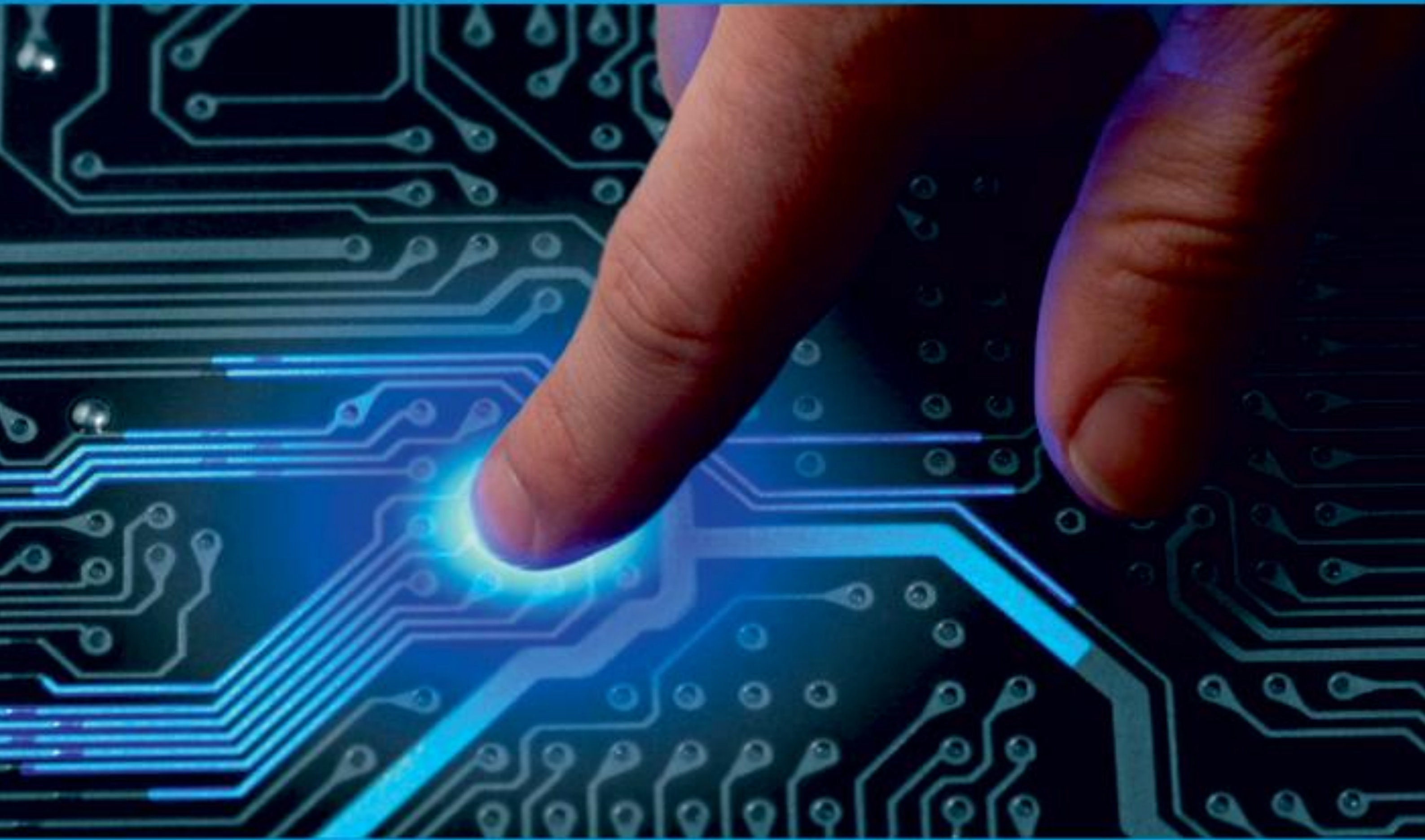
IJIRCCE

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



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 4, April 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 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104044 |

