AES-Based Steganography Using Blockchain: A Novel Approach for Secure Text Hiding in Encrypted Images

Batool Arif Salim*, Maalim A. Aljabery, Hameed Abdulkareem Younis
Faculty of Computer Science and Information Technology, Computer Science Dept., University of Basrah, Basrah, Iraq
E-mail: batool98almayahi@gmail.com, maalim.aljabery@uobasrah.edu.iq, hameed.younis@uobasrah.edu.iq
*Corresponding author

Keywords: steganography, blockchain, AES algorithm, CBC mode, UACI, NPCR, entropy analysis, correlation analysis, secure texts

Received: July 16, 2024

Steganography is a technique used to hide data within other data, emerging from the realization that information is valuable and must be concealed. By considering the potential of blockchain technology, which produces and stores data in an immutable chain, it is clear that steganography can be effectively applied alongside blockchain to hide information. This approach eliminates the need for traditional hiding methods. In this study, we aim to hide text messages within encrypted images using a new steganography-based blockchain, making them appear as ordinary encrypted images. The AES algorithm in CBC mode was used to encrypt both images and texts. Each image was split into 32-byte blocks, with a special block allocated for text, allowing for a text size of 32 characters. The robustness of the proposed technique against differential attacks was assessed using unified averaged changed intensity (UACI), number of pixels change rate (NPCR), entropy analysis, and correlation analysis. The outcomes are 99.6221% for NPCR, 33.5886 for UACI, and 7.9992 for the entropy value. Both statistical measures and differential metrics confirm the algorithm's effectiveness. This shows that the proposed encryption method generates random images and secure texts that are resistant to differential attacks and offer a prominent level of security.

Povzetek: Razvit je nov pristop steganografije z uporabo algoritma AES in blockchaina za varno skrivanje besedila v šifriranih slikah, s čimer dosega visoko odpornost na napade in izboljšano varnost podatkov.

1 Introduction

Textual data plays an important role in many practices [1]. Research on data security and data hiding over the years has demonstrated that combining steganography and encryption techniques can effectively conceal data and prevent its discovery [2]. Therefore, in this hiding approach, data preprocessing is necessary using certain cryptography techniques [3]. Most modern technologies utilize different transporter messages, including videos, images, and texts. Nevertheless, image files continue to be the most commonly used transporter format since they are easy to transmit between two actively communicating parties [4]. The novel steganography of blockchain-based technique is an essential contribution of this research that incorporates cryptography alongside steganography to enhance data security.

1.1 Image processing

Various data safeguarding procedures, such as cryptographic and data concealing strategies, have been proposed to address information security issues. Cryptographic methods scramble and convert private information into an indecipherable format for unauthorized individuals, providing significant security by altering the original data's format through encryption. However, encryption alone is not immune to security breaches, as its encrypted form can attract the attention of attackers and potentially be altered or breached. Consequently, it is an inadequate technique for ensuring data security. To address this, researchers often employ data disguising methods to conceal the presence of crucial data, making it less likely to be detected by intruders [3]. There are generally two encryption technique types: symmetric and asymmetric [5]. Symmetric encryption utilizes the identical key for both decryption and encryption by the sender and the recipient, as seen in the Advanced Encryption Standard (AES) [6]. Asymmetric key encryption, or public key encryption, uses different keys for encryption and decryption. The encryption process utilizes a public key, accessible to everyone, while the decryption process utilizes a private key, only accessible to authorized individuals. An example of this is the Rivest–Shamir–Adleman (RSA) algorithm [6].

1.2 Blockchain technology

Blockchain is a ground-breaking technology that enables the creation of distributed databases where information is stored as an ever-expanding chain. Once data is stored, it cannot be altered because each block is linked to the past one using a function of hash cryptography. This linkage ensures data consistency and prevents manipulation. Changing a single bit within the chain would necessitate

recalculating each hash from the block modified to the final block, which would consume significant energy [7].
Blockchain technology is one of the most crucial methods used to address security [8]. As a consensus-based system, blockchain requires each node to confirm the occurrence of a transaction and agree on all relevant details before adding them to the ledger based on blockchain technology (BCT) [5]. Attackers might, however, take advantage of the 51% weakness in the consensus mechanism to take control of the entire Blockchain [9]. Advantages of a blockchain include its ability to be tamper-proof and safeguard data from integrity-based assaults [10].

1.3 Steganography

Steganography research has evolved alongside technological advancements and emerging opportunities. There is a growing interest in integrating steganography with blockchain technology, driven by a better understanding of blockchain's potential in enhancing data security, leveraging distributed architecture, and ensuring anonymity. As a result, blockchain has become a compelling area of study in the field of steganography [4]. Steganography involves concealing data within other data, which can later be extracted at its destination This technique is mostly combined with encryption to provide an additional layer of data protection [11]. In digital images, data concealing is certainly the greatest technique since it makes it simple to conceal sensitive information in the images without compromising the image quality [12]. For steganography to be considered successful, it must meet certain requirements at a high level, including imperceptibility (undetectability), security, payload capacity, and robustness [2]. By embedding a secret text inside digital media, steganography aims to prevent attackers from seeing the hidden text and maintain the secrecy of the secret data [12].

