Encryption of Legal Asset Documents and Ownership Details

Yamini C [1*], N Priya [2]
*Corresponding Author, [1] Research Department of Computer Science, SDNB Vaishnav College for Women, Chrompet, Madras University, India.
[2] PG Department of Computer Science, SDNB Vaishnav College for Women, Chrompet, Madras University, India.

Abstract

In the current world of online transaction propaganda, the need for data security has reached a new height. The image and data shared online are vulnerable to exploitation by malicious individuals through different methods. Especially the legal asset documents meant for the buying and selling of land assets are at higher risk of being misused. This calls for a novel encryption method where the security of ownership details and asset documents are taken care of. This paper focuses on securing both the ownership details and the land asset documents using the techniques - Steganography, Scrambling, Blockchain and hybrid IndexedBitPointer method. The efficiency of the algorithm is measured using the metrics PSNR(Peak – Signal – Noise Ratio), SNR(Signal – Noise Ratio), and MSE(Mean Signal Error) and the results are plotted in a graph to show the difference between the dataset values.

Keywords: Blockchain, Image Steganography, Scrambling, Galois – Counter Mode, IndexedBitPointer Encryption.

1. Introduction

Technology nowadays is seen as a bane to the society as much as it is a boon. The misuse of the legal asset documents and their ownership data have become common in recent times. To overcome this, the legal asset documents and their respective data have to be secured. This can be done by encoding or encrypting the data and the image using certain algorithms. Furthermore, having a record of the data that has been encrypted and saved can be done through a blockchain. This paper focuses on encrypting the data using AES + GCM + IndexedBitPointer and encoded into the image using Image Steganography technique; This image is later scrambled and saved in a blockchain to provide security to the overall process.

There exist certain differences in the algorithm used in this paper and the earlier ones and that has been discussed here. The author of [1] speaks about steganography and its various trends. [2] gives us the various deep learning techniques that are used in the study of steganalysis. [3] talks about image encryption techniques, their attacks and how to defend them. The use of QR code, Hash function and Inter – Planetary file system to secure data with the help of blockchain is explained in [4]. In the paper titled “Image steganography for securing secret data using hybrid hiding model”, [5] a new algorithm called HIED – Image Hiding Encryption and Decryption is introduced. The paper referred in [6] compares the various pros and cons in the Image Steganography algorithms. The authors of [7], Chinni Prashanth, et. al., uses Fernet Key encryption to prove their point in data security. [8] speaks on Fernet encryption method for cloud data, where double layer encryption is used.

The papers referred above tends to use the concepts of Steganography, scrambling and blockchain in separate ways and are the methods are never correlated. This paper intends to change the perception and combines all the three above mentioned processes along with the concept of AES + GCM +IndexedBitPointer method to provide security to land asset ownership details and the asset document images. The concept of embedding the ownership data into the document image is a unique way, after which scrambling the image further would mean that both the document and its details are kept safe from miscreants. Later, this data is updated along with the document image in a blockchain, so as to keep track of the changes made to the document – i.e., buying or selling of the specified land.

2. Methodology

The use of online tools to deal with land asset transactions is a remarkable change to the traditional method. But this method has some flaws that help the miscreants to use it for fraudulent activities. To prohibit such activities, this paper brings forth a novel method where the ownership details of the particular land is encrypted and stored in the land document image itself. This document is further safeguarded by the means of image encryption techniques. Further, to keep track of the transactions and their respective encryption of document image, the concept of blockchain is brought additionally. There are various methods of encryption that can be done on the images and documents online. The paper referred in [9] performs encryption in client – server architecture using 3DES (Triple Data Encryption Standard) and Fernet encryption. [10] explains on the concept of KeyGuardian which is used to generate hash function, thereby performing encryption and decryption of the data. The concept explained in [11] is fernet key encryption, particularly in cloud data alone.

