IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Beyond Encryption: Harnessing Cryptography and Stenography for Robust Data Security

[1]Ravi Pratap Singh, [2]Dr. Bibek Kumar,

[1]M.Tech Scholar,[2]Assistant Professor
[1]Department of Computer Science & Engineering,
[1]Vishveshwarya Group of Institutions, Gautam Buddh Nagar, India

Abstract: By harnessing the potential of cryptography and steganography in tandem, this research seeks to explore the synergies between these techniques and their practical application in real-world scenarios. The study delves into various cryptographic algorithms and steganographic methods, examining their strengths, weaknesses, and compatibility. It investigates how these techniques can be integrated into a comprehensive data security framework that transcends traditional encryption practices.
The research also addresses the challenges associated with the combined use of cryptography and steganography. The integration of these techniques requires careful consideration of factors such as computational complexity, storage requirements, and the potential impact on data integrity. Balancing these aspects is essential to ensure that the security measures implemented are both effective and practical.

Index Terms **- Cryptography, Steganography, AES algorithm.**

1.1 Introduction

In today's digital age, the exchange, storage, and protection of information have become integral to various aspects of our lives. From personal communication to financial transactions, sensitive data is constantly transmitted over computer networks and the internet. However, this widespread reliance on digital channels also exposes data to various security threats. The unauthorized access, interception, and misuse of confidential information pose significant risks, leading to potential financial, reputational, and even personal harm. Thus, ensuring robust data security has become a critical imperative in our interconnected world.

The combination of cryptography and steganography presents a powerful approach to data security. By harnessing the synergies between these two techniques, it is possible to provide enhanced protection for sensitive information. Cryptography ensures the confidentiality of data through mathematical transformations and secure key management, while steganography adds an additional layer of obfuscation and camouflage, concealing the existence of the data itself. This combined approach offers a two-pronged defense against unauthorized access and strengthens the overall security framework.

1.2 Motivation

The motivation behind this research stems from the increasing need to go beyond traditional encryption techniques and explore innovative methods to secure data in a robust manner. As technology evolves and cyber threats become more sophisticated, it is crucial to stay ahead of potential vulnerabilities and ensure the confidentiality, integrity, and availability of sensitive information.

1.3 Problem Statement

The problem lies in the vulnerabilities associated with the use of encryption techniques as standalone measures. While encryption effectively obscures data from unauthorized individuals, the presence of encrypted information itself may draw attention and indicate the existence of sensitive data. This can potentially attract the interest of adversaries who may use different attacks to circumvent encryption and gain access to the secure data illegally. As such, there is a pressing need for additional layers of protection to counter such threats and enhance data security.

1.4 OBJECTIVES

- Explore the Fundamentals of Cryptography: This sub-objective involves a comprehensive examination of various encryption algorithms, both symmetric and asymmetric, their strengths, weaknesses, and applications.
- Analyze the limitations of encryption techniques: An in-depth investigation of the vulnerabilities and potential attacks that can compromise encrypted data.
- Evaluate the integration of cryptography and steganography: Integration of cryptography and steganography as a two-layered approach to data security.

1.5 SCOPE OF PROJECT

- This research encompasses the exploration and integration of cryptography and steganography techniques to enhance data security beyond traditional encryption methods.
- The research addresses the limitations of encryption techniques, the vulnerabilities associated with encrypted data, and the need for additional security measures.
- Evaluating the performance and effectiveness of the integrated cryptographic and steganographic methods, considering factors such as perceptual quality, capacity, robustness against attacks, and computational overhead.

1.6 EXISTING SYSTEM:

- Cryptography ensures message confidentiality, integrity, and verification through encryption, decryption, and hashing. Encryption converts data into ciphertext for secure transmission, while decryption reverses this process. Hashing generates unique hash values from messages, enabling integrity verification. Cryptography is vital for securing communication systems and protecting data authenticity.
- The recipient can confirm the integrity of the message if the sender supplies a cryptographic hash with it. By using modern cryptographic methods, which rely on intricate mathematical relationships and processes, messages can be securely protected and their authenticity ensured.

