IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023

DOI: 10.17148/IARJSET.2023.10719

Secure Communication

Jamuna S G[1], Janhavi R[2], Manaswini K M[3], Saleem S Tevaramani[4]

Dept of ECE, KSIT, Banglore, India[1-3]

Assistant Professor, ECE, KSIT, Bangalore, India[4]

Abstract: The information security has become one of the most significant problems in data communication. So it becomes an inseparable part of data communication. In order to address this problem, cryptography and steganography can be combined. This paper proposes a secure communication system. It employs cryptographic algorithm together with steganography. After that, a discrete wavelet transforms (DWT) based steganography is employed to hide the encrypted message in the cover image by modifying the wavelet coefficients. The performance of the proposed system is evaluated using peak signal to noise ratio (PSNR). The main purpose of this article is to present a new security system that enables exchange data more securely and by altering the file content structure, detecting illegal access and stopping the illegal operation.

INTRODUCTION

Secured communication refers to the process of transmitting information or data in a manner that ensures its confidentiality, integrity, and authenticity. It involves using various cryptographic techniques and security measures to protect sensitive information from unauthorized access, interception, or tampering. In today's digital age, where communication takes place over networks and the internet, securing sensitive information has become paramount. Secured communication is crucial in many domains, including personal communication, business transactions, government operations, and military activities. It ensures that only intended recipients can access and understand the transmitted data while preventing malicious entities from eavesdropping or modifying the information.In today's interconnected world, where information flows across networks and communication channels, securing sensitive data is of utmost importance. Secured communication is essential in various sectors, including personal communication, business transactions, financial services, healthcare, government operations, and military operations.

LITERATURE SURVEY

Secured communication based on WBAN[1]

Insaf Ullah, Muhammad Asghar Khan,Fazal Noor(2023) have proposed the enabling secured communication based on WBAN(wireless body area network) and HECC(hyperelliptic curve cryptography) to protect from cyber threats.it failed to provide real time communication due to the use of bilinear pairing.

Secured communication based on LBC[2].

Lang Lin,Qiliang Li,Xiaohu Xi(2022) have proposed Enabling secured communication based on LBC(linear block codes).It helps in realisation of communication between transmitter and receiver without chaotic synchronisation but it fails in distortion due to the high level of noise.The disadvantage of the above paper is that the robotic arm travels only in **180**° direction.

crypto- steganography healthcare management by using VPN[3]

Muhammed Sameer jabbar,samer saeed issa(2023) have proposed a crypto- steganography healthcare management by using VPN(virtual privet network),block chain technology.It gives evidence to increase capacity,imperceptibility and security to avoid the existing method problems.The major disadvantage is the volumes of medical data are crucial but yet difficult in communication between hospitals.

Security and privacy in metaverse based on GAN[4]

Yan Huang,Yi Joy Li,Zhipeng Cai(2023) have proposed security and privacy in metaverse based on GAN(Generative Adversarial Networks) Techniques are studied and it is the best way to protect users privacy is to cut the data exposure on the clints side.The disadvantage of this is there is a chances of leakage of private information.

Smart stratergy for data hiding based on cryptography and steganography techniques[5]

Tumma Srinivas Rao,Adhilakshmi Yanam (2023) have proposed smart stratergy for data hiding based on cryptography

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023

DOI: 10.17148/IARJSET.2023.10719

and steganography techniques are studied and it is the best way to give evidence to increase capacity and security to avoid the existing method problems.The disadvantage of this paper is it can be hacked very easily.

56GBs PAM4 physical secured communication based on quantim key distribution techniques[6]

Zhensen Goa,Ying Luo,Lihong Zhang (2023) have proposed 56GBs PAM4 physical secured communication based on quantim key distribution techniques and studied it is essential to explore advanced optical encryption technology to support high speed physical secure optical communication.Disadvantage of this paper is tolerance is critical for dicription.

METHODOLOGY

A. Proposed Method

1.Encryption: Encryption is a fundamental technique for securing communication. It involves converting the original message (plaintext) into an unreadable form (ciphertext) using an encryption algorithm and a secret key. The ciphertext can only be decrypted back into plaintext by authorized parties with the corresponding decryption key. Encryption prevents unauthorized access and eavesdropping during transmission.

2.Public Key Infrastructure (PKI): PKI is a system that utilizes asymmetric cryptography, which involves the use of a public key and a private key. In this system, each user has a unique key pair: a public key for encryption and a private key for decryption. The public keys are widely distributed, while the private keys are kept confidential. PKI ensures secure key exchange, message integrity, and authentication.

