IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁂ Peer-reviewed & Refereed journal ⁂ Vol. 13, Issue 12, December 2024

DOI: 10.17148/IJARCCE.2024.131223

CRYPTOGRAPHY TECHNIQUES FOR MULTIMEDIA COMMUNICATION

Manasa S[1], Monish R[2], Prerana HD[3], Rakshitha Yadav R[4], Lokesh GS[5]

Assistant Professor, Dept. of ECE, EWIT, Bengaluru, INDIA[1]

Student, Dept of ECE, EWIT, Bengaluru, INDIA [2,3,4,5]

Abstract: Secured data communication is crucial in the modern era of digital interactions. And also introduces a secure cryptographic technique for multimedia communication, incorporating audio, text, and image transmission using advanced technologies such as Light Fidelity (Li-Fi), Zigbee modules, and a Telegram bot. For audio communication, the system utilizes Li-Fi to transmit encrypted audio signals between a speaker and a solar-powered receiver, ensuring both security and energy efficiency. Solar panels are employed to power the communication system, making it sustainable and reducing dependency on external power sources. For text communication, Zigbee modules provide a low-power, reliable method for transmitting encrypted messages between the transmitter and receiver. Finally, a Telegram bot is integrated to enable the secure transmission of encrypted images, offering a user-friendly interface. The system applies cryptographic algorithms to protect data integrity and confidentiality across all communication channels. The proposed solution provides a comprehensive, energy-efficient, and secure multimedia communication framework, suitable for diverse applications.

Index Terms: Wireless communication , Encrypted data, Decryption, Zigbee modules, Cryptography, Multimedia, Li-Fi, Solar Panel, , Data Security, Sustainable Communication.

I. INTRODUCTION

With the exponential growth of digital data exchange, the need for secure communication systems has never been more critical. Traditional cryptographic methods are often insufficient when used alone due to the risk of intercepted keys. Combining cryptography with steganography offers a robust approach to secure communication. This project proposes a hybrid solution where data is hidden in multimedia files using the LSB method and encrypted with AES, a widely accepted standard for data security. The secured key is transmitted using Zigbee modules connected to Arduino devices, providing an additional layer of security. The proposed system ensures the integrity and confidentiality of data, making it highly suitable for sensitive communications.

How Cryptography Methods Used

Cryptography techniques for multimedia communication are used to ensure the confidentiality, integrity, authenticity, and non-repudiation of multimedia data such as images, audio, video, and text during transmission. These techniques protect the data from unauthorized access and tampering while preserving its quality and usability. Cryptography is essential for securing multimedia communication, ensuring confidentiality, integrity, and authenticity of images, audio, and video data. Symmetric-key cryptography offers fast encryption and decryption using a shared secret key, while public-key cryptography provides secure key exchange through public and private key pairs. Hash functions generate unique digital fingerprints for data integrity verification. However, challenges like large data sizes, With the exponential growth of digital data exchange, the need for secure communication systems has never been more critical. Traditional cryptographic methods are often insufficient when used alone due to the risk of intercepted keys. Combining cryptography with steganography offers a robust approach to secure communication. This project proposes a hybrid solution where data is hidden in multimedia files using the LSB method and encrypted with AES, a widely accepted standard for data security. The secured key is transmitted using Zigbee modules connected to Arduino devices, providing an additional layer of security. The proposed system ensures the integrity and confidentiality of data, making it highly suitable for sensitive communications.

How Cryptography Methods Used

Cryptography techniques for multimedia communication are used to ensure the confidentiality, integrity, authenticity, and non-repudiation of multimedia data such as images, audio, video, and text during transmission. These techniques protect the data from unauthorized access and tampering while preserving its quality and usability. Cryptography is essential for securing multimedia communication, ensuring confidentiality, integrity, and authenticity of images, audio, and video data. Symmetric-key cryptography offers fast encryption and decryption using a shared secret key, while public-key cryptography provides secure key exchange through public and private key pairs. Hash functions generate unique digital fingerprints for data integrity verification. However, challenges like large data sizes,

DOI: 10.17148/IJARCCE.2024.131223

1.1 Motivation

2 To develop a robust cryptography techniques for multimedia—spanning audio, text, image, and communication—stems from the rapid digitalization and increasing reliance on electronic media for personal, professional, and governmental purposes. Multimedia data, being inherently diverse in format and usage, is highly sensitive and susceptible to unauthorized access, duplication, manipulation, and interception during transmission or storage. With the rise in cyber threats, such as eavesdropping, tampering, and data breaches, safeguarding the confidentiality, integrity, and authenticity of multimedia content has become paramount.