In Phase 1, the ownership data which is stored in a text file is first encrypted using the novel AES + GCM +IndexedBitPointer method. The output of this process is an encrypted file that is not understandable when opened. In Phase 2, this file is further encoded into the document image. The encoding process is done through the concept of Image Steganography where the document image remains unaffected after the data encoding. For the Phase 3, the document image file that is received as the output from the above process is further made unrecognizable using the Image scrambling method. The concept of blockchain is introduced in the fourth Phase where the scrambled image is split into four parts and are updated in separate blocks of the blockchain. This remains a hidden job, whereas the updated ownership information (after buying / selling) is updated into a separate blockchain such that, each transaction is placed in one block and the latest transaction is updated on top.

3. Proposed work

3.1 Phase 1: Data Encryption using AES-GCM + IndexedBitPointer method

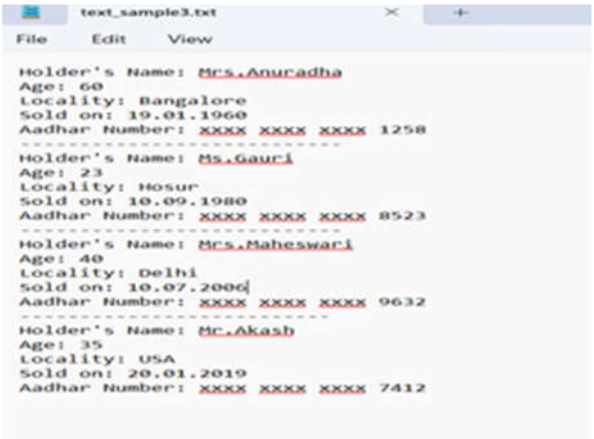

Figure 1. Ownership details text file.

In the past, authors haven't dealt with the concept of encrypting the ownership details of the land asset documents and only on encrypting the asset documents. The ownership details of any land asset data, shown here in figure 1, are sensitive information that needs to be secured. Hence the concept of encryption is used here in the form of AES + GCM + IndexedBitPointer method. The AES encryption abbreviates to "Advanced Encryption Standard". GCM (Galois Counter Mode) is used here for further protection. The concept of AES + GCM has been used since a very long time. The passcode used to generate the key for GCM is generally given by the user. For further security, here, the IndexedBitPointer method is used to automatically generate it with the use of the given text file. Securing the images is the further concept here. [12] discusses about encryption for medical images using El-Gamal cryptosystem and pseudo random number generator. [13] decides on the use of permutation along with blockchain to safeguard images. The

authors of [14], Zahid Iqbal Nezami, et. al., performs steganography with the use of Caesar and Vigenère cipher, where later on hash function is used on the result.

The IndexedBitPointer works under the concept of getting the 9 of the Most Significant Bits (MSB) of the text file and the Least Significant Bits (LSB) - 9 bits and uses them as the passcode. The key which is generated works under the principle given in equation. Here, the password is the one generated using the IndexedBitPointer method; Salt is generated through Random Bytes method; Key – Length: which is set to 32 by default; N - which describes the iteration count and is given by 2^11; r – which is block size and is set to 8; p – which gives the parallelism factor and is usually set to 1.

$$key = scrypt(password, salt, key\text{-}length = 32, N, r, p) \quad (1)$$

Figure 2. Encrypted output after AES + GCM + IndexedBitPointer.

The AES + GCM method works under the concept that the Key which is received from equation 1 and the Plaintext are encrypted to receive the Ciphertext. An authentication tag is generated with the use of ciphertext and additional data. The receiver can decipher the data only if they have both the ciphertext, key and the authentication tag data, which makes this system more secure comparatively. The encrypted output of the AES + GCM + IndexedBitPointer method is given in figure 2.

