IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A NOVEL ALGORITHM FOR RELIABLE CRIME RECORD TRANSMISSION

Dr. T. Loganayagi[1], V. M. Sowmya[2], D. Suchimitha[3] and C. Yashika[4]

Department of Cyber Security, Paavai Engineering College, India

Abstract:

In today's digital age, ensuring sensitive information's security and confidentiality is paramount. Steganography, a subfield of information security, offers a unique approach to concealing data within innocuous carriers to protect it from prying eyes. This paper presents a novel technique for hiding encrypted text within digital images through the art of steganography. The proposed method begins with the encryption of the plaintext using a secure cryptographic algorithm, ensuring that the original message is transformed into an unintelligible form. Subsequently, the ciphertext is embedded within an image file, carefully altering the pixel values to accommodate the hidden data while preserving the visual quality of the image. The choice of the image as a carrier medium is advantageous, as it leverages the ubiquity of images in digital communication, making the concealed information less conspicuous. An application used for this approach is NetBeans IDE an integrated development environment that supports application development, it highlights source code syntactically and semantically. Furthermore, our approach provides an additional layer of security by using steganography to hide the encrypted data within the cover file, making it difficult for unauthorized parties to detect the presence of sensitive data.

Keywords:

Confidentiality, Integrity, Encryption, Steganography, Symmetric key, Netbeans, Heidi SQL, Decryption, Secret key, User Interface.

1. INTRODUCTION

In our increasingly interconnected world, the safeguarding of sensitive critical actual as information has never been more than as individuals, organizations, and governments rely on digital means to communicate and store their data, the need for robust security measures has grown exponentially. A mid this digital landscape, steganography emerges as a discreet yet powerful tool in the arsenal of information security. It offers an ingenious approach to cloak valuable data within the seemingly innocuous facade of everyday digital content, shielding it from the prying eyes of potential adversaries. At its core, this method combines the strengths of encryption, which renders plaintext into an indecipherable form, and steganography, which expertly hides this encrypted treasure within the realm of digital imagery. The paper's approach is meticulous. It commences with the secure encryption of the plaintext using a robust cryptographic algorithm, ensuring that the original message undergoes a metamorphosis into a form that defies comprehension. Subsequently, the ciphertext is strategically embedded within an image file, all the while preserving the visual integrity of the image. ` The choice of images as the carrier medium holds the advantage of ubiquity in digital communication, rendering the concealed information inconspicuous and thus, less susceptible to unwanted attention. Balancing the scale between security and imperceptibility, this research delves into a variety of steganographic techniques, from the subtle embedding of data in the Least Significant Bit (LSB) to the employment of frequency domain approaches. The evaluation of the proposed method is grounded in empirical metrics, such as the Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index (SSI). These metrics ensure that the steganographic process maintains the quality of the image, reducing any noticeable degradation.The results of this study demonstrate not only the successful concealment of encrypted text within digital images but also underscore the technique's potential for safeguarding sensitive information, particularly in the realms of secure communication and data protection.

Nonetheless, as with any technological advancement, challenges and limitations persist. This paper devotes attention to these obstacles and considers the countermeasures that adversaries may employ. Furthermore, it delves into the ethical considerations surrounding the deployment of steganography, emphasizing the need for its responsible and lawful applications.

2. RELATED WORK

Poonams.Garg, Rajkumar Yadav etal,…[1] In the fast-paced digital age we find ourselves in today, the need for secure communication and data protection is more critical than ever. In this context, the field of image steganography takes center stage as a powerful tool in safeguarding sensitive information. This review paper is dedicated to providing an in-depth exploration of image steganography, shedding light on the many approaches employed to covertly hide data within digital images. Its primary objective is to offer readers valuable insights and background information on this intriguing and practical subject. Image steganography revolves around the art of concealing information within digital images, rendering it imperceptible to the human eye and casual observation. The focus of this review paper is to navigate through the labyrinth of techniques and strategies used in this process. It takes readers on a journey through the various methods, highlighting their unique attributes, advantages, and limitations. By doing so, it equips readers with a deeper understanding of how data can be seamlessly integrated into images while maintaining their visual integrity.

