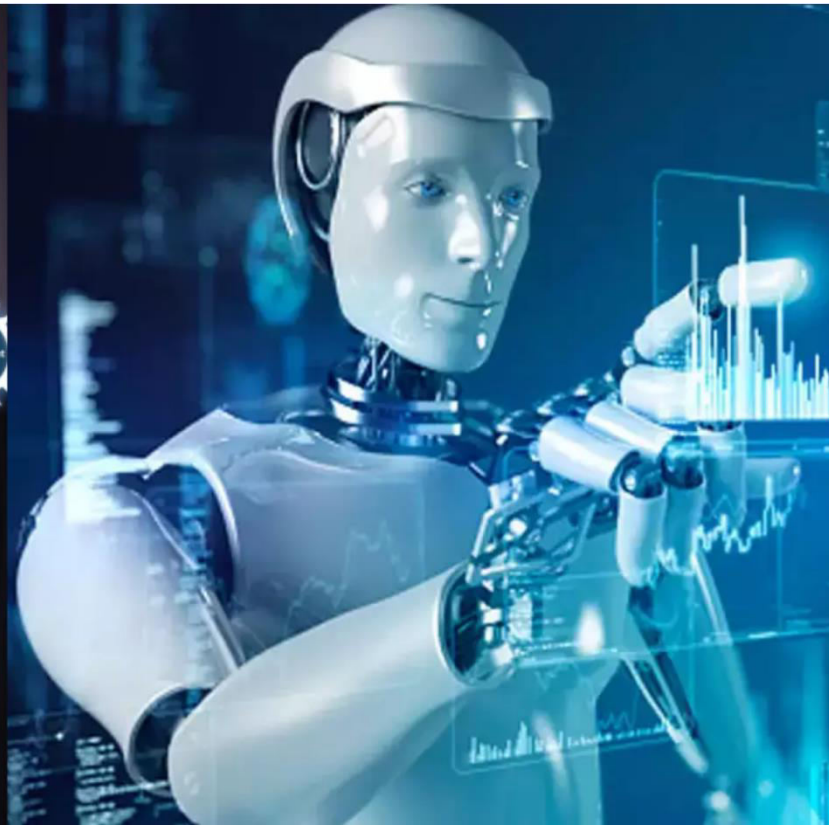
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 12, December 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412076|

A Secure Image and Audio Encryption and Decryption Framework using the AES Algorithm

Anusha J S, Kavya H V

P.G. Student, Department of Master of Computer Application, PES Institute of Technology and Management, Shivamogga, Karnataka, India

Assistant Professor, Department of Master of Computer Application, PES Institute of Technology and Management, Shivamogga, Karnataka, India

ABSTRACT: As more data is shared over unprotected networks multimedia data security has become crucial. This work offers a Python framework for encrypting and decrypting image and audio data based on AES. To guarantee privacy and integrity the system transforms multimedia content into byte sequences and processes them using AES-128/192/256 in CBC mode. The outcomes demonstrate that AES offers strong defence against statistical differential and brute-force attacks. The system is effective scalable and appropriate for the safe transfer and storage of multimedia data including audio and images.

KEYWORDS: AES, Multimedia Security, Cryptography, Image Encryption And decryption, Audio Encryption And Decryption, Python, CBC Mode, Symmetric Encryption.

I. INTRODUCTION

In today's digital world, images and audio are widely shared through online platforms, making data security a critical concern. Unauthorized access to multimedia data can lead to privacy loss and security threats. Therefore, there is a strong need for effective encryption techniques to protect such information.The Advanced Encryption Standard (AES) is a popular symmetric key algorithm known for its high security and fast performance. This paper presents an AES-based image and audio encryption and decryption system using Python. The proposed method securely converts images and audio into an unreadable format and restores them accurately using a secret key. The system provides an efficient and reliable solution for protecting multimedia data.