3.2 Phase 2: Encoding of the ownership data into the document image

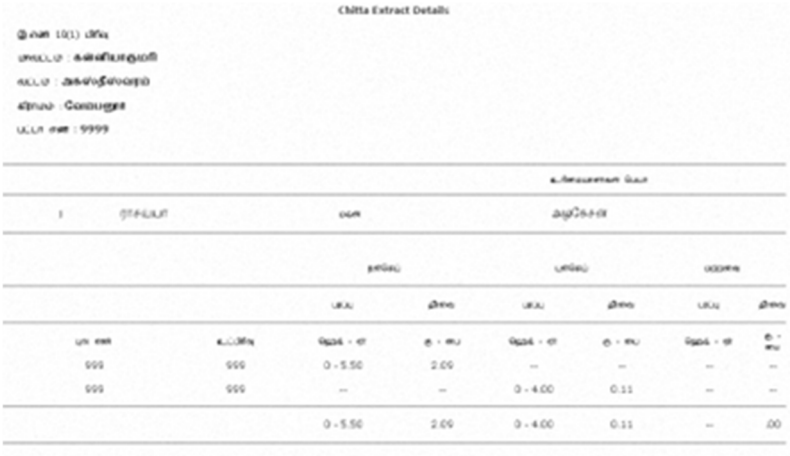

Figure 3. Land asset document image.

The concept of hiding data in another medium is termed as Encoding. In this case, the sensitive details such as the ownership details of any specific land are hidden inside its own document image, which is shown in figure 3. This can be done using the concept of Image Steganography, which basically means hiding one form of data into another. Here, the text data is hidden into the image form. The ownership details which were encrypted in the previous phase, is encoded into the document image. The said process would mean that the ownership data is kept safe from the eyes of the miscreants which would in turn help in reducing the “blackmail” concept of land acquirers. This concept has been explored by some in the recent years. [15] speaks about reversible data hiding between buyer and seller, where the data hidden can be reversed and

reclaimed. The author referred in [16] speaks about digital watermarking and image steganography, their similarities and differences and also the advancements in that stream.

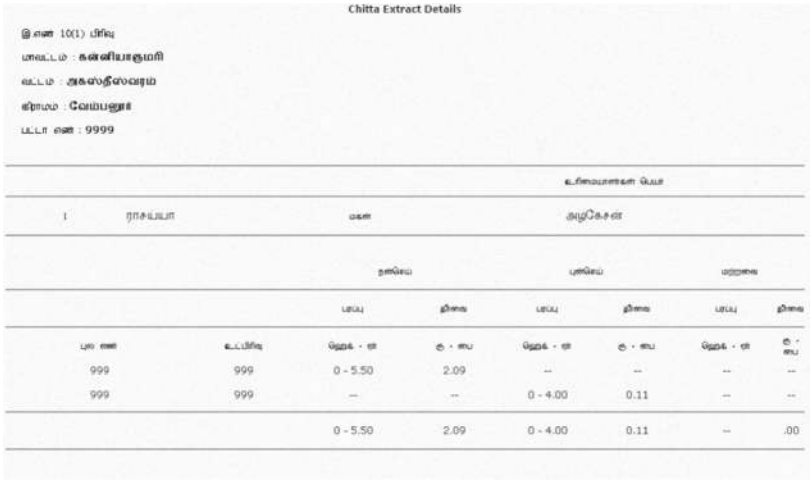

Figure 4. The output of Image Steganography.

For the concept of steganography, the data file's length is taken and an array constituting only zeros that is the same length as the file is constituted using zeros_like command. By adding the zeros_like array with the maximum value (in this case, 255) and later subtracting it by 1 will give the and_mask which is shown in equation 2 (an output sample is shown in the below block), The or_mask in this case would be the file_data which is the text file that we used to process. Later on, the process of bitwise-AND is performed on the and_mask and the concept of bitwise-OR is performed on the or_mask to proceed with the encoding. Here, the input data is like - File Data [1 0 0 ... 0 0 1]; zeros_like: [0 0 0 ... 0 0 0]; and_mask: [255 254 254 ... 254 254 255]. This gives us the output, as in figure 4, where the image doesn't show any difference from the earlier original image used for encoding. The result is termed as one best feature of encoding where misuse is reduced when there is not enough evidence of the data hidden in the image.

