Blockchain Technology Based Image Steganography

Jahnavi S[1], Pradeep S[2], Navtej P[2], Medini HS[2], Mamisha[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.**

***Index Terms* -- Image Steganography, Etherum Blockchain , Decentralised 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 tamperproof 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,t ext. 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 (nonfungible 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 1 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.

II. PROBLEM STATEMENT

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. This can have number of potential benefits including increased security, improved user privacy ability to easily and securely authenticate users across multiple platforms.

III. RELATED WORK

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. 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 mentioned show the data can be transferred between sender and receiver. Here they have proposed three algorithms for steganography in the blockchain technology, they are 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.

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 image elements such as edges, textures, etc." in cover images. 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 1 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).

IV. MATERIALS

The combination of image steganography and the Ethereum blockchain is to create a secure and decentralized system for storing user identity information. The user's data is embedded within an image, making it difficult for anyone to tamper with or steal the data. Moreover, the use of the Ethereum blockchain provides additional security by ensuring that the data is stored in a decentralized manner, meaning that it is not controlled by a single entity or organization. This decentralized nature of the system also provides users with more control over their authentication, as they are not dependent on a centralized authority to verify their identity. Overall, this system offers a more secure and reliable way of storing user identity information, which is particularly important in today's digital age where data breaches and identity theft are common. Fig 1 shows the process of user authentication.

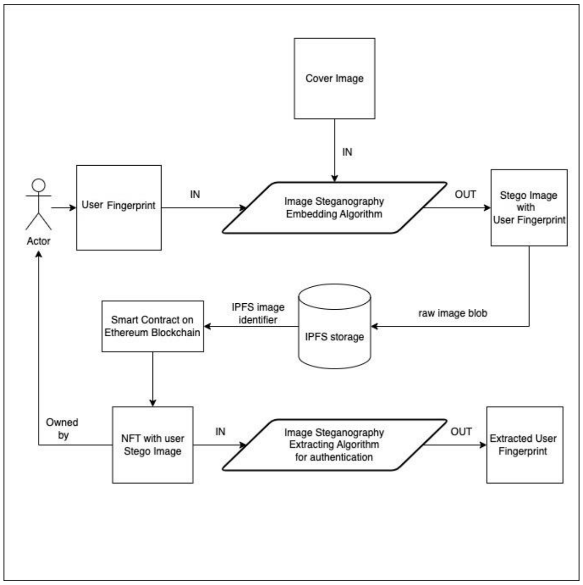


Fig 1.Block Diagram for Methodology

To design the system architecture for user autentication we require following modules:

1. **IPFS (InterPlanetary File System)**:

IPFS is decentralized because it loads the content from thousands of peers instead of one centralized server. Every piece of data is cryptographically hashed, resulting in a safe, unique content identifier: CID Fig2. shows actually how IPFS processes.

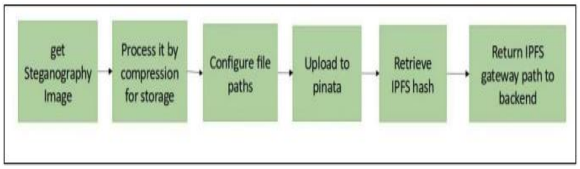


Fig 2:IPFS

2.Smart Contract:

Smart contracts are at the heart of the blockchain revolution, providing the building blocks for decentralized applications.A smart contract is a contract expressed as a piece of code that's designed to carry out a set of instructions.With smart contracts, however, there's no middleman. There's no person or company holding your information or verifying it. The blockchain verifies and holds information for you.Fig3 shows how smart contract helps in storing the data of minted NFT.

