iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.49978

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Data Security using Variant of Hill Cipher

Srija Pulluri[1], Srijith Patha[2], Neha Madapati[3], Lokeshwari Vinya V[4], Satya Kumar C[5]
[1, 2, 3]*B.Tech Student, Department of CSE, Vardhaman College of Engineering, Hyderabad*
[4, 5]*Assistant professor, Department of CSE, Vardhaman College of Engineering, Hyderabad*

Abstract: ***Data is first collected, and the Pixel Repetition Technique is used to perform pre-processing, Payload capacity, attack protection, and visual quality. To rise the security of information concealing, The LSB information hiding algorithm of data using secret key has been presented to strengthen the security of information concealing. It increases human visual abilities, integrates information concealment and cryptography, and uses identity identification based on digital signature and encryption technology. It is based on a scheme where the receiver can retrieve secret data by applying the A* algorithm backwards. Last but not least, we tested safety and peak signal-to-noise ratio (PSNR). With stronger security and higher PSNR, the enhanced LSB data steganography technique using encryption technology is superior to the standard LSB data steganography method.***
Keywords: A* Algorithm, Data Encryption Standard, RC4 algorithm, Python script, Pixel Repetition Method, AES Cryptosystem, LSB EMBEDDING.

I. INTRODUCTION

Spread spectrum, transform domain, and model-based data steganography are among the various types of steganography. The spatial domain and the transform domain are in opposition to one another. Using pixel value, a hidden message is directly integrated in the spatial domain. However, the STF (Spatial to Frequency) data in question is first transformed using one of the aforementioned transformations before being used in transform domain approaches. They consist of the discrete wavelet transform (DWT), discrete cosine transform (DCT), ridgelet transform, hadamard transform, dual tree, curvelet transform, and others. Afterwards, embedding is done in certain transform coefficients. The modern advancements in communication and information technology produce data that is easily and plainly accessible. Establishing secure communication is also essential. The most crucial necessity is also to create secure communication. Several methods are developed to achieve secure communication. Steganography is one such technique [1].Steganography is used to convey data via multiple types of media, including data, video, audio, and more [2]. Steganography, then, is the art of hiding data. The word "steganographia" in Greek is the source of this. The words "steganos" and "graphia" are combined to form this term. This indicates that this specific methodology has been employed since antiquity. By using this method, data is transmitted securely and without interruption from outside parties from the sender to the recipient. By using this data masking mechanism, the data is also reliable and constant during the transfer. There are now a number of problems with the evolving steganography technologies. For VQ (Vector Quantization) compressed data, this study's [3] RDH (reversible Data Hiding) approach was also suggested. The goal of this work was to develop an effective IM (Index Mapping) scheme from the embedding perspective by reviewing a few IT (Information Theory) topics. The empirical results show that, in terms of compression embedding capacity and efficiency, the recommended strategy outperforms the conventional methods.

Steganography consists of four modules. They are listed below.

1) CO (Cover Object) – Data hiding is performed in this CO.
2) SD (Secret Data) – Within the CO, the hidden-data is positioned.
3) SO (Stego Object) – state of CO after the data is hidden inside.
4) SK (Stego Key) – Hide function is used for the hidden data within the CO.

Depending on the medium used for Production, steganography can be divided into many types. Data steganography, for instance, is the use of original data to create a CI (Cover Data). Similar to this, there are several varieties of steganography, including text, sound, and video steganography. In this study [4], CO was derived from medical data. The data steganography can be divided into two primary groups. The two main types have been identified as the spatial and frequency domain approaches [5-7]. Many steganography approaches consider both areas. For instance, this study introduced data segmentation and AIO (Artificial Immune Optimization). This method quickly selects the effective template to embed. Hence, it is not necessary to search through all of the data to locate a specific template for embedding. Moreover, IBM introduced DES (Data Encryption Standard), which the US later recognised as a standard.

It takes sixteen rounds to finish the encryption process. However, the DES can be broken by a brute-force attack. By using the LSB (Least Significant Bit) approach to embed the secret data in the cover medium, the communication is made secure in this case. Moreover, computing time must be kept to a minimum. There are numerous methods for hiding data. However, hardware implementation is challenging. among all the conventional approaches, there is data hidden [10]. In order to achieve data steganography, the current study proposes unique methodologies for encryption and decryption.