II. LITERATURE SURVEY

Multimedia encryption has changed over time moving from straightforward selective techniques to complex chaos and AES-based methods. One of the first image encryption methods specifically designed for progressive transmission was presented by Kuo (1993). His technique gave early insight into bandwidth-efficient and compression-friendly encryption by enabling partial image reconstruction while maintaining the security of fine details [1].

Subsequently Huang et al. examined the effects of AES on images using ECB CBC and CTR among other operation modes. They discovered that while stronger modes like CBC and CTR offer greater security and high randomness weaker modes like ECB reveal visual patterns. Their research demonstrated that image encryption requires the use of appropriate operational strategies in addition to AES [2].

Jamal et al. (2025) developed a protected S-box design which combined 1D chaotic maps with finite-field theory for security purposes. Their design implemented better confusion and nonlinearity and differential attack resistance which enhanced block cipher security for multimedia applications. The method led to the development of hybrid systems which unite chaos with AES encryption to protect digital images and audio content [3].

Sathiyamurthi and Ramakrishnan (2017) created a speech encryption method through Chaotic Shift Keying (CSK) for audio data protection. Their system used chaotic carriers to hide speech information which became

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412076|

understandable only when the receiver achieved synchronization. The system delivered robust security protection while using minimal processing power which made it appropriate for real-time voice transmission [4].

Tarabay et al. (2023) presented a low-power chaos-based encryption method for fog computing images. Their approach addressed the requirements of edge devices with limited resources by combining diffusion and chaotic permutation to produce high entropy low correlation and quick processing [5].

III. ADVANED ENCRYUPTION STANDARD ALGORITHM

A popular symmetric key encryption algorithm the Advanced Encryption Standard (AES) is renowned for its robust security and quick speed. Data is divided into fixed-size blocks and multiple rounds of mathematical operations including key addition permutation substitution and mixing are then applied. By converting the original data into an unintelligible format these procedures guarantee that no one can decipher it without the right secret key. AES supports key sizes of 128 192 and 256 bits because it strikes a balance between speed and security AES-128 is the most widely used. The procedure is easy to implement and very effective for large files because the same key is used for both encryption and decryption. AES is used in this project to secure audio and image files by first encrypting them and then precisely restoring them during decryption. AES is the best option for multimedia security applications due to its reliable performance and robust defence against attacks.