Amna Hussain, Muhammad Usama Anwar, etal,…[2] In the contemporary landscape of digital communication and information security, the fields of steganography and steganalysis play pivotal roles. Steganography involves the art of concealing information within different forms of media, and this survey is designed to explore these practices across a range of media types, with a specific emphasis on images. This comprehensive survey aims to shed light on the intricate world of data hiding and detection, providing valuable insights into the challenges and advancements within the domain. The term 'media' in this context encompasses a broad spectrum of data carriers, including text, audio, and images. While the abstract explicitly highlights the significance of images, this survey takes a holistic approach, covering steganographic and steganalytic techniques across this diverse array of media. This comprehensive scope allows readers to gain a well-rounded understanding of the practices of embedding and extracting hidden data.

NitinK.Nagwani, SachinV. Vaidya etal,…[3] The exchange and storage of information have evolved immensely, and with that evolution comes a pressing need for data security and confidentiality. Image steganography, a subfield of information security, represents a powerful technique that is dedicated to concealing data within seemingly ordinary digital images. This paper serves as a gateway to this fascinating world designed with the intent of providing newcomers with a comprehensive and accessible introduction to image steganography. The central focus of this paper is to unravel the basic concepts and principles that underlie the art of embedding data within digital images. It acts as a guiding light for individuals who are taking their first steps into this intriguing domain. By offering a foundational understanding of image steganography, this paper equips readers with the knowledge and insights required to comprehend the core mechanisms and processes involved in this clandestine practice.

E.Poornima, Srinivasulu Sirisala, P.Dileep Kumar Reddy ,G. Ramesh etal,…[4] The proposed generic framework represents a sophisticated and versatile solution designed to address the complexities of sharing data within the intricate realm of a Hybrid Cloud environment. At its core, this framework relies on the advanced principles of Attribute Based Cryptography (ABC) to introduce a paradigm shift in data security and privacy. By leveraging ABC, the framework enables a dynamic and fine-grained control mechanism for data access, departing from conventional approaches. The intricacies of user attributes become pivotal in determining access policies, offering a nuanced and customized approach to data sharing. This attribute-centric model not only enhances confidentiality but also establishes a foundation for controlled and tailored sharing practices across diverse cloud environments. Through the incorporation of ABC, the framework navigates the challenges associated with secure data sharing, providing a comprehensive and adaptive solution that aligns seamlessly with the evolving landscape of Hybrid Cloud architectures. This innovative approach contributes to the establishment of a robust and privacy-conscious infrastructure for organizations seeking to optimize data sharing capabilities while maintaining a heightened level of security.

Mua'ad Abu-Faraja, Abeer Al-Hyarib, Ismail Altaharwaa, Zaid Alqadic and Basel J. A. Alid etal,…[5] It is critical to safeguard confidential data, especially secret and private messages. This study introduces a novel data cryptography approach. The new approach will be capable of encrypting and decrypting any communication size. The suggested approach will use a sophisticated private key with a convoluted structure. The private key will have 5 components with a double data type to prevent guessing or hacking. The confidential data will produce two secret keys, the first of which will be taken from the image key. These keys will be vulnerable to slight changes in private key information. To maximize the approach's efficiency, the suggested method will deal with lengthy messages by splitting them into chunks. On the other hand, the chaotic logistic map model will be used to create the second key. The suggested technique will be implemented, and several sorts of analysis (sensitivity, quality, security, and speed analysis) will be undertaken to demonstrate the benefits of the proposed method. The quality metrics MSE, PSNR, and CC will be computed to validate the suggested method's quality. To illustrate the efficiency of the proposed technique, encryption and decryption times will be measured, and cryptography throughputs will be determined. Various PKs will be tried throughout the decryption process to demonstrate how sensitive the produced outputs are to changes in the private key. The suggested approach will be tested, and the results will be compared to the results of existing methods to demonstrate the improvement offered by the proposed method.