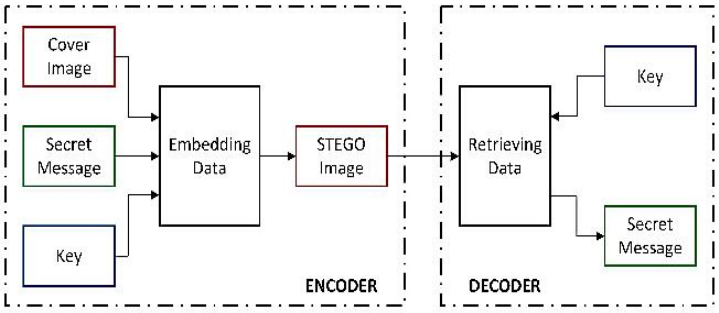


Figure.1. Fundamental steganography architecture

Least Significant Bit-embedded Advanced was suggested by the study as a method for achieving data steganography through a series of phases[11-12]. The image above. 1. Illustrates the basic steganography architecture. The cover data, secret message, and key are utilised in the figure.1 above to embed the data in order to obtain the stego data. During the encryption process, this is done. In contrast, employing the key during the decryption stage allows for the retrieval of the secret message.

II. LITERATURE SURVEY

S. Karakus and E. Avci employed a significant amount of data to conceal their identities and guarantee the quality of the stego image. MSE, RMSE, PSNR, SSIM, and UQI measures for visual quality analysis have been used to assess theeffectiveness of the proposed method. As the cover object, various sized medical images that were acquired from the Dicom library's open access database have been used. even used 256*256 size pictures without data compression to conceal 10,000 characters of data.

A study by C. Y. Roy and M. K. Goel combines various encryption algorithms to ensure that data is transmitted securely without leakage or unauthorised access. In this research, a method for secure transfer of confidential data is described that incorporates many steganography-based methods. Finally, before embedding the secret data into the cover image, it is encrypted using the DES (Data Encryption Standard) technique. The encrypted data is next represented in hexadecimal format. Then, in order to conceal sensitive information inside the cover image, embedding using the Least Significance Bit (LSB) is done. Convolutional Neural Network (CNN) picture de-noising is also utilised to improve the cover image with secret encrypted data approaches.[13]

P. Rahmani and G. Dastghaibyfard used Vector quantization (VQ)-compressed images utilising reversible data concealing. In order to build an efficient index mapping mechanism from the perspective of embedding capacity, numerous information theory principles are examined in this paper. Each position in the sorted codebook is divided into a number of intervals by the recommended index mapping procedure, which then allocates each interval to a position with a high hit rate. The experimental findings demonstrate that the proposed technique significantly outperforms the existing schemes in terms of embedding capacity and compression-embedding efficiency.

A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K.-H. Jung as well as M. Hussain used steganography and watermarking, both employed to conceal secret messages. Steganography's primary goal is to preserve confidential data and hide the existence of communications[14-15]. In contrast, watermarking is used to safeguard the accuracy of confidential information, whether or not it also hides communication's existence from prying eyes. The primary goal of watermarking software is to safeguard the contents' intellectual property.

M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K.-H. Jung employed multiple encryption techniques to improve confidentiality, and the LSB approach was employed to embed data into the picture[16]. The suggested framework is straightforward and modular for simple comprehension. This was done to make it possible to quickly implement future modifications without having to perform significant programme upgrades.When further modules are required, they are simple to install. The platform has been created in a modular way. Before being put together to form the complete structure, several of the components were examined separately. The gadget was then tested for several image formats and was determined to be functional.

S. Karakus and E. Avcı stated that in order to assure good image quality, stego image was used in this investigation to increase the quantity of data that might be hidden. The study uses the commonalities between the pixels to suggest a new optimization-based strategy. Visual quality analysis measures were utilised to gauge the effectiveness of the suggested strategy.Several sized medical photos that were taken from the Dicom library's open access database have been used as the cover object.A. Miri and K. Faez offered a unique evolutionary algorithm-based spatial steganography technique (GAs). The embedding capacity and distortion are boosted by the scheme's use of novel operations to improve least significant bits (LSB) matching between the carrier and the stego image. These processes include optimal vertical and horizontal pixel scanning, circular shifting, secret bit flipping, and secret data transposition. An optimization would be the incorporation of large amounts of data into an image while maintaining the integrity of the carrier image. By doing comprehensive experimental testing of the proposed scheme and comparing it to the state-of-the-art steganography schemes, it is shown that the suggested scheme outperforms the relevant GA-based steganography approaches.

