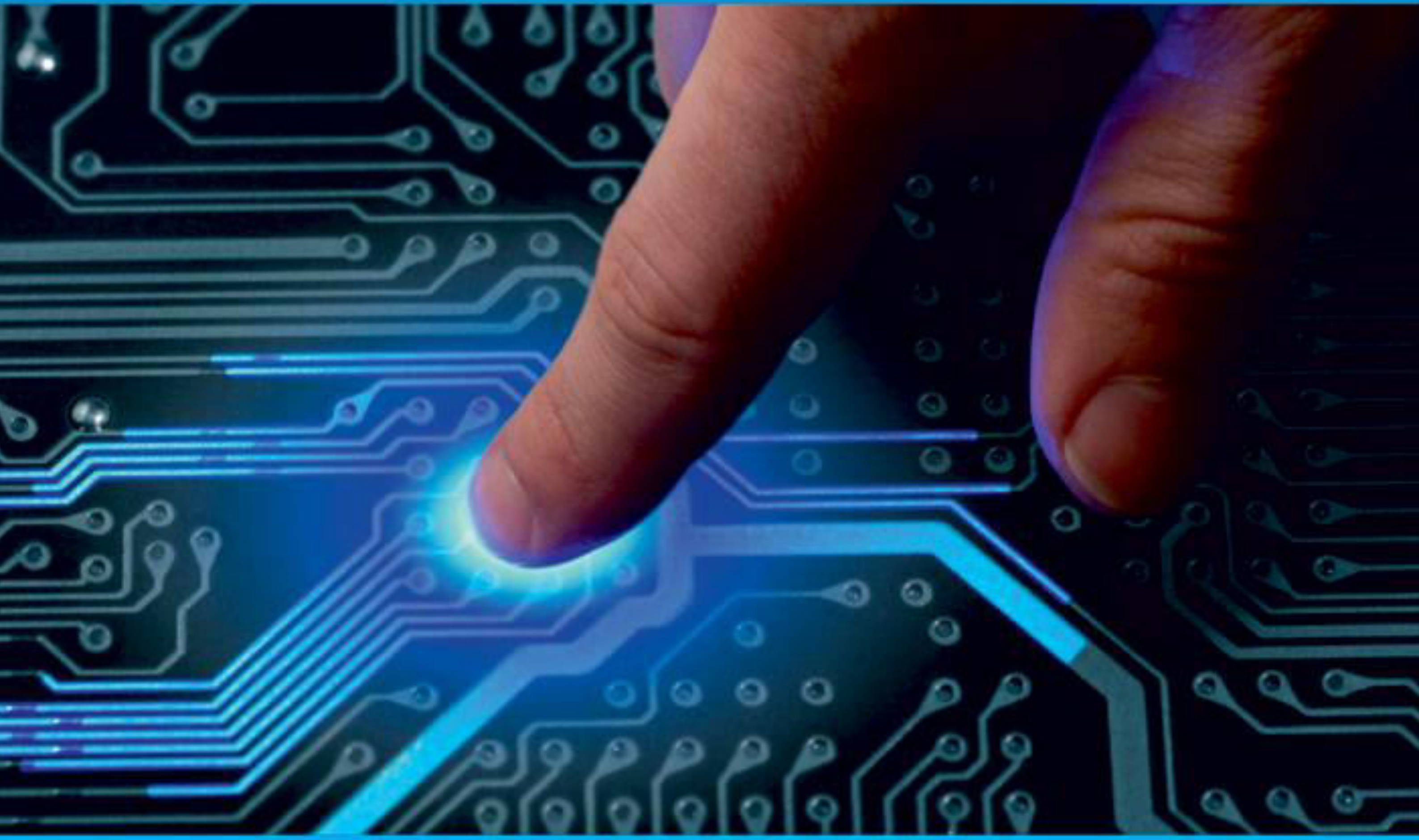
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105061 |

A Secure Chat Communication Using LSB Steganography and AES Algorithm

Vaishnavi Mamankar, Kanchan Mahajan, Diksha Chaudhari, Sayali Jagtap, Prof. Naved Raza Q. Ali

Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, India

Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, India

Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, India

Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, India

Professor, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, India

ABSTRACT: Online communication using the internet is a medium between sender and receiver to communicate. Therefore, the online communication application must be able to communicate through digital media like texts, images, audio, video, or any other files in a faster way with less delay and more security. This communications are not always secure when they are attacked by attackers. In this paper we proposed system consisting of two techniques Least Significant Bit (LSB) for embedding message to the cover image that replaces least significant bit of each pixel with the bits of message to be hidden and Advanced Encryption Standard (AES) algorithm to encrypt message before embedding into cover image that. In addition Extended AES algorithm is used that uses AES as well as caesar cipher to provide double security to the message and Firebase as a backed to host database. This chatting system with security of steganography and cryptography. The results of this study prove that this methods provides security to messages with very simple operations. The imperceptibility quality of the stego image is also excellent with a PSNR value above 50 dB and the added layer of encryption make it safer.