3. PROPOSED METHOD

In the realm of secure cloud computing, the storage of encrypted data in the cloud and the controlled issuance of decryption keys to authorized users are fundamental principles. To maintain data security and access control, the data owner must also encrypt the data when a user's access is revoked and issue new decryption keys to valid users. However, in the complex environment of cloud computing, characterized by multiple distributed cloud servers and unreliable network communications, ensuring that these re-encryption commands are reliably received and executed becomes a challenging task.

In the era of digitization, securing sensitive information is paramount, especially when dealing with crime records. This project aims to develop a secure crime record sharing system by leveraging advanced techniques in cryptography and steganography. Cryptography ensures secure data transmission, while steganography conceals sensitive information within seemingly innocuous media files. This system, developed using NetBeans for application design and HeidiSQL for database management, addresses the critical need for confidentiality.

The modular nature of a NetBeans Platform application gives you the power to meet complex requirements by combining several small, simple and easily tested modules encapsulating coarsely-grained application features. Powerful versioning support helps give you confidence that your modules will work together, while strict control over the public APIs your modules expose will help you create a more flexible application that's easier to maintain. Since your application can use either standard NetBeans Platform modules or OSGi bundles, you'll be able to integrate third-party modules or develop your own. Most serious applications need more than one window.

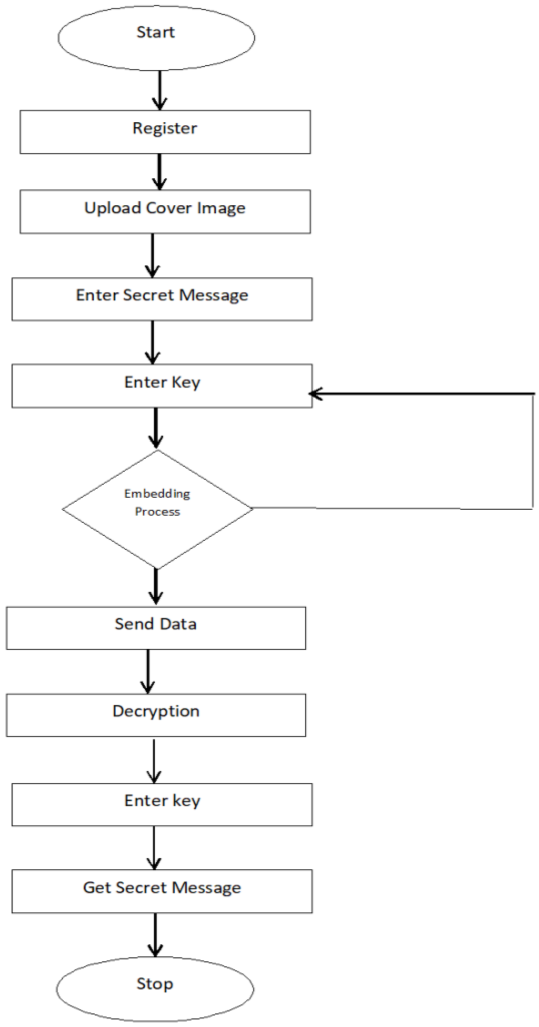


Fig. 1.1 Data Flow Diagram

Coding good interaction between multiple windows is not a trivial task. The NetBeans window system lets you maximize/minimize, dock/undock, and drag-and-drop windows, without you providing any code at all. Swing and JavaFX are the standard UI toolkits on the Java desktop and can be used throughout the NetBeans Platform. Related benefits include the ability to change the look and feel easily via "Look and Feel" support in Swing and CSS integration in Java FX, as well as the portability of GUI components across all operating systems and the easy incorporation of many free and commercial third-party Swing and Java FX components.