M. Umair examined the operation and application of various symmetric block cypher algorithms[17]. They conducted a comparison analysis towards the end. In terms of security, they thought Blowfish and Serpent are the greatest options. They even conducted a comparative examination of asymmetric algorithms as future work. As part of research, they'd also like to simulate encryption and decryption operations in order to obtain real-world outcomes for various techniques.

A new steganography method that preserves data integrity and confidentiality has been developed by Ahmed Hambouz, Yousef Shaheen, Abdelrahman Manna, Dr. Mustafa Al-Fayoumi, and Dr. Sara Tedmori. Data secrecy is achieved by secretly encoding the data bits within stego data. The SHA 256 hashing algorithm is used to hash the decoding and encoding variables to ensure integrity.

III. EXISTING WORK

The LSB embedding position is controlled and encrypted to ensure that the hidden information cannot be extracted without the corresponding private key. This technique provides an additional layer of security, making it difficult for unauthorized individuals to access the data. To prevent the forgery of the hidden information, a text segmentation method is employed to extract the text. This technique ensures that the data is authentic and has not been tampered with, making it suitable for applications that require a high level of security and authenticity. The proposed pre-processing method enhances the performance of crop images. By improving the quality of the images, the subsequent processing steps are more accurate, resulting in better outcomes. The RC4 algorithm is used to generate an encryption key. This algorithm provides a robust and secure method for generating encryption keys, ensuring that the data is protected and can only be accessed by authorized individuals.

IV. PROPOSED WORK

To achieve data steganography, numerous ways were presented. The Pixel Repetition Technique is used to perform pre-processing once the data has been obtained as input. The pre-processing technique suppresses a variety of undesired distortions while preserving the important data properties for later processing. Next, data encryption employs the advised AES cryptosystem. By using this procedure, communication security is achieved. The hidden data is concealed inside a data set using the newly proposed LSB embedding. The receiver then extracts the secret data using the recommended system's reverse operation by the A* Algorithm. To confirm the suggested system's performance effectiveness, an analysis was conducte.[18].To scale up the image that was utilised as input, PRM (Pixel Repetition Method) is used. By repeating the pivot or seed pixel until it creates a block (2*2), the (X*Y) input image is scaled up. As a result, a cover that is twice as big as the supplied image (2X*2Y) is created. The C (2X*2Y) is the Cover Image (CI), which is created from the input image. 2*2 original image block is taken into account. The scaled-up image is then retrieved, as seen in the figure below.

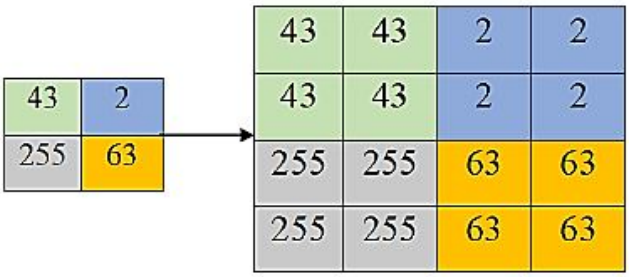


Figure.1. Pixel Repitation Method

Fig. 1 shows the architecture diagram, where all the mobile devices are connected to an application layer, which is responsible for handling user requests and executing various functionalities. The application layer acts as an intermediary between the mobile devices and the database layer. The application layer is responsible for handling tasks such as managing contacts, setting alarms, and obtaining location data. These tasks are executed using various functions and APIs provided by the application layer. Once the tasks are executed, the data is sent to the database layer for storage. The database layer is where the data is stored permanently. This layer is responsible for storing and retrieving data using SQL commands like "insert into table" and "select from table" and many more. The database layer plays a crucial role in the architecture diagram as it serves as the central hub for data storage and retrieval. Overall, the architecture diagram shows a clear separation of concerns between the mobile devices, application layer, and database layer. This separation of concerns allows for efficient and scalable data processing and management. To get 2*2 blocks, each pivot or seed pixel is repeated. Thus, it is known as PRM (Pixel Repetition Method). The computational complexity is reduced when preprocessing is done using PRM. The cryptographic algorithm known as AES (Advanced Encryption Standard) is used in an unthinkable way to encrypt textual data. It also goes by the name "symmetric-key algorithm." This demonstrates that both decryption as well as encryption use the same key. Moreover, different-sized block cyphers are used. Nowadays, AES is a reliable security technique since it is backed by hardware and software. AES also has a number of benefits. Here is a list of them:

- In contrast to improvements in the capacity to do EK (Exhaustive Key) searches, the flexibility of the built-in key length allows for some future proofing.
- For the encryption process, this technology employs long key lengths of 128, 192, and 256 bits, making it resistant to attacks. There haven't yet been any actual-world cryptographic attacks that have targeted AES [19-20].

