J. Sci. Trans. Environ. Technov. 2023, 17 (2) : 31 - 35

SECURING LEGAL ASSET DOCUMENTS USING BLOCKCHAIN AND CRYPTOGRAPHIC SECURITY FEATURES

YAMINI C and Dr. N. PRIYA

[1] Research Scholar, Research Department of Computer Science, SDNB Vaishnav College for Women, Chrompet, Madras University, India.
[2] Associate Professor, PG Department of Computer Science, SDNB Vaishnav College for Women, Chrompet, Madras University, India.

Article History
Received: **08.10.2023**
Revised and Accepted: **12.11.2023**
Published: **16.12.2023**

https://doi.org/10.56343/STET.116.017.002.005
www.stetjournals.com

ABSTRACT

Securing Information holds a large part of giving out only Genuine Information around and through the Internet. The Information that is passed through the Internet needsto be genuine records of those available. Any record is Genuine only if it passes by or is possessed by the rightful owner. To make sure that the Information is in Safe Hands and has not been mishandled, various Security features can be enabled for them to remain encoded. This includes saving the details of the viewers in some cases. In this paper, we intend to provide the cryptographic security features along with the Blockchain methodology for the secure processing of legal asset documents.

Keywords: Blockchain Cryptography, Encryption, ImageProcessing, Security features.

1. INTRODUCTION

Ever Since all the transactionshave been made Online, the download of legal asset related like Encumbrance Certificate, Patta documents have become common. But, not all documents that are downloaded are said to be genuine. Kapur and Akshay (2013) tells us about the various land dealings being done based on these records. There may be some tampering of documents. Later on, these documents are passed on toothers for further processing which would lead to fraudulent methods of usage of the particular document. In these cases, watermarking of that document and also securing the data and the process through Blockchain technology would mean that the data remains secure and the malpractices done are reduced. They may not be fully eradicated, but the extent to which these are done can be reduced.

The encryption of these documents and some security features in them has been done in some cases. For instance, the E-Stamp Paper has some security features like Bar Code, Unique Certificate Number and the Indian Emblem.

Similar Security features can be found in the Currency banknotes of various Countries. The Security featuresvary from different kind of ink to Fonts that differ through different kinds of lighting. Mishra and Suhag (2017) and Oleg and Yaroslav, (2020) suggested the use of Image watermarking and Blockchain features combined together for further security purposes where they intend to do that for medical images alone. When it comes to land documents, a secure approach is needed to safeguard them.

P-ISSN 0973-9157
E-ISSN 2393-9249

YAMINI C
Research Scholar, Research Department of Computer Science, SDNB Vaishnav College for Women, Chrompet, Madras University, India.

2. CHALLENGES

- The documents that are downloaded may or may not be genuine.
- When these documents are later used for transactions it would lead to fraudulent practices and transactions.
- For instance, In recent times, Patta documents have been duplicated without the knowledge of the owner.
- These were then used to do fraudulent saleof the specific portion of land and so on.
- Some of the documents may be passed- down through generations but the origin ofthe land or the document tends to remain unknown.
- These may cause confusion among general public whereas the origin of possession remains a secret.

3. EXISTING METHODOLOGY

Currently, we have certain featuresthat are used as Security credentials in any document. When it comes to legal document, not much have been done. There is a need for more security to be provided to these documents since they are confidential.Arpita *et al.*, (2019), Megias *et al.*, (2021) and Brabin *et al.*, (2022) gives us an idea of how to proceed with further image security concerns and features and also about the ones where medical images are termed sensitive so the data shown outside is also limited very much. For example, we can take the Government documents or Certificates available for download from online sources. Fraudulent preparations ofdocuments are being reported in a large amount and these can be tackled if we have the Security features intact for them. Here, in existing cases, if we take patta documents, We go to the website, login there and directly download the documents. This would mean that any person having a login can do it. This could be dangerous at times. As said earlier, it could be misused. These are some of the sample cases available. Many scholars have worked on the related topics like Cryptography and Image scrambling earlier. Related to Cryptography, Mona *et.al.*, (2014) uses Image encryption techniques and channel coding. Chaotic maps are used here that are based on Cryptography. They give us a wide range of Security and would help in real-time data more.

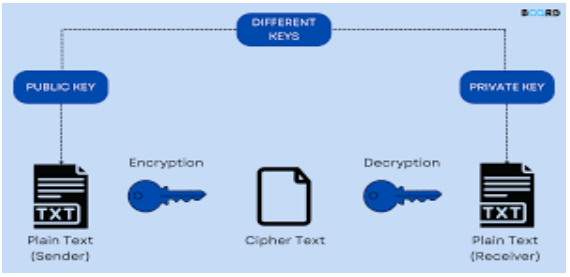

Figure 3.1 Cryptography – Process and Result.

Figure 3.1 shows us the general concept of Cryptography. It branches out to various other methods of cryptography as well later on. The image depicts how Plain text by sender is encrypted using a Public key to make it Cipher text. The Decryption is done using the same key thatis made Private such that only the receiver knows about that. Once the decryption is done, the original text is received back by the Receiver. In the mean while all the other ways used to decode the encrypted text would result in error only.