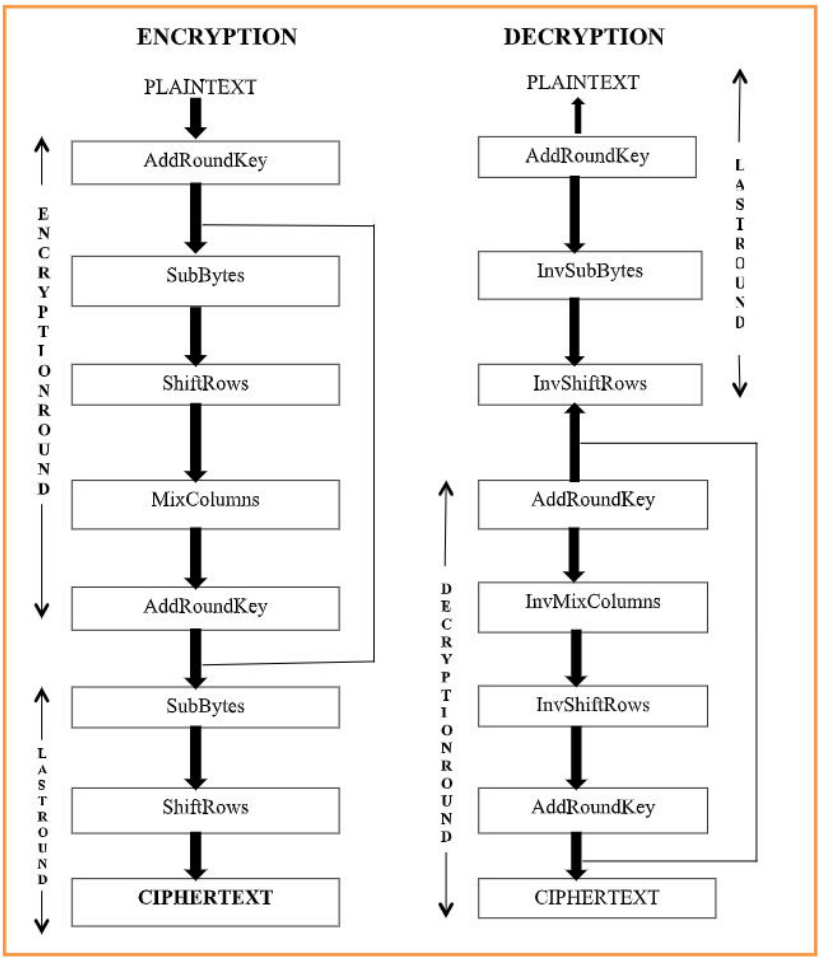


Fig.1 Encryption and Decryption Process in AES

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412076|

IV. PROPOSED METHODOLOGY

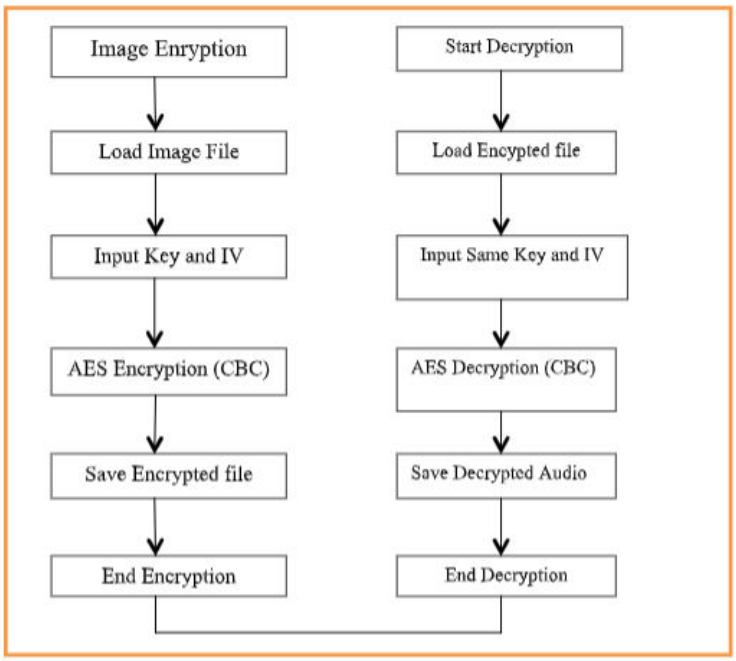


Fig. 2 Data Flow Diagram

The suggested methodology is a series of actions intended to securely and effectively encrypt and decrypt multimedia files using AES. An image or audio file is first input into the system which then transforms it into a raw byte stream that can be encrypted. In this preprocessing stage sample values for audio or pixel values for images are read and organized into a continuous byte array. Next a secure random number generator is used to create an Initialization Vector (IV) and a secret AES key. To ensure unpredictability and thwart attacks these cryptographic values are crucial. A chosen AES mode such as CBC or CTR is used to encrypt the data after it has been padded in accordance with the AES block size requirement. A ciphertext file which looks entirely random and unintelligible is used to store the encrypted output. The system retrieves both the ciphertext and the matching IV during decryption. AES mode and the same secret key are used to decrypt the ciphertext back into padded plaintext. By transforming the bytes back into image pixels or audio samples the padding is eliminated and the original multimedia format is restored. This guarantees that the original content can be recovered without loss. A number of tests including timing analysis histogram comparison entropy measurement and correlation analysis are carried out to validate the system. These assessments gauge how random encrypted data is and how well decryption works. The approach guarantees that the suggested system is safe dependable and able to safeguard private multimedia data while it is being stored and transmitted.