1.2 Objectives

Develop a secure data communication application using Python for LSB-based steganography and AES encryption. Implement Arduino and Zigbee modules for encrypted key transfer between transmitter and receiver devices. Integrate real-time feedback through LCD displays for enhanced user experience. Ensure secure key entry via a 4x4 keypad on the receiver side .Ensure that multimedia content (audio, text, and images) is accessible only to authorized users.

II. METHODOLOGY

The methodology section outline the plan and method that how the study is conducted. This includes Universe of the study,sample of the study, Data and Sources of Data, study’s variables and analytical framework. The details are as follows:

To develop a robust cryptography techniques for multimedia—spanning audio, text, image, and communication—stems from the rapid digitalization and increasing reliance on electronic media for personal, professional, and governmental purposes. Multimedia data, being inherently diverse in format and usage, is highly sensitive and susceptible to unauthorized access, duplication

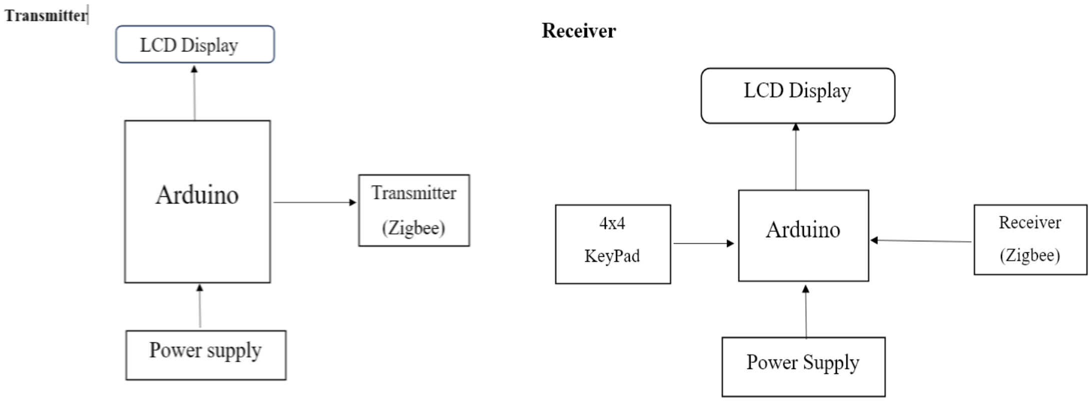


Fig 1.1 Block diagram for Text communication

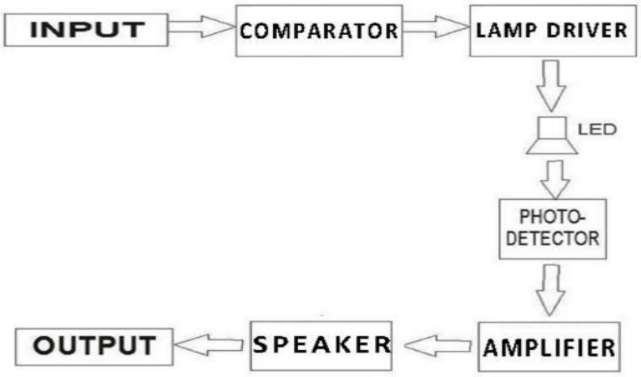


Fig 1.2 Block Diagram for Audio Communication

DOI: 10.17148/IJARCCE.2024.131223

HARDWARE USED:

- Ardino UNO.
- Power Supply
- 4x4 keypad
- LCD Display.
- Speaker
- Solar panel
- Zigbee Modules
- LED and Resister
- Battery

SOFTWARE USED:

- **Coding Language:** Python (Python 3.8 or higher).
- **IDE:** Jupyter Notebook (Anaconda Navigator).
- **UI Framework:** Tkinter (Python GUI).
- **Libraries/Frameworks:**
  - OpenCV for image processing.
  - TensorFlow or PyTorch for machine learning models.
  - Telegram API for notification system.
  - NumPy and Pandas for data manipulation.

Arduino UNO : The Arduino UNO is a versatile and widely-used microcontroller board, built around the ATmega328P chip. It is a part of the open-source Arduino platform, designed to make electronics more accessible to everyone, from beginners to experienced engineers.