2. EXPLORE THE FUNDAMENTALS OF CRYPTOGRAPHY:

The term "cryptography primitives" refers to the methods and instruments used in cryptography that is be used only when necessary to provide some certain set of security based services. These primitives are the building blocks of cryptographic systems, providing the necessary means to achieve desired security objectives. By utilizing different cryptographic primitives, such as encryption, decryption, hashing, and others, various security services can be effectively provided.

- Encryption
- Hash Function
- Message Authentication Code
- Digital Signatures

3. ANGORITHM

- The RSA algorithm is used to extract the plaintext data from a specified file and encrypt it.
- The encryption & decryption processes follow the given pattern for same plaintext M & ciphertext C.
- Ciphertext is calculated as $C = (M \wedge e) \bmod n$ where M is plain-text, e is encryption-exponent & n is modulus.

$$C = (M \wedge e) \bmod n$$

- The plain-text (M) obtained by performing decryption process as (C^d) mod n, where C is ciphertext, d is decryption-exponent & n means modulus.

$$M = (C \wedge d) \bmod n$$

- Plain-text (M) obtained by performing the decryption process, where M is plaintext, e is encryption exponent, d means decryption-exponent, and n is mod.

$$M = ((M\wedge e)\wedge d) \bmod n$$

- Plaintext is calculated, where M means plaintext, e means encryption-exponent, d is decryption-exponent and n is modulus.

$$M = (M\wedge ed) \bmod n$$

- Sender and receiver both need to be aware of what n is.
- Hence, this encryption algorithm functions as public-key, uses public key (PU) { c, n }, and private key (PR) of { d , n }.

4. OUR SYSTEM

4.1 SYSTEM ARCHITECTURE

- Figure shows the system architecture. In this system, I merged two distinct concealment methods, Steganography and cryptography.
- Employing the widely acclaimed RSA algorithm, the message undergoes a cryptographic transformation, resulting in its encryption and ensuring a formidable level of data security.
- To embed the encrypted data into an image, we employ the modified LSB approach.
- For secure communication, the sender and receiver agree on concealment and encryption keys. These keys can be shared securely or exchanged during communication to establish a confidential channel.
- To begin the process of applying cryptography & steganography, we did conversion of input into Base-64 then saved results text in text-file. From there, we did implementation of cryptography and steganography techniques.

