RESEARCH
www.commprac.com
ISSN 1462 2815

# EXPLORING DOCUMENT SECURITY: TECHNIQUES, METRICS AND CHALLENGES

**Yamini C [1] and N. Priya [2]**

[1] Research Department of Computer Science, SDNB Vaishnav College for Women, Chrompet, Madras University, India. Email: chivkulayamini@gmail.com
[2] PG Department of Computer Science, SDNB Vaishnav College for Women, Chrompet, Madras University, India. Email: drnpriya2015@gmail.com

**DOI: 10.5281/zenodo.12896696**

**Abstract**

In today's world, Security for any means has become really important. That stands for either hard copy or the soft copy of any document. The concept of online transactions or simply digital transactions has become a rage over a period. To accommodate such stuffs, there arises a need of transforming hard copies of document into soft copy ones. This would further lead to the crisis where there is a need to provide security for these soft copies. The documents when maintained as soft copies are vulnerable to all sorts of attacks either through bugs and/or through human errors. These human errors are the ones that need to be taken care of in a large scale. Some people believe in sharing documents through online with their peers or others of same interest. This may lead to the misuse of these documents when they fall into wrong hands. Then, the security of these documents becomes a topic to dwell on. In this paper, a study was conducted based on the ways to secure data and the techniques or algorithms that can be used to do it. There are many different technologies based on the type of data that is being encrypted. These are being discussed along with the papers that were taken into account for various data Security methods.

**Keywords:** Document Security, Cryptography, Image Encryption, Data Hiding, Bit-Plane.

## 1. INTRODUCTION

Data present in documents can be of many types like Confidential or just simple usable data. They may be critical data like in transactional data or payment data and so on. These data sources or resources need to be safeguarded. To safeguard them, various methods have been used throughout the years. The methods may vary based on the type of data. This article focuses on those various methods that were used throughout the years and were described in articles.

Duplication of data is possible up to some extent which includes copying of data as such for performing illegal transactions and some are meant to deceive another person. There are many other reasons too for which duplication or illegal use of documents is being done. The following is a study of some techniques used for safeguarding the documents from being misused.

Safeguarding of documents can be done using various technologies and the technologies differ based on various types of documents. The purpose of the document decides the use of the technologies or their algorithms.

The objective of this Paper would be to find the most suitable method: -

- To provide security to legal asset documents
- To add details of ownership of the document along with it.
- To show the history of a document and the various owners for that.
- To make tracking of transactions using a legal document easier.

Some of the basic challenges faced through the process are:

- 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 sale of the specific portion of land and so on.
- Some of the documents may be passed-down through generations but the origin of the land or the document tends to remain unknown.
- These may cause confusion among general public whereas the origin of possession remains a secret.

## 2. TECHNIQUES

Data would be of various types some of which are audio and video. These need to be secured if they are sensitive or Critical.

**Existing methodology:**

- Currently, we have certain features that 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.
- For example, we can take the Government documents or Certificates available for download from online sources.
- Fraudulent preparations of documents 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.

There are various methods with which the data can be secured. Some of them use Data hiding as a technique while some encrypt the data using keys and secure them. The technologies are of a wide range. Many related papers were referred and some are discussed below.

### 2.1 Image Scrambling

Image Scrambling is a part of data security. It comes under the concept of data hiding. This means that the Images when scrambled, means when re-arranged, would remain safe and a secret from malicious sources. When the data is embedded into such

images through other methods, the data is kept safe and can be taken only by valid people.

Nowadays, this becomes a part of cryptography, even though it is not definitely encryption through an algorithm.

[6] 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 this image is unscrambled, the original image is returned back.

[29] Concludes that Image scrambling can be done two-way using Arnold transform algorithm. Arnold transform can be confusing at times due to its complexity.

The Arnold transform algorithm processes under the concept where the n numbers of iterations are performed and n is used as the key. The image is encrypted by shuffling the planes simultaneously. This is done for numerous times.

The Sudoku pairs are used to scramble blocks here and are then used as a part of Image Scrambling.