Prarthana and Pawar (2015), in their research paper regarding Image Scrambling titled "A Comprehensive Survey on Image Scrambling Techniques" suggested that image scrambling can be used in real-time for the safeguarding of data and gives us example of Sudoku puzzle and Rubik's cube.

Here, the image matrix is got and scrambled which would result in a matrix that is very different from the original image. Then when we unscramble this image, we can get the original image (Fig.3.2.)

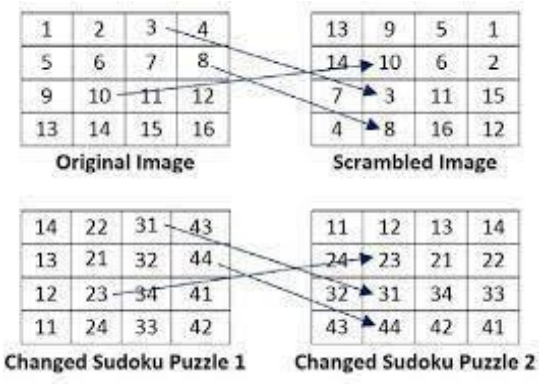

Figure 3.2 Image Scrambling used by SudokuPuzzle

Here, Block scrambling method is used. The image blocks are scrambled such that it cannot

be recognized which means that only when it is got back in its original form or unscrambled, can any person identify the original data. For Steganography, Alan et al., (2013), Modak and Pawar (2015) and Nizami *et al*., (2022) use an approach where for encryption Caesar cipher and Vignere cipher are used to get the encrypted data.

They are then combined with the hash function for Steganography purposes.

This would lead to increase in speed and security when compared to the other methods of LSB Image Steganography algorithms.

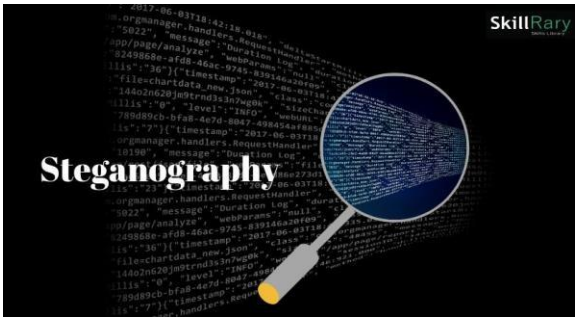

Figure 3.3 Steganography for data in images

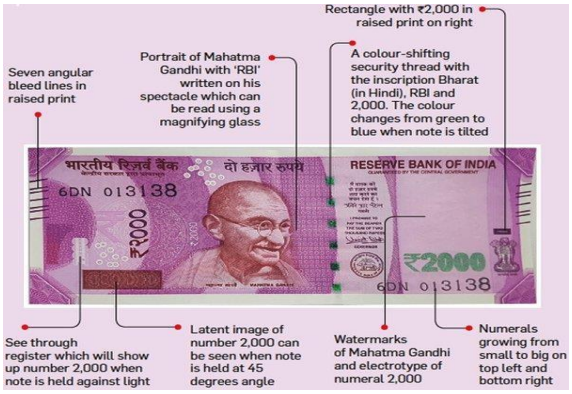

Figure 3.4 Example for Steganography

Here, in images 3.3 and 3.4, they depict Steganography. The figure 3.3 gives us what Steganography actually is – Hiding data inside another data that can be image or plain text. In figure 3.4, we have the Indian currency that also uses Steganography for security purposes and to stop malpractices. give us a general example of how data can be embedded into an image for Security features. It shows Indian Currency and its Security features. The Indian currency has various security features such as:

1] Colour Shifting ink when it is exposed to light.
2] Micro print of the currency value.
3] RBI written on the Spectacles of Mahatma Gandhi which is not visible to naked eyes.
4] Some other typographic unique features that cannot be duplicated much easily.

4. PROPOSED METHODOLOGY

In this new methodology, we intend to combine both the Blockchain and the Security features watermarking technologies to give more security to the images. This would mean that the watermarking data is encoded using theHashing technique and further saved in theBlockchain So that once the data is secured, further misuse can be detected and stopped. The concept similar to this one was explained earlier in (Franco 2020), Katarzyna and Ogiela (2021), Mannepalli et al., (2021), and Na Ren (2021). All the said articles specify the use of Blockchain and Image watermarking to ensure security of the images and also to present the details of the images to genuine viewers. The techniques used till now would not allow digital images all the time. The documents or particulars downloaded through the web still remain unsafe only. They may be misused in any form. Once, the security features are encrypted or encoded in the image, this can be reduced. Further protection to these encoded imagesis provided through the process of saving the decryption data or the Security featuresin the Watermarking of the image.

- The documents or particulars downloaded through the web still remain unsafe only. They may be misused in any form.
- Once, the security features are encrypted or encoded in the image, this can be reduced.
- Further protection to these encoded images is provided through the process of saving the

ownership details of the document so that to ensure correct possession of the data.

