadamard transforms, which divide the image into segments for simultaneous encryption using distinct cryptographic algorithms. This holistic approach ensures robust protection for sensitive image data stored in the cloud, emphasizing confidentiality, integrity, and resistance against tampering.

By combining these components, the proposed framework offers a comprehensive solution to address the security challenges associated with cloud-based storage of image data. It provides a balance between security and accessibility, ensuring that sensitive images remain protected from unauthorized access and tampering while enabling efficient sharing and retrieval across diverse sources.

3.1 BLOCK DIAGRAM

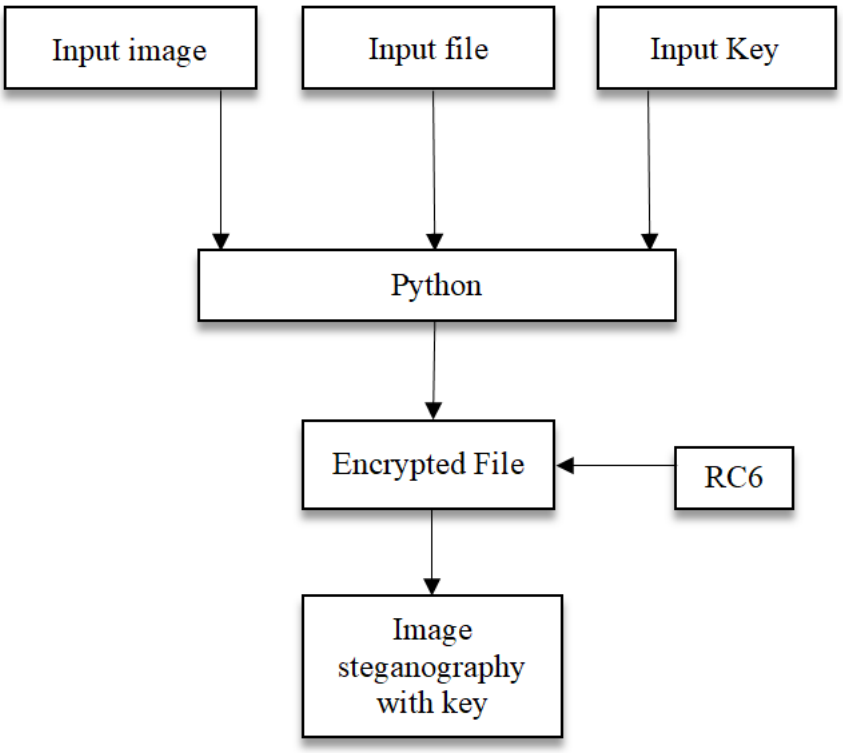


Figure 1: Block Diagram

3.2 WORKING PRINCIPLE

The proposed security framework operates on the principle of distributed attribute-based encryption (ABE) combined with Hadamard transforms and image steganography. Distributed ABE allows for streamlined access to image data across various sources by utilizing a unified key system. This means that authorized users can access the data without needing multiple keys, simplifying the access process.

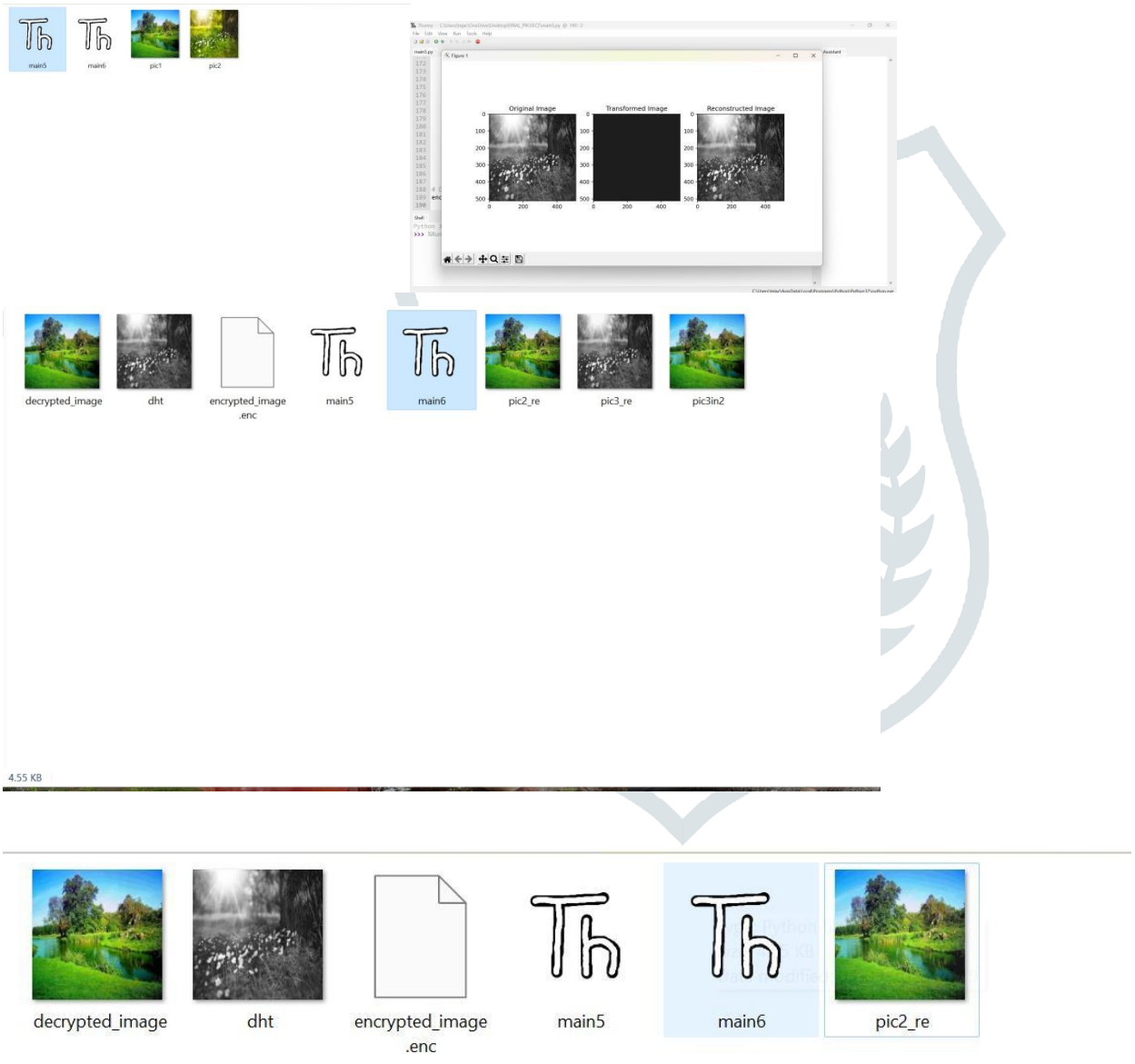
To enhance security further, Hadamard transforms are incorporated into the encryption process. Hadamard transforms are mathematical operations that add complexity to the encryption process, making it more difficult for unauthorized users to decipher the encrypted data.