$$\text{and\_mask} = \text{zeros\_like} + \text{max value} - 1 \qquad (2)$$

3.3 Phase 3: Scrambling of the specified document image.

Rendering an image unrecognizable is one of the key features of securing the image data. This process has various methodologies, out of which here, Image Scrambling is chosen. Scrambling is used to mix-up the bytes and make it differ from the original data. A classic example of scrambling would be the 'Sudoku' puzzle. [17] uses Arnold Transformation and Image scrambling, where using 'n' as a key, iterations are performed on the data to receive a heavily scrambled image. Here, scrambling is used such that the document image that has the data encoded, is scrambled in some specific parts. Those parts are given by the mask that is used.

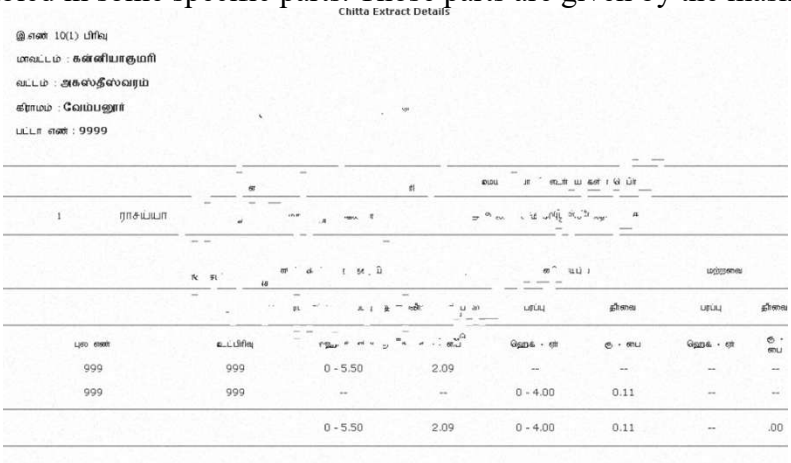

Figure 5. The output of Image Scrambling.

A mask that is of the user's requirement can be created and is later on processed, shuffled with the original image matrix. This renders the image different, and in most cases unrecognizable. The output of this Scrambling process is given in figure 5. The above process would mean that the image is secured from fraudulent transactions as well as the data encoded inside the image is safe from misuse. The legitimate receiver of this information should have to descramble using the same mask to get the original image, which proves security in the other end as well.

3.4 Phase 4: Updating the image blockchain with the split images of the encoded – scrambled document.

The data and image security part of the transactions have been dealt with. But the process of recording or updating the said transaction at a place is another important job that has to be done. To pursue this, the concept of blockchain is introduced here. The transactions done are added into the text file that is encoded in the image. So, the image file can be saved in the blockchain and updated every time the transactions change or gets added. The paper referred in [18] establishes Imagechain, a concept similar to blockchain, where images along with the link to the next information file are saved in each block. [19] intends to provide security to online buying – selling process with the help of digital watermarking combined with blockchain. The concept of digital watermarking using wavelet transform combined with Blockchain is explained in [20] to securely transfer images online. [21] merges blockchain, file system transfers and watermarking to securely transfer and make transactions using files online. Angular vector method combined with Zero watermarking is used to secure images and data online, which is explained in [22]. Ethereum blockchain technique presents good amount of security and can be combined with watermarking is what is explained in [23]. Oleg Evsutin, et. al., in [24] explains about handling micro-controllers using blockchain technology along with digital watermarking. Based on the study done on various papers that have used blockchain in image encryption transactions before, this paper proposes the method specified below.