V. EXPERIMENTAL RESULTS

In this project, we tested how well the AES algorithm encrypts and decrypts images and audio files When we encrypted the files, the image became completely scrambled and the audio turned into noise, so no one could understand the original content .After decryption, both the image and audio returned to their original form without any changes or loss in quality The system worked smoothly, and the encryption and decryption processes were completed quickly. These results show that AES provides strong security while still being fast and accurate for both image and audio data.

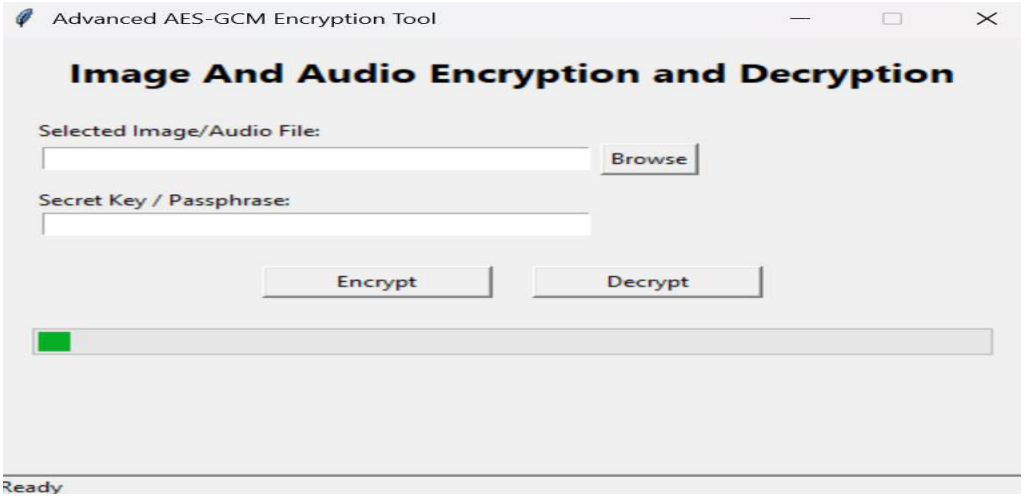
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

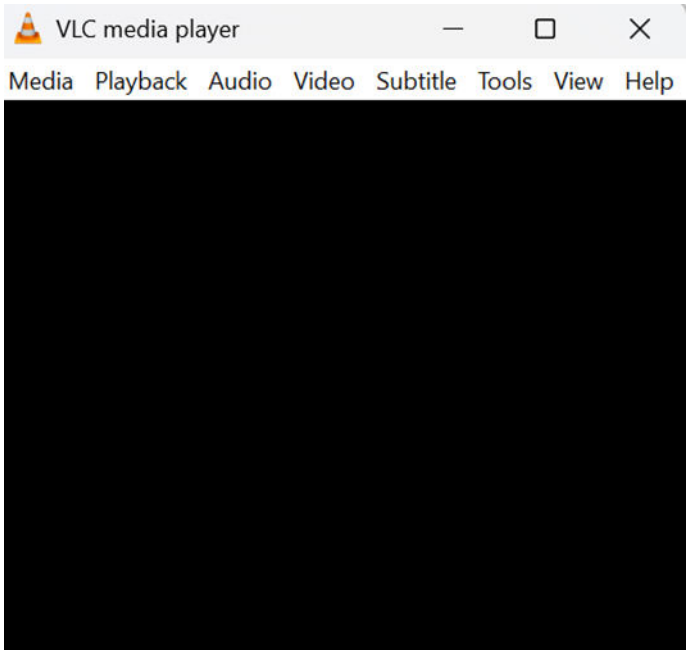
Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412076|



User Interface

The user interface of the project is designed to be clean and easy to use. It provides simple buttons to select an image or audio file and choose whether to encrypt or decrypt it. After the user uploads a file and clicks the desired option, the system processes it and shows a success message or displays the result. With just a few clicks, users can perform encryption or decryption without any technical knowledge. The interface is straightforward, user-friendly, and quick to operate.