KEYWORDS- LSB (Least Significant Bit), MSB (Most Significant Bit), Extended AES (Advanced Encryption Standard), Firebase, Image Steganography, Cryptography.

I. INTRODUCTION

Nowadays, the Internet plays an important role in communication which helps the sender and receiver to communicate better. But sometimes it lacks security or data may get hacked by a third party. So, to improve security and hide the data from third-party steganography comes into the picture. Steganography is derived from Greek words i.e. Steganós and Graptos which means cover writing [3]. It is also known as the "invisible" transmission of data [1]. It is used to hide the message inside another cover media like image, text, audio, video, etc. Instead of sending a common message, the message will get embedded inside cover media and the media will get transmitted that will look like simple media like image, text, audio, and video but after proper decryption, we can get the hidden message inside cover media. Without proper knoledge of the procedure, it is difficult to recover the hidden factor [1]. Steganalysis is the reverse of Steganography. Steganography is used to hide the data and Steganalysis is used to recover the hidden data. Cryptography is another factor that is used to encrypt the data. It is a technique that is used to convert plain text into cipher text which is not properly readable to humans. So even after hiding the data inside the cover media and recovering it becomes difficult to read the data which provides another level of security [24].

In this proposed system we are implementing a chatting application that is a combination of steganography, cryptography, and Firebase. For embedding the data inside the cover image, we are using the Least Significant Bit (LSB) technique [1] and the Extended AES algorithm for proper encryption and decryption of data [20]. The experimented image i.e., RGB and grayscale images both can be used to hide the data. The data or message size should be less than the size of the image size so the proper intensity of the image will be maintained. First, both the message and the image will get converted into binary format. The RGB image will contain pixels of 24 bits. The data will get hidden in the LSB of each pixel i.e., Red, Green, and Blue which are divided into 8 bits each. For encryption, we are using a key as the length of the sender and receiver id for proper bit shifting. The extended Advanced Encryption Standard algorithm is difficult to crack and is more secure than traditional algorithms like AES, RSA, and SHA.

This techniques provides better security and flexible communication between sender and receiver. In this project, we are providing an open-source messaging system for secure and secret transmission with a privacy protection feature. It has powered by image steganography.

II. RELATED WORK

Yani Parti Astuti et al. [2] proposed a simple and safe way to hide messages in LSB techniques. As the traditional LSB method is simple and predictable. It needs a way to improve the security of hidden messages. To tackle this problem the XOR operation has done three times to encrypt the message before it gets embedded in the LSB. To facilitate the process of encryption and decryption of messages three MSB bits are used as keys in XOR operations.

Dr. Amarendra K et al. [3] have studied simple LSB techniques. In this technique, they used LSB (Least Significant Bit) and a symmetric key between both the sender and the receiver for the purpose of encryption and decryption of the message. This method is very simple and also it is easy to use. They used both the concept of cryptography and steganography as cryptography for the encryption of data and steganography for hiding data below cover media. It only works on grayscale images and it needs bits that will get minimum resolution between the original image and the stego image.

Wei Lu, Member of IEEE et al. [5] proposed a halftone image steganographic scheme that aims to generate stego images with good visual quality and strong statistical security of anti-steganalysis. First, the concept of pixel density is proposed and a novel construction called pixel density histogram (PDH) is proposed to design a "±1 embedding" scheme for halftone images. Then they optimized density pair selection to select density blocks that can improve visual quality. Finally, the messages are embedded through pixel density transition, where a novel pixel flipping strategy has been proposed, which can maintain the structural dependence by optimizing the pixel mesh Markov transition matrix (PMMTM). The proposed steganography scheme can achieve strong statistical security of anti-steganalysis with good visual quality without degrading the embedding capacity.

Oleg Evsutin et al. [7] studied methods of steganography and watermarking which implement embedding in digital object's hidden information sequences for various purposes. They reviewed works demonstrating current trends in development of methods and algorithms for data hiding in digital images.They focused on contemporary works illustrating current research directions in the field of information embedding in digital images.

Omar Elharrouss et al. [11] proposed a k-LSB-based method using k least bits to hide the image. For decoding the hidden image, a region detection operation has used to know the blocks that contain the hidden image. The resolution of the stego image can be affected, for that an image quality enhancement method has used to enhance the image resolution. To demonstrate the effectiveness of the proposed approach, they compared that with some of the state-of-the-art methods.

