IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AI-Based Image Steganography

Jahnavi S [1], Nayana S [2], Pruthivika V [2], Chandini S [2], Pushpamala S [2]
[1] Assistant Professor, Department of CSE, Dayananda Sagar Academy of Technology and Management, Bangalore, India
[2] Student, Department of CSE, Dayananda Sagar Academy of Technology and Management, Bangalore, India

Abstract: Steganography is a technique for concealing sensitive information inside of cover image. In order to prevent detection, this technique involves concealing biometric within a cover image. When someone views an image that contains secret information, they are unaware that it contains any such information. The project offers a very basic application that, by concealing communication, makes the manual labour easier. We printed out information about the project's image steganography technology, which uses the PSO methodology and the EMD method to enable secure communication. In order to guarantee that embedded information can securely defend against attacks, efforts to improve robustness and embedding capacity are required. The user will find this program to be incredibly convenient and time-efficient.

1. INTRODUCTION

The security of data becomes an important and crucial concept as a result of the significant losses and digital signal transmission caused by unauthorised access to data and the rising demand in both. Encryption and steganography procedures are used to protect data and keep it safe from unauthorised access. Security is the most crucial idea in any transmission channel communication process between sender and recipient. The use of cutting-edge secure network technologies makes it possible to handle risks and obstacles, but they are insufficient to ensure the confidentiality of information transmitted between sender and receiver. Information security therefore requires additional security measures. Steganography, which meaning "covered writing" or "concealed writing," has Greek roots. The ability to conceal the existence of a message is the primary distinction between steganography and cryptography. The safeguarding of information from nefarious or unwelcome outsiders is the common objective of steganography and cryptography. The concealing procedure is carried out using a chosen private or secret key to increase the difficulty of the hiding process. The embedding method will embed the secret information in the host image. A stego-image is then sent to the receiver through a transmission medium or communication channel after the embedding process. Using the same or a different key, depending on the type of steganography initially chosen, the receiver recovers concealed information encoded using the embedding technique by the sender from the received stego-image. To achieve this, the receiver will use an extraction technique on the stego-image. Many uninvited individuals or parties become aware of a stego-image through transmission from the sender to the receiver without being able to access the concealed contents of a stego-image.

The diagram of the Exploiting Modification Direction is shown below:

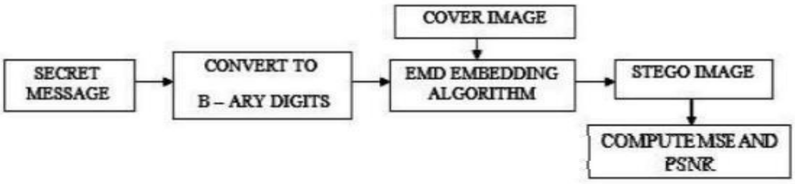

Figure 1: EMD EMBEDDING SCHEME

From the above figure 1, as we use two algorithms to hide secret biometrics inside a cover image for better payload capacity and better results without any loss of information. This hidden image is transformed into a stego-image and then transmitted over a communication channel to the decoder.

2. LITERATURE SURVEY

The literature survey details on research made related to the proposed system

‘Blockchain for steganography: advantages, new algorithms and open challenges’ which is developed by Omid Torki, Maeda Ashouri-Talouki, and Mojtaba Mahdavi for developing steganography in the blockchain [1]. This paper encloses the advantages of the blockchain and its specific features. The authors’ have described how the transmission of data happens between the sender and the receiver. The hierarchical deterministic wallet(HDW) method is used. The sender-receiver relationship is briefly described by the author. The method is used for creating a public key the and HDW algorithm is also taken. The HDW algorithm shows how the user gains profit or loss in the bitcoins. The evaluation process is based on the HDW algorithm process. They are evaluated using some main specifications namely visibility, Robustness, security, and capacity. The challenges discussed here are about the unique features that come out in steganography. One of the crucial challenges is finding the blockchain uniqueness not only in biometrics but also in money-related transactions and digital currencies and the other hand is of identifying the methods for improving the quality of the data, even more, better in future improvements.