3.Secure Protocols: Secure communication protocols provide a framework for exchanging encrypted data securely over a network. Examples of such protocols include Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for securing web communications, Secure Shell (SSH) for remote logins, and Pretty Good Privacy (PGP) for email encryption.

4.Digital Signatures: Digital signatures use asymmetric cryptography to provide data integrity and authentication. A digital signature is created by applying a hash function to the message, encrypting the hash with the sender's private key, and attaching it to the message. The recipient can verify the signature using the sender's public key, ensuring that the message has not been tampered with and originated from the claimed sender.

5.Physical Security: Physical security measures, such as secure data centers, access controls, and proper disposal of sensitive information, are also critical to safeguarding communication systems and preventing unauthorized access.

6.Regular Auditing and Monitoring: Implementing a monitoring and auditing system helps identify and respond to any potential security breaches promptly.

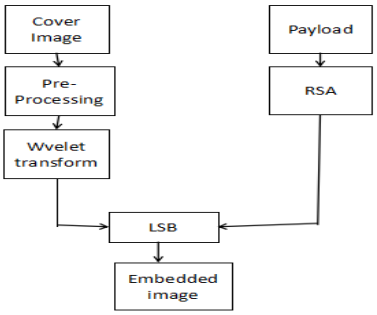

Figure 1

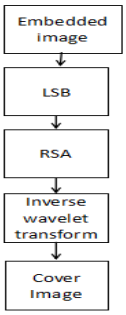

Figure 2

The components used are:

A)**Encryption Algorithms:** Encryption algorithms are fundamental components of secured communication. They are responsible for transforming plaintext data into ciphertext, making it unreadable to unauthorized parties. Common encryption algorithms include Advanced Encryption Standard (AES), RSA, and Elliptic Curve Cryptography (ECC).

B)**Public Key Infrastructure (PKI):** PKI is a framework that provides the necessary components for secure communication using asymmetric encryption. It involves the use of digital certificates, public and private key pairs, and a trusted Certificate Authority (CA) to facilitate secure key exchange, authentication, and digital signatures.

C)Wavelet transform:- The wavelet transform is a mathematical technique that analyzes signals or data in both the time and frequency domains. It is commonly used in image processing to decompose an image into different scales and orientations, allowing for the analysis of local image features at different levels of detail.

D)RSA:- RSA (Rivest-Shamir-Adleman) is an asymmetric cryptographic algorithm commonly used for encryption and digital signatures. While RSA is primarily designed for encrypting and decrypting data, it is not typically directly applied

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023

DOI: 10.17148/IARJSET.2023.10719

to images. Instead, RSA is used to secure the transmission or storage of encryption keys or digital signatures associated with images

E)LSB:- The "Least Significant Bit" (LSB) technique is a simple method used for steganography, which is the practice of hiding information within other data. When LSB is applied to an image, it involves manipulating the least significant bit of each pixel's color channel to embed hidden data.

