IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain Technology Based Image Steganography

Ms.Jahanvi S[1], Navtej P [2],Medini H S[2], Mamisha[2] ,Pradeep 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: The model is based on the steganography method using a neural network, symmetric encryption and cryptographic hash functions. Steganography is the process of hiding private or sensitive information within something that appears to be nothing be a usual image. Steganography involves hiding Text Messages, so it appears that to be a normal image or other file. Our project aims to provide a secure and tamper-proof way of authenticating user identity across multiple platforms. We accomplish this by using a combination of image steganography and the Ethereum blockchain. Specifically, we hide user identity information within images using Image steganography, and then store these images on the Ethereum blockchain as non-fungible tokens (NFTs). This allows us to create a verifiable and immutable record of each user's identity, which can be easily authenticated on any platform that supports the Ethereum blockchain.

Keywords—Image Steganography,Etherum Blockchain,LSB,Decentralized method

I. Introduction

Steganography is a technique for hiding data within other data, which can then be extracted upon reaching its destination. This technique can be used in conjunction with encryption as an additional layer of protection for the data. Steganography is often used for transmitting data over insecure network channels, such as the internet, which is commonly used for exchanging digital media by individuals, private companies, institutions, and governments. However, the availability of tools that can exploit the privacy, data integrity, and security of transmitted data has increased the risk of malicious threats, eavesdropping, and other subversive activities. One solution to this problem is data encryption, where the data is converted into a cipher text using an encryption key, and then converted back into plain text using a decryption key at the receiving end.

This project was developed to create a system for securely storing user identity information using a combination of image steganography and the Ethereum blockchain, to provide a secure and decentralized way to authenticate users. Pros of this system are that it provides a more secure and tamper-proof way of storing user identity information compared to traditional methods and provides users more control over their authentication as it is decentralized.The motivation for this project comes from the fact that the current system of authentication is heavily centralized and susceptible to tampering and single points of failure. By using a decentralized approach based on blockchain technology, we aim to provide a more secure and tamper-proof way of authenticating user identity. This can have a number of potential benefits, including increased security, improved user privacy, and the ability to easily and securely authenticate users across multiple platforms.

This project is used for securing online privacy and secret information such as video,audio,text. To meet the requirements,we use the simple and basic approach of steganography. Such steganography algorithms will be used in this project to generate images with the hidden text. These images will then be stored as NFTs (non-fungible tokens) on the Ethereum blockchain, which is a decentralized ledger that allows for secure and immutable storage of data, using which we will enable the authentication of users.

The current system of user authentication is centralized and susceptible to tampering and single points of failure, which can compromise the security and privacy of user identity information. Our project aims to address this problem by using a decentralized approach based on blockchain technology to create a secure, tamper-proof, and verifiable record of user identity for user authentication.

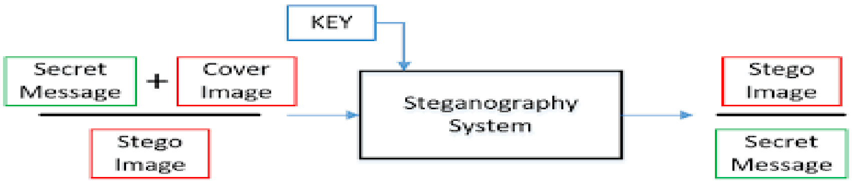

Fig:LSB Based Image Steganography Method

II. LITERATURE REVIEW

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.In this paper authors have discussed about benefits of blockchain in steganography,which contains the capacity without changing original data to immerse the hidden data.Here authors have mentione show the data can be transferred between sender and reciever.Here they have proposed three algorithms for steganography in the blockchain technology,theyare-High Capacity algorithm,medium capacity algorithm,wallet(how)algorithm.

High Capacity Algorithm is used for exchanging the stegaography algorithms and can hide one color image in another color image .Medium capacity algorithm is used for immersing the hidden data.A hierarchical deterministic (HD) wallet is commonly used to store the keys for those who are handling cryptocurrencies such as Ethereum .One of the drawback in this methods is that it is difficult to find the blockchain features that can immerse and provide algorithms and in other hand working on the improvement of the quality of the data even more better in the future.