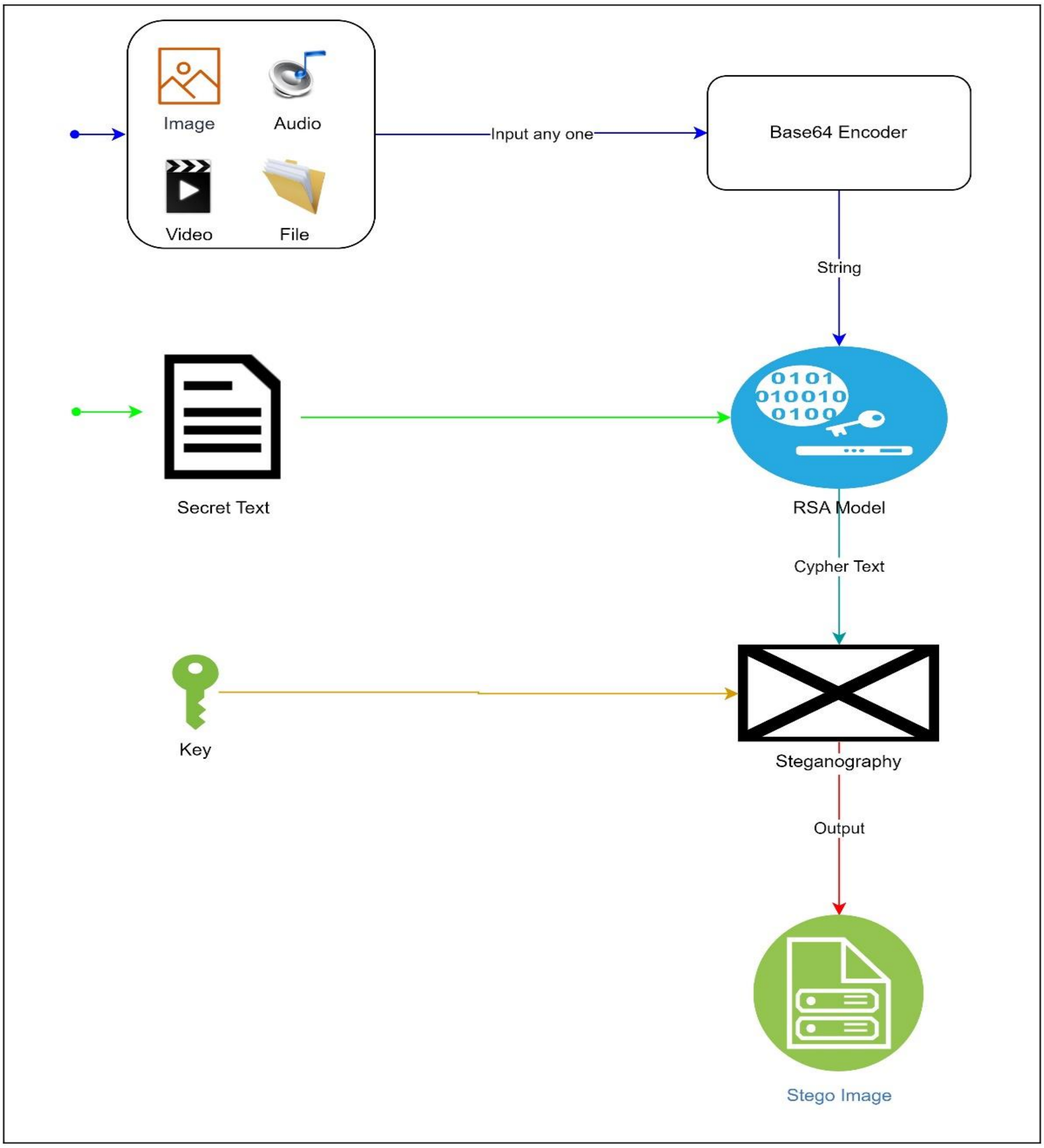

Fig-4.1: System Architecture

4.2 ACTIVITY DIAGRAM FLOW

Activity diagrams serve as graphical depictions of stepwise activities and actions, encompassing features such as choice,iteration, and concurrency. These diagrams, within Unified Modeling Language, enable the modeling of computational and organizational workflows, along with the representation of intersecting data flows. While their primary purpose is to illustrate the flow control, activity diagrams can incorporate elements that exhibit movement of data between activities through one or more data-stores.