Khalil Ibrahim Mohammad Abuzanouneh et al. [14] proposed a technique for pixel selection i.e., Protecting at multiple stages using a pixel selection technique for improving steganography. To make the Steganalysis process more complicated the secret file is distributed randomly and embedded into the cover image. Image undergoes four stages PSNR, MSE, histogram analysis, and relative entropy. They introduced an algorithm that consists of complex and multiple random keys which reduce the detection of secret data. This algorithm provides a relative PSNR value which maintains the intensity of the image and provides image of good quality.

Prof S. Athinarayanan et al. [16] they had studied and used two algorithms (a)Shamir's (k, n) threshold scheme and (b) AES (Advanced Encryption Standard) Algorithm. Shamir (k, n) threshold scheme is used in the key management where it uses k shares out of n shares to regenerate the key during decryption. AES (Advance encryption standard) algorithm is used for encryption as well as decryption process. In this system the data is firstly gets encrypted with standard encryption algorithm then the key is splitted into multiple key managers. Then every key which is splitted is again gets encrypted and stored. Then the Shamir' s algorithm used to manage the keys.

Sreyam Dasgupta et al. [20] has discussed issues of data security for this they proposed algorithm: Extended AES Algorithm with custom configurable Encryption. To add more security to the existing algorithm they added additional security layer which is of modified Caesar Cipher encryption where the key will get changed for every word of the message. This additional layer is undiscoverable and customized so it will become less prone to attacks. They also discussed the uses of this algorithm as Internet banking, e-commerce transactions, top – secret government Intel, medical or legal files and phone conversations.

Dr. Abhay Kasetwar et al. [35] studied and developed a chat application project which consists of a chat server. It has embedded in two applications-the client application and the server application. Client application that runs on the client's web browser and server application which runs on any network server. The development of the chat application has been done using JavaScript, React.js, and client-server concepts. The application supports both private and public types of group conversations.

III. PROPOSED METHOD

It is a security-relevant data transmission system using image steganography in which we proposed three main methods online data transmission, message embedding, and message extraction. There is some sort of confidential data like military related or any other information that we can't transfer openly due to security reasons that's why we use image steganography.