With this technique, the secret message-corresponding bits are substituted for the image's LSB (Least Significant Bits) in some or all of its bytes. This technique can be used with a variety of data kinds and formats. Thus, this method is the most important steganography technique used today. Steganalysis can be applied to this method. In order to increase security, the raw data is encrypted before being embedded. This strategy has proven to be the foundation for numerous MCD message-hiding techniques (Multimedia Carrier Data). Moreover, this can be used in particular data domains. For instance, a concealed data may be incorporated into the frequency coefficients of a JPEG image or the colour values of an RGB bitmap. LSB is the basic steganography technique. In this case, the cover image's pixels are immediately presented with data. This approach has clear, measurable value. Hence, the change in an image is invisible to average individuals. For each each pixel, the insertion procedure is carried out by altering the LSB bit-plane. This approach offers several advantages. Here is a list of them:

- It offers straightforward implementation and is easy to understand.

Least Significant Bit Steganography, often known as LSB Steganography, is a technique for secretly enclosing data in any type of digital medium, in this case, an image. Pictures are composed of pixels, which often refer to a specific pixel's color. These pixel values in a grayscale image vary from 0-255, with 0 being black and 255 denoting white. When employing LSB picture steganography, the last bit value of a pixel won't dramatically change the colour. A cover image has the info integrated into it. The result of the process are Stego Images.

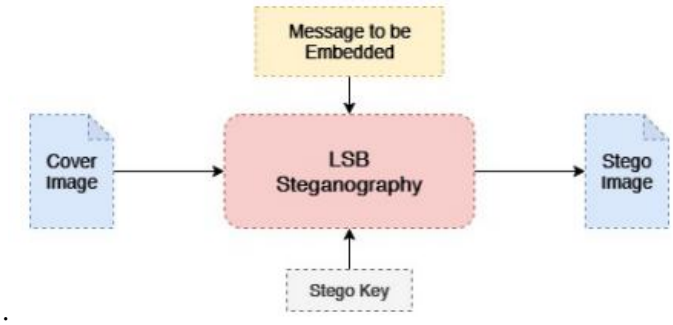


Figure.3. LSB Steganography

The steps above are necessary to use LSB Steganography to conceal a message within an image: Greyscale conversion is made to the cover image. The message is binary-converted. The image's pixels are examined one by one, and a temporary variable named temp is started for each pixel

Set temp to 1 in all other circumstances and to 0 if the message bit and the LSB of the pixel value match. Change the output image pixel to reflect the temporary variable value, temp, applied to the image pixel value. This is repeated until the message is well ingrained. The output image is written to the disc when the entire message has been inserted.[20]