Power Supply: The power supply is a crucial component in any electronic system, providing the necessary electrical energy for the operation of devices and circuits. In the case of the Arduino UNO, the board can be powered through two primary sources: via the USB connection or through an external power supply.

LCD DISPLAY :An LCD (Liquid Crystal Display) is a widely used type of screen technology that provides a clear, energy-efficient way to display information in electronic devices. In the context of microcontroller-based projects, such as those involving the Arduino UNO, an LCD display is often used to show real-time data, system status, or user feedback. Typically, a 16x2 LCD display is used in Arduino projects, featuring 16 columns and 2 rows of characters. These displays utilize a liquid crystal solution sandwiched between two layers of polarizing material to control the passage of light, allowing the display to show text or simple graphics.

4X4 Display : A 4x4 display typically refers to a 4x4 matrix keypad, which is a common input device used in electronic projects to allow users to enter data through a grid of buttons. This keypad consists of 16 buttons arranged in 4 rows and 4 columns, providing a simple interface for user input.

Speaker: A speaker in a hardware context is a device that converts electrical signals into sound. It works by using an electromagnetic mechanism, where an audio signal passes through a coil of wire, creating a magnetic field that interacts with a permanent magnet.

Solar Panel : A solar panel is a device that converts sunlight into electricity through the photovoltaic (PV) effect. It consists of many individual solar cells made from semiconductor materials, typically silicon, which absorb sunlight and release electrons.

Zigbee: Zigbee is a wireless communication protocol designed for low-power, short-range communication between devices, typically used in IoT (Internet of Things) applications. Operating on the IEEE 802.15.4 standard, Zigbee enables devices to communicate over a mesh network, allowing them to relay messages to one another and extend the network range.

LED and Resistor: An LED (Light Emitting Diode) and a resistor are often used together in electronic circuits to control the flow of electricity. The LED emits light when current flows through it, but it requires a specific voltage and current to operate efficiently and safely. If too much current flows through an LED, it can be damaged.

DOI: 10.17148/IJARCCE.2024.131223

Battery: A Battery, commonly referred to as a coin cell or button cell, is a small, portable energy source used in various electronic devices to provide low, consistent power. These batteries are typically used in devices such as wristwatches, remote controls, calculators, and motherboards to power real-time clocks (RTC) and store settings in the event of power loss.

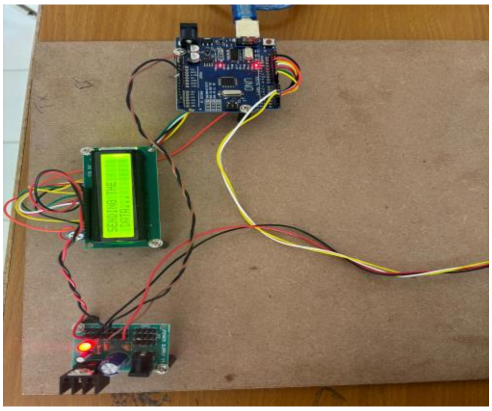
TELEGRAM BOT: . They can handle text, multimedia files, and even support interactive elements like buttons, forms, and inline queries. Bots can integrate with external APIs and databases, enabling real-time updates like weather forecasts, news, and stock prices. One of the key advantages of Telegram bots is their ability to function 24/7, providing a cost-effective, scalable solution to engage users and automate repetitive tasks

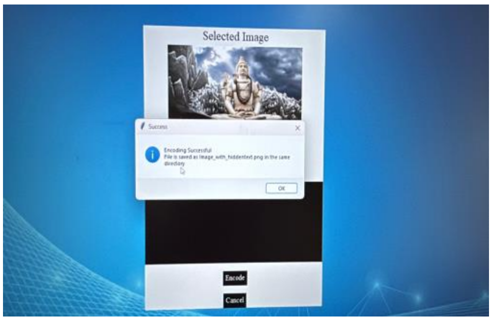
III. IMPLEMENTATION

The implementation of secure multimedia communication involves the integration of cryptographic techniques across different communication channels, including Li-Fi for audio, Zigbee for text, and Telegram Bot for image transmission. In audio communication, the process begins with capturing the audio using a microphone, which converts sound into digital data. The digital audio is then encrypted using the AES (Advanced Encryption Standard) algorithm, which is a symmetric key encryption method known for its security and efficiency. The encrypted audio is modulated into light signals by a Li-Fi modulator and transmitted via a Li-Fi transmitter. At the receiver's end, a photodetector captures the modulated light signals, and the data is demodulated and decrypted using the AES decryption algorithm. The decrypted audio is decoded and played via a speaker. The system is powered by solar panels, which provide sustainable energy to the entire Li-Fi communication system. For text communication, the message is typed by the user, then encoded and encrypted using RSA (Rivest-Shamir-Adleman) or ECC (Elliptic Curve Cryptography), both of which are asymmetric encryption techniques used for securely exchanging encryption keys and ensuring data confidentiality.