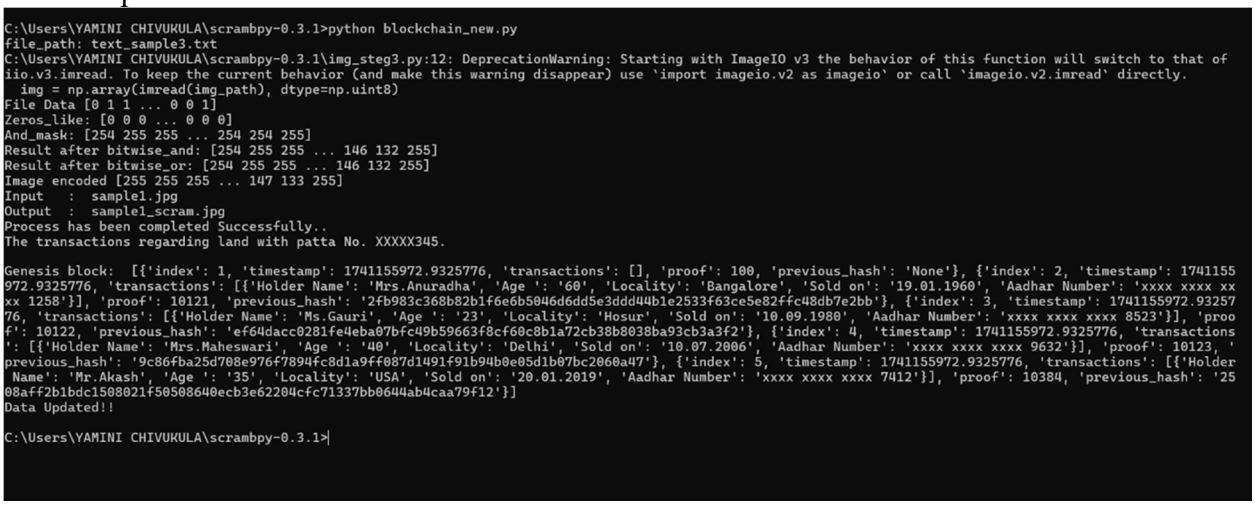

Figure 6. The command prompt for the processing of Blockchain.

The new transaction added is kept in a new block and is added over every time the whole process is repeated. This way, a record is kept of the transactions and image, as well as any anomaly found can be scrutinized from its start. The successful transaction to a new block is acknowledged through the message received in the command prompt or the console, which is shown in figure 6. Here, the genesis block is displayed along with its features such as the index – which is the array index, timestamp – the time at which the transaction was created, transactions – in this case, they are the document images and previous hash – the hash value of the previous block. At the end of this, a transaction successful message is being displayed. This method and the whole process is fool proof in case of ownership data, document image and transactions security.

4. Results and discussion

The effectiveness of any process is validated using the metrics. Here, the encryption process and the scrambling process are validated collectively using the PSNR, SNR and the MSE values. Here, five samples' data are presented in the table 1. For the dataset, about 40 document images were taken for the process. [25] concludes that the algorithm 'LSB_EE_20' gives best results in terms of efficiency and PSNR; and this concept is used here to compare with the accuracy and efficiency of the AES + GCM + IndexedBitPointer method.

The agenda of the whole process is to secure the document image and ownership details from miscreants. The scrambled document images have minimum blur generally but their clarity isn't affected much. The clarity before and after encryption is measured using PSNR, SNR and MSE metrics. Here, PSNR stands for Peak - Signal - Noise Ratio and SNR expands into Signal - Noise Ratio, whereas MSE means Mean - Square Error. The acceptable values of PSNR lies between 30 dB to 50 dB and for SNR, it lies between 20 dB and 40 dB . These acceptable values categorize as the images that have good clarity comparatively with their original image. As per the results received, the samples used have given a good and acceptable outcome in the PSNR, SNR and MSE metrics calculation. This means that the encryption has been a success as well as the clarity and the visibility is acceptable. Table 2 provides us with the average of the values for the whole of 40 document images and their ownership details taken. The graph in figure 7 gives us the pictorial representation of the average values. The curve shows how the values are all in acceptable range and have good metric result as well.

Table 1. The data with five samples and their outputs with MSE, PSNR and SNR values.