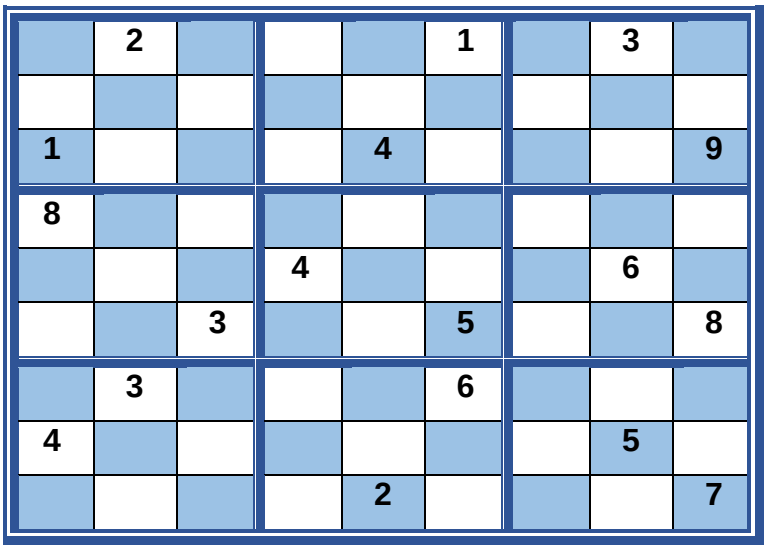


**Fig 2.1: This shows a sample SUDOKU image**

## 2.2 Bitplane

This is a set of bits arranged corresponding to a given bit position (MSB or LSB types) in a binary number representing signals. A Bitplane is meant to be regarding a discrete digital signal. For instance, audio or video forms may be taken.

The Most Significant Bit can be the most effective one with higher or critical approximation values of the plane and LSB- Least Significant Bit would give us the lower values. Image Scrambling is also used here. This would mean that the Planes of an image are changed and then those bits are used as a key for the encryption of the original image.

[1] Suggested a new bit plane decomposition algorithm using Image Scrambling where result is received. This would mean that any image similar to the source image is taken and bit plane methodology is used for decomposition of that image. It is then used as

the key for the encryption. The Plane that can be used as key can be decided by the user itself.

[5] Concluded that Arnold scrambling, a technique that uses Arnold transform algorithm and Bit Scrambling, which is performed as Bit Plane Decomposition can be used for the encryption and decryption process.

Compared to the later one, the earlier is said to be simpler and easier to workout. Since Arnold Scrambling becomes somewhat confusing. Image Scrambling generally is a topic that is more common and known than Arnold Scrambling.

Here, the bit plane with number of Most Significant bits would contribute more when compared to the Least Significant ones. This is because; the Most Significant ones are of larger intensity. The sample images given along with their plane mentioned from Image 2.2 to Image 2.9 show us the different highlighted portions according to the scrambling methods.

**Fig 2.2: Plane 0**

**Fig 2.3: Plane 1**

**Fig 2.4: Plane 2**

**Fig 2.5: Plane 3**

**Fig 2.6: Plane 4**

**Fig 2.7: Plane 5**

**Fig 2.8: Plane 6**

**Fig 2.9: Plane 7**

### 2.3 Steganography

Steganography is the technique of concealing a message inside another or even more in new format itself.

Here, one can conceal a new message within another one where the message that is visible may be unimportant or the concealed message may be offensive or critical. These concealing may be done in both audio and video files. Most recent examples of these uses are Micro-Ink which would be very small like 1cm in diameter.

[7] Uses an approach where for encryption Caesar cipher and Vigenère 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.

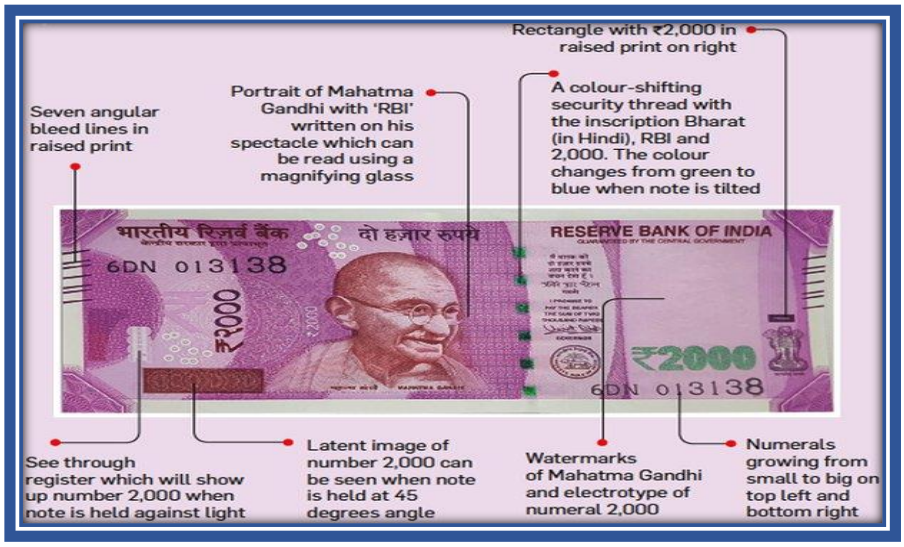


**Fig 2.10: Image of Indian Currency –Rupee with its various security features**

The image 2.10 would 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) Color 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.
5) Numbers written in Braille script.
6) Raised up print that is shown at a certain angle.
7) Watermark of Mahatma Gandhiji and electrolyte numerical of the currency written

Out of these features, almost 4 or 5 of the features are part of Steganography. It has its basics here and hence any data can be embedded into an image. Image steganography can be done with data being embedded into the image and still the clarity can remain the same. Here, in figure 2.11. The original image is given. The text

file is given in 2.12. Once the image steganography is performed, the result is displayed in 2.13. This shows that the original image and the resultant output image is the same and with the same clarity. This would help more in concealing the data in the image but the intruder not being able to recognize the encoded image.