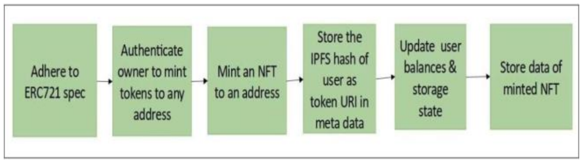

Adhere to ERC721 spec
Authenticate owner to mint tokens to any address
Mint an NFT to an address
Store the IPFS hash of user as token URI in meta data
Update user balances & storage state
Store data of minted NFT

Fig 3: Smart contact

3.Backend:

Backend is built to handle image inputs and outputs and correctly encode and decode for authentication. Fig 4 shows the basic process for uploading and processing files in a system that uses unique user identifiers and temporary local storage for efficient processing and future use. Fig 5 shows how securely user identity data can be encoded into a steganography image and store it on a distributed file system. This process provides a secure and decentralized way to authenticate user identity data, which can be useful in various applications. Fig 5 shows how the images can be decoded for authentication purposes. It is used to retrieve and authenticate user identity data that was previously encoded and stored using steganography and the Ethereum blockchain. This endpoint is part of a larger system that provides a secure and decentralized way for users to authenticate themselves, which can be useful in various applications, such as online identity verification, secure document storage, and decentralized authentication systems.

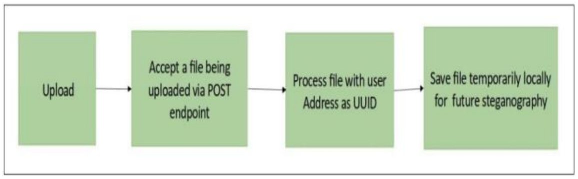

Upload
Accept a file being uploaded via POST endpoint
Process file with user Address as UUID
Save file temporarily locally for future steganography

Fig 4:Uploading and Processing Files

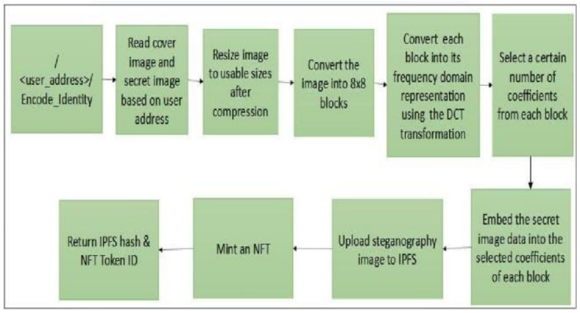

/<user_address>/ Encode_Identity
Read cover image and secret image based on user address
Resize image to usable sizes after compression
Convert the image into 8x8 blocks
Convert each block into its frequency domain representation using the DCT transformation
Select a certain number of coefficients from each block
Embed the secret image data into the selected coefficients of each block
Upload steganography image to IPFS
Mint an NFT
Return IPFS hash & NFT Token ID

Fig 5:Encoding of User Identity Data

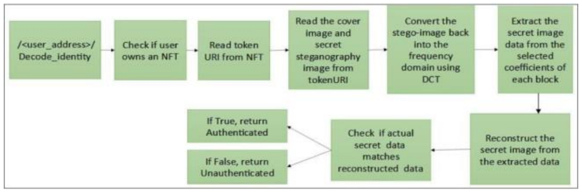

/<user_address>/ Decode_identity
Check if user owns an NFT
Read token URI from NFT
Read the cover image and secret steganography image from tokenURI
Convert the stego-image back into the frequency domain using DCT
Extract the secret image data from the selected coefficients of each block
Reconstruct the secret image from the extracted data
Check if actual secret data matches reconstructed data
If True, return Authenticated
If False, return Unauthenticated