‘The PSO–Blockchain-based Image Steganography: towards a new method to secure updating and sharing COVID-19 data in decentralized hospitals intelligence architecture’ that is published by A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, K. I. Mohammed, O. S. Albahri, A. S.Albahri & M. A. Al-Salem is developed for securing the medical data of COVID-19 during the lockdown and pandemic [2]. This survey describes how the transmission of data takes place in three different methods i.e. pre-hiding, secret image data hiding, and secret stego image transmission using the PSO algorithm. This proposed system is based on finding the bit location in the given host image for hiding the COVID-19 data. In the validation process, they have brought two types of attacks namely spoofing and brute-force attacks. The evaluation process undergoes methods like PSNR value and MSE(mean square error) to bring out the effective methods from the steganography. The claims described are about the usage of the hash function, challenges faced discussions of why the blockchain is needed. The main limitation here portrayed is that this proposed system is not practiced or tested on real-world world data or examples of infected and suffered cases. The reason is because of the pressurized lockdown and affected. The future work is enclosed to work on the limitation that is specified above that the real patient’s data. Work to improve the payload capacity, confidentiality, and protection of medical data.

‘The Securing images with Fingerprint Data using Steganography and Blockchain’ which is developed by S. Pramothini, Y.V.V.S. Sai Pavan, N. Harini [3] will brief about the security and the confidentiality that is maintained. The paper gives s description of the major terminologies says fingerprint identification, digital watermarking technique, and lastly introduction to the blockchain. Fingerprint Identification uses biometrics, the Digital Watermarking is all about the technique that is applicable to images, audio, and video. It is also proved that it maintains legal rights and copyrights. In this paper, the asymmetric algorithm is made use called RSA and ECC. This algorithm in turn enhances security. The introduction to the blockchain is based specifically on currency transaction issues. It is a superior media that focuses on guaranteed transaction processes. The procedure of this system is of four phases such as scanning the biometrics(fingerprint), encoding the data received, and indexing the final phase is the validation of the extracted image.

The scheme of authenticable medical of image sharing its based on the small shadow embedded of QR code and framework of the blockchain by the Wenying Wen, Yunpeng Jian, Yuming Fang, Yushu Zhang, and Baolin Qiu [4]. This survey paper gives an authenticated medical of image-sharing scheme that based on the shadow embedded called a QR code with the framework of the framework in it. Firstly, The piece of small shadow of image taken by the employing of the image-sharing of secret method based on the method of Chinese remainder. The image-shadow will combine into the code called QR code with error of correction specified in it. It will not ensure confidentiality and principles of the image shadow transmit in the public channel it will avoid the problems. when the encryption of the secret key is lost and it will not improve. Comparing the existing of the excellent scheme, The scheme will uses the hash of bit stream for the authentication process and its employs the smart contracts to the authentication and also restoration. Therefore the local road will be reduced. In addition , The experiments will validate the improved the secret of medical image without the loss of data. The cover of the QR code is more in good condition and also safe. In this method is suitable for the medical image of content protection and secure of sharing.

‘The LSB Image Steganography is inverted using the Adaptive of the Pattern to Improve the Imperceptibility’ by the Supriadi Rustad and De Rosal Ignatius Moses Setiadi and Abdul Syukur and Pulung Nurtantio Andino [5]. This stream will take the adaptive approach into account. Additionally, it can choose the most effective design for reducing the ratio of errors found in embedded images or messages. This adaptable pattern has the potential to be optimised for the LSB inverted technique substitution. This method is based on the pattern in the stored image's two bits and least-significant bit (LSB). Prior to the embedding procedure, the message will be checked along with the image container of the bits, and using LSB substitution, the error ratio for the different patterns will be obtained. This pattern will be chosen to incorporate the image because it has the lowest mistake rate.
The value of the PSNR is ranges from the 52.49 to 57.45 and the SSIM is ranges from the point-too-point capacity. The proposed method will be able to work powerfully with the advantage of the significant imperceptibility of value and it is proven to. The advantage of the LSB inversion technique is that when the smaller ratio of bit value is reached or got for the each pattern.