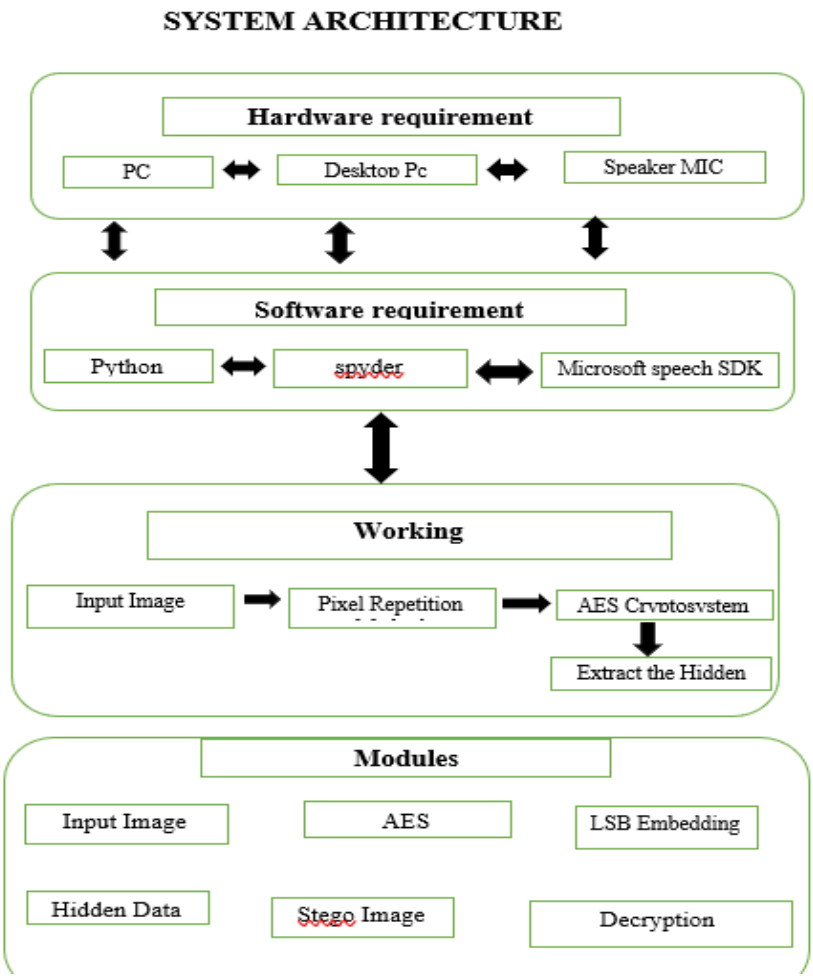


Figure.4. System Architecture

A* Search algorithms are allegedly "brainier" than other traversal techniques. It basically just means that the algorithm is intelligent, which makes it stand out from other conventional algorithms. Further details concerning this fact are provided in the sections that follow. It's crucial to remember that this method is frequently employed in games and online maps to find the shortest distance (approximation).

A. Advantages

1) This method has a low encryption and decryption time, making it a practical choice for real-world applications.
2) The key generation process is simplified, particularly when compared to other methods that use complex algorithms, due to its use of the AES algorithm.
3) However, there is a risk that the hidden data can be extracted by the receiver through the reverse process using the A* algorithm, potentially com promising the confidentiality of the data.
4) To ensure its effectiveness, this method is based on a thorough analysis to validate its performance efficiency, making it a reliable choice for protecting sensitive information.
5) Overall, these factors highlight the strengths and limitations of this method and the importance of carefully considering the trade-offs between security, efficiency, and practicality when selecting a cryptography or steganography technique for a particular application

V. CONCLUSION

This essay discusses the encryption and decryption of the processed data. The Pixel Repetition Technique is used to perform pre-processing on the data after it has been collected as input. Data steganography is accomplished by encryption and decryption using a number of methods. Pre-processing is carried by using the Pixel Repetition Technique. The data is encrypted by using the proposed AES method, and then the data is then embedded using LSB to perform data improvement and recover the concealed data to execute on analysed data to confirm its performance effectiveness. Data steganography is accomplished by encryption and decryption using a number of methods. Pre-processing is carried by using the Pixel Repetition Technique. pixel adjustment through the proposed innovative OPAP-based CNN in order to retrieve the hidden data. Several algorithms have applications that consider society.