MSE	AES + Fernet	AES + GCM	Scrambled - encoded AES + GCM + IndexedBitPointer
Sample 1	1.0	1.0	1.0
Sample 2	0.0	0.0	0.0
Sample 3	1.0	1.0	1.0
Sample 4	0.0	0.0	0.0
Sample 5	1.0	1.0	1.0
SNR	AES + Fernet	AES + GCM	Scrambled - encoded AES + GCM + IndexedBitPointer
Sample 1	25.64	21.52	28.65
Sample 2	31.01	19.23	31.52
Sample 3	25.31	23.61	32.51
Sample 4	31.23	19.54	33.21
Sample 5	34.21	21.40	36.55
PSNR	AES + Fernet	AES + GCM	Scrambled - encoded AES + GCM + IndexedBitPointer
Sample 1	36.81	31.45	37.54
Sample 2	38.21	34.21	41.05
Sample 3	42.02	32.23	43.56
Sample 4	41.25	30.15	40.21
Sample 5	43.65	35.56	45.53

Table 2. The average values of the forty samples of dataset with their MSE, PSNR and SNR values.

	Sample -1 (AES + Fernet)	Sample -2(AES + GCM)	Sample -3 (Scrambled - encoded AES + GCM + IndexedBitPointer)
MSE	0.6	0.6	0.6
SNR	29.48 dB	21.06 dB	32.488 dB

PSNR	40.388 dB	32.72 dB	41.578 dB

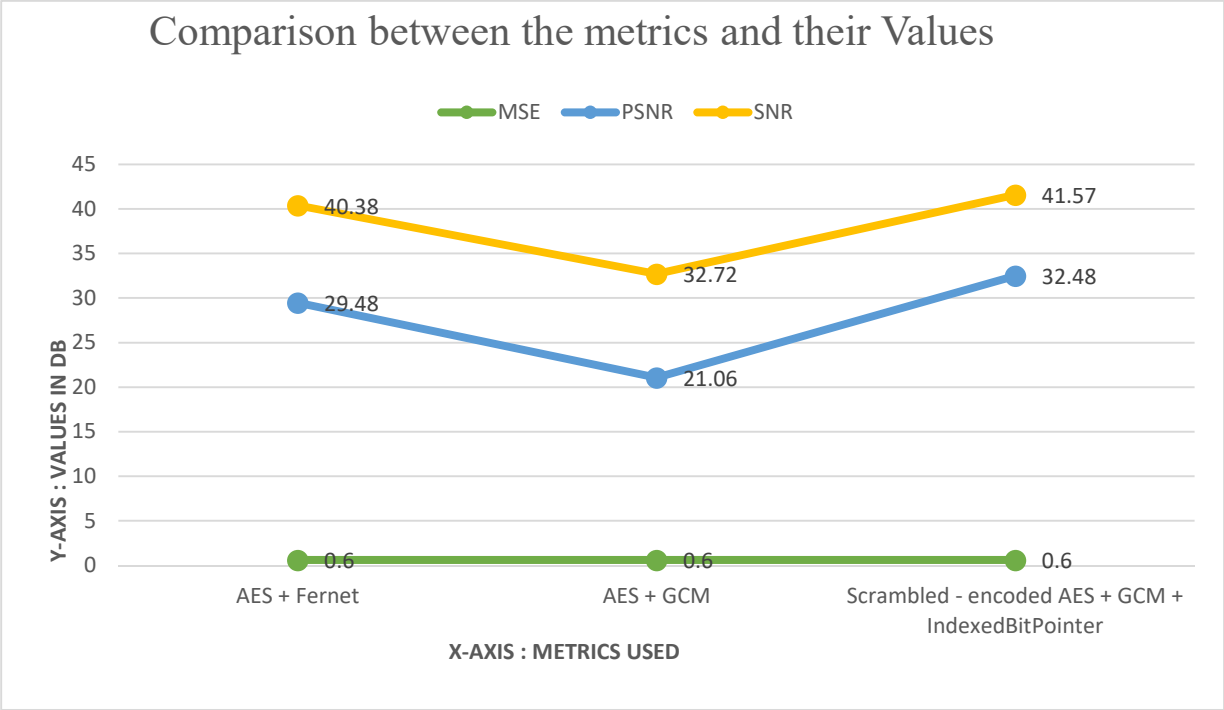

Figure 7. The graph representing average values of MSE, PSNR and SNR for the dataset.