With the NetBeans Platform you're not constrained by one of the typical pain points in Swing: the J Tree model is completely different to the J List model, even though they present the same data. The NetBeans Nodes API provides a generic model for presenting your data. The NetBeans Explorer & Property Sheet API provides several advanced Swing components for displaying nodes. In addition to a window system, the NetBeans Platform provides many other UI- related components, such as a property sheet, a palette, and complex Swing components for presenting data, a Plugin Manager, and an Output window.

3.1 TOMCAT ARCHITECTURE

Tomcat's architecture follows the construction of a Matrushka doll from Russia. In other words, it is all about containment where one entity contains another, and that entity in turn contains yet another. In Tomcat, a 'container' is a generic term that refers to any component that can contain another, such as a Server, Service, Engine, Host, or Context. Of these, the Server and Service components are special containers, designated as Top Level Elements as they represent aspects of the running Tomcat instance. All the other Tomcat components are subordinate to these top level elements. The Engine, Host, and Context components are officially termed Containers, and refer to components that process incoming requests and generate an appropriate outgoing response.

Nested Components can be thought of as sub-elements that can be nested inside either Top Level Elements or other Containers to configure how they function. Examples of nested components include the Valve, which represents a reusable unit of work; the Pipeline, which represents a chain of Valves strung together; and a Realm which helps set up container-managed security for a particular container. Other nested components include the Loader which is used to enforce the specification's guidelines for servlet class loading; the Manager that supports session management for each web application; the Resources component that represents the web application's static resources and a mechanism to access these resources; and the Listener that allows you to insert custom processing at important points in a container's life cycle, such as when a component is being started or stopped. Not all nested components can be nested within every container. A final major component, which falls into its own category, is the Connector.

It represents the connection end point that an external client (such as a web browser) can use to connect to the Tomcat container.

Fig 1.2

3.2 TOP LEVEL COMPONENTS

The Server and Service container components exist largely as structural conveniences. A Server represents the running instance of Tomcat and contain some or more Service children, each of which represents a collection of request processing components.

3.2.1 SERVER

A Server represents the entire Tomcat instance and is a singleton within a Java Virtual Machine, and is responsible for managing the life cycle of its contained services.

The following image depicts the key aspects of the Server component. As shown, a Server instance is configured using the server.xml configuration file.

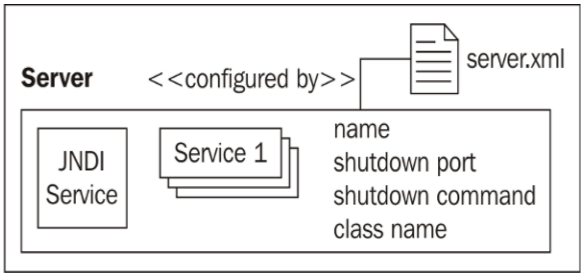


Fig 1.3

3.2.2 SERVICE

While the Server represents the Tomcat instance itself, a Service represents the set of request processing components within Tomcat.

A Server can contain more than one Service, where each service associates a group of Connector components with a single Engine.

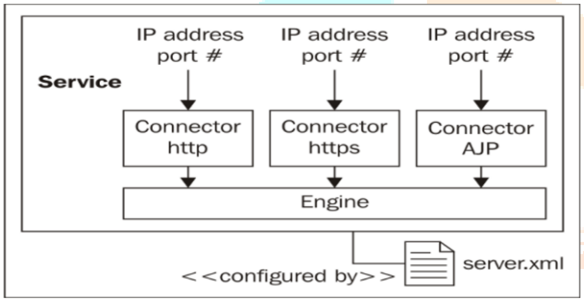


Fig 1.4

3.2.3 CONNECTOR

A Connector is a service endpoint on which a client connects to the Tomcat container. It serves to insulate the engine from the various communication protocols that are used by clients, such as HTTP, HTTPS, or the Apache JServ Protocol (AJP). Tomcat can be configured to work in two modes—Standalone or in Conjunction with a separate web server.

In standalone mode, Tomcat is configured with HTTP and HTTPS connectors, which make it act like a full-fledged web server by serving up static content when requested, as well as by delegating to the Catalina 23 engine for dynamic content.