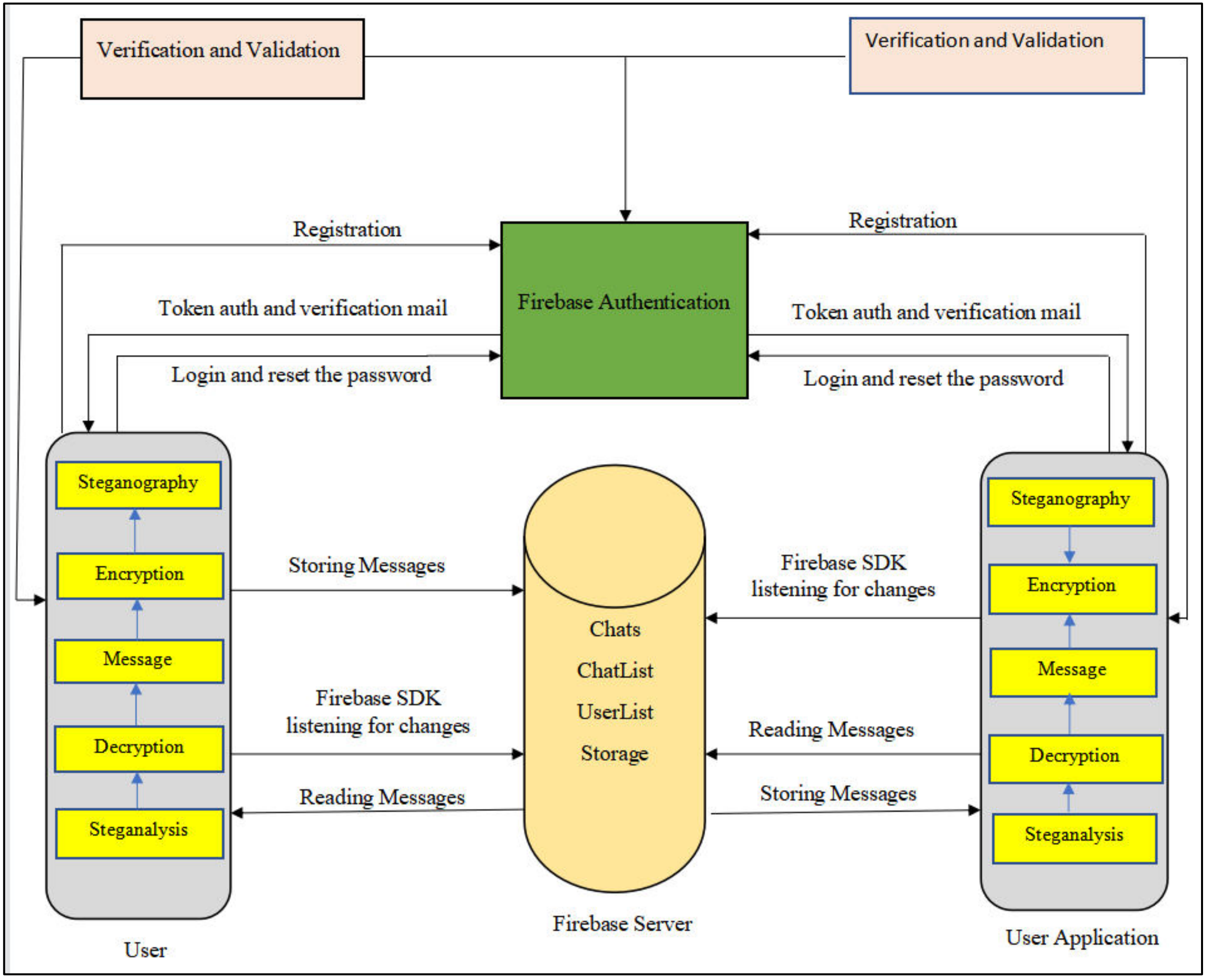


Fig. 1. Proposed Architecture of Chat Application

In this web application, we are using google firebase as the backend to store cover images, text files, and messages. User has to simply register by clicking on signup with their email and password if already register they can simply sign into the system. When the user is successfully signed into the application, the user can search for another user. The user can able to create their profile according to which they can identify each other. User can delete their accounts as well as their chat. This web application is designed using Reactjs, Nodejs, and firebase. Users can reply to the received message by just typing the reply message and pressing the send button. The user can also sign out from the current device and can sign in to another device through their account details. The following figure shows the message exchange process in detail.

Algorithms Used:

There are two types of algorithms used in this process one for embedding and extraction purposes and another for encryption and decryption purposes.

1. LSB (Least Significant Bit)
2. AES (Asymmetric Encryption Standard)

1. LSB

A] Embedding Scheme

For embedding we used the LSB algorithm, this scheme required input as a cover image and the text message or file that user wants to hide. While the output obtained is a stego image.

Here are the steps for the embedding process

1. Take a Colour image and message as input.
2. Convert the image and message into binary format.
3. Compare the size of the secret message to the cover image.
4. If the last three bits are “000” replace the first 2 bits from the LSB of the image with the message.
5. If it contains “1” in the last 3 bits so replace 1 bit of image from LSB with a secret message.
6. Continue until the end of the message.
7. Get the stego image as output.

B] Extraction Scheme:

For the extraction process, the required input is a stego image. While the output is plain text retrieved from a stego image.

Here are the steps for the Extraction process

1. Take a stego image as input.
2. Extract each of LSB bit from the stego image until the end bit is found.
3. Reconstruct the collecting LSB bits from the stego image.
4. Transform the LSB bits to the corresponding characters.

2. AES

A] Encryption Scheme:

In the encryption, the scheme required to input in the form of plain text and a key for encryption. While the output obtained is a cipher Text.

Here are the steps for the encryption process:

Step 1: Read Plain Text and Key
Step 2: Encrypt text using the Caesar cipher technique
Step 3: For AES encryption derive the round keys from the initial key
Step 4: In SubBytes, each byte is substituted by another byte
Step 5: In ShiftRows every row is shifted a particular number of times
Step 6: MixColumn does matrix multiplication
Step 7: Output of this XOR-ed with the corresponding round key.

B] Decryption Scheme:

In Decryption, the scheme required input in the form of ciphertext and key for decryption. While the output obtained is plain Text.