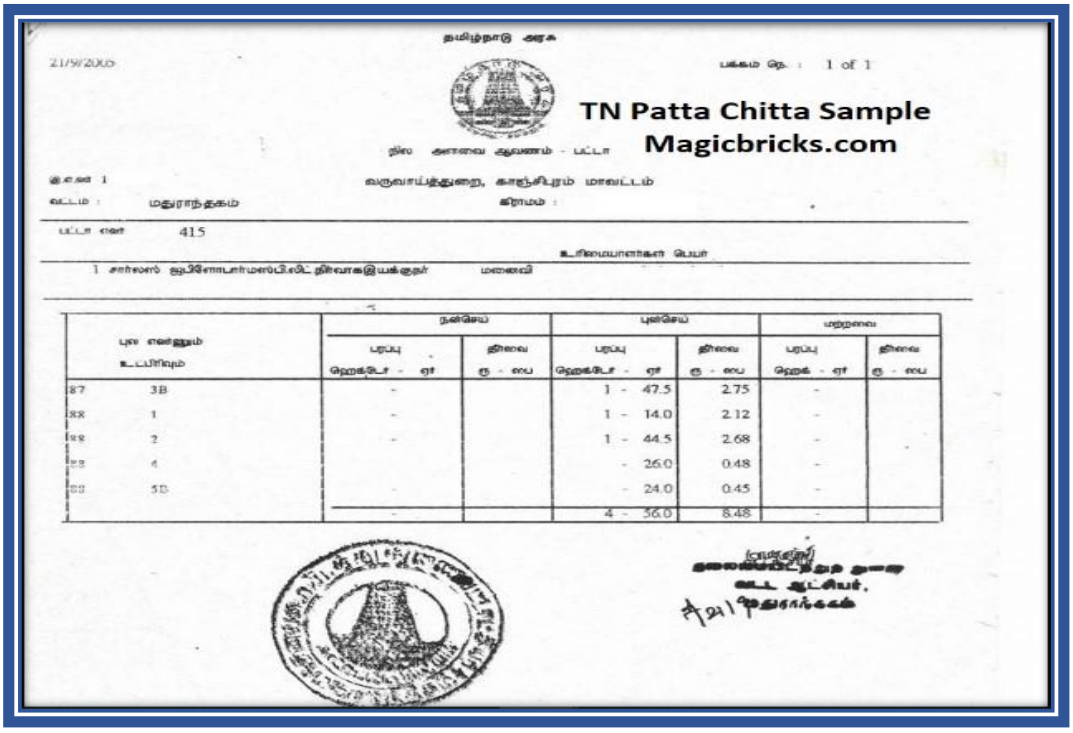


**Fig 2.11: The original image taken for embedding data**

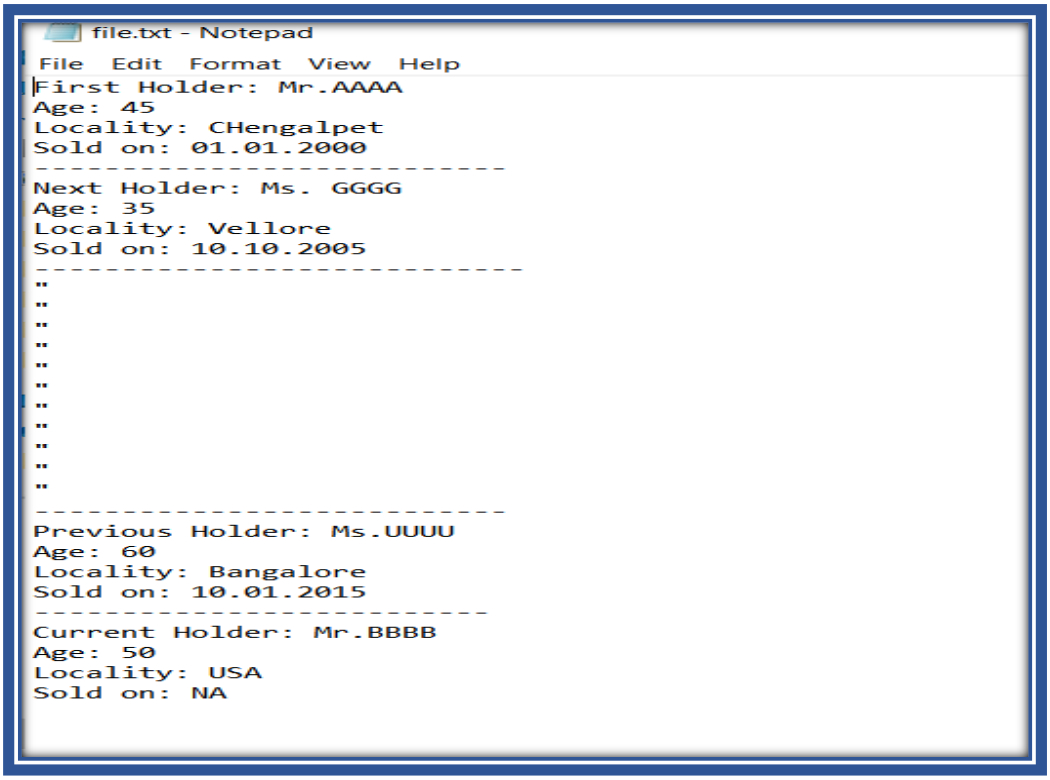


**Fig 2.12: The file with the text data**

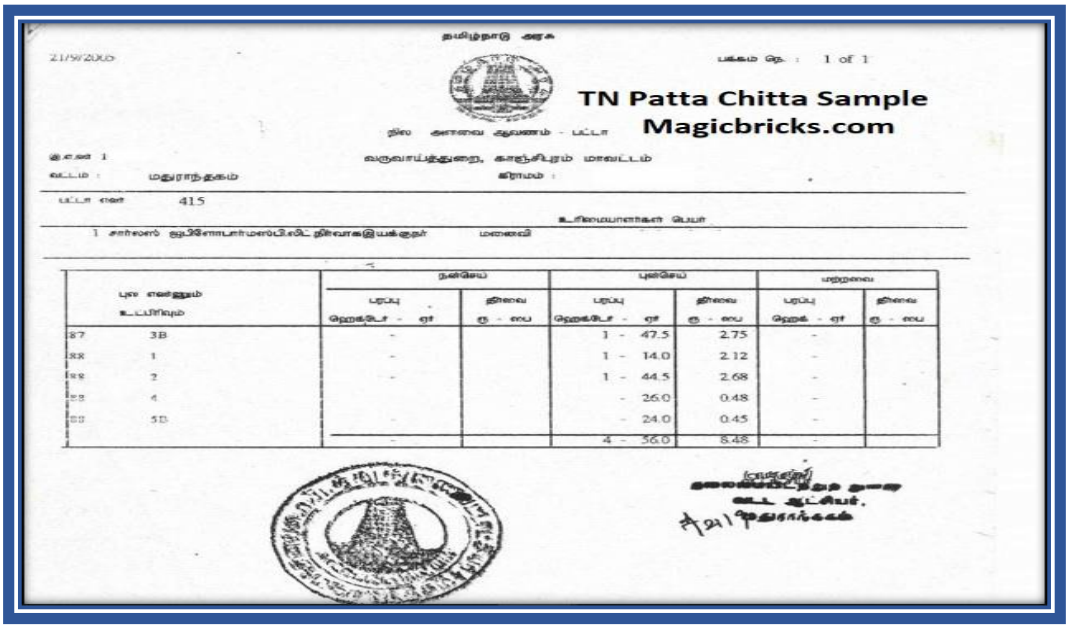


**Fig 2.13: The resultant image with the text embedded into it**

## 2.4 Cryptography

It means sending a message through a secured channel by encrypting them using a code and which is later on decrypted by using another code. The code used is called as a key. In Cryptography, there are various algorithms that are commonly used. Some are the AES, DES, RSA and so on. In each and every algorithm, the process of encrypting and the number of rounds of encryption varies. As well as the way the encryption is done. For example, in AES, there 13 rounds of process which would result in encrypting the whole data. For decryption, the same method is used, but with the reversing of the processes done. [8] 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.