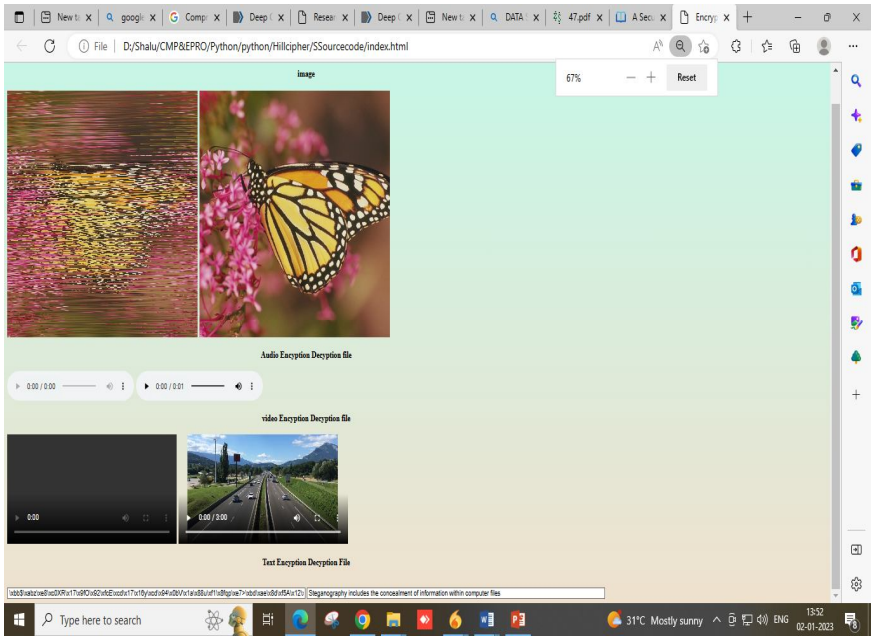


Figure.5. Output

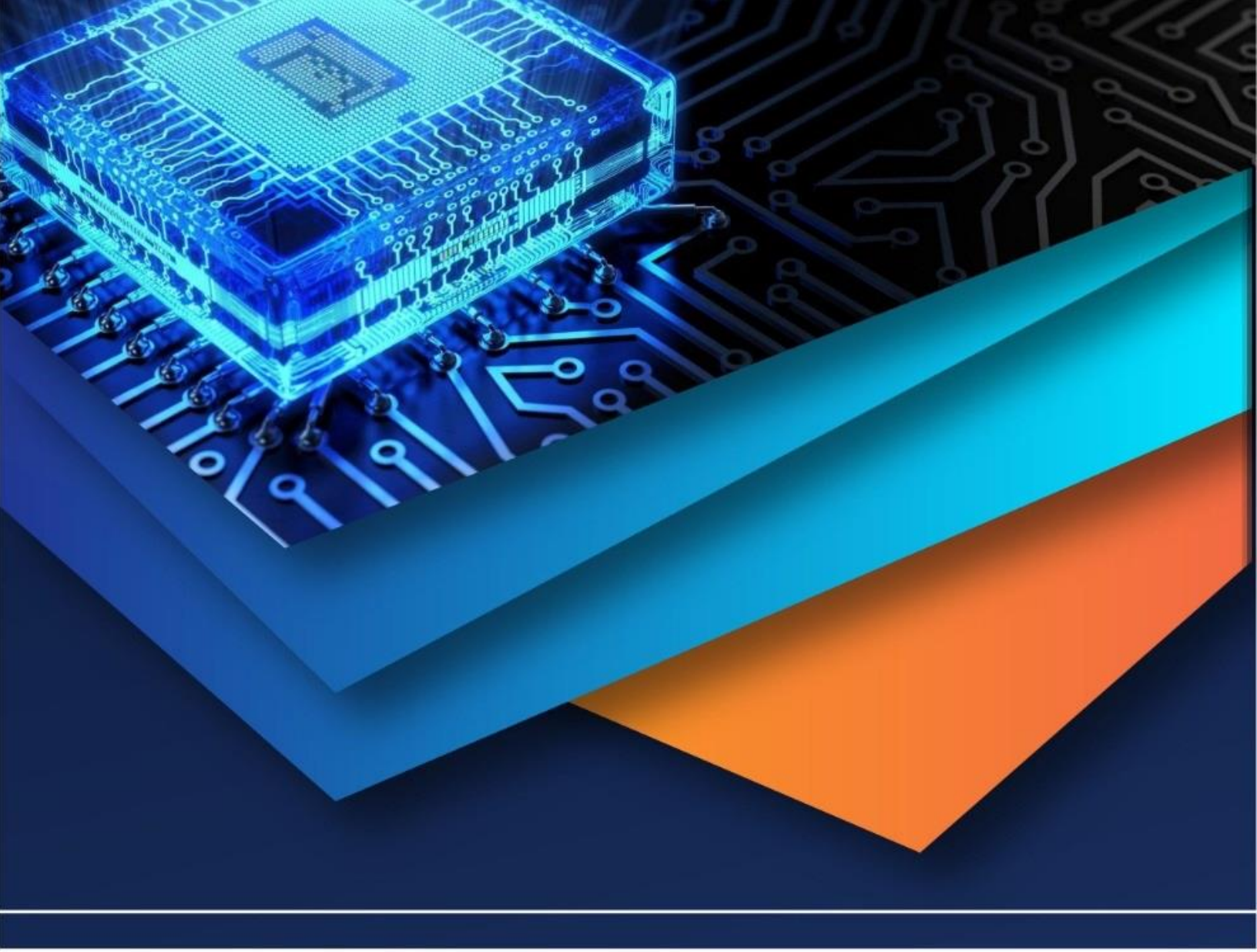
VI. FUTURE WORK

Data steganography is accomplished by encryption and decryption using a number of methods. Pre-processing is carried by using the Pixel Repetition Technique. pixel adjustment through the proposed innovative OPAP-based CNN in order to retrieve the hidden data. Several algorithms have applications that consider society.