Here are the steps of the decryption process:

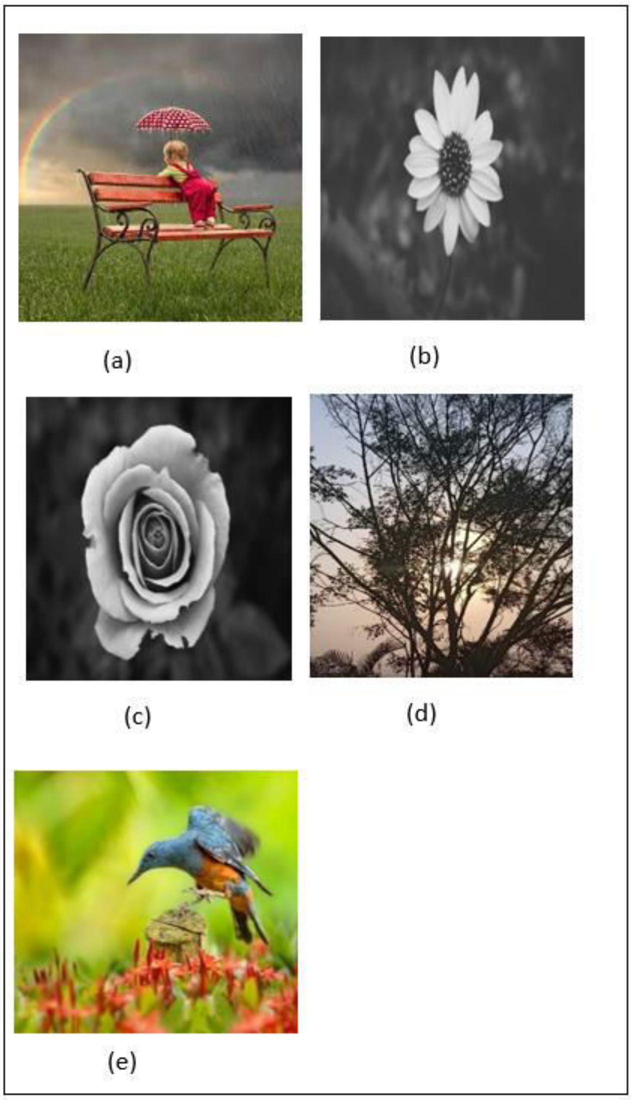
Step 1: Read cipher text and Key
Step 2: For AES decryption derive the round keys from the initial key
Step 3: Inverse MixColumn does matrix multiplication
Step 4: In ShiftRows every row is shifted a particular number of times
Step 5: In Inverse SubBytes S-box is used as a look-up table to refer to the byte substitution.
Step 6: Decrypt cipher text using Caesar Cipher.

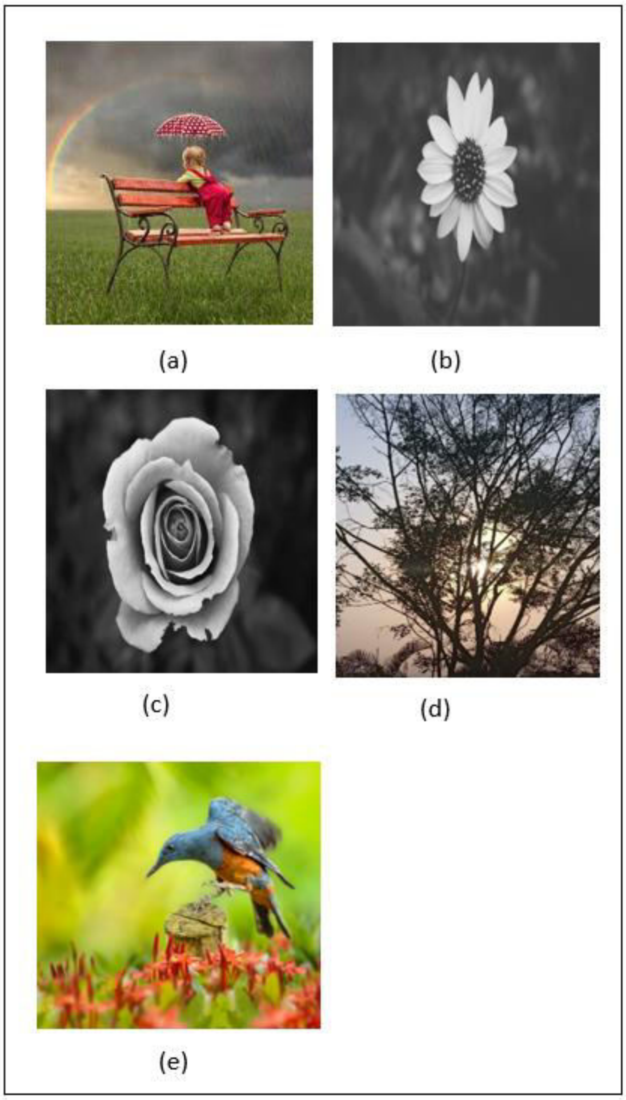
IV. EXPERIMENTS AND RESULTS

Experiment conducted in this research using some color images and grey scale images as a cover image and plaintext as a message, See Figure 2 as a cover image.