'A Novel and Robust Hybrid Blockchain and Steganography Scheme',Mustafa Takaoğlu and et al, have proposed blockchain steganography method with the OTA (Ozyavas–Takaoglu–Ajlouni) those algorithm that is used to solve the many current problems.These are requirements that steganography needs to consider the payload capacity,security and robustness. Robustness means that the data that is hidden that uses any steganographic method can be obtained from stego-multimedia without any reduction after the rotation and resizing.The proposed method experiences the size limitation on the hidden data and this data cannot be determined by the stegnalysis method.The proposed alogorithm contains two process,one is steganography process and another is sending stego data using OTA-chain blockchain method.The OTA-chain platform will be obtained when its front-end is achieved.In this proposed algorithm,private server is used to store the multimedia in the form of covers.the URL of this multimedia is stored in the form of blocks in OTA-chain.However using this algorithm the hidden data cannot be determined using the steganalysis method,So they use their own novel structure.The plain data text is divided into number of bits depending on the size.These is plain data text contains bit patterns.So the search begins to match these plain text patterns with the bit pieces .Once the match is found then it will stored as indices in the array.This process is cyclic.Once the first match is found it will move to find the next match until the end of the cover multimedia file.Once it reaches end then again it starts searching from the begining. With this we can conclude that the proposed OTA algorithm is a new approach for steganography method with blockchain technology .So here we used OTA algorithm and OTA-chain method and tested them using real data.Outcome of using this algorithm was that it performed with low cost system , with more security and there is no limitation for hiding information.

Atique ur Rehman and et al, have proposed a convolutional neural network based encoder-decoder architecture for embedding of images as payload.The majority of the work in image steganography has been done to conceal a particular text message under a cover image. To incorporate the most hidden information possible without changing the original image, all known algorithms have focused on locating either "noisy regions" or “low level elements such as edges , textures, etc ”in cover image.The main benefit of the strategy is that any form of image may be used with it because it is general.
They make use of the notion that CNN layers learn an image feature hierarchy, starting with low-level generic features and moving up to high-level domain-specific features. In order to conceal the information from the payload images, the encoder recognises key features from the cover image, and the decoder learns to distinguish those hidden features from the “hybrid” image.They have used CIFAR10 dataset for the cover images and MNIST dataset or the payload images, and for this experiment they are able to hide 29.1% payload in the cover images.They used both of the images from the MNIST dataset to make the experiment more general and were able to cover up the 33.3% payload in the cover image. As a result, they have come to the conclusion that the suggested algorithm is incredibly generic and that one may successfully guarantee large payloads using the same architecture.

One million photos were selected at random to create a subset of 8,000 images. This experiment was able to hide a payload of 33.3% in the cover image.Finally, they have demonstrated a brand-new encoder-decoder architecture for image steganography that is based on CNN. This technique directly accepts a picture as payload in contrast to other methods, which only took into account binary representation as payload. It then employs two encoder-decoder networks to embed and securely retrieve the image from the cover image. By demonstrating great results with strong payload capacity on a variety of wild-image datasets, they have carried out extensive trials and empirically demonstrated the superiority of the suggested strategy.

Mohsin, Ali & Zaidan, A. & Bahaa, Bilal & Mohammed, K. & Albahri, O.s & Albahri, A.s & Alsalem, M.A. (2021). PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture. This is particularly important for maintaining the confidentiality and integrity of the data as well as ensuring its availability in the event of network failure. To address these challenges, this study proposes a new approach of steganography-based blockchain method in the spatial domain as a solution. This method involves the use of a particle swarm optimization algorithm and hash functions to hide secret health COVID-19 data in hospital databases while maintaining high levels of confidentiality and image quality. The proposed method is discussed in three steps: pre-hiding, secret data hiding, and transmission. The proposed method was then validated and evaluated.

Alafandy, Khalid & El-Rabaie, El-Sayed & Faragallah, Osama & Elmahalawy, Ahmed. (2019). High Security Data Hiding Using Cropping Image and Least Significant Bit Steganography.This paper presents a technique for securely hiding data using image cropping and LSB steganography. The technique involves extracting predefined secret coordinates from the cover image, dividing the secret text message into sections equal to the number of image crops, and using LSB to embed each section of the secret message into an image crop with a secret sequence using the cover image's color channels. The resulting stego image is obtained by reassembling the image and stego crops. The proposed technique is evaluated and compared to other state-of-the-art techniques based on visualization, extraction difficulty for unauthorized viewers, PSNR, and CPU time. The experimental results show that the proposed technique is more secure compared to traditional techniques.