5. Conclusion

The need for security is quenched when appropriate measures are taken to safeguard data. The recent news burst regarding misuse of the land asset documents without the knowledge of their owners, calls for immediate action. To do the same, this paper provides with a whole new process where the ownership data in a text file is encrypted, then encoded into its document image. Further, this image is scrambled to make it blur but not reveal its sensitivity. Furthermore, the image is stored in a blockchain by splitting it. And every time a new transaction is made, a blockchain is created and the new updated document image is stored there. In this way, all of the security need is satisfied and the response given is a document image with clarity and without any hint of sensitive data encoded into it. Also, whenever there is any duplicate document going around in the chain, it is easy to recognize it with some background information. This gives us a breakthrough for the security concerns provided.

Funding information

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author contributions statement

Yamini, C -Data Curation, Conceptualization, Design, Formal Analysis, Project Administration, Writing - Original Draft, Investigation. N. Priya -Data Curation, Conceptualization, Design, Resources.

References

[1] P. C. Mandal, I. Mukherjee, G. Paul, and B. N. Chatterji, "Digital image steganography: A literature survey," *Inf Sci (N Y)*, vol. 609, pp. 1451–1488, Sep. 2022, Doi: 10.1016/j.ins.2022.07.120.

[2] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[3] M. Kaur and V. Kumar, "A Comprehensive Review on Image Encryption Techniques," *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15–43, Jan. 2020, doi: 10.1007/s11831-018-9298-8.

[4] M. Li, L. Zeng, L. Zhao, R. Yang, D. An, and H. Fan, "Blockchain-Watermarking for Compressive Sensed Images," *IEEE Access*, vol. 9, pp. 56457–56467, 2021, doi: 10.1109/ACCESS.2021.3072196.

[5] S. Kaur, S. Bansal, and R. K. Bansal, "Image steganography for securing secret data using hybrid hiding model," *Multimed Tools Appl*, vol. 80, no. 5, pp. 7749–7769, Feb. 2021, doi: 10.1007/s11042-020-09939-7.

[6] G. V and I. G, "A review on image steganographic techniques based on optimization algorithms for secret communication," *Multimed Tools Appl*, vol. 82, no. 28, pp. 44245–44258, Nov. 2023, doi: 10.1007/s11042-023-15568-7.

[7] C. Prashanth, D. Bala Sai Teja, and L. V, "Securing the data in cloud using fernet technique," *Easychair - Preprint*, 2022, Accessed: Mar. 15, 2025. [Online]. Available: https://easychair.org/publications/preprint/8g5X/open

[8] P. Anon and S. S. Tyagi, "Enhancing Security of Cloud Data through Encryption with AES and Fernet Algorithm through Convolutional-Neural-Networks (CNN)," *International Journal of Computer Networks and Applications*, vol. 8, no. 4, p. 288, Aug. 2021, doi: 10.22247/ijcna/2021/209697.

[9] M. Siti Munirah *et al.*, "The Performance of the 3DES And Fernet Encryption in Securing Data Files," *J Theor Appl Inf Technol*, vol. 102, no. 3, pp. 812–820, Feb. 2024, Accessed: Mar. 15, 2025. [Online]. Available: https://www.researchgate.net/publication/381232402_The_Performance_of_the_3DES_and_Fernet_Encryption_in_Securing_Data_Files

[10] M. Singh, "Enhancing Data Security with KeyGuardian: Application of Fernet for Digital Asset Protection," *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, vol. 08, no. 05, pp. 1–5, May 2024, doi: 10.55041/IJSREM34392.