Encrypted Image

An image that has been altered using the AES algorithm to completely conceal its original appearance is called an encrypted image. The encrypted image appears as a random pattern of pixels with no discernible structure or meaning rather than the original image. This guarantees that without the right decryption key no one will be able to decipher or retrieve information from the picture. The encrypted image can be flawlessly restored to its original state with the correct key.

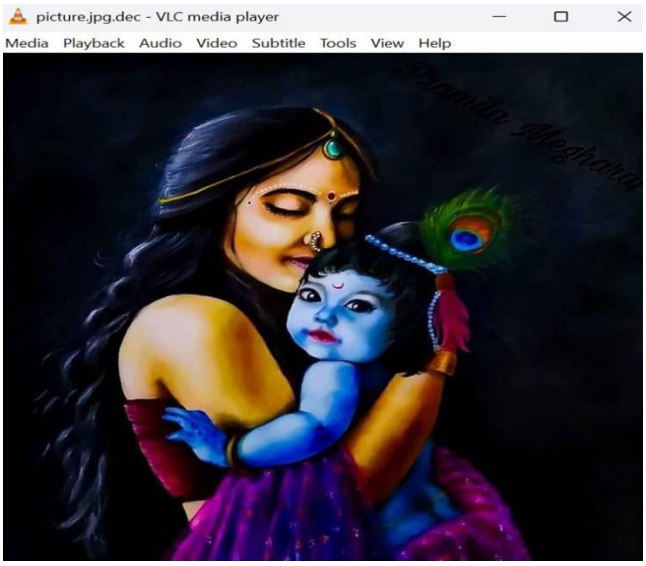
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

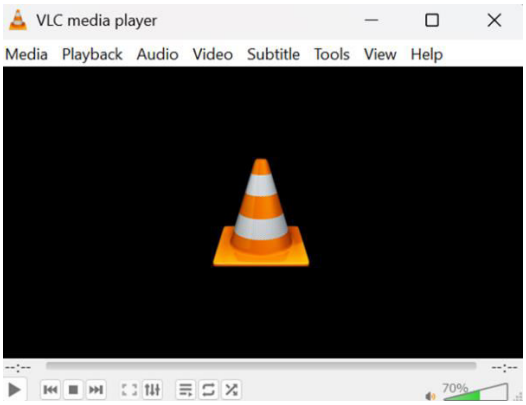
Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412076|

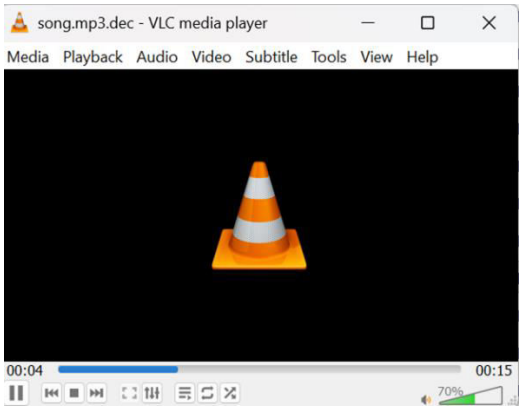


Decrypted Image

The original image that is recovered following the reversal of the AES encryption procedure is known as a decrypted image. The encrypted random-looking pixels are restored to their original visual form when the right key and IV are used. With no loss of data or quality the decrypted image is identical to the original. This demonstrates the precision and security of the encryption and decryption process.



Encrypted Audio



Decrypted Audio

Encrypted audio is an audio file that has been protected using the AES algorithm. After encryption, the original sound is converted into noise and cannot be understood by anyone. This ensures that the audio remains secure during storage or transmission. Decrypted audio is obtained when the correct secret key is used to reverse the encryption process. The decrypted audio sounds exactly like the original without any distortion. This proves that the encryption and decryption process is accurate and reliable.