‘The method hybrid will using the 3-DES and DWT and LSB for the secure of the image steganography algorithm’ by the Ardiansyah G and Sari C.A and Setiadi D.R.I.M and Rachmawanto E.H 2017 [6]. The paper is proposed by combining two Steganography domains that are paired with the Cryptography technique. The goal is to make a confidential data or secret data even when have the more secure and also inaccessible to the unknown peoples or the public. By usage of the 3-DES method, the messages are encrypted. As seen, on one hand the cover image is to breakdown into the four subdivision of the band with the use of DWT. LH, HL and HH of the subdivision are selected to the embedded of the encrypted messages based on the LSB method. The lastly, Inverse of DWT (IDWT) to get stego of the image reconstruction. This method will be measured in its quality with the PSNR and MSE. This experiment results, we have contain the PSNR. The result of the value is 55.30 dB. The image of the message size is 64 * 64 and also 49.023. The DB of the message size is (128 * 128) respectively. The extraction process is perfectly done in these cases.

‘The survey of the Comprehensive image steganography: The Techniques and Evaluations and trends in the future research’ by the Kadhim I.J and Premaratne P and Vial P.J and Halloran B (December 2019) [7] . Our daily lives involve the sharing and storage of sensitive information. Therefore, numerous authors and researchers have focused on protecting, preserving, and transmitting any confidential data. Steganography is the term used to describe this system's technique for blending hidden information into discrete digital media, such as audio, video, and images. The widely utilised and readily accessible digital photographs are heavily represented in this research survey work across several sorts of media. The use of digital image steganography is the main area of focus. the most recent contributions to every category across many mediums. Additionally, it offers essays that give a thorough overview of the image. The overall operation, specifications, elements, various forms of suggested systems, and regular conduct of assessments are all included in steganography. Here, various analysis performance metrics for assessing steganographic systems will also be covered.

‘The steganography of the new image method with the optimum of pixel similarity for hiding the data in the medical images.’ By the Karakus S and Avci E [8].Two key elements in image steganography are the ability to conceal object coverage and the ability to conceal image quality data. with the purpose of lowering the visual quality that humans can see. The assailants won't draw attention to themselves. The major objective is to raise the quantity of the amount to be hidden and the stego's image in order to maintain a high-quality image. The new optimization that is based on the newly introduced method will be included in the paper. This system is suggested to improve the image quality. Performance of the suggested method has been evaluated, and metrics of the form of MSE, RMSE, PSNR, SSIM, and UQI will be used to visualise the quality of the analysis. as a means of concealment. The medical photos in various sizes have been used. It can be found in the Dicom library database's open access. The doctor will make comments on the various things that their medical photographs have concealed. There is a discrepancy in the average value, according to the results. The PSNR value is 66.5374, followed by 59.4420 and 56.3936.

‘The layer of double secret of secure images sharing the scheme for biometrics’ by the Elavarasi Gunasekaran and Vanitha Muthuraman [9]. The most frequently employed technique is a biometric one, followed by an authentication procedure that prevents a person from being vaguely recognised based solely on their physical or behavioural characteristics. Think about the biometrics method. Iris scanning is also regarded as one of the most reliable and safe methods for maintaining privacy. The system's database will be challenged to safely store the iris template. It is very simple to steal or corrupt from the system. Discuss the technique that can also be used effectively to protect the privacy of these biometric picture transmissions across open channels. Additionally, it is possible to increase access control by having the person who will be receiving the photographs authenticate them. As a result, this study suggests a created and effective double-layered safe secret image sharing scheme for the system's biometrics. This method, known as the Double Layered of the Safe Secret Images for Sharing Scheme, is regarded as one of the best methods available at the moment since it increases double protection for sensitive data by not combining the two levels. The second layer of secret sharing will be accomplished using Shamir's secret in sharing approach after the first layer, threshold, which is based on secret sharing, is completed.