Here is the study of how cover image used in steganography:

By viewing in normal way humans cannot identify the difference between cover image and stego image. To analyze image difference and image quality we have used certain tools in this experiment are PSNR (Peak Signal-to-Noise Ratio), MSE (Mean Squared Error) and image histogram. By comparing stego image with cover image measurements have taken.





For calculation of MSE used formula 1 and for calculation of PSNR used formula 2

$$MSE = \frac{1}{a \times b} \sum_{l=0}^{a-1} \sum_{l=0}^{a-1} [C(l,m) - S(l,m)]^2 \quad (1)$$

$$PSNR = 10\, log_{10} \left(\frac{255}{MSE}\right)^{2} \qquad (2)$$

Where,
a number of rows in cover image
b number of columns in cover image
l, m size of image
C cover image
S stego image

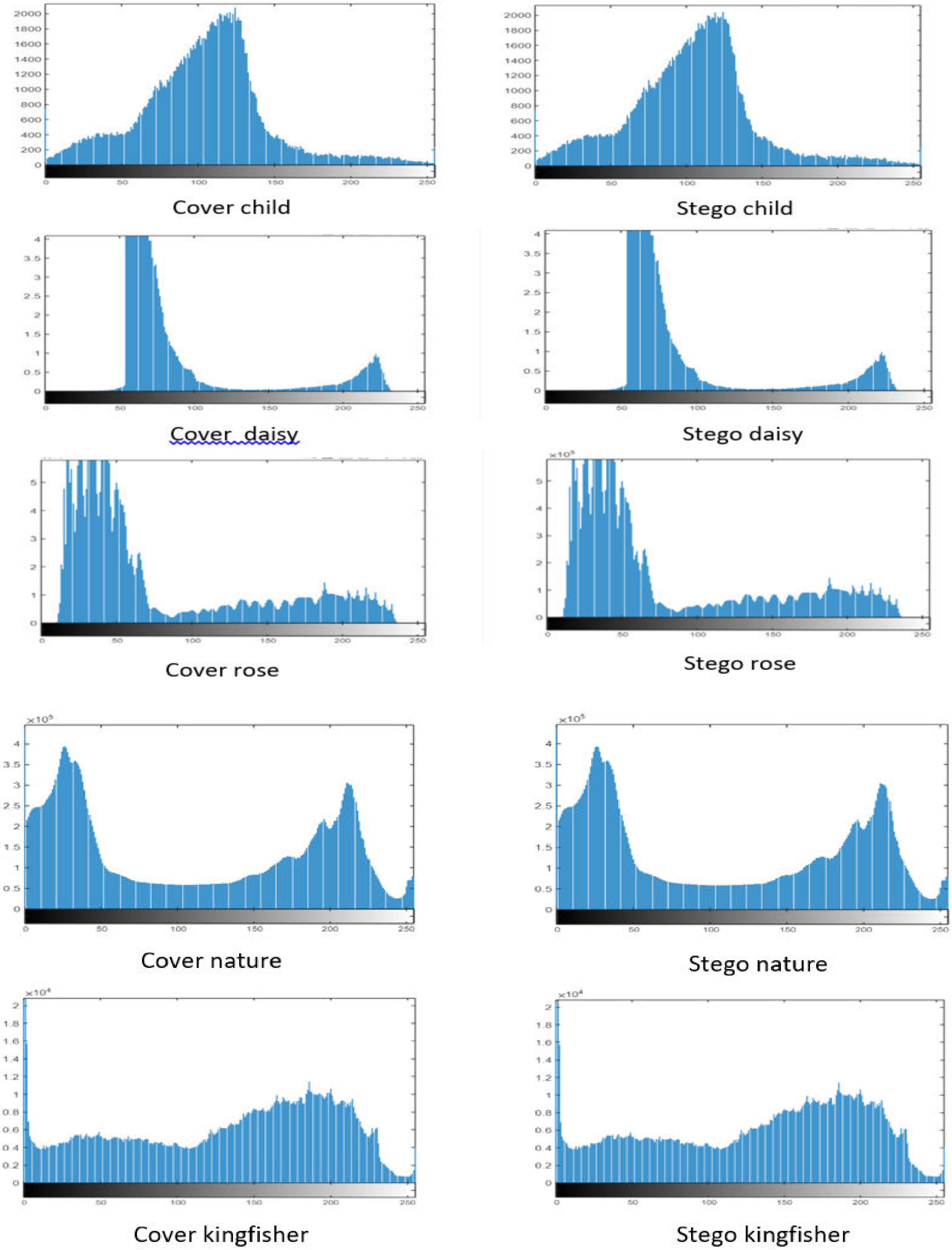
The measurement of PSNR and MSE values of images are shown in Table 1.