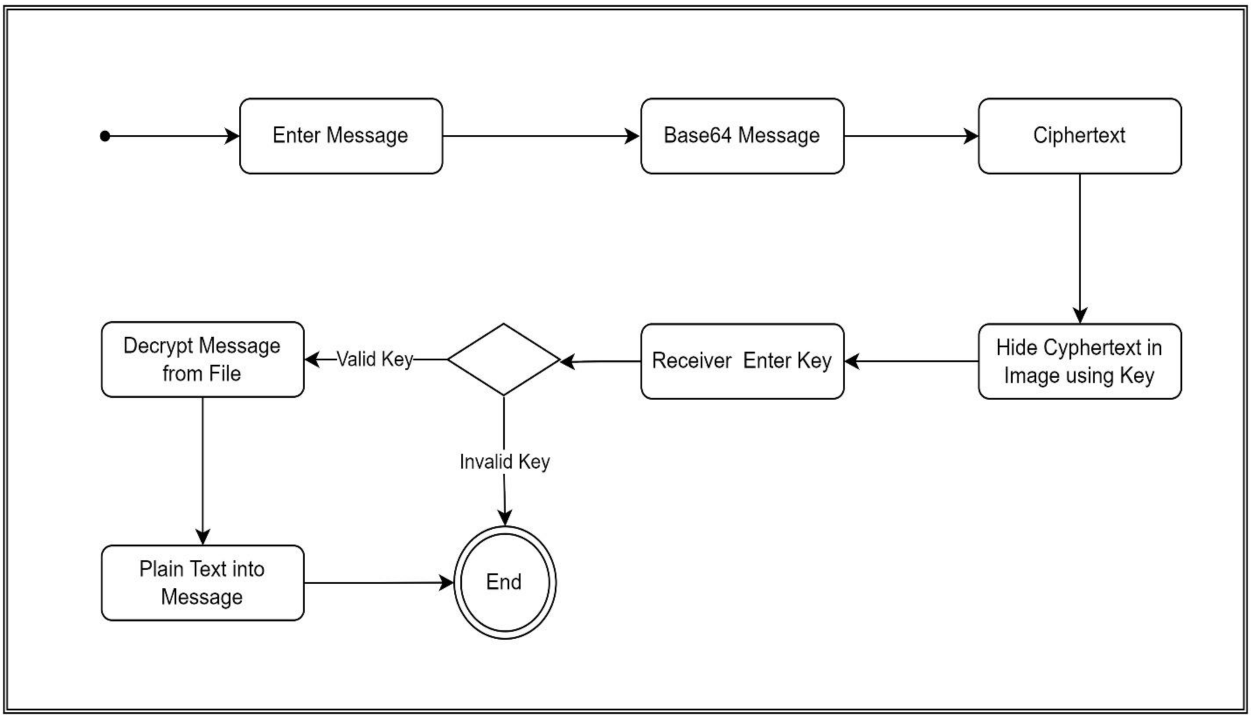

Fig- 4.2: Activity Flow

4.3 SEQUENTIAL DIAGRAM

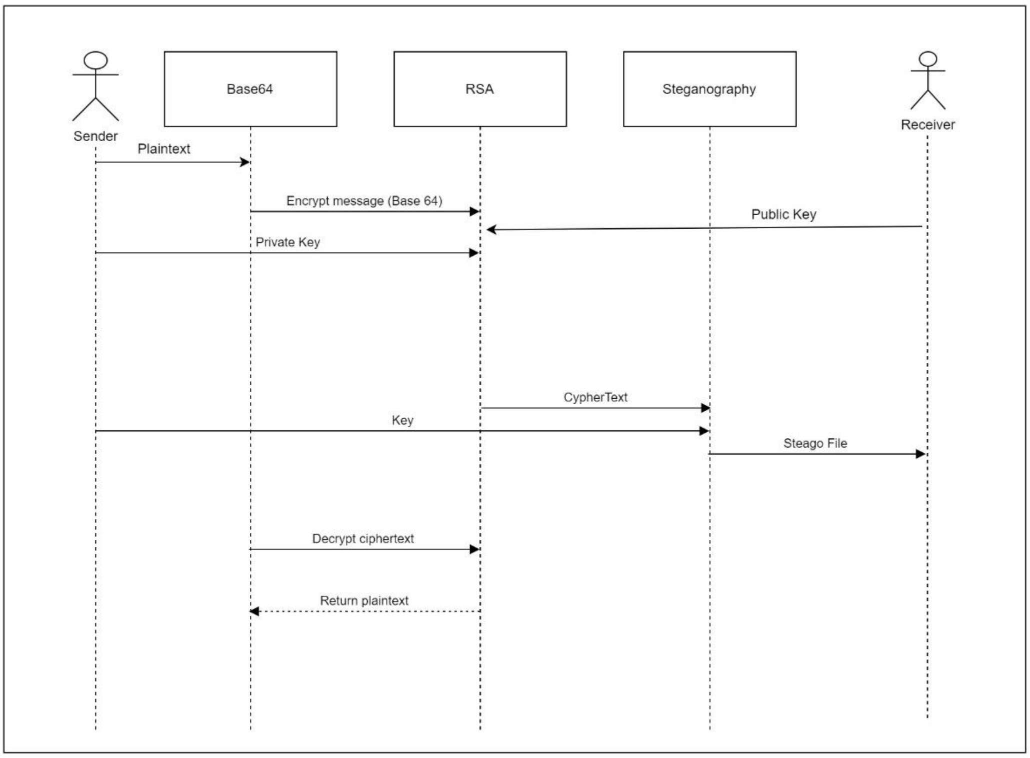

Fig-4.3: Sequential Diagram

5. RESULTS

5.1 PERFORMANCE RESULTS

Module	File Name	Resolution	Encryption Time (In Sec)	Decryption Time(In Sec)
Base-64	ijkl1.png	1080x2160	0.15531	0.0191
Base-64	ijkl2.jpg	512x320	0.03119	0.0064
Base-64	ijkl3.png	1024x768	0.016	0.0052
Base-64	ijkl4.jpg	1024x760	0.014	0.0050
Base-64	mno.mp3	__	0.19112	0.0611
Base-64	klp.mp4	__	0.29004	0.0860
RSA	__	__	8.4	17.7
Steganography	xyz.png	1080x2160	25.9	6.7

5.2 PERFORMANCE MEASUREMENT

Success rate of the total system's execution in light of the aforementioned factors determines the performance measure.

- After embedding, the secret information's integrity shouldn't be compromised.
- To the naked eye, stego item must almost remain unchanged.
- Data that has been extracted should be accurate.

The results of our research and experimentation have been highly promising. Our novel steganography method, combined with the RSA algorithm, has demonstrated impressive capabilities in securely hiding various types of data within color images. Our approach successfully concealed text, images, audio, and videos, making them imperceptible to unauthorized individuals. The combination of image files and RSA proved to be particularly effective, showcasing their high capacity for data concealment and robust security. These results validate the efficacy of our methodology in providing enhanced security for digital data communication, underscoring the potential for its practical application in real-world scenarios.

6. CONCLUSION

Our primary focus revolves around ensuring robust security for digital data communication across networks. To achieve this objective, we have meticulously designed a system that effectively combines the powerful features of steganography and cryptography, resulting in superior performance. Our research efforts have yielded a novel and innovative steganography technique, seamlessly integrated with the renowned RSA