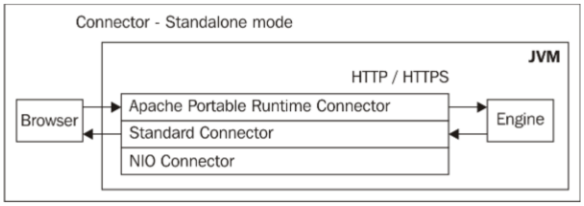

Connector - Standalone mode
JVM
HTTP / HTTPS
Browser
Apache Portable Runtime Connector
Standard Connector
NIO Connector
Engine

Fig 1.5

4. COMBINATION OF CRYPTOGRAPHY AND STEGANOGRAPHY

Law enforcement agencies constantly grapple with the challenge of balancing collaboration and data security. Sharing sensitive crime records across jurisdictions is crucial for tackling complex criminal activities, but traditional methods often leave data vulnerable to interception. This is where a novel approach combining cryptography and steganography emerges as a powerful solution.

Imagine a system where crime record data is first encrypted using robust algorithms like AES, scrambling the information into an unreadable format.

This initial layer of security ensures confidentiality – even if intercepted, the data remains unintelligible without the decryption key. However, for an extra layer of protection, steganography comes into play. Encrypted data is then seamlessly embedded within a seemingly innocuous digital carrier file, such as an image or audio file.

Techniques like Least Significant Bit (LSB) embedding achieve this feat by modifying the least significant bits of the carrier file, effectively hiding the data in plain sight. The beauty lies in the fact that the carrier file appears unaltered to the naked eye, further concealing the existence of the sensitive information.

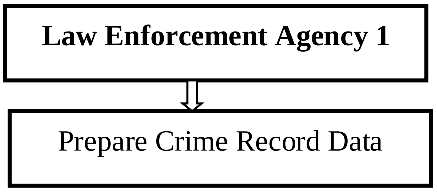
To facilitate secure exchange between authorized agencies, a secure key exchange protocol like Diffie-Hellman comes into play. This protocol allows agencies to establish a shared secret key without ever revealing the actual key itself.

This shared key is then used to decrypt the embedded data at the receiving agency. Once received, steganographic techniques extract the original crime record data, making it accessible for investigative purposes.

5. RESULT AND DISCUSSION

This approach offers a multitude of benefits. Firstly, the combination of encryption and steganography provides a layered defense, significantly enhancing data security.

Secondly, it fosters improved collaboration between law enforcement agencies by enabling the secure and efficient sharing of critical crime records. This can lead to faster investigations, better coordination, and ultimately, a safer society.



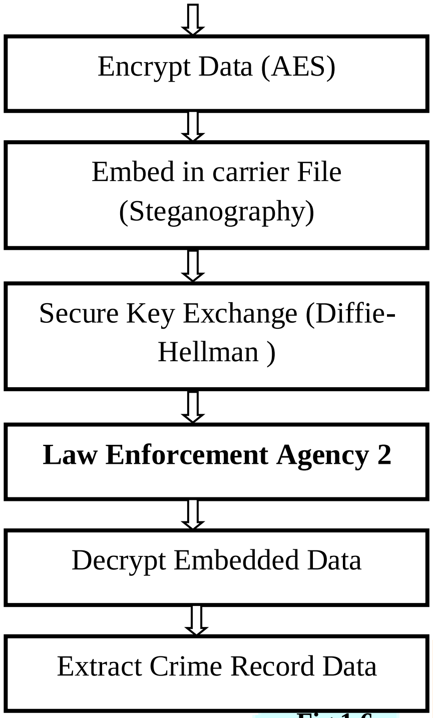
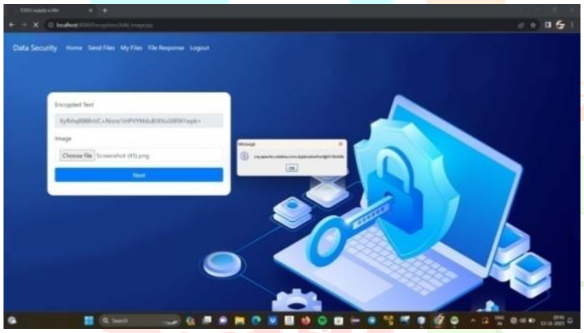

