IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, October 2023

Blockchain Based Data Steganography

Tanvi Vikhe, Sejal Deore, Sakshi More, Pooja Vaishanav
Department of AIML (Artificial Intelligence & Machine Learning)
Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India

Abstract: *Blockchain based Data Blockchain based Steganography is the system of hiding records which may be text, photo or video Interior a cowl photo. The secret facts are hidden in a way that it not seen to the human eyes. Deep gaining knowledge of era, which has emerged as a powerful tool in diverse programs along with image Blockchain based Steganography, has obtained increased interest lately. The principal purpose of this paper is to explore and talk numerous deep getting to know strategies available in image Blockchain based Steganography area. Deep gaining knowledge of techniques used for photograph Blockchain based Steganography can be broadly divided into 3 classes - traditional strategies, Convolutional Neural community-primarily based and general adverse community-based methods. Along with the technique, A problematic precis on the datasets used, experimentalu. S.A. Taken into consideration and the assessment metrics Normally used are defined in this paper. A table summarizing all of the info also are provided for clean Reference. This paper targets to assist the fellow researchers by means of compiling the current tendencies, challenges and few destinies course on this field.*

Keywords: Blockchain based Data Blockchain based Steganography, GAN Blockchain based Steganography, CNN Blockchain based Steganography, records hiding, Image statistics hiding

I. INTRODUCTION

Generation has blitz scaled during the last years leading to A wide utilization of multimedia for transferring records, particularly Blockchain Typically, the switch happens over Insecure community channels. Specially, the net has Won multiplied recognition for exchanging digital media and people, personal groups, establishments, governments Use those multimedia facts transfer techniques for exchanging

Statistics. Even though there are various blessings attached with It, one distinguished downside is the privateness and safety of the facts. The provision of several easily available equipment Capable of exploiting the privateness, records integrity and safety of the facts being transmitted has made the opportunity of Malicious threats, eavesdropping and other subversive activities. The distinguished solution is information encryption where the Data is converted right into a cipher text domain the usage of encryption Key. At the receiving end, the cipher textual content is transformed into Undeniable textual content the usage of a decryption key. The usage of facts encryption the unique statistics isn't seen, however, cipher text is visible in

A scrambled shape to human eyes leading to suspicion and in addition scrutiny. A brand-new studies topic, Blockchain based Steganography, has Won popularity in this context to hide the records that is not Perceptible to human eyes. Information hiding strategies have been available for a long term however their importance has been growing recently. The primary reason is the growth inside the facts traffic via the Net and social media networks. Even though the objectives of cryptography and Blockchain based Steganography are similar, there may be a Subtle difference. Cryptography makes the information unbreakable and unreadable but the cipher textual content is seen to human eyes. Blockchain based Steganography, which is used to cover the records in plain Sight, lets in the use of huge form of the name of the game statistics Paperwork like image, textual content, audio, video and documents. Digital watermarking is every other method wherein confidential record is

Embedded to say ownership. Cryptography is the popular Approach used for statistics hiding, however, Blockchain based Steganography is Gaining popularity in recent times. Blockchain based Steganography may be defined because the procedure of hiding a Secret small multimedia information inside some other however lots large

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, October 2023

II. BACKGROUND

Steganography and cryptography are two different methods for protecting the confidentiality and integrity of information. The purpose of steganography is to hide the existence of secret messages in the digital environment in a way that does not reveal them. The main purpose of steganography is to transmit secret messages securely through images. Steganography does not change the structure of the password, but since it is hidden in plain sight, the changes cannot be seen. Cryptography protects information from unauthorized persons by changing its meaning. The use of encryption is based on the confidentiality of the data coding system. When the coding system is known, the system of the field can also be known or followed. Shorthand technology allows messages to be sent over digital media. This communication technology is invisible between the sender and receiver, while cryptography covers the integrity of the message so that no one other than the sender and receiver can send or receive it. Cryptography is a mathematical study of various aspects of information security such as information integrity, authentication, and information security. However, these technologies need to be further explained to help understand the advantages of their combination.

III. SUMMERY

After examining all existing methods, these methods are generally divided into three groups: image Blockchain based Steganography methods, CNN-based image Blockchain based Steganography methods and GAN-based image Blockchain based Steganography methods. Traditional methods are methods that use methods that have nothing to do with machine learning or deep learning algorithms. Many methods are always based on LSB technology. While CNN-based methods rely on deep neural networks to embed and extract secret messages, GAN-based methods use some GAN variants. Figure 1 shows the blockchain-based data Blockchain based Steganography and steganalysis architecture. As shown in Figure 1, the input is a cover image and the secret word can be secret word text or image. The DL model can be CNN-based or GAN-based. The Blockchain based Steganography module generates a blockchain-based Blockchain based Steganography image, while the steganalysis model uses the blockchain-based Blockchain based Steganography image as input to capture and possibly extract secret messages. In some aspects, the quality of the output image is normal or the blockchain-based steganographic image is provided as output. Text, coloured or grey images are often used as confidential information. When determining existing studies in various groups, two factors are taken into account: the nature of the latent environment and the technology used. for secret notes.