A Survey on Image Steganography and Cryptography

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: Nowadays, communication through internet is a significant way to exchange information. Therefore, the online communication application must be able to communicate through texts, images, videos or any other electronic files or documents in a faster way with less delay as well as with security. This paper reviews about cryptography and steganography. Cryptography is used for encryption of the message or data. It is used to convert the plain text into cipher text and decryption is used to convert the cipher text into plain text. Steganography is used for hiding the data inside cover media. There are different types of media to hide like text, image, audio, video etc. Steganalysis is the rival method of steganography it detects the presence of embedded information in cover media. This paper reviews on LSB (Least Significant Bit) technique for embedding message into cover media, AES (Advanced Encryption Standard) algorithm for encryption or decryption purpose and firebase is a backend application development platform which provides real-time database and hosting of application becomes easy. This paper provides review and analysis on different LSB techniques like bit inversion, LSB using XOR operation, compressed file, photo crypt algorithm, AMBTC compression technique. It also provides better ways for data embedding inside image which provides more security and better encryption algorithm that is AES. Firebase is a software development kit for faster implementation of application.

KEYWORDS: Cryptography, Image Steganography, LSB (Least Significant Bit), AES (Advanced Encryption Standard).

I. INTRODUCTION

Technology has evolved over the past few years through which communication of digital multimedia data are easily transmitted over the web. Therefore, the security of digital multimedia is crucial for protecting susceptible multimedia data from malicious interference in the process of public channel transmission. To guarantee the security of multimedia cryptography and information hiding are considered. By encryption and decryption operations using secret keys cryptographic techniques transform the multimedia data between incomprehensible and comprehensible forms. Information hiding embeds multimedia data into digital cover media. Sometimes the data of cover media gets lost or destroyed unavoidably. As a result, the embedded multimedia data will be unavailable. To overcome this restriction, secret sharing has been put forward. Many methods have been applied in providing security such as cryptography, steganography, watermarking, and digital signatures.