IV. RESULTS

As discussed above initially the proposed model will be helpful in secure communication. For text-based communication, ZigBee modules (low-power, short-range communication modules) are an ideal solution for secure data transmission. The ZigBee communication protocol is enhanced with encryption techniques like RSA (asymmetric encryption) or elliptic curve cryptography (ECC) to secure the text messages. The transmitter encrypts the text data before transmitting it via ZigBee, and the receiver device decrypts the message using the corresponding private key.




Selected Image

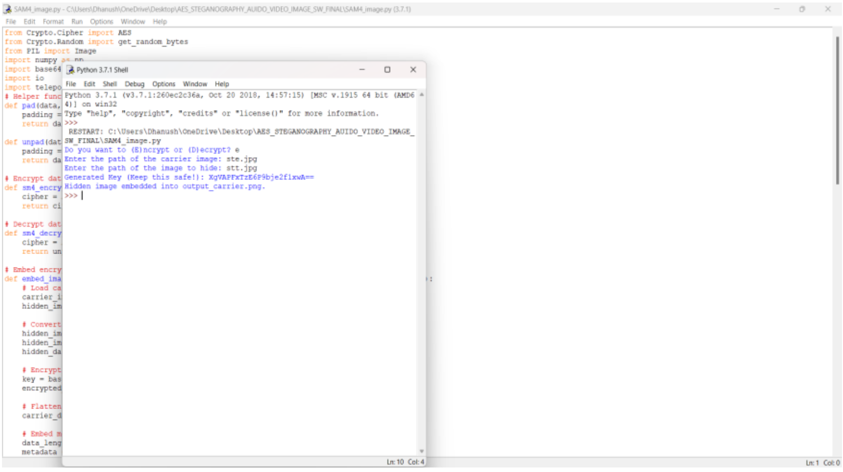
Success

Encoding Successful
File is saved as image_with_hiddentext.png in the same directory

Fig4.1.1 Text Communication

DOI: 10.17148/IJARCCE.2024.131223

In image communication, Telegram bots offer an efficient platform for transmitting encrypted images. Telegram allows for file sharing, and the communication of images can be protected using end-to-end encryption (E2EE). Before sending the image, it is encrypted using symmetric key encryption (AES), ensuring that only the intended recipient with the decryption key can access the image. Telegram bots can automatically handle the encryption and decryption process, providing seamless protection for the images being shared.


SAM4_image.py - C:\Users\Dhanush\OneDrive\Desktop\AES_STEGANOGRAPHY_AUIDO_VIDEO_IMAGE_SW_FINAL\SAM4_image.py (3.7.1)
File Edit Format Run Options Window Help
Python 3.7.1 Shell
File Edit Shell Debug Options Window Help
Ln: 10 Col: 4
Ln: 1 Col: 0

```
from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes
from PIL import Image
import numpy as np
import base64
import io
import telepo
# Helper func
def pad(data,
    padding =
    return da

def unpad(dat
    padding =
    return da

# Encrypt dat
def sm4_encry
    cipher =
    return ci

# Decrypt dat
def sm4_decry
    cipher =
    return un

# Embed encry
def embed_ima
    # Load ca
    carrier_i
    hidden_im

    # Convert
    hidden_im
    hidden_im
    hidden_da

    # Encrypt
    key = bas
    encrypted

    # Flatten
    carrier_d

    # Embed m
    data_leng
    metadata
```

```
Python 3.7.1 (v3.7.1:260ec2c36a, Oct 20 2018, 14:57:15) [MSC v.1915 64 bit (AMD6
4)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
 RESTART: C:\Users\Dhanush\OneDrive\Desktop\AES_STEGANOGRAPHY_AUIDO_VIDEO_IMAGE_
SW_FINAL\SAM4_image.py
Do you want to (E)ncrypt or (D)ecrypt? e
Enter the path of the carrier image: ste.jpg
Enter the path of the image to hide: stt.jpg
Generated Key (Keep this safe!): XgVAPFxTzE6P9bje2f1xwA==
Hidden image embedded into output_carrier.png.
>>>
```

Fig 4.1.2 Image Communication

For audio communication, the integration of Li-Fi (which uses visible light for data transmission) with cryptographic techniques ensures secure and efficient transmission of audio signals. Li-Fi's high bandwidth and fast data transfer rates make it ideal for secure real-time audio communication. The use of speakers and solar panels in this system ensures that the audio signals are transmitted wirelessly using light signals while powering the system sustainably. Audio signals are first encrypted using symmetric key cryptography (e.g., AES – Advanced Encryption Standard) to prevent unauthorized interception and to maintain data integrity during transmission.