IV. LIMITATIONS

Blockchain based Steganography is based on the same logic as encryption. If Alice wants to send Bob an image with a secret message, she must first accept Bob's Blockchain based Steganography. According to the encryption standard, Bob can be sure that he receives some ciphertext. However, in standard Blockchain based Steganography it is difficult for Bob to know when an image is just an image. Consider this scenario: Alice lends Bob a digital camera without telling him to pay extra for every 73 bytes in the image she sends. Since Bob was unaware of Alice's Blockchain based Steganography efforts, the multitude of photos he received from her only diminished Bob's chances of letting Alice borrow his digital camera again. The amount of material that can be stored in the media is generally limited by the size of the media. The less limited the integrity of the medium, the greater the ability to store material. For example, sentences depend on the rules of the English language and specific topics of conversation. It will be difficult for me to hide the hidden words in this passage because there are so many ways to change reality within these boundaries. In contrast, consider the spotlight. It is difficult to retain information. This text is encoded in 8-bit ASCII and is 254 bytes long. The password is 23 bytes; It is about ten times smaller than the load, but it is significant. Random investment poisoning is a rare disease contracted by careless Internet users. This tragic disease causes affected individuals to receive bad writing in the body of the text. Please do not confuse this virus with blatant Blockchain based Steganography. Large uncompressed image of a static TV as shown. Aside from the fact that the value of television is still questionable in the first place, it is not surprising that a large amount of data can be embedded in such images.

V. PURPOSE

First, a new steganography method based on the PSO algorithm is proposed to hide secret messages within host images. This algorithm is used to find the best bit position to hide secret information in the host image. The advantage of this

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, October 2023

method is to reduce the distortion of the steganographic image. The ideal location is where confidential information can be retrieved with minimal disturbance. This method determines the starting pixel, the number of least significant bits (LSB) used for each pixel, and the array of pixels in the scanned image used for bit embedding. This work develops and presents a new spatial domain steganography technique by removing and adding new components of the PSO algorithm and using blockchain technology to hide the medical information of COVID-19 patients. Moreover, the steganography plan is divided into three stages: previously hidden, confidential information, and confidential information regarding the treatment of COVID-19. In general, information hiding methods are evaluated based on transparency, reliability and ability to hide information, mainly based on the stability of their performance against interference and signal processing, interference and speed calculation of the plan in the hidden and extracted data. However, the accuracy of each measurement depends on the application.

VI. CONCLUSION

Blockchain based Data Steganography is a method of sending secret messages by hiding them clearly visible in a cover image. Deep learning is widely used in many fields and has also been applied to steganography studies. Examination of all relevant activities leads to their rough division into three groups. The software and links mentioned in this article are just examples of steganography tools available. Steganography and steganalysis applications are beginning to gain more attention as they adapt to the needs of governments, businesses, and individuals. As privacy issues continue to evolve with digital communications, steganography will inevitably play an increasingly important role in society. Therefore, it is important that we understand digital steganography and its importance. Ethical issues of the use of steganography and steganalysis are equally important. By using steganography, software can easily transmit private information without the user's permission or knowledge. Watermarks have become an issue in digital rights management disputes, and advanced steganalysis tools can affect them. It is easy to write about similar abuses of steganography and steganalysis. Despite the lack of press given to steganography and steganalysis, these fields present interesting problems whose solutions will have profound effects on the Internet and Internet communication. Steganography, as mentioned, enhances rather than replaces encryption. Messages are not secure simply by virtue of being hidden. Likewise, steganography is not about keeping your message from being known it’s about keeping its existence from being known.

V. ACKNOWLEDGMENT

Especially Prof. We would like to express our gratitude to our mentors and experts. P.B. Rajole gave important advice for our work and studies. We also thank AIML Engineering and its staff for their continuous support. We thank Professor N.V. Kapade for his support and understanding.

Thank you doctor. K.V., We thank Chandratre, Dean, Loknete Gopinathji Munde Institute of Engineering Education and Research, Nashik for his support and permission to complete this project. We thank our employees for supporting them, and we thank our parents, friends, and everyone else who supported us throughout this project.

REFERENCES

[1]. Kumar, A., & Pooja, K. (2010). “STEGANOGRAPHY-A DATA HIDING TECHNIQUE.” International Journal of Computer Applications, 9(7), 19-23.

[2]. S. Katzenbeisser and F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston, 2000.

[3]. R. Das and T. Tuithung, ‘‘A novel steganography method for image based on Huffman encoding,’’ in Proc. 3rd Nat. Conf. Emerg. Trends Appl. Comput. Sci., Mar. 2012, pp. 14–18.

[4]. Nagham Hamid et.al, “Image steganography techniques: an overview”, International Journal of Computer Science and Security, vol. 6, no. 3, 2012.

[5]. E. H. Rachmawanto, C. A. Sari et al., "Secure image steganography algorithm based on dct with otp encryption", Journal of Applied Intelligent System, vol. 2, no. 1, pp. 1-11, 2017.

[6]. Dinh C. Nguyen, Ming Ding, Pubudu N. Pathirana and Aruna Seneviratne, Blockchain and AI-based Solutions to Combat Coronavirus (COVID-19)-like Epidemics: A Survey, 2020.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, October 2023

[7]. Suresh, K. S., & Kamalakannan, T. (2023). Digital Image Steganography in the Spatial Domain Using Block-Chain Technology to Provide Double-Layered Protection to Confidential Data Without Transferring the Stego-Object. International Journal of Intelligent Systems and Applications in Engineering, 11(2s), 61-68.

[8]. Horng, J. H., Chang, C. C., Li, G. L., Lee, W. K., & Hwang, S. O. (2021). Blockchain-based reversible data hiding for securing medical images. Journal of Healthcare Engineering, 2021.

[9]. A. Singh and H. Singh, ''An improved LSB based image steganography technique for RGB images,'' in Proc. IEEE Int. Conf. Electr., Comput. Commun. Technol. (ICECCT), Mar. 2015, pp. 1–4.

[10]. Suresh, K. S., & Kamalakannan, T. (2023). Digital Image Steganography in the Spatial Domain Using Block-Chain Technology to Provide Double-Layered Protection to Confidential Data Without Transferring the Stego-Object. International Journal of Intelligent Systems and Applications in Engineering, 1l(2s),