‘The representation of the sparse that based on the image steganography using the Particle Swarm of Optimization and wavelet of transform’ by the Karakus S and Avci E [10]. Steganography is an approach used in data hiding or confidentiality matters. Image steganography is the process which can image is used in the form of covering the object or a host image. The two important factors in image steganography are Data hiding capacity and image quality. To make inferior of the image quality is identified by the human vision system and hence,its attracts the attention of the unknowns. The main thing of this study is to increase the number of the data will be hidden and the stego of images to improve the high quality of images. It has the new method of optimization that is based on the proposed of the system using similar features in the pixels study. such as MSE and RMSE and PSNR, SSIM, and UCI have been used to test visual quality analysis.

The cover of object,They have the different shapes of the medical images that are used .It is obtained from the open-access of the Dicom library database. Doctor will comments the hidden of the data from medical images in variety of capacities. They have the various experiments, Thee result of the average of PSNR value is 66.5374 and 59.4420 and 56.3936 respectively. The Threshold is based on the sharing the secret of the data will be performed and the second layer is based on the sharing the secret of the data will be performed.

3. RESEARCH METHODOLOGY

The user should make advantage of the application. Two tab choices, such as encrypt and decrypt, will be available to the user . The application shows a screen where the user can select and save an image file if they decide to encrypt data .The application asks the user where they want to save the secret file and displays a page where they may only select an image file if they decide to decrypt the file. Any type of graphic file canutilizedised to encrypt the secret data and hide it. Decryption is used to retrieve biometric information from an image file. We will use the EMD(exploiting modification direction) approach for this procedure as shown in figure 2.

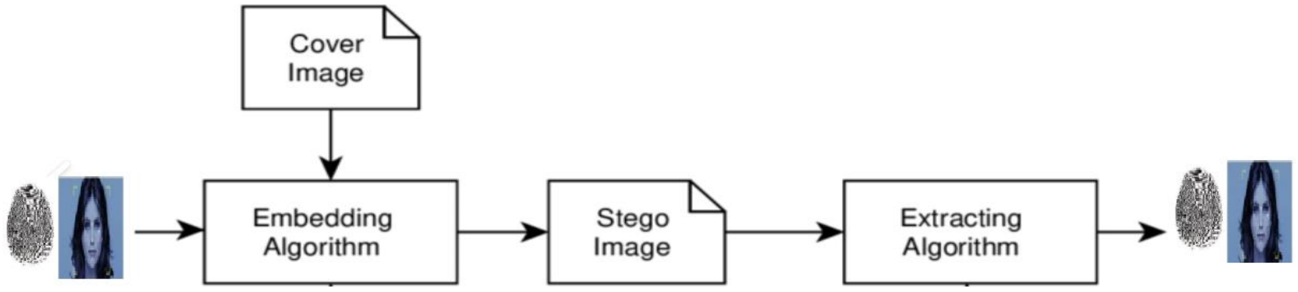

Figure 2: Overview of system

3.1 Particle Swarm Optimization (PSO)

Kennedy and Eberhart introduced the concept of particle swarm optimization in 1995. One of the bio-inspired algorithms is particle swarm optimization (PSO). Any dataset search for an optimal solution in the solution space is performed using what is regarded as a straightforward method. While utilising it to find the best answer. If a bird looks for food randomly while flying, for instance, all of the other birds in the flock can learn about it and collaborate to make the best hunt for the flock as a whole. The best solution found by the flock while simulating a flock of birds is also the best solution in the space, therefore it is possible to suppose that each bird is assisting in our search for the perfect answer in a high-dimensional problem space. We can never verify the actual global optimal solution can be found, and it typically isn't, thus this is a heuristic solution. The PSO solution is frequently, nonetheless, pretty near to the overall ideal.

3.2 Exploiting Modification Direction (EMD)

In comparison to matrix encoding and run length encoding, the basic EMD approach has the highest embedding efficiency and embedding rate. The secret digit (d) in the (2n+1)ary notational system, which is converted from binary confidential information using this procedure, is carried by n pixels, allowing for the transmission of one secret digit. The secret message is therefore first transformed into secret digits using the (2n+1)ary notational scheme, and each secret digit is then embedded into a pixel group (g1, g2... gn). The value of the extraction function fe is determined by using the formula: fe (g1,g2,....gn) = (g1*1+g2*2+. +gn*n) mod (2n+1). If fed, only one pixel from the pixel group has to have its value increased or decreased by one.If fe = d, then changing any number of pixels has no purpose, and the process continues until only one secret digit remains. The same equation is applied to each pixel group (g1, g2, gn) to track the secret digits during the extraction procedure of the secret data. The message is then deciphered by converting all the secret digits from (2n+1)-array notation back into binary representation. Below figure 3, shows embedding stage.