algorithm. By concealing data within images, our approach thwarts the attempts of potential attackers, rendering them oblivious to the presence of hidden information. Implementing our methodology using Python programming language, we have achieved remarkable success in concealing diverse forms of data, including text, images, audio, and videos, within vibrant color images. The extensive experiments conducted have conclusively shown that our fusion of image files and the RSA algorithm offers unparalleled advantages, primarily due to their immense capacity and security prowess.

7. REFRENCES

[1] Pradyumna Alhad, Abhinav Tonde, Atharva Bhokare , Pratiksha Dabade, Ms. Prachi Nilekar, “Secure Information Transmission Using Steganography And Cryptography” International Journal of Creative Research Thoughts. V10, 2022.

[2] Marwa E. Saleh, Abdelmgeid A. Aly, Fatma A. Omara, “Data Security Using Cryptography and Steganography Techniques” International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, 2016.

[3] Ms. Arati Appaso Pujari, Mrs. Sunita Sunil Shinde, “Data Security using Cryptography and Steganography”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. V (Jul.-Aug. 2016).

[4] H.Abdulzahra, R. AHMAD, and N. M. NOOR, “Security enhancement; Combining cryptograhy and steganography for data hiding in images,” ACACOS, Applied Computational Science,pp.978-960,2014.

[5] P. R. Ekatpure and R. N.Benkar, “A comparative study of steganography & cryptography,”2013.

[6] M. H. Rajyaguru, “Cryptography-combination of cryptography and steganography with rapidly changing keys ,”Interntional Journal of Emerging Technology and Advanced Engineering,ISSN ,pp.2250-2459,2012.

[7] D. Seth. L. Ramanathan, and A.Pandey, “Security enhancement; Combining cryptography and steganography,” International Journal of Computer Applications(0975-8887)Volume,2010.

[8] J. V. Karthik and B. V. Reddy, “Authentication of secret information in image steganography,” International Journal of Computer Science and Network Security(IJCSNS), vol. 14, no. 6. P. 58. 2014