[11] A. Jain and P. De, "Enhancing Database Security for Facial Recognition using Fernet Encryption Approach," in *2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, IEEE, Dec. 2021, pp. 748–753. doi: 10.1109/ICECA52323.2021.9676065.

[12] A. Banik, Z. Shamsi, and D. S. Laiphrakpam, "An encryption scheme for securing multiple medical images," *Journal of Information Security and Applications*, vol. 49, p. 102398, Dec. 2019, doi: 10.1016/j.jisa.2019.102398.

[13] 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, p. 185, 2023, doi: 10.1504/IJICS.2023.131100.

[14] Z. I. Nezami, H. Ali, M. Asif, H. Aljuaid, I. Hamid, and Z. Ali, "An efficient and secure technique for image steganography using a hash function," *PeerJ Comput Sci*, vol. 8, p. e1157, Nov. 2022, doi: 10.7717/peerj-cs.1157.

[15] Z. Meng, T. Morizumi, S. Miyata, and H. Kinoshita, "Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, IEEE, Jul. 2018, pp. 359–364. doi: 10.1109/COMPSAC.2018.10258.

[16] D. Brabin, C. Ananth, and S. Bojjagani, "Blockchain based security framework for sharing digital images using reversible data hiding and encryption," *Multimed Tools Appl*, vol. 81, no. 17, pp. 24721–24738, Jul. 2022, doi: 10.1007/s11042-022-12617-5.

[17] A. Satish, E. Vara Prasad, R. Tejasvi, P. Swapna, and R. Vijayarajan, "Image Scrambling through Two level Arnold Transform," in *Alliance International Conference on Artificial Intelligence and Machine Learning (AICAAM)*, Apr. 2019, pp. 329–337. Accessed: Mar. 15, 2025. [Online]. Available: https://www.alliance.edu.in/aicaam-conference-proceedings/Papers/Image-Scrambling-through-Two-Level-Arnold-Transform.pdf

[18] K. Koptyra and M. R. Ogiela, "Imagechain—Application of Blockchain Technology for Images," *Sensors*, vol. 21, no. 1, p. 82, Dec. 2020, doi: 10.3390/s21010082.

[19] F. Frattolillo, "A Watermarking Protocol Based on Blockchain," *Applied Sciences*, vol. 10, no. 21, p. 7746, Nov. 2020, doi: 10.3390/app10217746.

[20] P. K. Mannepalli, V. Richhariya, S. K. Gupta, P. K. Shukla, and P. K. Dutta, "Block Chain Based Robust Image Watermarking Using Edge Detection And Wavelet Transform," Aug. 20, 2021. doi: 10.21203/rs.3.rs-766105/v1.

[21] D. Megías, W. Mazurczyk, and M. Kuribayashi, "Data Hiding and Its Applications: Digital Watermarking and Steganography," *Applied Sciences*, vol. 11, no. 22, p. 10928, Nov. 2021, doi: 10.3390/app112210928.

[22] N. Ren, Y. Zhao, C. Zhu, Q. Zhou, and D. Xu, "Copyright Protection Based on Zero Watermarking and Blockchain for Vector Maps," *ISPRS Int J Geoinf*, vol. 10, no. 5, p. 294, May 2021, doi: 10.3390/ijgi10050294.

[23] A. Abrar, W. Abdul, and S. Ghouzali, "Secure Image Authentication Using Watermarking and Blockchain," *Intelligent Automation & Soft Computing*, vol. 28, no. 2, pp. 577–591, 2021, doi: 10.32604/iasc.2021.016382.

[24] O. Evsutin and Y. Meshcheryakov, "The Use of the Blockchain Technology and Digital Watermarking to Provide Data Authenticity on a Mining Enterprise," *Sensors*, vol. 20, no. 12, p. 3443, Jun. 2020, doi: 10.3390/s20123443.

[25] A. A. Abdulla, "Digital image steganography: challenges, investigation, and recommendation for the future direction," *Soft comput*, vol. 28, no. 15–16, pp. 8963–8976, Aug. 2024, doi: 10.1007/s00500-023-09130-8.