Table 1. Results of PSNR and MSE

Image Name	**PSNR** (Peak Signal-to-Noise Ratio)	**MSE** (Mean Squared Error)
Child	54.7139	0.2196
Daisy	86.4977	0.0001
Rose	97.6471	0.0000
Nature	54.756	0.0035
Kingfisher	72.6323	0.2175

The mean-square error (MSE) and the peak signal-to-noise ratio (PSNR) are used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

In addition, histogram measurement is done using 'imhist' function of the MATLAB.



Cover child

Stego child

Cover daisy

Stego daisy

Cover rose

Stego rose

Cover nature

Stego nature

Cover kingfisher

Stego kingfisher

Fig. 4.The histogram of the cover-image (left) and the stego-image (right)

While testing the proposed steganography method in our project, the histogram of the cover image is compared with that of the stego image. The system utilizes a novel steganalysis algorithm that successfully detects any stego-image by analyzing the difference between the histograms of the cover image and the suspicious image. The histogram of the stego image exhibits a more split pattern compared to the cover image, indicating the presence of hidden information.

V. CONCLUSION

As with the increasing number of cyber threats, popular instant messaging apps have become more vulnerable to attack, making it necessary to adopt advanced methodologies to secure online communication. Therefore, this proposed system offers a practical solution to the security challenges faced by instant messaging apps, and its use of image steganography could provide an additional level of security to protect sensitive information from unauthorized access.

The proposed system provides a secure means for clients to send messages to one another. This system encrypts messages and hides them within random images before sending them to Firebase, from where they are forwarded to the appropriate client. In our system we had used LSB algorithm for image steganography and AES algorithm for encryption purpose.The experiments have proven the effectiveness of the LSB algorithm. Available parameters and quality analyses using PSNR which is above 50 dB and MSE values have been provided as well. We have performed experiments and feature comparisons with related schemes to indicate the advantages of our approach.Future scope includes the integration with block chain technology, development of mobile applications, application in IoT devices, and integration with other applications, which can provide additional benefits and applications of the secure communication and data protection.The proposed system provides secure communication with encryption and steganography techniques, and has potential for further development.

REFERENCES

[1]Manish Munikar, "Image Steganography: Basic Concepts and Proposed Algorithm" Technical Report, June 2016.
[2] Y. P. Astuti, et al. "Simple and Secure Image Steganography using LSB and Triple XOR Operation on MSB" *International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia*, pp. 233-238, 2018.
[3] Dr. Amarendra K, V. N. Mandhala, B. C. Gupta, G. G. Sudheshna, and V. V. Anusha, "Image Steganography Using LSB"*International Journal of Scientific & Technology Research*, vol. 8, no. 12, pp. 1966-1970, Dec. 2019.
[4] A. Setyono and D. R. I. M. Setiadi, "Securing and Hiding Secret Message in Image using XOR Transposition Encryption and LSB Method" *in Proceedings of the IOP Conference Series: Journal of Physics: Conference Series*, vol. 1196, no. 1, p. 012051 2019.
[5] W. Lu, Y. Xue, Y. Yeung, H. Liu, J. Huang, and Y. Shi, "Secure Halftone Image Steganography Based on Pixel Density Transition" *in Proceedings of the IEEE Access*, vol. 7, pp. 69052-69061, 2019.
[6] J. Qin, J. Wang, Y. Tan, H. Huang, X. Xiang, and Z. He, "Pixel-value-ordering-based image steganography with minimal modification of original image" *IEEE Access*, vol. 8, pp. 155625-155639, 2020.
[7] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital Steganography and Watermarking for Digital Images: A Review of Current Search Directions" *IEEE Access*, vol. 8, pp. 90470-90487, 2020.
[8] R. Kumar, N. Kumar, and K.-H. Jung, "Color image steganography scheme using gray invariant in AMBTC compression domain" Multidimensional Systems and Signal Processing, vol. 31, no. 3, pp. 1005-1026, Jul. 2020.
[9] J.-H. Horng, C.-C. Chang, and G.-L. Li, "Steganography using the quotient value differencing and LSB substitution for AMBTC compressed images" *IEEE Access*, vol. 8, pp. 153193-153208, 2020.
[14] K. I. M. Abuzanouneh and M. Hadwan, "Multi-stage protection using pixel selection technique for enhancing steganography" *International Journal of Communication Networks and Information Security (IJCNIS),* vol. 13, no. 1, pp. 56-65, Apr. 2021.
[15] W. A. Alawsi, H. K. Obayes, and S. M. Hussain, "A Novel Image Encryption Approach for IoT Applications" Webology, vol. 19, no. 1, pp. 51-61, Jan. 2022.
[16] S. Athinarayanan, S. Nivetha Priya, and R. Supriya, "Secure Data with Key Managers by Using Shamir Scheme and AES Algorithm" *International Journal of Computer Science Trends and Technology (IJCST)*, vol. 5, no. 2, pp. 93-96, 2017.
[17] A. I. Sallam, E.-S. M. EL-Rabaie, and O. S. Faragallah, "HEVC Selective Encryption Using RC6 Block Cipher Technique" *IEEE Transactions on Broadcasting*, vol. 63, no. 3, pp. 578-587, Sep. 2017.