VI. CONCLUSION

This work effectively shows how to use AES-based encryption and decryption in Python to protect multimedia data in a safe and effective manner. In order to maintain quick processing and lossless recovery the system applies AES in secure modes and converts image and audio files into byte streams. The experimental results verify that the decrypted files exactly match the original content while the encrypted outputs appear entirely random and disclose no useful

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412076|

information. The approach is flexible simple to use and appropriate for practical uses like cloud storage digital media sharing and secure communication. All things considered this study emphasizes AES as a dependable and useful method for protecting sensitive multimedia in contemporary digital settings.

VII. FUTURE ENHANCEMENT

The proposed AES-based image and audio encryption system can be enhanced in several ways in the future. More secure AES modes such as AES-GCM can be implemented to provide both data confidentiality and integrity. The system can be extended to support video encryption to protect complete multimedia content. A graphical user interface with more features can be developed to improve user interaction and ease of use. Cloud and IoT-based deployment can also be explored to secure multimedia data during online storage and transmission. Additionally, combining AES with chaotic or hybrid encryption techniques may further strengthen security against advanced attacks.

REFERENCES

[1] C.J.Kuo, Novel image Encryption Technique and its application in progressive transmission. Journal of Electron imaging 24 1993 pp345-351.
[2] "The AES Application in Image Using Different Operation Modes" Chi-Wu Huang1, Che-Hao Chiang2, Chien-Lun Yen2, Yi-Cheng Chen1, Kuo-Huang Chang2 and Chi-Jeng .
[3] S. S. Jamal, R. Ali, M. K. Jamil, S. A. Nooh, F. Alblehai, and Gulraiz, ''Secure S-box construction with 1D chaotic maps and finite field theory for block cipher encryption,'' Alexandria Eng. J., vol. 125, pp. 278–296, Jun. 2025.
[4] P. Sathiyamurthi and S. Ramakrishnan, ''Speech encryption using chaotic shift keying for secured speech communication,'' EURASIP J. Audio, Speech, Music Process., vol. 2017, no. 1, pp. 1–11, Dec. 2017.
[5] S. Y. Tarabay, A. Twakol, A. S. Samrah, and I. Yasser, ''A secure and efficient cryptography system based on chaotic maps for securing data image in fog computing,'' Int. J. Comput. Netw. Inf. Secur., vol. 15, no. 1, pp. 64–80, Feb. 2023,
[6] Dutta, W., Mitra, S., & Kalaivani, S. (2017, November). Audio encryption and decryption algorithm in image format for secured communication.
[7] Albahrani, E. A., Alshekly, T. K., & Lafta, S. H. A review on audio encryption algorithms using chaos maps-based techniques. Journal of Cyber Security and Mobility.
[8] Hayder Raheem Hashima, Irtifaa Abdalkadum Neamaab. Image Encryption and Decryption in A Modification of ElGamal Cryptosystem in MATLAB.
[9] Subramanyan B., Vivek M. Chhabria, T. G. Sankar Babu — "Image Encryption Based on AES Key Expansion"
[10] xinyi zhou, wei gong, wenlong fu, lianjing jin ,an improved method for lsb based color image steganography combined with cryptography, icis 2016, june 26-29, (2016).
[11] M.Anand Kumar,Dr.S.Karthikeyan "Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms" I. J. Computer Network and Information Security,vol.2,issue22,2012.
[12] In May 2009 "Audio encryption using higher dimensional chaotic map" R Gnanajeyaraman, K.Prasadh 2, Dr.Ramar3, Research scholar, Vinayaka Missions University, Salem, Tamilnadu, India.
[13] R.Gnanajeyaraman K.Prasadh, Dr.Ramar "Audio encryption using higher dimensional Chaotic map "International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.
[14] B.Subramanyan, Vivek.M.Chhabria, T.G.Sankar babu, Image Encryption Based on AES Key Expansion, 2011.
[15] J. V. Gorabal and Manjaiah D. H, "Image Encryption Approach for Security Issues"

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details