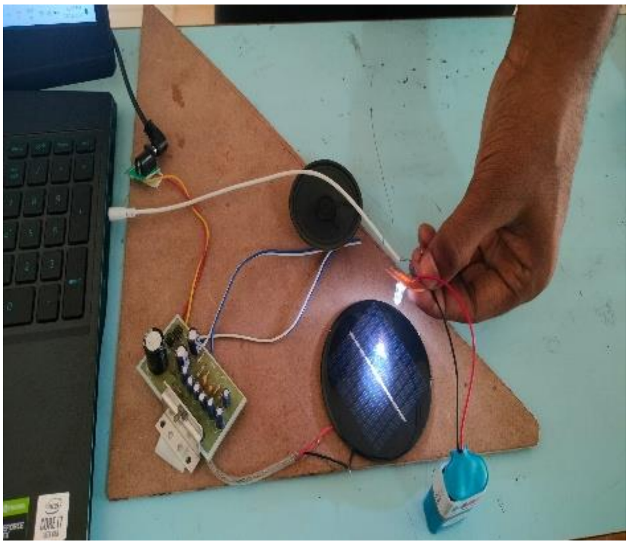


Fig 4.1.3 Audio Communication

V. CONCLUSION

The integration of cryptographic techniques into multimedia communication using Li-Fi, ZigBee, and Telegram bots ensures the secure transmission of audio, text, and image data across various platforms. Li-Fi, utilizing light signals for high-speed audio communication, can be paired with encryption methods like AES to protect audio content while leveraging solar panels for energy efficiency. ZigBee modules with encryption standards such as RSA or ECC enable secure, low-power text communication, particularly useful in IoT and smart home applications.

DOI: 10.17148/IJARCCE.2024.131223

Telegram bots enhance the security of image communication by employing end-to-end encryption, ensuring confidentiality and data integrity during transmission. These technologies provide scalable, efficient, and secure solutions for multimedia communication, ensuring that sensitive data in audio, text, and image formats is protected against unauthorized access. This approach is highly relevant in industries like healthcare, defense, and smart environments, where security and reliability are paramount.

FUTURE SCOPE

Advancements in post-quantum cryptography will be crucial to enhance security, especially as quantum computing threatens traditional encryption methods. The integration of AI and machine learning could further optimize encryption and decryption processes, enabling more adaptive, real-time security measures for audio, text, and image communication. Additionally, the expansion of 5G/6G networks will provide faster, more reliable communication channels, improving the efficiency of these cryptographic techniques, especially for high-bandwidth applications like image and audio streaming.

REFERENCES

[1]. Zhang, X., Liu, L., & Zhang, L. (2023). Li-Fi-based Communication Systems: A Survey on Security and Cryptographic Techniques. Journal of Optical Communications and Networking, 15(2), 111-126.

[2].Khan, S., & Ahmed, Z. (2023). Telegram Bots in Secure Cloud Storage and Image Sharing: A Review of Cryptographic Solutions. International Journal of Information Security, 25(1), 99-113.

[3]. Ali, F., & Ahmad, A. (2022). Leveraging Telegram Bots for Secure Image Transmission in Social Networks: Cryptographic Techniques and Privacy Considerations. International Journal of Computer Applications, 174(5), 20-28.

[4].Abo Alhassan, M., & Khalil, A. (2022). Security Enhancements for ZigBee Networks: A Cryptographic Approach to IoT Communication. Journal of Communications and Networks, 24(1), 33-45.

[5]. Sharma, A., & Bansal, S. (2022). Enhancing Privacy and Security in Multimedia Communications: A Comprehensive Review of Cryptographic Methods. Journal of Information Security and Applications, 64, 1-14

[6]. Koch, L., & Baum, J. (2021). Multimedia Encryption in IoT Networks: Cryptographic Techniques for Audio, Image, and Text Data. Springer International Publishing.