[18] K. P. Choudhury, S. Kakoty, and L. P. Saikia, "Improvement of Advanced Encryption Standard Algorithm Using Row Transformation and 200 Bit Data Block" *International Journal in Research Engineering and Computer Engineering (IJRECE)*, vol. 6, no. 3, pp. 26-29, 2018.

[19] V. Lytvyn, I. Peleshchak, R. Peleshchak, and V. Vysotska, "Information Encryption Based on the Synthesis of a Neural Network and AES Algorithm" in *IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 90-95, 2019.

[20] S. Dasgupta and P. Das, "Extended AES Algorithm with Custom Encryption for Government-level Classified Messages*" International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, no. 8, pp. 231-236, 2019..

[22] S. Yi, J. Zhou, and Z. Yun, "Reversible Data Hiding Method in Encrypted Images Using Secret Sharing and Huffman Coding" in *IEEE International Conference on Information Science and Technology (ICIST*), pp. 494-499, 2021.

[23] J. J. Wang and S. F. Tan, "A New Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step" *Int. J. Comput. Electr. Autom. Control Inf. Eng. (IJCEEICE*), vol. 9, no. 1, pp. 39-44, 2021.

[24] J. Kaur, S. Lamba, and P. Saini, "Advanced Encryption Standard: Attacks and Current Research Trends " in *IEEE International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 1-5, 2020.

[25] A. H. Ali and A. M. Sagheer, "Design of Secure Chatting Application with End-to-End Encryption for Android Platform" *Iraqi Journal for Computers and Informatics*, vol. 43, no. 1, 2017.

[26] N. Chaudhari, S. Shinkar, and P. Pagare, "Chatting Application with Real Time Translation" *International Research Journal of Engineering and Technology*, vol. 05, no. 05, pp. 1239-1243, May 2018.

[27] S. S. Reddy Emmadi and S. Potluri, "Android Based Instant Messaging Application Using Firebase" *International Journal of Recent Technology and Engineering*, vol. 7, no. 5S2, pp. 137-141, Jan. 2019.

[28] M. A. Mokar, S. O. Fageeri, and S. E. Fattoh, "Using Firebase Cloud Messaging to Control Mobile Applications" in *International Conference on Computer, Control, Electrical and Electronics Engineering (ICCCEEE19)*, 2019.

[29] A. Sarjit, Srivishak, Siddarth, S. Kumar and Preethi, "Web Based Chat System Using React Framework" 2020.

[30] D. Dembla, D. Dubey, and K. Joshi, "Modern Android Based Secure Chat Application Using Firebase" *International Journal of Advanced Computational Engineering and Networking,* vol. 9, no. 5, pp. 251-256, May 2021.

[31] D. Sharma, M. Agarawal, H. Upadhyay, and G. Akilarasu, "Developing Chat Application Using Firebase" *International Research Journal of Engineering and Technology*, vol. 8, no. 4, pp. 1014-1018, Apr. 2021.

[32] D. Therokar, D. Pohare, M. Kolte, P. Sonar, and P. Bute, "Social Media Application Development in Android with Firebase" *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT),* vol. 2, no. 2, May 2022.

[33] A. Kumar and A. Kumar, "Research paper on Group chatting Application" in 2022.

[34] S. Kadam, R. Hanmante, A. Nikale, J. Khot, and D. Nitture, "WEB BASED CHAT APPLICATION" *International Research Journal of Modernization in Engineering Technology and Science,* vol. 04, issue 04, April-2022.

[35] A. Kasetwar, R. Gajbhiye, G. Papewar, R. Nikhare, and P. Warade, "Development of Chat Application" *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 10, issue 5, pp. 1573-1579, May 2022.

[36] M. M. Rahman, "A DWT, DCT and SVD based watermarking technique to protect the image piracy" *International Journal of Managing Public Sector Information and Communication Technology (IJMPICT)*, vol. 4, no. 2, pp. 1-13, June 2013.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.379

doi® crossref

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 ✆ 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com