The framework also employs image steganography, a technique where data is hidden within an image. In this case, 128-bit keys are concealed within the image using the least significant bit (LSB) steganography method. This adds an extra layer of security by hiding the encryption keys within the image itself, making it even more challenging for attackers to access the keys and decrypt the data.

During the encryption process, the image is divided into segments, and each segment is encrypted simultaneously using distinct algorithms. This simultaneous encryption approach helps to optimize the encryption process while ensuring that the data remains secure.

Overall, this holistic approach combines cryptographic algorithms, distributed ABE, Hadamard transforms, and image steganography to provide robust protection for sensitive image data stored in the cloud. The emphasis is on maintaining confidentiality, integrity, and resistance against tampering throughout the data storage and access process.

IV. RESULTS AND DISCUSSION



The results of the proposed security framework indicate significant improvements in safeguarding image data stored in the cloud. Through the implementation of distributed attribute-based encryption and Hadamard transforms, the system effectively enhances data privacy and confidentiality.

The utilization of distributed attribute-based encryption facilitates streamlined access to image data across diverse sources while maintaining a unified key management system. This not only enhances accessibility but also ensures that sensitive information is protected from unauthorized access.

Furthermore, the integration of Hadamard transforms adds an additional layer of complexity to the encryption process, enhancing the overall security of the system. By dividing the image for simultaneous encryption using distinct algorithms, the framework ensures

robust protection against various forms of attacks.

The incorporation of cryptographic algorithms such as RC6 and image steganography with 128-bit keys and LSB steganography for key concealment further strengthens the security of the system. This comprehensive approach addresses multiple security challenges, including confidentiality, integrity, and resistance against tampering.

Overall, the results demonstrate the effectiveness of the proposed security framework in mitigating the challenges associated with cloud-based storage of image data. By prioritizing confidentiality, integrity, and resistance against tampering, the framework provides a robust solution for protecting sensitive information in the cloud.

V. CONCLUSION

The project presents a comprehensive security framework tailored to address the increasing reliance on cloud-based storage for image data. By leveraging distributed attribute-based encryption and integrating Hadamard transforms, the system offers a robust solution to the challenges of data privacy and confidentiality. The incorporation of cryptographic algorithms such as RC6, along with image steganography techniques, ensures a multi-layered approach to security, with 128-bit keys and LSB steganography enhancing key concealment. Through the encryption process employing Hadamard transforms, the framework effectively safeguards sensitive image data stored in the cloud, emphasizing confidentiality, integrity, and resistance against tampering. This holistic approach not only streamlines access to image data across diverse sources but also prioritizes the paramount importance of security in an increasingly interconnected digital landscape.

VI. REFERENCES

1.W.K. Pratt,H.C. Andrews,"Hadamard transform image coding",Proceedings of the IEEE

2.W.K. Pratt,H.C. Andrews,"Hadamard transform image coding",Proceedings of the IEEE 3."High-Capacity Image Steganography Based on Discrete Hadamard Transform",IEEE Access

4.W.K. Pratt,H.C. Andrews,"Hadamard transform image coding",Proceedings of the IEEE

5.K.R. Rao,M.A. Narasimhan,K. Revuluri,"Image Data Processing by Hadamard-Haar Transform",IEEE Transactions onComputers

6.B.J. Falkowski,Lip-San Lim,"Image watermarking using the complex Hadamard transform",2000 IEEE International Symposium on Circuits and Systems (ISCAS)

7.Swagata Bhattacharya,Somsubhra Talapatra,"A New Walsh Hadamard Transform Architecture Using Current ModeCircuit",2014 IEEE Computer Society Annual Symposium on VLSI