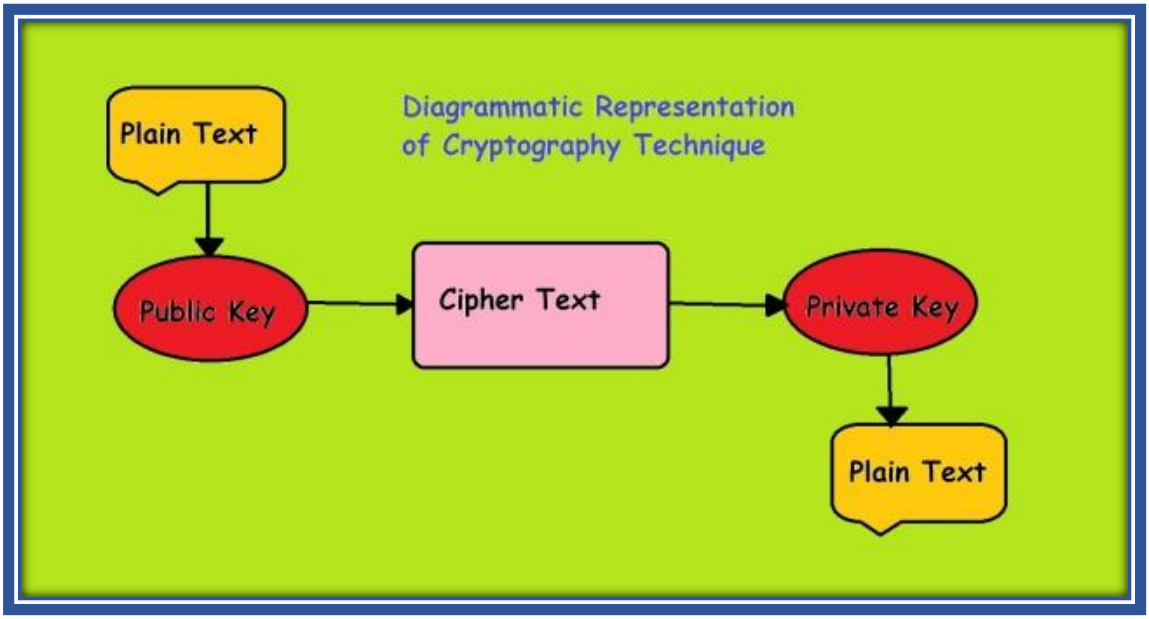


**Fig 2.14: Cryptography concept**

The image 2.14 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 that is 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.

### 2.5 Blockchain

Blockchain is defined as a mathematical structure that can store data corresponding to a particular detail or the component specified.

From [10], [11], [12] and [13], which are based on the concept of Blockchain and its various methods of implementation; it can be concluded that, Blockchain is becoming a trending technology while using medical images nowadays. Physicians would like to see the various stages of improvement or the disease of a patient along with the comments or descriptions given for them respectively. [14] And [15] also add to that, Blockchain would mean that the data is safe and can be viewed only by the necessary person only.

[2] Tells us about how to encrypt an image securely using Blockchain. Here, the images are scrambled and random permutation is used and blocks are obtained.

These blocks are later mapped with cipher blocks. The Blockchain is obtained using the SHA-512 hash. That is later embedded in covering audio signal for enhanced protection. Here, the image is taken first and encrypted and then the Block permutation is performed on that for shuffling them. Later the data is embedded that needs to be sent along with the image.

Once the receiver gets the specified data, they need to decrypt them first to get the data and the image separately after which the data is kept secret as it is and after reversing the process of encryption, the original image is returned as supposed. The figure 2.15 gives us the overall process of Blockchain technology used for image and data security.