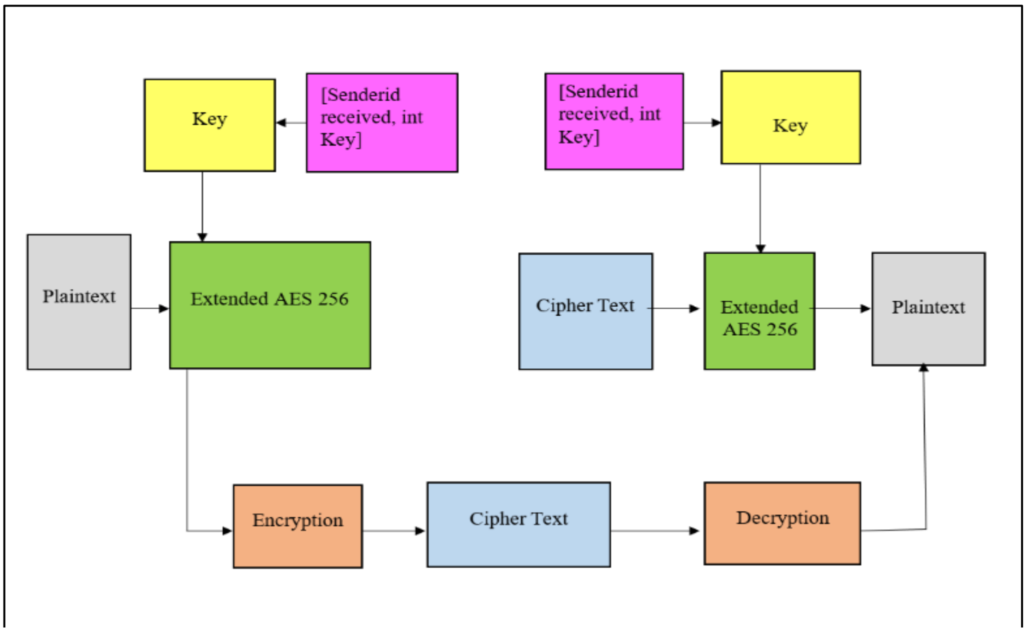


Fig 1. Encryption and Decryption process

Steganography is the science of hiding data on other media called cover media.Data hiding in the image is divided into two domains namely spatial domain and frequency domain. In the frequency domain the message is hidden by first transforming the cover image. There are different types of watermarking techniques like transform domain and spatial domain. Transform domain consist of discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD) and their cross relation [36]. While in the spatial domain the secret message is inserted directly by changing the pixel value of the cover image. LSB and MSB are the most popular techniques in spatial domain.The well-known strategy that is used for steganography is the LSB. This strategy works when the size of cover media is longer than the communication document or message to hide. If image is grayscale, then applying LSB technique to every byte of 24-bit pictures then last three bits of image pixels can be encoded with message values that needs to hide [11].

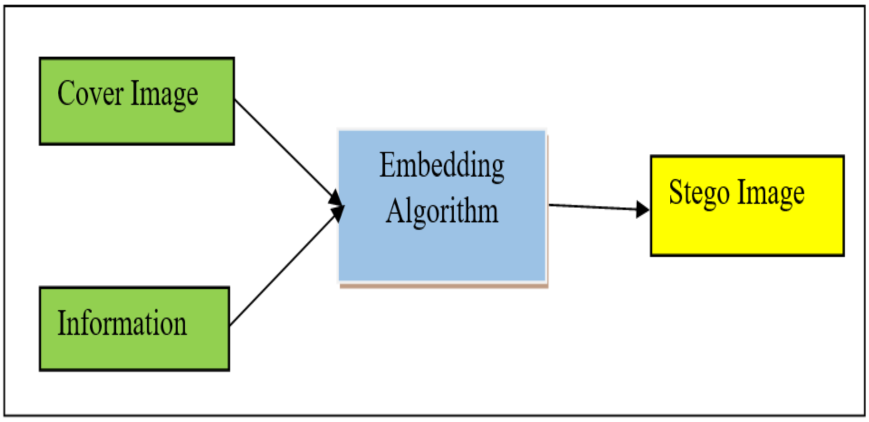


Fig.2. Image Steganography

Encryption is the process of changing an original data into confidential data that cannot be read; while the decryption process is a process where the confidential data will be transformed back into the initial original data. In this scenario, the Advanced Encryption Standard (AES) is a symmetric block cipher selected to shield secret information. Under the influence of U.S. government and U.S. security strategies, this is the most common encryption mechanism opted for network security, now it has become one of the well-liked standards of all executive steps for improved safety measures in the networks. It can be applied to various network domains for example wireless sensor network or Internet of things network as well. AES is implemented in network environment encryption susceptible information with the medium of software and hardware worldwide.

II. LITERATURE SURVEY

Many researchers had proposed various techniques to implement cryptography and steganography. In this section we are analyzing traditional as well as latest techniques to implement data hiding and message embedding. This literature survey includes the following techniques:

1) Survey on LSB techniques
2) Survey on Encryption algorithm techniques
3) Survey on Firebase and React Framework

1. Survey on LSB technique for steganography

Manish Munikar studied steganography and proposed a LSB technique with a slight change in the algorithm [1]. He implements photo crypt algorithm which states that a message with secret key is used to embed the message inside the cover media. The algorithm is used to provide security with the help of password (Key) protection. Mostly the message is embedded in the LSB but it is decided with the help of secret key. So, the intended receiver is able to decrypt the message with the help of valid key.