5. EXTENT TO WHICH WORK CAN PROGRESS

Even though this method would meansecuring the document, it also has its limitations. Since the data is being stored through blockchains after encoding them, it would mean the time taken to process would increase. Also that the amount of data stored would increase in some cases. For example, if we use this method for saving the details of all the owners of a particular document would need to be mentioned there. This would mean that the large amount of data stored may or may not be useful in all cases. In the cases of documents that aremeant to be shared between people or passed on to future owners like the documents related to ownership of any asset would mean that the old owners are also permitted to use the document and also the new owners are allowed to view and access the document. If we create the watermarking and the encryption with the details of the owners encoded in them, practical difficultiesarise in these places since a large number of owners can be allowed for the asset. In these cases, the suggested method would mean a large amount of data that can be termed as Unnecessary as well time taken can be more when compared to normally.

6. CONCLUSION

This type of watermarking and Blockchain techniques can be used for Medical images and also for other Government documents that are meant tobe circulated online. In case of medical images, the analysis for any disease can be saved in the Blockchain and it is meant only for the purpose of viewing by the specified medical professionals. For the government documents, as specified above, the ownership information of the particular document canbe saved alongside.

REFERENCES

Alan, Anwer Abdulla, Sabah A. Jassim, and Harin Sellahewa. 2013. Efficient high- capacity steganography technique. *In:*Proc. SPIE 8755, Mobile Multimedia/Image Processing, Security, and Applications 2013, 875508 (28 May 2013); https://doi.org/10.1117/ 12.2018994

Arpita Banik, Zeba Shamsi and Dolendro Singh Laiphrakpam. 2019. An encryption scheme for securing multiple medical images. *Journal of Information Security and Applications,* 49. 2019. https://doi.org/10.1016/j.jisa.2019.102398

Brabin, D., Ananth, C. and Bojjagani, S. 2022. Blockchain based security framework for sharing digital images using reversible data hiding and encryption. *Multimed Tools Appl* 81 :24721-24738 . https://doi.org/10.1007/s11042-022-12617-5

Franco Frattolillo, 2020.A Watermarking Protocol Based on Blockchain. *Appl. Sci.* 10, 7746. https://doi.org/10.3390/app10217746

Kapur, Jyotika and Baregar, Akshay. 2013. Security Using Image Processing. *International Journal of Managing Information Technology.* 5. 13-21. 10.5121/ijmit.2013.5202. https://doi.org/10.5121/ijmit.2013.5202

Katarzyna, Koptyra and Marek R. Ogiela, 2021.Imagechain-Application of Blockchain Technology for Images. *Sensors* 2021, 21, 82. https://doi.org/10.3390/s21010082 PMid:33375606 PMCid:PMC7796195

Li, Ming , Zeng, Leilei , Zhao, Le , Yang, Renlin , An, Dezhi and Fan, Haiju. 2021. Blockchain-Watermarking for Compressive Sensed Images. *IEEE Access.* PP. 1-1. 10.1109/ACCESS.2021.3072196. https://doi.org/10.1109/ACCESS.2021.3072196

Mannepalli, Praveen, Richhariya, Vineet , Gupta, Susheel , Shukla, Piyush and Dutta, Pushan. 2021. Block Chain Based Robust Image Watermarking Using Edge Detection And Wavelet Transform. https://doi.org/10.21203/ rs.3.rs-766105/v1.

Megías D, Mazurczyk W, and Kuribayashi M. 2021. Data Hiding and Its Applications: Digital Watermarking and Steganography. *Applied Sciences.* 11(22):10928. https://doi.org/10.3390/app112210928

Mishra, Prachee and Roopal, Suhag . 2017. LAND RECORDS AND TITLES IN INDIA. State-Finances: A Study of Budgets, RBI; PRS, September 2017

Mursi, Mona ,Ahmed, Hossam , Abd El-Samie, Fathi and Abd-elaziem, Ayman. 2014. Image Security With Different Techniques Of Cryptography And Coding: A Survey. *IOSR Journal of Computer Engineering*. 16. 39-45. 10.9790/0661-16313945.

Na Ren, Yazhou Zhao, Changqing Zhu, Qifei Zhou, Dingjie Xu. 2021. Copyright Protection Based on Zero Watermarking and Blockchain for Vector Maps. *Int. J. Geo-Inf.* 10, 294. https://doi.org/10.3390/ijgi10050294

Nezami ZI, Ali H, Asif M, Aljuaid H, Hamid I, Ali Z. 2022. An efficient and secure technique for image steganography using a hash function. *Peer.J Computer Science* 8:e1157 https://doi.org/10.7717/peerj-cs.1157 PMid:36532801 PMCid:PMC9748815

Oleg Evsutin and Yaroslav Meshcheryakov, 2020. The Use of the Blockchain Technology and Digital Watermarking to Provide Data Authenticity on a Mining Enterprise. *Sensors* 20 :3443; doi:10.3390/s20123443. https://doi.org/10.3390/s20123443 PMid:32570837 PMCid:PMC7349180

Prarthana, Madan Modak and Vijaykumar Pawar. 2015 A Comprehensive Survey on Image Scrambling Techniques. *International Journal of Science and Research* (IJSR, 4(120): 813-818.