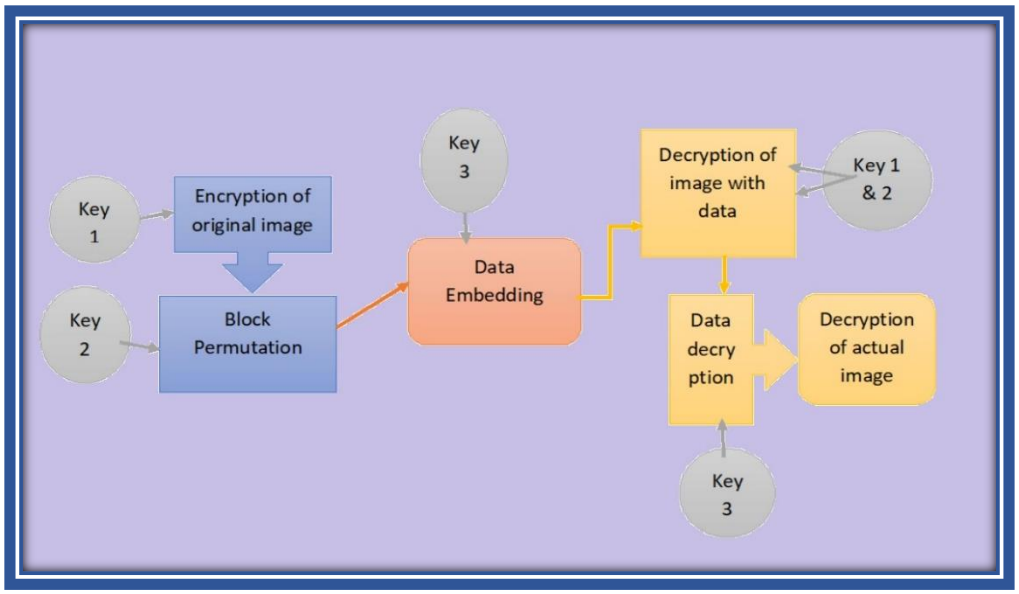


**Fig 2.15: Diagram depicting the process of Blockchain**

## 3. COMPARISON OF THE TECHNIQUES:

In this paper, over all the methods that have been discussed, Blockchain would mean more efficient and Successful encryption technology.

Even though Steganography holds half importance in Image encryption trend nowadays, but Blockchain gives us more place for research and also for improvisation.

Of all the technologies given above, the most trending ones would be Image scrambling and Blockchain. Image scrambling can be confusing sometimes due to its excessive calculative approach, whereas Blockchain would mean a simpler way to encrypt image as well as save some other data over that.

Here, let us take the comparison between these technologies so as to get the superior one. When these technologies are considered individually, different score of efficiency is received and when they are compared along with others like for example, Bitplane along with Image Scrambling is popular and so on. The efficiency score is different.

## 4. METRICS CONSIDERED

### 4.1 Accuracy:

When it comes to accuracy, Cryptography can be considered as well as Blockchain technology. Because, these are the latest and most used ones.

When considering both of them together, the accuracy tends to be higher than when they are taken separately. The rest of the technologies also give us the result but the accuracy rate tends to lessen down in them.

### 4.2 Efficiency

The efficiency would depict as to which level can the result be accepted and dependency of the technologies.

As seen in table 4.1, the efficiency of Blockchain is higher when the other technologies such as Steganography and Scrambling are involved. Cryptography gives us much higher one compared to Steganography.

This is because the latter one was used from olden times and cryptography gives the latest version.

### 4.3 Reliability

The reliability would tell us how much the results are dependable. When compared using various algorithms of the above-mentioned technologies, Cryptography has a wide range of algorithms and performs well and has more recent updates. This holds good for Blockchain also.

### 4.4 Security

This is one of the most important metrics that needs to be checked. Security is provided through all the technologies since they are basically used for encryption purposes only. But the level differs. Blockchain would provide security for the data and cryptography uses algorithms for that. Some of these algorithms are complex which would make it difficult for them to be processed at the earlier stages.

**Table 4.1: Table depicting the metrics and the comparisons of the Technologies considered**

| Techniques | Authors Referred | Algorithms Used | Pros | Cons | Efficiency (Comparatively) |
|---|---|---|---|---|---|
| **Image Scrambling** | [6], | Rubic's Cubic algorithm, Arnold Transformation | Simple and easy to work | Uses basic methods so need of more efficiency is there | Has some negative effects and termed as not much efficient |
| | [29] | Arnold Scrambling , Arnold transform | | | |
| **Bit Plane** | [1] | Bit-level scrambling algorithm | Similar to Image Scrambling | Even after doing this, confusion exists in the model | Efficient when considered with Image Scrambling |
| | [5] | Bit plane slicing and image rotation, Arnold Scrambling. | | | |
| **Cryptography** | [8], | Image encryption and channel coding techniques. | Familiar approach but various techniques | Encryption can be done using various methods where some are not satisfactory | More than Steganography |
| | [18], | Permutation – Diffusion architecture | | | |
| | [21], | ElGamal Cryptosystem | | | |
| | [28] | Novel Non-linear Chaotic algorithm | | | |
| **Steganography** | [3], | Short-Time Fourier Transform, Piece-Wise Linear Chaotic Map | Easier to understand and does the necessary correctly | Old style method of encryption | Not much when compared with cryptography |
| | [7], | Encryption based on hash function | | | |
| | [17], | AES Algorithm and Image steganography | | | |
| | [25], | Image watermarking and its advancements | | | |
| | [27] | Fibonacci like bit-plane mapping | | | |
| **Blockchain** | [2], | Blockchain combined with steganography | Can extend to save more details | Requires additional storage space | Efficient when taken alongside other technologies |
| | [10], | A Novel watermarking technique with the blockchain technology. | | | |
| | [11], | Edge detection using discrete wavelet transform | | | |
| | [12], | Watermarking, Blockchain and file system techniques combined. | | | |
| | [13], | Zero watermarking along with Blockchain | | | |
| | [14], | Watermarking along with Ethereum blockchain. | | | |
| | [15], | Blockchain and digital watermarking | | | |
| | [22], | Hash function, QR Code, Inter-Planetary File System | | | |
| | [23] | Reversible data hiding and encryption | | | |

**Table 5.1: Comparison of the Techniques and the Metrics**

| | Image Scrambling | Bit Plane | Steganography | Cryptography | Blockchain |
|---|---|---|---|---|---|
| **Accuracy** | Higher compared to other techniques | Not much since this is used along with Image scrambling | Higher compared to other techniques | Higher compared to other techniques | Higher compared to other techniques |
| **Efficiency** | More efficient in terms of small images | Doesn't matter since always used with Image scrambling | More efficient and used since a very long time | More efficient compared to other techniques since protection is higher | Efficient in terms of medical images as mostly used there |
| **Reliability** | Reliable but not as much as the latest technologies | Not much when compared to other techniques | Reliable because of Security features embedded | Reliable since it uses password for protection | Reliable when information is not much confidential |
| **Security** | Secures the image | Not much since this is used along with Image scrambling | Higher for the embedded data | Higher for the embedded data but then image is also password protected | Higher for the embedded data than the image |

## 5. CONCLUSION

This Study was conducted in regards with the various methods of Encryption and Decryption and the methods through which data can be made more secure.

The main purpose of this study is to learn on the various techniques used for image encryption and storage of data and also to compare and get the most relevant and easier one in the process. The comparison is given in table 5.1 and that gives us the related conclusion.

Through this study and references in [4], [19] and [24] tells that, Data can be encrypted, scrambled, rearranged, hidden and also encoded to keep it safe from assailants. Also, Blockchain method also yields us another advantage wherein one can get or save other details regarding the data along with encrypting it and keeping it safe.

### References

1) Yicong Zhou, Weijia Cao, C.L. Philip Chen, "Image encryption using binary bitplane", ELSEIVER, Signal Processing, Volume: 100, (2014), Pages: 197-207, https://doi.org/10.1016/j.sigpro.2014.01.020

2) P.L. Chithra and R. Aparna, "Blockchain-based image encryption with spiral mapping and hashing techniques in dual level security scheme", International Journal of Information and Computer Security Vol. 21, No. 1-2, https://doi.org/10.1504/IJICS.2023.131100

3) Marwa A. Nasr, Walid El-Shafai, Nariman Abdel-Salam, El-Sayed M. El-Rabaie, Adel S. El-Fishawy and Fathi E. Abd El-Samie, "Efficient information hiding in medical optical images based on piecewise linear chaotic maps", Journal of Optics, Volume – 52, (2023), http://dx.doi.org/10.1007/s12596-023-01128-7

4) Manju Kumari, Shailender Gupta and Pranshul Sardana, "A Survey of Image Encryption Algorithms", 3D Research 8, 37 (2017), http://dx.doi.org/10.1007/s13319-017-0148-5

5) R. Aarthi, Mrs. S.Kavitha, “Image Encryption Using Binary Bit Plane and Rotation Method for An Image Security”, International Journal of Engineering Development and Research, Volume 5, Issue 2, (2017).

6) Prarthana Madan Modak, Dr. Vijaykumar Pawar, “A Comprehensive Survey on Image Scrambling Techniques”, International Journal of Science and Research (IJSR), Volume:4, (2015), Pages: 813-818, ISSN (Online): 2319-7064.

7) Zahid Iqbal Nezami, Hamid Ali, Muhammad Asif, Hanan Aljuaid, Isma Hamid, Zulfiqar Ali, “An efficient and secure technique for image steganography using a hash function”, PeerJ Computer Science, (2022), https://doi.org/10.7717/peerj-cs.1157

8) Mona F. M. Mursi, Hossam Eldin H. Ahmed, Fathi E. Abd El-samie, Ayman H. Abd El-aziem, “Image Security with Different Techniques of Cryptography and Coding: A Survey”, IOSR Journal of Computer Engineering, Volume: 16, Pages :39-45, (2014), http://dx.doi.org/10.9790/0661-16313945

9) Katarzyna Koptyra and Marek R. Ogiela, “Imagechain—Application of Blockchain Technology for Images”, Sensors (2021), Volume: 21(1), 82, https://doi.org/10.3390/s21010082

10) Franco Frattolillo, “A Watermarking Protocol Based on Blockchain”, Applied Sciences, (2020), Volume: 10(21), 7746, http://dx.doi.org/10.3390/app10217746

11) Praveen Kumar Mannepalli, Vineet Richhariya, Susheel Kumar Gupta, Piyush Kumar Shukla, Pushan Kumar Dutta, “Block Chain Based Robust Image Watermarking Using Edge Detection and Wavelet transform”, IEEE Access, Volume 9, (2021), http://dx.doi.org/10.21203/rs.3.rs-766105/v1