Yani Parti Astuti et al. [2] has proposed in the research that instead of using simple LSB (Least Significant Technique) they are working on image steganography using LSB and Triple XOR Operation on MSB (Most Significant Technique). As LSB technique is easy to use but it's also very vulnerable to third party attacks. So, to improve security of the system Triple XOR operation on MSB of pixel is done. In our system we are going to make our system more secure by keeping its PSNR value near about 50 db. which is good and gives image intensity proper.

Dr. Amarendra et al. [3] has studied on simple LSB technique. In this technique they had used LSB (Least Significant Bit) and symmetric key between both the sender and the receiver for the purpose of encryption and decryption of 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 encryption of data and steganography for hiding data below cover media. It only works on grayscale image. In our method we are going to convert the color image into the grayscale image and then perform the operations. And the message size should be less than that of image.

Andik Setyono et al. [4] has proposed a LSB technique for message embedding having advantages like payload and imperceptibility. But using basic LSB technique is very weak and hackers can easily identify the image containing data so they implement a new transposition encryption algorithm and perform XOR operation based on key on largest bit of cover image. In the embedding process the input in the form of image, then data which needs to hide in the form of .txt file and encryption key is used and the row variable is calculated by using ceil function and then get secondary key for decryption process. So, in this way encryption and decryption is stated in this paper.

Wei Lu, Member of IEEE et al. [5] proposed a research paper on Secure Halftone Image Steganography Based on Pixel Density Transition. The main goal of this paper is to propose a halftone-based image steganography technique that helps to develop stego images which have high visual quality and secure the stego images from strong Steganalysis tools. In this paper, the concepts like pixel density, pixel density histogram, and Pixel Mesh Markov transition matrix are used.

Jiaohua Qin et al. [6] proposed a paper on coverless image steganography based on Generative Adversarial Network. In traditional image steganography methods message that the user wants to transmit needs to be covered or embedded into another cover media. But, information of the cover media can be easily detected by using some Steganalysis tools which leads to the leakage of the secret messages. To avoid this Generative Adversarial Network (GNN) popular deep learning technology is used to hide secret messages into the cover media in a more secure way and to skip the Steganalysis tools.

Oleg Evsutin et al. [7] proposed a paper on Digital Steganography and Watermarking for Digital Images: A Review of Current Search Directions. The aim of the paper is to protect confidential information from leaking, identifying the reason and source of information leakage as well as protecting it from the unauthorized user accessing it without authentication and making changes to it. All these issues are handled with the help of steganography and digital image watermarking by embedding and extracting the information. In this paper analysis of previously used techniques and currently available techniques for steganography and digital image watermarking is done.

Rajiv Kumar et al. [8] proposed a new AMBTC (Absolute Moment Block Truncation Coding) compression domain. The compressed color image is embedded by the secret data keeping gray pixel values intact. Initially the color image is partitioned each component (R, G, B) with same block size and calculate variance and standard deviation. After that the two-block having minimum variance is compressed by using AMBTC and they are embedded by the secret data. The gray pixel values are kept invariant and the complex color block's pixel value is adjusted by looking at the new compressed color block pixel value.

Ji-Hwei Horng et al. [9] proposed a paper on Steganography using the quotient value differencing and LSB substitution for AMBTC compressed images. The paper consists of quotient value differencing (QVD) and the least significant bits (LSBs) method to hide secret data in an absolute moment block truncation coded (AMBTC) image.

Mrs. N. Dhivya et al. [10] had studied some theoretical concepts on how to secure network while using cryptography and steganography. Generally, Network security is used to prevent unauthorized access to the network while communication between sender and receiver. Different network security devices are used like active devices, passive devices, preventive devices, Unified Threat Management (UTM) which includes firewalls, web catching, content filtering etc. Intrusion Detection System which includes CRC etc. There are different types of cryptography like symmetric key, hash functions, Asymmetric key. And different forms of steganography like text, audio, video, image. This paper is overall view of cryptography and steganography providing network security.