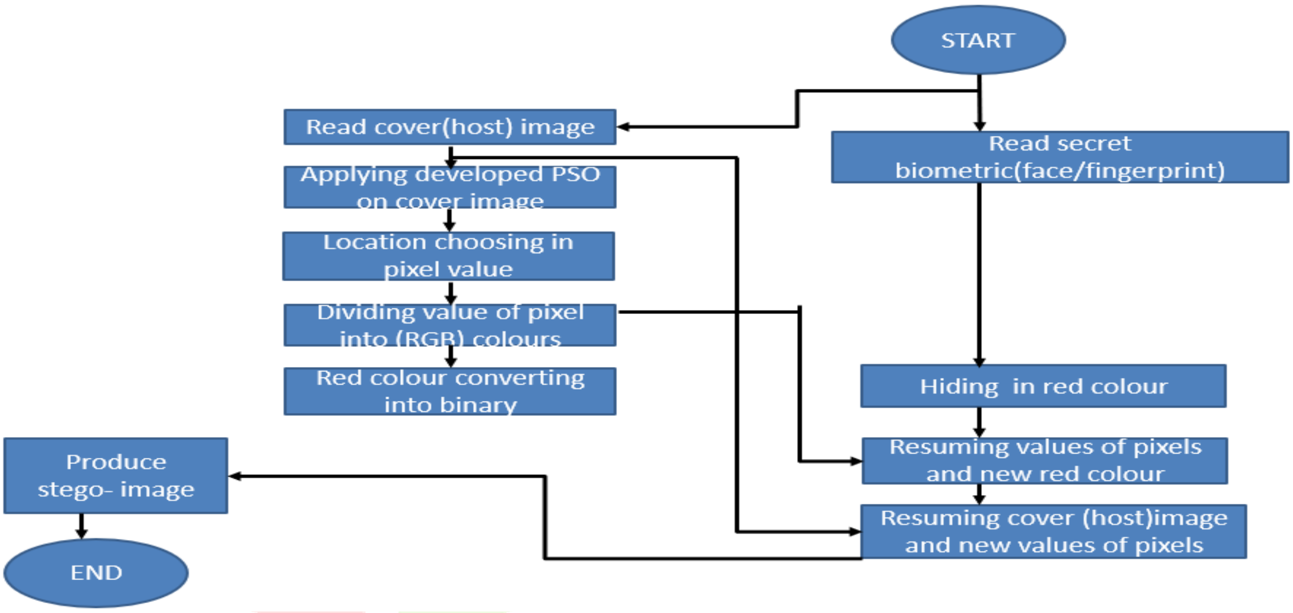
START
Read cover(host) image
Read secret biometric(face/fingerprint)
Applying developed PSO on cover image
Location choosing in pixel value
Dividing value of pixel into (RGB) colours
Red colour converting into binary
Hiding in red colour
Resuming values of pixels and new red colour
Resuming cover (host)image and new values of pixels
Produce stego- image
END

Figure 3: Flowchart of Embedding stage

4. CONCLUSION

Blockchain is a peer-to-peer network for the transmission of data, and steganography is a communication technique, thus the benefits of blockchain can be widely used to steganography operations. The advantages of using blockchain techniques for steganography analysis are covered in the study. This includes the capacity of the blockchain platform to support data transmission and storage needs, as well as the capability to insert concealed data without manually altering the original data. This will primarily eliminate the need for steganographers when creating and implementing a new platform for data transmission and storage. For steganography in blockchain, two algorithms have been proposed: one is a high-capacity algorithm for the Key encryption process and the steganography algorithm exchange and switching methods, and the other is a medium-capacity algorithm for embedding hidden data.