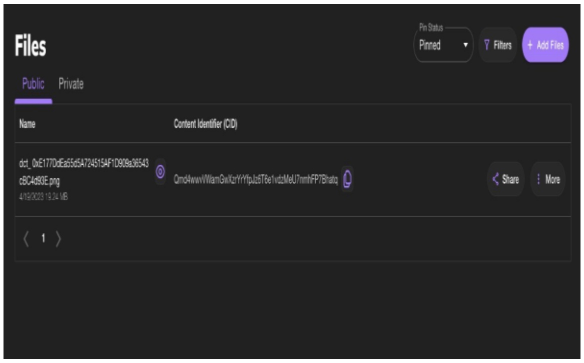
Fig 6:Decoding of User Identity Data

V. METHODS

The main objective of building a system for biometric-based authentication using DCT image steganography and IPFS storage is to provide a secure and efficient way to authenticate users. To achieve this, several tasks need to be accomplished. Firstly, biometric data sets must be collected from users and stored securely in compliance with data protection regulations. Next, an efficient DCT image steganography algorithm must be developed to encode and decode images. This algorithm should be able to integrate seamlessly with the rest of the system and handle large volumes of images. The encoded images will then be stored using the Inter Planetary File System (IPFS), which should be secure, reliable, and able to handle large volumes of images. To mint these encoded images as NFTs for SSO authentication, a smart contract needs to be created on the Ethereum blockchain. This smart contract should be secure and able to handle large volumes of transactions. A backend also needs to be developed that can handle image inputs and outputs and correctly encode and decode the images for authentication purposes. The backend should be designed to handle a large number of image requests and be able to process them efficiently. Finally, a user interface should be created to allow clients to interact with the system. The UI should be user-friendly, easy to navigate, and able to correctly send data to the backend and handle backend responses. Overall, the successful completion of these tasks will result in a secure and efficient system for biometric-based authentication using DCT image steganography and IPFS storage.

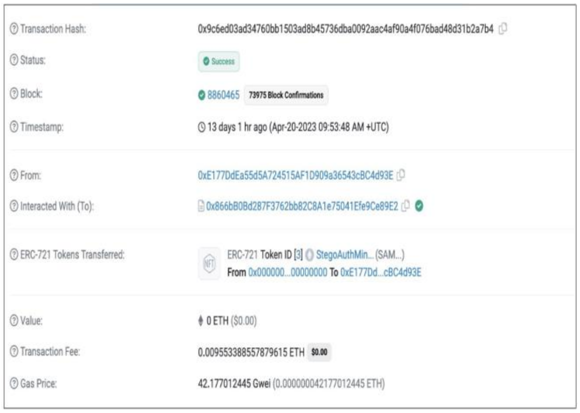
VI. RESULTS

The experiments were conducted and results were acquired for the proposed Blockchain based Image Steganography. To accomplish the high secret image security, imperceptibility, confidentiality and robustness against different steganalysis attacks, the proposed steganographic technique is implemented to evaluate the best visibility for secret image.



Name	Content Identifier (CID)
dct_0xE177DdEa55d5A724515AF1D909a36543cBC4d93E.png 4/19/2023 19.24 MB	Qmd4wwvWamGwXzrYrYfpJz6T6e1vdzMeU7nmhFP7Bhatq

Fig 7:Pinta Image Storage



Transaction Hash:	0x9c6ed03ad34760bb1503ad8b45736dba0092aac4af90a4f076bad48d31b2a7b4
Status:	Success
Block:	8860465 73975 Block Confirmations
Timestamp:	13 days 1 hr ago (Apr-20-2023 09:53:48 AM +UTC)
From:	0xE177DdEa55d5A724515AF1D909a36543cBC4d93E
Interacted With (To):	0x866bB0Bd287F3762bb82C8A1e75041Efe9Ce89E2
ERC-721 Tokens Transferred:	ERC-721 Token ID [3] StegoAuthMin... (SAM...) From 0x000000...00000000 To 0xE177Dd...cBC4d93E
Value:	0 ETH ($0.00)
Transaction Fee:	0.009553388557879615 ETH $0.00
Gas Price:	42.177012445 Gwei (0.000000042177012445 ETH)

Fig 8: NFT minting transaction

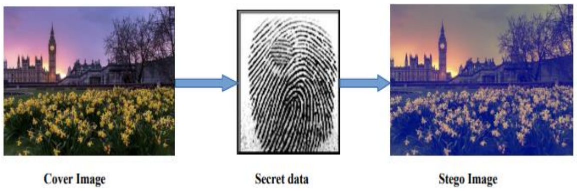


Fig 9: Hiding Secret Data

VII. CONCLUSION AND FUTURE SCOPE

The objective of this project is 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.

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. Here we have used the combination of image steagnography and Etherum Blockchain to securely store the user information in a system. Blockchain is used for transmission of data and steganography is used for communication process, So the blockchain technology can be used in the steganography various methods. Steganography application software provides the purpose how to use image formats to hide any kind of files inside them.

The scope of the project is secure online privacy and secures secret information in carriers such as a video, audio, digital image, 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 goal of this project is provide the better results without any loss of information and provide more secure and tamper-proof way to store user identify information compared to other traditional methods.

REFERENCES

[1]. Mustafa Takaoˇglu, 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).

[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,

[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.

[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