Omar Elharrouss et al. [11] proposed a paper on the image steganography approach based on K-least significant bits (K-LSB). This paper consists of LSB coding, a K-LSB method that uses K least bits to hide the image. The main aim of this paper is to enhance image quality by using image quality enhancement methods and decoding the hidden images using region detection operations.

Nandhini Subramanian et al. [12] proposed a research paper on Image Steganography: A Review of the Recent Advances in that they mentioned image steganography means hiding any kind of information like text, image, video or document inside a cover image in such a way that it is not visible to anyone except authorized users. The objective of this paper is to explore and study various deep-learning technologies related to image steganography. There are three categories for image steganography in deep learning traditional methods, CNN-based and GAN-based methods.

Nandhini Subramanian, (Member, IEEE) et al. [13] proposed a research paper on End-to-End Image Steganography Using Deep Convolutional Autoencoders. In this paper, a simple autoencoder architecture is used to hide a secret image inside the cover image and to extract that secret image from the stego image. This paper consists of three types of datasets which are COCO, CelebA, and ImageNet. various technics are used to measure performance such as Signal-to-Noise Ratio, hiding capacity, etc. The main goal of this paper is to hide a secret image in such a way that has higher hiding capacity, security, and robustness.

Khalil Ibrahim Mohammad Abuzanouneh et al. [14] proposed a new technique for pixel selection i.e., Providing protection at multiple stages using pixel selection technique for improving steganography. To make the Steganalysis process more complicated the secret file is distributed randomly and embedded into cover-image. Image undergoes four stages like PSNR, MSE, histogram analysis, relative entropy. In this paper they introduce new algorithm that consist of complex and multiple random keys which reduce the detection of secret data. Advantage of this algorithm is that it provides relative PSNR value which maintains the intensity of image and provide image of good quality.

Wasan A. Alawsi et al. [15] states that as the use of IOT in digital and financial sector increases so providing security to data became crucial. So, in this research they used 4 levels of security for the encryption and decryption of the image. At 1st level conformal mapping is done means the image is converted with same characteristics into different appearance. At 2nd level they used RSA algorithm for image encryption. At 3rd level they used LSB method for embedding image into image. At 4th level they compressed the resulted image with GZIP algorithm. So, by using 4 different levels they implement their system.

2. Survey on Encryption algorithms and techniques

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.

Ahmed I. Sallam et al. [17] has studied High-Efficiency Video Coding (HEVC) selective encryption (SE) technique which is basically encrypts highly sensitive data on video bit stream. This present the RC6 based video encoding encryption of sensitive video bits with lower complexity and fast encoding bits for real time applications. Also, this paper compares the proposed RC6-based HEVC SE and the HEVC algorithm which uses Advanced encryption Standard (AES) for encryption.

Kirti Prakash Choudhury et al. [18] has proposed the Improvements in Advance Encryption Standard (AES) algorithm. This new technique provides stronger encryption as it provides higher security and enhance the process speed. This algorithm uses data block of size 200-bit, key of 5 * 5 matrix format also additional Row Transformation stage before the Shift Row step for each round in Advance Encryption Standard (AES) algorithm. The extra step of calculation is added in this algorithm to make this more secure.

Vasyl Lytvyn et al. [19] has proposed a system of Information encryption based on the synthesis of neural network and AES (Advanced Encryption Standard (Rijndael)) algorithm. This encryption system uses diagonalized matrix of weight coefficient where synaptic connections of the neural network used as the basis of vectors of input image. This provides every time for each new input image. The system provides constantly changing and newer keys every time for each input. It increases the cryptographic stability of this algorithm while comparing with the other algorithms.

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.

Miguel Morales-Sandoval et al. [21] discussed the security issues in cloud storage and proposed approach for storage and retrieval of encrypted data using attribute-based encryption (ABE). This approach has three different levels a) bulk data encryption outsourced to the cloud b) Management of keys for accessing encrypted data using digital envelops in attribute bases encryption c) construction of novel for Attribute Based Searchable Encryption (ABSE). These three levels support the security level which is 128 bit or greater.