REFERENCES

[1] S. Karakus and E. Avci, "A new data steganography method with optimum pixel similarity for data hiding in medical data," Medical Hypotheses, vol. 139, pp. 109691-109691, 2020.
[2] C. Y. Roy and M. K. Goel, "Visual Cryptographic Steganography with Data Integrity," Lovely Professional University, 2017.
[3] P.Rahmani and G.Dastghaibyfard, "An efficient histogram-based index mapping mechanism for reversible data hiding in VQ-compressed data," Information Sciences, vol. 435, pp. 224-239, 2018.
[4] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K.-H. Jung, "Data steganography in spatial domain: A survey," Signal Processing: Data Communication, vol. 65, pp. 46-66, 2018.
[5] S. D. Ahmadi and H.Sajedi, "Data steganography with artificial immune system," in 2017 Artificial Intelligence and Robotics (IRANOPEN), 2017, pp. 45-50.
[6] A. Miri and K. Faez, "Adaptive data steganography based on transform domain via genetic algorithm," Optik, vol. 145, pp. 158-168, 2017.
[7] M. Umair, "Comparison of Symmetric Block Encryption Algorithms," ResearchGate, 2017.
[8] A. K. Sahu and G. Swain, "A review on LSB substitution and PVD based data steganography techniques," Indonesian Journal of Electrical Engineering and Computer Science, vol. 2, pp. 712-719, 2016.
[9] L. Laimeche, A. Meraoumia, and H. Bendjenna, "Enhancing LSB embedding schemes using chaotic maps systems," Neural Computing and Applications, pp. 1-19, 2019.
[10] N. A. Loan, S. A. Parah, J. A. Sheikh, J. A. Akhoon, and G. M. Bhat, "Hiding electronic patient record (epr) in medical data: A high capacity and computationally efficient technique for e-healthcare applications," Journal of biomedical informatics, vol. 73, pp. 125-136, 2017.
[11] K. Sakthidasan and N. V. Nagappan, "Noise free data restoration using hybrid filter with adaptive genetic algorithm," Computers & Electrical Engineering, vol. 54, pp. 382-392, 2016.

[12] J. Kim, H. Park, and J.-I. Park, "CNN-based data steganalysis using additional data embedding," Multimedia Tools and Applications, vol. 79, pp. 1355-1372, 2020.
[13] S. Nipanikar , V. H. Deepthi, and N. Kulkarni, "A sparse representation based data steganography using particle swarm optimization and wavelet transform," Alexandria engineering journal, vol. 57, pp. 2343-2356, 2018.
[14] A. Miri and K. Faez, "An data steganography method based on integer wavelet transform," Multimedia Tools and Applications, vol. 77, pp. 13133-13144, 2018.
[15] M. Kaur and M. Juneja, "A new LSB embedding for 24-bit pixel using multi-layered bitwise XOR," in 2016 International Conference on Inventive Computation Technologies (ICICT), 2016, pp. 1-5.
[16] K. Sreehari and R. Bhakthavatchalu, "Implementation of hybrid cryptosystem using DES and MD5," in 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 2018, pp. 52-55.
[17] S. A. Parah, J. A. Sheikh, J. A. Akhoon, and N. A. Loan, "Electronic Health Record hiding in data for smart city applications: A computationally efficient and reversible information hiding technique for secure communication," Future Generation Computer Systems, vol. 108, pp. 935-949, 2020.
[18] G. Ardiansyah, C. A. Sari, and E. H. Rachmawanto, "Hybrid method using 3-DES, DWT and LSB for secure data steganography algorithm," in 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2017, pp. 249-254.
[19] D. K. Sarmah and A. J. Kulkarni, "Improved cohort intelligence—a high capacity, swift and secure approach on JPEG data steganography," Journal of information security and applications, vol. 45, pp. 90-106, 2019.
[20] A. Hambouz, Y.Shaheen, A. Manna, M.Al-Fayoumi, and S. Tedmori, "Achieving Data Integrity and Confidentiality Using Data Steganography and Hashing Techniques," in 2019 2nd International Conference on new Trends in Computing Sciences (I)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY