DOI: 10.2478/ias-2024-0006 • JIAS • 19(2) • 2024 • 72-79

# Security Features on and with Documents: A Survey

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

1 Research Department of Computer Science, SDNB Vaishnav College for Women, Chrompet, Madras University, Chennai – 600044. India; chivkulayamini@gmail.com
2 PG Department of Computer Science, SDNB Vaishnav College for Women, Chrompet, Madras University, Chennai – 600044. India; drnpriya2015@gmail.com

**Abstract:** In today's world, document security has become essential. That stands for either a hard copy or a soft copy of any document. The concept of online, or digital, transactions has become increasingly prevalent in recent years. To accommodate these transactions, there arises a need to transform hard copies of documents into soft copies. This would further lead to a 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 human errors. These human errors are the ones that need to be taken care of on a large scale. Some people believe in sharing documents online with their peers or others of the same interest. This may lead to the misuse of these documents when they fall into the 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, Steganography, Scrambling, Blockchain

## 1 Introduction

Data present in documents can be of many types like confidential or just simple usable data. They may be critical data like transactional data, 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 the various methods that were used throughout the years and were described in articles.

Data duplication is possible to some extent, including copying data to perform illegal transactions, some of which are meant to deceive another person. There are many other reasons for duplication or illegal use of documents. The following is a study of some techniques used for safeguarding documents from misuse.

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

## 2 Techniques

data would be of various types, some of which are audio and video. If they are sensitive or critical, they need to be secured.

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 to, and some are discussed below.

### *2.1 Image Scrambling*

Image Scrambling is a part of data security and comes under the concept of data hiding. This means that the images, when scrambled, remain safe and secret from malicious sources. This would, in turn, keep the data scrambled and can be taken only by valid people.

Today, this has become a part of cryptography, even though it is not definitely encryption through an algorithm.

Ref. [1] suggested that image scrambling can be used in real time to safeguard data and gave us examples of Sudoku puzzles and Rubik's cubes. Here, the image matrix is obtained and scrambled, which results in a matrix that is very different from the original image. Then, when this image is unscrambled, the original image is returned.

Ref. [2] Concludes that Image scrambling can be done two-way using the 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 has been done numerous times.

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

## *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.

Ref. [3] Suggested a new bit-plane decomposition algorithm using Image Scrambling where the 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 a key can be decided by the user themself.

Ref. [4] Concluded that Arnold scrambling, a technique that uses the Arnold transform algorithm, and Bit Scrambling, which is performed as Bit Plane Decomposition, can be used for the encryption and decryption process.

The former is said to be simpler and easier to workout than the latter since Arnold Scrambling becomes somewhat confusing. Image Scrambling is generally a topic that is more common and known than Arnold Scrambling.

Here, the bit plane with a 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.

## *2.3 Steganography*

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

Ref. [5] 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 an increase in speed and security when compared to the other methods of LSB Image Steganography algorithms.

The Fig. 1 would give us a general example of how data can be embedded into an image for Security features.

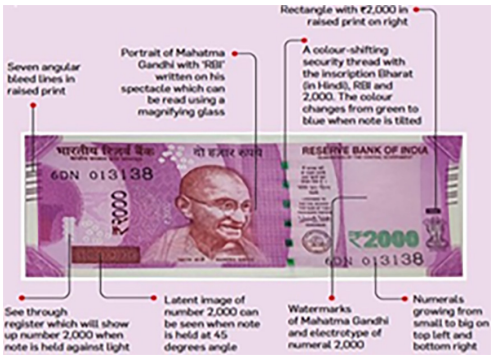


***Figure 1.*** Indian Rupee with its features that are highlighted

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. Microprint of the currency value.
3. RBI written on the Spectacles of Mahatma Gandhi, which is not visible to the naked eye.
4. Some other typographic unique features that cannot be duplicated easily.
5. Numbers written in Braille script.
6. Raised-up print that is shown at a certain angle.
7. The watermark of Mahatma Gandhi and electrolyte numerical of the currency written

Out of these features, almost four or five are part of Steganography. It has its basics here, and hence, any data can be embedded into an image.

## *2.4 Cryptography*

It means sending a message through a secured channel by encrypting it using a code, which is later decrypted by using another code. The code used is called a key.

In Cryptography, there are various algorithms that are commonly used. Some are the AES, DES, and RSA. 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.

Ref. [6] 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 2 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 the sender is encrypted using a Public key to make it Cipher text.

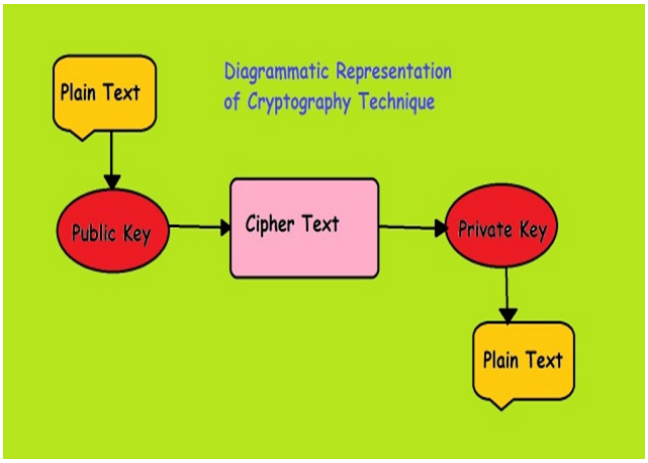


***Figure 2.*** Cryptography concept

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 Refs. [7-10], 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 to them respectively. Refs. [11, 12] also adds that Blockchain would mean that the data is safe and can be viewed only by the necessary person.

Ref. [13] 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 signals 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.

## 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 the importance in the Image encryption trend nowadays, Blockchain gives us more place for research and also for improvisation.

Of all the technologies given above, the most trending ones are 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 images and save some other data over that.

Let us compare these technologies to find the superior one. When these technologies are considered individually, they receive different efficiency scores, and when they are compared with others, for example, Bitplane and Image Scrambling are popular, their efficiency scores are different.

## 4 Metrics Considered

### *4.1 Accuracy*

When it comes to accuracy, Cryptography and blockchain technology can be considered, as they are the latest and most used.

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 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 2, the efficiency of Blockchain is higher when 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 reliable the results are. When compared using various algorithms of the above-mentioned technologies, Cryptography has a wide range of algorithms that perform well and have more recent updates. This holds good for Blockchain as well.

### *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.

## 5 Comparison of the Methods and their Metrics

Here, the comparison between the techniques is explained in table 1.

Also, table 2 gives us the metrics and their functionality in regards with the techniques are given.

***Table 1.*** Comparison according to Techniques

| **Image Scrambling:** |
|---|
| **Authors Referred:** [2], [4] |
| **Algorithms Used:** Rubic's Cubic algorithm and Arnold Transformation,<br>Arnold Scrambling |
| **Pros:** Simple and easy to work |
| **Cons:** Uses basic methods so need of more efficiency is there |
| **Efficiency (Comparatively):** Has some negative effects and termed as not much efficient |
| **Bit Plane:** |
| **Authors Referred:** [3] |
| **Algorithms Used:** Image encryption algorithm using Bitplane, Arnold Scrambling |
| **Pros:** Similar to Image Scrambling |
| **Cons:** Even after doing this, confusion exists in the model |
| **Efficiency (Comparatively):** Efficient when considered with Image Scrambling |
| **Cryptography:** |
| **Authors Referred:** [12] |
| **Algorithms Used:** An algorithm based on Chaos and improved DES |
| **Pros:** Familiar approach but various techniques |
| **Cons:** Encryption can be done using various methods where some are not satisfactory |
| **Efficiency (Comparatively):** More than Steganography |
| **Steganography:** |
| **Authors Referred:** [1], [14], [15] |
| **Algorithms Used:** Embedding and Extracting algorithm, Caesar/ Vigenère cipher |
| **Pros:** Easier to understand and does the necessary correctly |
| **Cons:** Old style method of encryption |
| **Efficiency (Comparatively):** Not much when compared with cryptography |
| **Blockchain:** |
| **Authors Referred:** [5], [6], [7], [8], [9], [10], [13], [16], [17] |
| **Algorithms Used:** Blockchain technology, Steganography |
| **Pros:** Can extend to save more details |
| **Cons:** Requires additional storage space |
| **Efficiency (Comparatively):** Efficient when taken alongside other technologies |

***Table 2.*** Comparison according to Metrics

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

## 6 Conclusion:

This study was conducted in regard to 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 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 1 and that gives us the related conclusion.

This study and references in Refs. [14], [18], and [19] tell that Data can be encrypted, scrambled, rearranged, hidden, and encoded to keep it safe from assailants. The blockchain method also yields us another advantage: one can get or save other details regarding the data along with encrypting it and keeping it safe.

**References:**

[1] Koptyra, K. and Ogiela, M.R. (2021). 'Imagechain—Application of blockchain technology for images. *Sensors*, 21(1), 82. Available at: https://doi.org/10.3390/s21010082.

[2] Satish, A., Vara Prasad, E., Tejasvi, R., Swapna, P. and Vijayarajan, R. (2019). 'Image Scrambling through Two level Arnold Transform'. *Alliance International Conference on Artificial Intelligence and Machine Learning (AICAAM)*, 2019.

[3] Zhou, Y., Cao, W. and Chen, C.L.P. (2014). 'Image encryption using binary bitplane'. *Signal Processing*, 100, 197-207. Available at: http://dx.doi.org/10.1016/j.sigpro.2014.01.020.

[4] Modak, P.M. and Pawar, V. (2015). 'A comprehensive survey on image scrambling techniques. *International Journal of Science and Research (IJSR)*, 2015, 813-818.

[5] Frattolillo, F. (2020). 'A watermarking protocol based on blockchain'. *Application Sciences*, 10(21), 7746. Available at: https://doi.org/10.3390/app10217746.

[6] Mannepalli, P.K., Richhariya, V., Gupta, S.K., Shukla, P.K. and Dutta, P.K. (2021). 'Block chain based robust image watermarking using edge detection and wavelet transform'. *IEEE Access*, 9, 2021. Available at: http://dx.doi.org/10.21203/rs.3.rs-766105/v1.

[7] Ren, N., Zhao, Y., Zhu, C., Zhou, Q. and Xu, D. (2021). 'Copyright Protection Based on Zero Watermarking and Blockchain for Vector Maps'. *International Journal of Geo-Information*, 10, 294. Available at: https://doi.org/10.3390/ijgi10050294.

[8] Abrar, A., Abdul, W. and Ghouzali, S. (2021). 'Secure Image Authentication Using Watermarking and Blockchain'. *Intelligent Automation & Soft Computing*, 2021, 577-591. Available at: http://dx.doi.org/10.32604/iasc.2021.016382.

[9] Evsutin, O. and Meshcheryakov, Y. (2020). 'The Use of the Blockchain Technology and Digital Watermarking to Provide Data Authenticity on a Mining Enterprise'. *Sensors*, 20, 3443. Available at: http://dx.doi.org/10.3390/s20123443.

[10] Mishra, P. and Suhag, R. (2022). 'State-Finances: A Study of Budgets, RBI; PRS, "LAND RECORDS AND TITLES IN INDIA"'. Available at: https://prsindia.org.

[11] Banik, A., Shamsi, Z. and Laiphrakpam, D.S. (2022). 'An encryption scheme for securing multiple medical images. *ScienceDirect*, 2022. Available at: https://doi.org/10.1016/j.jisa.2019.102398.

[12] Meng, Z., Morizumi, T., Miyata, S. and Kinoshita, H. (2018). 'Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain'. *2018 IEEE COMPSAC*, 2018. Available at: http://dx.doi.org/10.1109/COMPSAC.2018.10258.

[13] Chithra, P.L. and Aparna, R. (2023). 'Blockchain-based image encryption with spiral mapping and hashing techniques in dual level security scheme'. *International Journal of Information and Computer Security*, 21, 185-204. Available at: https://doi.org/10.1504/IJICS.2023.131100.

[14] Nasr, M.A., El-Shafai, W., Abdel-Salam, N., El-Rabaie, E.S.M., El-Fishawy, A.S. and Abd El-Samie, F.E. (2023). 'Efficient information hiding in medical optical images based on piecewise linear chaotic maps. *Journal of Optics*, 2023, 1852-1866. Available at: https://doi.org/10.1007/s12596-023-01128-7.

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

[16] Li, M., Zeng, L., Zhao, L., Yang, R., An, D. and Fan, H. (2021). 'Blockchain-Watermarking for Compressive Sensed Images'. *IEEE Access*, 9, 2021. Available at: http://dx.doi.org/10.1109/ACCESS.2021.3072196.

[17] Brabin, D., Ananth, C. and Bojjagani, S. (2022). 'Blockchain based security framework for sharing digital images using reversible data hiding and encryption'. *Multimedia Tools and Applications*, 81, Springer, 24721-24738. Available at: https://doi.org/10.1007/s11042-022-12617-5.

[18] Kumari, M., Gupta, S. and Sardana, P. (2017). 'A survey of image encryption algorithms. *3D Research*, 37, 2017. Available at: https://ui.adsabs.harvard.edu/link_gateway/2017TDR.....8..148K/doi:10.1007/s13319-017-0148-5.

[19] Kaur, M. and Kumar, V. (2020). 'A Comprehensive Review on Image Encryption Techniques'. *Arch Computat Methods Eng*, 27, Springer, 15-43. Available at: https://doi.org/10.1007/s11831-018-9298-8.

**Author Biographies**

**Yamini C** Received B.Sc. and M.Sc. degrees in Computer Science in the years 2019 and 2021, respectively, from SDNB Vaishnav College for Women, Chennai – Affiliated with the University of Madras. She has presented papers in international conferences. She is currently a Research Scholar at SDNB Vaishnav College for Women since 2023. Her research interests include Image Processing, Deep Learning. She can be contacted through email: chivkulayamini@gmail.com

**N. Priya** A technically skilled academician having more than 15 years of teaching experience. She completed both her UG and PG degrees with distinction. She was awarded a Ph.D. from Bharathiar University Coimbatore. She served as the head of the UG Department of Computer Application from 2004 to 2019 at SDNB Vaishnav College for Women, Chennai. She has also been a member of the Academic Audit and review panel in other institutions. She has chaired several sessions in International Conferences. She has published and presented more than 20 research articles and completed many NPTEL courses. She is a recognized research supervisor at the University of Madras. Her research areas include data mining, image processing, neural networks, network programming, and fuzzy logic. Currently, she is working as an associate professor in the PG Department of Computer Science, SDNB Vaishnav College for Women, Chennai. She can be contacted at email: drnpriya2015@gmail.com