Shuang et al. [22] proposed the reversible data hiding in encrypted images (RDHEI). The algorithm combines the image encryption and image sharing process which generates n number of shares which will get stored to the cloud storage. This algorithm uses (k, n) threshold secret sharing technique where at least k number of shares require to recover the original image and less than k share cannot recover the image also the size of each share is smaller than original image that can save the storage spaces. By using Huffman Coding algorithm differences of pixel in image block and secret data are embedded into this share.

Wang Ji Jun et al. [23] has discussed the drawbacks of existing Advanced Encryption Standard (AES) algorithm like the uses of multiple s-box increasing time complexity, to solve this they proposed a solution which is s-box image encryption scheme. This system firstly constructs S-box of size 10 X 26 using low dimensional system, then secondly, they used dynamic encryption step algorithm which destroys the correlation between the source image pixels which provides higher security with less complexity.

Jagpreet et al. [24] has studied the AES (Advance Encryption Standard) algorithm, how it is better than existing encryption algorithms and its drawback, also they have explored the other algorithm which can be used for securing data such as the machine learning techniques Artificial Neural Networks (ANN) which is used for protection from side channel attack for images. Also, they discussed some recent developments which are effective differential power analysis (DPA) and hybrid encryption algorithm using LZW. They proposed new model for the detection of attacks in AES.

3. Survey on firebase and React framework

Ammar Hammad Ali et al. [25] proposed a system which is a secure chatting application which is end to end encrypted for mobile phone which uses Android operating system. In this system they use an AES encryption algorithm for encryption purpose. For the voice and image security processes the proposed application used the symmetric algorithm RC4 for this purpose.

Nikhil Chaudhari et al. [26] states that this paper described model for intranet users where users can chat and translate messages in whatever language they want. Internet connectivity is not mandatory. So, there by it reduces the cost of communication. Also, this modelfocuses on landmark detection, image backup, image theft alert on demand. The model make use of juxtapose as server which allow user to message on a single network. The message is of limited size as the message access its dedicated size an exception occurs.

Sai Spandhana Reddy Emmadi et al. [27] proposed a research paper on an Android Based Instant Messaging Application Using Firebase. Communication through the internet is becoming more popular day by day. These chatting applications should be able to share different kinds of data like files, documents, images videos, etc. There are different types of databases firebase is one of them which provides a real-time database and cloud services that help developers to develop this kind of application easily. Android is one of the famous technologies which provides a platform for developing instant messaging applications. The main aim of this paper is to develop an android-based instant messaging application for performing real-time communication between sender and receiver/users. The android-based application allows users to communicate with each other through text messages with the help of the internet. To use this kind of application both users should be connected to a proper internet connection.

Mohamed Abdalla Mokar et al. [28] has proposed the system which make use of FCM technology for sending messages to multiple devices at the same time. Also using FCM we can send message to single device also.

Akhilesh Sarjit et al. [29] proposed a study on web chat using React framework. Previous chat applications were based on PHP and MYSQL for front-end and back-end development. Php which is an acronym for Hypertext Pre-processor is a widely used, open-source, scripting language that can be embedded with HTML and used for web development. MYSQL is an open-source relational database management system that consists of a multithreaded SQL server that supports different back ends. There are various such technologies used like jQuery which is a fast, small, and easy-to-use JavaScript library which is used for HTML document traversal and manipulation, event handling, animation and develop ajax based applications. The modern approach of jQuery allows dynamic web pages and web application development. So, using the React framework we can improve the performance parameter and data transmission is done between the point-to-point connection between servers. The main goal of this paper is to show by using React Framework how we can implement the virtual space concept and enhance performance over existing applications developed using PHP.

Divyam Dembla et al. [30] developed a chatting system which uses firebase as backend. this system uses aes256 encryption algorithm for encryption purpose. Also, in this android application they implemented optical character recognition feature using google vision. In this the sender and receiver id`s and an integer key are used to encrypt and decrypt data at client side.