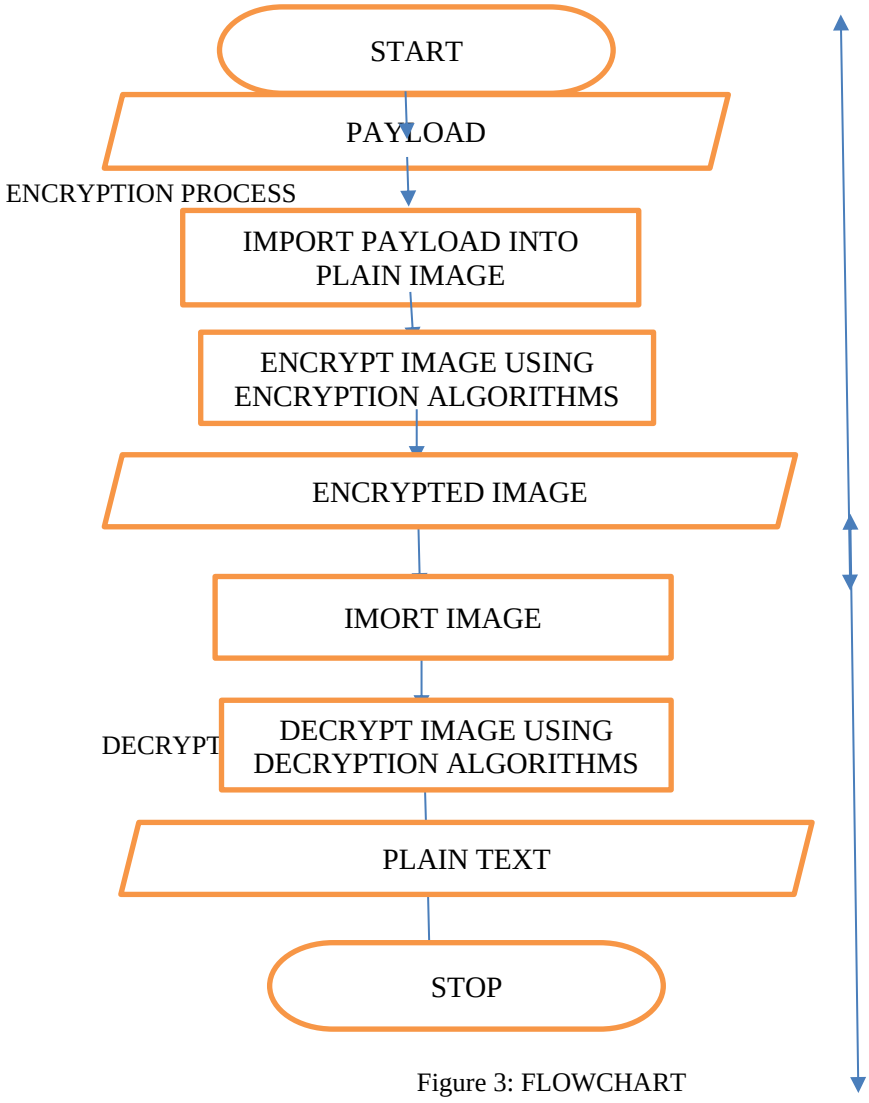

Figure 3: FLOWCHART

RESULTS

The result of secured communication is a communication process that provides confidentiality, integrity, authenticity, and protection against security threats. It instills trust, complies with regulations, and reduces the risk of data breaches, ensuring that sensitive information remains secure throughout the communication lifecycle.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023

DOI: 10.17148/IARJSET.2023.10719

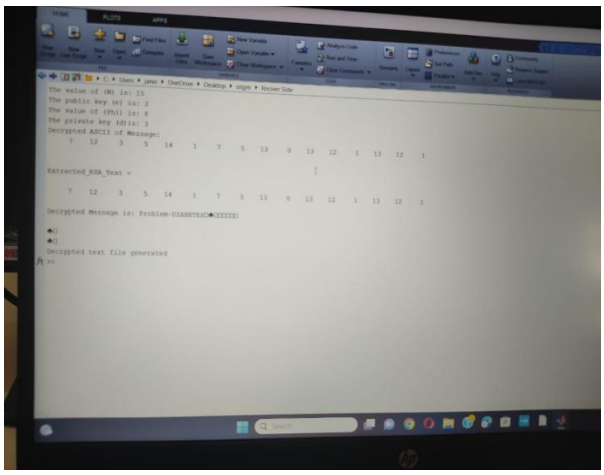

Figure 4

Figure 5

Figure 6

REFERENCES

1.Stallings, W. Cryptography and Network Security: Principles and Practice (7th Edition). Pearson.2017
2.Schneier B . Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.2015
3.Diffie, W., & Hellman, M. E. New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.1976
4.Ferguson, N schneier B & Kohno, T. Cryptography Engineering: Design Principles and Practical Applications. Wiley.2010
5.Rescorla, E. SSL and TLS: Designing and Building Secure Systems (2nd Edition). Addison-Wesley Professional.2018
6.D. P. Agrawal and Q-A. Zeng, Introduction to Wireless and Mobile Systems (2nd Edition, published by Thomson, April)
2005
7. J.K. and K. Ross, Computer Networking (2nd Ed, Addison Wesley) 2003
8.The schematics are illustrated in U.S. Patent 613,809 and describes "rotating coherers".
9.Bauer, Craig , The Early History of Voice Encryption, Boston Studies in the Philosophy and History of Science, vol. 324, Cham: Springer International Publishing, pp. 159–187, 2017
10."High-tech bugging techniques, and a costly fix". Popular Science. August 1987.
11.Pell, Stephanie K, and Christopher Soghoian. "Your secret stingray's no secret anymore: The vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy." Harv. JL & Tech 28(1).2014