Khalaf, Ashraf A. M. & Fouad, Osama & Hussein, Aziza & Hamed, Hesham & Kelash, Hamdy & Ali, Hanafy. (2019). Hiding data in images using DCT steganography techniques with compression algorithms. Steganography is the art and science of secretly communicating information through the use of a cover object, such as an image, without drawing attention to the fact that the message is being transmitted. It has gained significant attention in recent times due to its ability to conceal the very existence of the message. This paper presents a comparison of two different steganography techniques. The first technique employs the Least Significant Bit (LSB) method without any encryption or compression. The second technique involves first encrypting the secret message and then using LSB, as well as transforming the image into the frequency domain using the Discrete Cosine Transform (DCT). The LSB algorithm is implemented in the spatial domain, where the payload bits are inserted into the least significant bits of the cover image to create the stego-image. On the other hand, the DCT algorithm is implemented in the frequency domain, where the stego-image is transformed from the spatial domain to the frequency domain and the payload bits are inserted into the frequency components of the cover image. The performance of these two techniques is evaluated using the parameters Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR).

III. METHODS AND PLANNING OF WORKS

We planned to start our work by first using image steagnography domain in our project so that we can get images related to it and can be used and once the image is been displayed or processed then it can be covered to the further step. Next we will be using Image steganography algorithms such as LSB so that it can be a security for the required authentication once the authorized user is sending it and its approved then it can be moved to the further steps. Then next we will be blockchain technology s that it can be used by the user to securely store the generated images on a decentralizedd ledger and generate NFTs that can be further used for authentication.

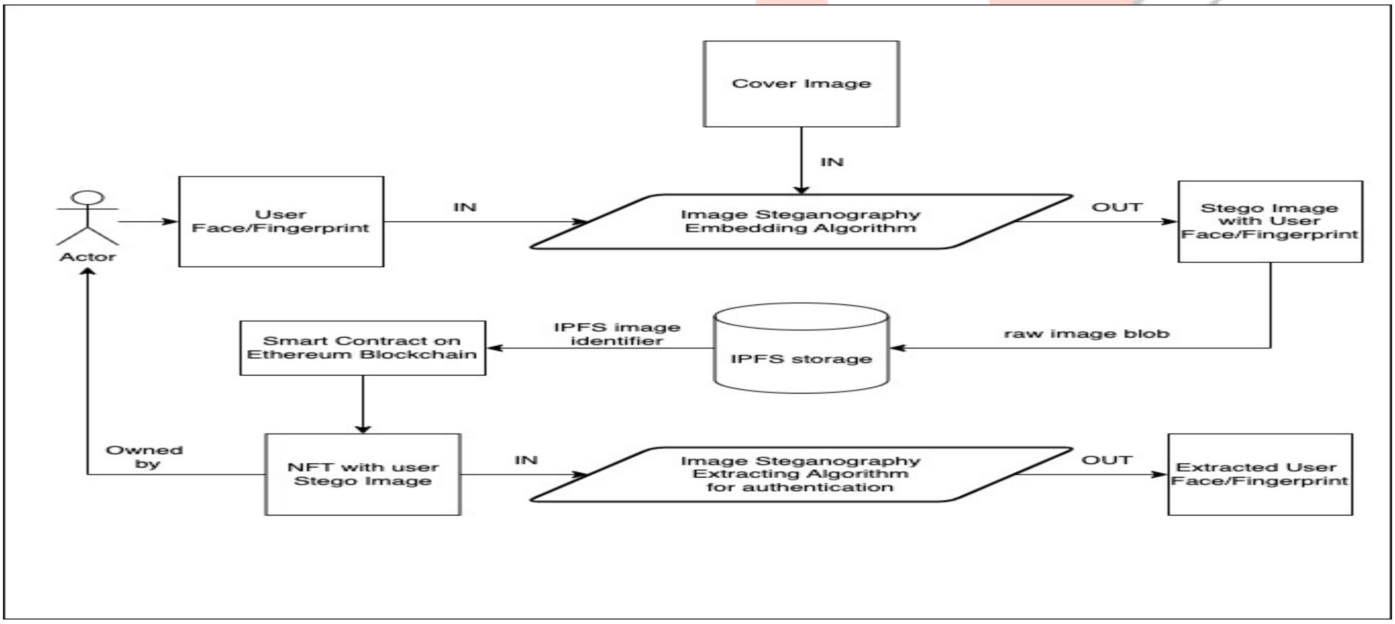
Cover Image
IN
Actor
User Face/Fingerprint
IN
Image Steganography Embedding Algorithm
OUT
Stego Image with User Face/Fingerprint
Smart Contract on Ethereum Blockchain
IPFS image identifier
IPFS storage
raw image blob
Owned by
NFT with user Stego Image
IN
Image Steganography Extracting Algorithm for authentication
OUT
Extracted User Face/Fingerprint