Devesh Sharma et al. [31] proposed a chatting system which provides end to end encryption and uses firebase for exchanging messages between its users. This system uses XSalsa20 encryption calculation for encoding the message and Poly1305 to figure a Message Authentication Code (MAC). Each message has its own different key and nonce which brings better security for each single message in such finding one of the keys can't unscramble past messages.

III. CONCLUSION

This paper presented various techniques for image steganography and cryptography which provides double layer security for encryption of data. Image steganography considers two major parts that is spatial domain and transform domain. Emerging techniques based on DWT, DCT are less susceptible to attacks and keeping the difference between normal image and stego image minimum. But these techniques have less embedding capacity. And it has limitation that message size should be less that image size.

According to research there are different encryption algorithms like Rivest-Shamir-Adleman (RSA), Secure Hash algorithm (SHA) algorithm, Data Encryption Standard (DES), RC4 but AES algorithm is better than other algorithms as it is less prone to attacks. There are different LSB techniques like compressing file, inverse bit operation, LSB using XOR operation, photo crypt algorithm, AMBTC technique. By using different key techniques LSB can be used. The change in intensity of image can be calculated by PSNR value. The mean squared error can also help to detect the change in plain image and stego image.

Firebase provides a powerful and versatile platform for developing real-time chatting applications. Its comprehensive set of features and tools enable developers to easily build and scale chat apps with minimal effort. From real-time messaging to user authentication and data storage, Firebase offers a robust solution for chat app development.

REFERENCES

[1] Manish Munikar, "Image Steganography: Basic Concepts and Proposed Algorithm," Technical Report, June 2016; available: https://www.researchgate.net/publication/337305858_Image_Steganography_Basic_Concepts_and_Proposed_Algorithm.

[2] Y. P. Astuti, et al. "Simple and Secure Image Steganography using LSB and Triple XOR Operation on MSB," in Proceedings of the 2018 *International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia*, 2018, pp. 233-238, doi: 10.1109/ICOIACT.2018.8356239.

[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; available: https://www.ijstr.org/final-print/dec2019/Image-Steganography-Using-Lsb.pdf.

[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, 2019, p. 012051, doi: 10.1088/1742-6596/1196/1/012051.

[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, 2019, pp. 69052-69061, doi: 10.1109/ACCESS.2019.2914078.

[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, doi: 10.1109/ACCESS.2020.3016982.

[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, doi: 10.1109/ACCESS.2020.2995852.

[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.

[10] N. Dhivya and S. Banupriya, "Network Security with Cryptography and Steganography,"*International Journal of Engineering Research & Technology (IJERT)*, vol. 9, no. 8, pp. 789-796, Aug. 2020.

[11] O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, "Image steganography approach based on K-least significant bits (K-LSB)," in 2020 *International Conference on Machine Learning and Cybernetics (ICMLC)*, 2020, pp. 1471-1476.

[12] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "A novel steganography scheme based on K-LSB and local histogram equalization," in 2021 *International Conference on Computing, Networking and Communications (ICNC)*, 2021, pp. 646-650.

[13] N. Subramanian, I. Cheheb, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "A novel image steganography technique based on K-LSB and DWT-SVD," IEEE Access, vol. 9, pp. 94702-94715, 2021.

[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)*, 2019, pp. 90-95.

[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.

[21] M. Morales-Sandoval, M. Hinojosa Cabello, H. M. Marin-Castro, and J. L. Gonzalez Compean, "Attribute-Based Encryption Approach for Storage, Sharing and Retrieval of Encrypted Data in the Cloud," in *IEEE 8th International Conference on Cloud Computing (CLOUD),* 2020, pp. 142-147.

[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*), 2021, pp. 494-499.

[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)*, 2020, pp. 1-5.

[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.

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