5. REFERENCES

[1] Omid Torki, Maede Ashouri-Talouki, Mojtaba Mahdavi. 'Blockchain for steganography: advantages, new algorithms, and open challenges'. arXiv:2101.03103v1 [cs.CR] 8 Jan 2021

[2] A. H. Mohsin , A. A. Zaidan1 , B. B. Zaidan , K. I. Mohammed , O. S. Albahri , A. S.Albahri & M. A. Alsalem(2022).'PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralized hospitals intelligence architecture'. https://doi.org/10.1007/s11042- 020-10284-y

[3] S. Pramothini, Y.V.V.S. Sai Pavan, N. Harini. 'Securing Images with Fingerprint Data using Steganography and Blockchain. International Journal of Recent Technology and Engineering (IJRTE)ISSN: 2277-3878,
Volume-7 Issue-4S2, December 2018

[4] Wenying Wen, Yunpeng Jian, Yuming Fang, Yushu Zhang, and Baolin Qiu. 'Authenticable medical image-sharing scheme based on embedded small shadow QR code and blockchain framework'. https://doi.org/10.21203/rs.3.rs-1806415/v1

[5] Supriadi Rustad, De Rosal Ignatius Moses Setiadi, Abdul Syukur, Pulung Nurtantio Andono(2020).'InvertedLSB Image Steganography using Adaptive Pattern to Improve Imperceptibility'.10.1016/j.jksuci.2020.12.017

[6] Ardiansyah, G., Sari, C.A., Setiadi, D.R.I.M., Rachmawanto, E.H.'Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm'.2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE). IEEE, pp. 249– 254.https://doi.org/10.1109/ICITISEE.2017.8285505.

[7] Kadhim, I.J., Premaratne, P., Vial, P.J., Halloran.'A comprehensive survey of image steganography: Techniques,Evaluations, and trends in future research.Front. Comput. Neurosci., 11 December 2019. Final yearproject: AI-Based Image Steganography Dept. of CSE, DSATM 2021-22 Page 29

[8] Karakus, S., Avci, E.'A new image steganography method with optimum pixel similarity for data hiding in medical images.'(March 2022).https://doi.org/10.1016/j.mehy.2020.109691

[9] Elavarasi Gunasekaran & Vanitha Muthuraman.'Double layer secure secret images sharing scheme for biometrics'(August 2021).2022, Distributed and Parallel Databases

[10] Nipanikar, S.I., Hima Deepthi, V, Kulkarni,. N. 'A sparse representation based image steganography using Particle Swarm Optimization and wavelet transform' (December2018). https://doi.org/10.1016/j.aej.2019.09.005.

[11] S Jahnavi, C Nandini. 'Novel multifold secured system by combining multimodal mask steganography and naive based random visual cryptography system for digital communication'. Journal of computational and theoretical nanoscience , American Scientific Publishers, 17 (12), 5279-5295, https://doi.org/10.1166/jctn.2020.9420

[12] S. Jahnavi and C. Nandini, "Smart Anti-Theft Door locking System," 2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE), 2019, pp. 205-208, doi: 10.1109/ICATIECE45860.2019.9063836.

[13] Nandni, C., Jahnavi, S. (2021). Quantum Cryptography and Blockchain System: Fast and Secured Digital Communication System. In: Bhateja, V., Satapathy, S.C., Travieso-González, C.M., Aradhya, V.N.M. (eds) Data Engineering and Intelligent Computing. Advances in Intelligent Systems and Computing, vol 1407. Springer, Singapore. https://doi.org/10.1007/978-981-16-0171-2_43

[14] Jahanvi Shankar, C Nandini. 'Hybrid Hyper Chaotic Map with LSB for Image Encryption and Decryption'. Scalable Computing: Practice and Experience, universitatea de vest din Timisoara, Volume 23, Issues 4, pp. 181–191, DOI 10.12694/scpe.v23i4.2018181-192.

[15] Jahnavi S, Dr.C. Nandini. 'DIGITAL DATA SECURITY USING VISUAL CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES: AN EXTENSIVE REVIEW'. Journal of Emerging Technologies and Innovative Research 5 (9), 212-218