12) Ming Li, Leilei Zeng, Le Zhao, Renlin Yang, Dezhi An, Haiju Fan,” Blockchain-Watermarking for Compressive Sensed Images”, IEEE Access, Volume 9, (2021), http://dx.doi.org/10.1109/ACCESS.2021.3072196

13) Na Ren, Yazhou Zhao, Changqing Zhu, Qifei Zhou, Dingjie Xu, “Copyright Protection Based on Zero Watermarking and Blockchain for Vector Maps”, International Journal of Geo-Information, (2021), Volume: 10, 294, https://doi.org/10.3390/ijgi10050294

14) Alsehli Abrar, Wadood Abdul, Sanaa Ghouzali,” Secure Image Authentication Using Watermarking and Blockchain”, Intelligent Automation & Soft Computing, Volume: 28(2), Pages: 577-591, (2021), http://dx.doi.org/10.32604/iasc.2021.016382

15) Oleg Evsutin, Yaroslav Meshcheryakov, “The Use of the Blockchain Technology and Digital Watermarking to Provide Data Authenticity on a Mining Enterprise”, Sensors (2020), Volume: 20, 3443, http://dx.doi.org/10.3390/s20123443

16) Prachee Mishra, Roopal Suhag, State-Finances: A Study of Budgets, RBI; PRS, “Land Records and Titles in India”, https://prsindia.org.

17) Jyotika Kapur, Akshay. J. Baregar, “Security using image processing”, International Journal of Managing Information Technology, Volume: 5, No.2, Pages: 13-21, (2013), http://dx.doi.org/10.5121/ijmit.2013.5202

18) Yong Wang, Kwok-Wo Wong, Xiaofeng Liao, Guanrong Chen, “A new chaos-based fast image encryption algorithm”, ScienceDirect, Applied Soft Computing, Volume: 11(1), Pages: 514-522, (2009), http://dx.doi.org/10.1016/j.asoc.2009.12.011

19) Shi Liu, Changliang Guo, John T. Sheridan, “A review of optical image encryption techniques”, Science Direct, Optics & Laser Technology, Volume: 57, Pages: 327-342, (2013), http://dx.doi.org/10.1016/j.optlastec.2013.05.023

20) Prof. P. B. Khatkale, Prof. K. P. Jadhav, Prof. M. V. Khasne, “Data Hiding in Document Images Using Digital Watermarking”, International Journal of Engineering Research and Technology (IJERT), Volume: 1 Issue 6, (2012), https://doi.org/ 10.17577/ijertv1is6340

21) Arpita Banik, Zeba Shamsi, Dolendro Singh Laiphrakpam, “An encryption scheme for securing multiple medical images”, ScienceDirect, Journal of Information Security and Applications, Volume: 49, (2022), http://dx.doi.org/10.1016/j.jisa.2019.102398

22) Z. Meng, T. Morizumi, S. Miyata and H. Kinoshita, "Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain," IEEE (COMPSAC), Volume: 2, (2018), http://dx.doi.org/10.1109/COMPSAC.2018.10258

23) Brabin, D., Ananth, C. and Bojjagani, S., “Blockchain based security framework for sharing digital images using reversible data hiding and encryption”, Multimedia Tools and Applications, Volume: 81, Pages: 24721–24738, (2022), http://dx.doi.org/10.1007/s11042-022-12617-5

24) Kaur, M., Kumar, V. “A Comprehensive Review on Image Encryption Techniques”, Archives of Computational Methods in Engineering, Volume: 27, Pages: 15–43, (2020), https://doi.org/10.1007/s11831-018-9298-8

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

26) Zhi-Hong Guan, Fangjun Huang, Wenjie Guan, “Chaos-based image encryption algorithm”, Physics Letters A, Volume: 346, Issues 1–3, (2005), Pages: 153-157, https://doi.org/10.1016/j.physleta.2005.08.006

27) Alan Anwer Abdulla, Sabah A. Jassim, and Harin Sellahewa "Efficient high-capacity steganography technique", Proceedings of SPIE - The International Society for Optical Engineering, 8755, http://dx.doi.org/10.1117/12.2018994

28) Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li, “A new chaotic algorithm for image encryption”, Chaos, Solitons and Fractals, Volume 29, Issue 2, (2006), Pages 393-399, https://doi.org/10.1016/j.chaos.2005.08.110

29) Satish A, Erapu Vara Prasad, Tejasvi R, Swapna P, Vijayarajan R, “Image Scrambling through Two Level Arnold Transform”, Alliance International Conference on Artificial Intelligence and Machine Learning (AICAAM), (2019).