Fig: Flowchart for proposed method

Methodology we used for developing this project are:
1. Image steganography algorithms such as LSB is used to hide secret user information in images to avoid detection.
2. The output of each image hidden using steganography, is stored on IPFS, a decentralized file storage platform, and the metadata relating to this is stored on the ethereum blockchain, so as to make it immutable.
3. The IPFS metadata stored on ethereum will be on a smart contract that can map it to users as a non-fungible token so that only one specific user can use this for authentication, and it cannot be copied, or tampered with.

4. This final output image can then be used for authentication by the user.
5. During the authentication phase, the same image steganography algorithm will reveal the base input image, which can be verified for finding out the user's identity.
6. This authentication setup is to be a simple plugin that a wide range of systems can use as a reliable SSO Login mechanism.

IV. REFERENCES

[1]. Mustafa Takao˘glu, Adem Özyava¸s , Naim Ajlouni , Ali Alshahrani and Basil Alkasasbeh (2021). “:A Novel and Robust Hybrid Blockchain and Steganography Scheme”.

[2]. Atique ur Rehman, Rafia Rahim, Shahroz Nadeem, and Sibt ul Hussain(2018). “End-to-End Trained CNN Encoder-Decoder Networks For Image Steganography”.

[3]. A. A. Zaidan, A. H. Mohsin, B. B. Zaidan, K. I. Mohammed, O. S. Albahri(2021) " PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture "

[4]. Omid Torki, Maede Ashouri-Talouki, Mojtaba Mahdavi(2021) “Blockchain for steganography: advantages, new algorithms and open challenges”

[5]. Subhedar, M.S., Mankar, V.H. (2014). “Current status and key issues in image steganography”

[6]. Glorot, X., Bengio, Y(2010). “Understanding the difficulty of training deep feed forward neural networks”.

[7] Nipanikar, S.I., Hima Deepthi, V., Kulkarni, N.’ A sparse representation based image steganography using Particle Swarm Optimization and wavelet transform’(December 2018).https://doi.org/10.1016/j.aej.2019.09.005.

[8] P. McCorry, S. F. Shahandashti, and F. Hao, “A smart contract for boardroom voting with maximum voter privacy,” in International Conference on Financial Cryptography and Data Security, pp. 357–375, Springer, 2017.

[9] M. Xu, H. Wu, G. Feng, X. Zhang, and F. Ding, “Broadcasting steganography in the blockchain,” in International Workshop on Digital Watermarking, pp. 256–267, Springer, 2019.

[10] L. Zhang, Z. Zhang, W. Wang, R. Waqas, C. Zhao, S. Kim, and H. Chen, “A covert communication method using special bitcoin addresses generated by vanitygen,” CMC-Comput Mater Contin, vol. 65, no. 1, pp. 597–616, 2020.

[11] J. Partala, “Provably secure covert communication on blockchain,” Cryptography, vol. 2, no. 3, p. 18, 2018.

[12] Kadhim, I.J., Premaratne, P., Vial, P.J., Halloran.'Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research'.Front. Comput. Neurosci., 11 December 2019.

[13] 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

[14] 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.

[15] 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

[16] 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.

[17] 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