Encrypt Data (AES)
Embed in carrier File (Steganography)
Secure Key Exchange (Diffie-Hellman)
Law Enforcement Agency 2
Decrypt Embedded Data
Extract Crime Record Data

Fig 1.6

Finally, the ability to redact or anonymize sensitive information within records before encryption adds another layer of privacy protection for individuals.



Encrypted Text: [illegible]

Image: Screenshot (45).png

Fig 1.7

However, implementing such a system requires careful consideration of technical aspects. Choosing the right encryption algorithm is crucial, balancing the need for robust security with the processing power limitations of potential user devices. Similarly, steganographic techniques need to be carefully selected to maximize data hiding capacity while minimizing distortion to the carrier file, ensuring the file remains inconspicuous. Secure key management protocols and mechanisms for storing these keys securely are also paramount to prevent unauthorized access.

6. CONCLUSION

In conclusion, the practice of hiding encrypted text within digital images using steganography represents a powerful and versatile approach to enhancing the security and confidentiality of sensitive information in the digital age. This technique combines the strengths of encryption and steganography, leveraging the ubiquity of digital images for covert data storage while ensuring that the concealed information remains inconspicuous to casual observers. Throughout this exploration, we have delved into the fundamentals of this process, understanding how encryption transforms plaintext into an unintelligible form and how steganography seamlessly embeds this cipher text within images. The careful alteration of pixel values ensures that the visual quality of the image remains intact, striking a balance between security and imperceptibility.

REFERENCES

[1]Kunal K. M., et al.,(2016), A Mathematical Model for Secret Message Passing usingStenography. IEEE ICCIC, 1-6.

[2] Ghanwat, D. and Rajan, R. S. (2013). Spread Spectrum-based Audio Steganography in the Transformation Domain. Global Journal of Advanced Engineering Technologies, 2(4):66-77. 2013.Adeboje, O. T., Adetunmbi, A. O. and Gabriel, A. J. (2020).

[3] Embedding Text in Audio Steganography System using Advanced Encryption Standard and Spread Spectrum. International Journal of Computer Applications(0975-8887). DOI:10.5120/ijca2020919. Volume 177, Number 41. Pp 46-51.

[4] Olomo, R., Misra, S., Ahuja, R., Adewumi, A., Ayeni, F. and Mmaskeliunas, R. (2020). Image Steganography and Steganalysis Based on Least Significant Bit (LSB). In: Singh P., Panigrahi B., Suryadevara N., Sharma S., Singh A. (eds) Proceedings of ICETIT 2019. LectureNotes in Electrical Engineering, vol 605. Springer, Cham.

[5] Ramandeep Kaur, Pooja, “XOR Encryption Based Video Steganography”, International Journal of Science and Research (IJSR), Vol.4, Issue 11, November 2015.

[6] Mamta Juneja and Parvinder Singh Sandhu, “Improved LSB based Steganography Techniques for Color Images in Spatial Domain”, International Jounal of Network Security, Vol.16, No. 6, pp- 452-462, Nov.2014.

[7] Hemant Gupta, Setu Chaturvedi, “Video Steganography Through LSB Based Hybrid Approach”, International Journal of Computer Science and Network Security, vol.14, No.3, pp 99-106

[8] Atallah M. Al-Shatnawi, “A New Method in Image Steganography with Improved Image Quality”, Applied Mathematical Sciences, Vol. 6, 2012, no. 79, pp .3907 – 3915.

[9] Krishan Kumar, Deepti D. Shrimankar, Navjot Singh, (2017), V-LESS: a Video from Linear Event SummarieS, CVIP17, 1-6.