The rest of the research is planned as follows: section 2 gives a literature review, section 3 delivers related works, section 4 proposes encryption model, section 5 discusses performance evaluation metrics, and section 6 discusses. Finally, section 7 concludes.

2 Literature review

Proposed the Ozyavas Takaoglu–Ajlouni (OTA) algorithm as a new strategy for blockchain steganography which removes the shortcomings encountered by conventional blockchain steganography technology and within this framework, they introduced OTA-chain and a new OTA-steganography algorithm, furthermore, the suggested strategy will resolve two principal defects of the present strategy: minimal resistance to steganalysis following stego-operation and the restriction placed on the amount of data that can be concealed in the cover multimedia [2].

To introduce a novel method for covertly concealing medical data, the proposed approach divides private COVID-19 records into multiple segments, which are then hidden within various host images. A hash is used as a pointer to identify the stego images across different hospitals. So, concealing in this way renders the suggested technique extremely hard to breach by a hacker, furthermore, the anticipated stego images have an elevated quality degree since the embedding capability of the host images is calculated before the private data are hidden (not greater or fewer than the embedding capacity), this step offers an elevated degree of confidentiality [4].

Developed a project to provide a secure and tamper-proof way of authenticating user identity across multiple platforms by using a combination of image steganography and the Ethereum blockchain, this is done by hiding user identity information within images using image steganography and then storing these images on the Ethereum blockchain as Non-Fungible Tokens (NFTs), this allows to create a verifiable and immutable record of each user's identity, which can be easily authenticated on any platform that supports the Ethereum blockchain [11].

A safety scheme based on blockchain is suggested for exchanges of digital images in a multi-participant setting, in the suggested method, to generate space for data concealing, the digital image is initially compressed, followed by embedding of the user signature and the encryption of the entire image; JPEG lossy compression is used for compression to generate elevated capacity, while any symmetric block cipher or stream cipher is utilized in encryption, consequently, experimenting outcomes display that the suggested blockchain-based frame offers elevated safety and the suggested reversible data concealing scheme produces elevated image quality and capacity [12].

Proposed a scheme of Reversible Data Hiding on the Encrypted Images (RDHEI) for incorporating personal data into medical images, to evacuate additional space for data embedding capacity, this suggested scheme utilized stream cipher, then the doctor encrypts patients’ medical histories and afterward produces a Ciphered Steganography Medical Image (CSMI) via the RDHEI scheme, in which the encrypted medical history is incorporate into patient’s medical image, finally, to provide an integrity check, the hash value of CSMI is saved in a blockchain system frequently employed for upcoming authentication [13].

3 Related works

Prince and Yungcheol [5], suggest using a permission private blockchain in the context of the IIoT to protect the image during encryption, so that image data's security and privacy are guaranteed by this approach, which stores the image's cryptographic pixel values on the blockchain, consequently, the encrypted results demonstrate how successful the suggested scheme is at preventing data leaks and maintaining security.

Malika and Rama [14], propose a technique to encrypt images based on blockchain and Feedback Carry Shift Register (FCSR), the proposed solution encrypts images and stores values on the blockchain, so that the FCSR ensures image information security and the blockchain ensures the security and privacy in the transit.

Bhaskaran et al. [15], introduced a new Blockchain Secure Optimal Lightweight Cryptography established on the

Image Encryption (BC-LWCIE) method of the environment of industrial 4.0, this method includes the creation of hash function based on ideal LWC with ideal key production utilizing the algorithm of Chicken Swarm Optimization (CSO) which originates the fitness function through the maximizing of Peak Signal of Noise Ratio (PSNR), besides, cryptologic the pixel values for an encrypted image within the BCT are kept by the BC-LWCIE method for guaranteeing confidentiality within Industrial Internet of Things (IIoT) environment.

Saba et al. [16], this study proposes a Blockchain-based Chaotic Arnold's cat map Encryption scheme (BCAES), that’s because cloud storage solutions are open and can be subject to various security risks, so by using Arnold's cat map encryption algorithm, BCAES first encrypts the image and then transfers the encrypted image to a cloud server and saves endorsed plain image document in a blockchain.

Tables 1 (a and b) illustrate the summary of the results of the related works.

Table 1-A: Related works results

Ref.	Type of image	Color of image	Images	Entropy (bits)	UACI (%)	NPCR (%)
Prince and Yungcheol 2020, [5]	Benchmark image	gray	Cameraman Lena Man Truck	7.9972 7.9978	33.4187	99.6023
Malika and Rama 2021, [14]	Benchmark image	gray	Lena Cameraman Peppers Baboon	7.9986	33.45	99.69
Bhaskaran et al. 2022, [15]	Benchmark image	color gray	Airplane Baboon Barbara Cameraman House Lena			99.340 99.230 97.260 99.470 96.890 99.570
Saba et al. 2024, [16]	Medical image	color	Image (1) Image (2) Image (3) Image (4) Image (5)	7.9992 7.9991 7.9992 7.9992 7.9992	33.21	99.63

Table 1-B: Related works results

Ref.	Correlation Coefficient					
	Image		Color of image	Horizontal	Vertical	Diagonal
Prince and Yungcheol 2020, [5]	Cameraman	Original image		0.944198	0.961276	0.899276
		Encrypted image		-0.042225	0.036725	-0.058265
Malika and Rama 2021, [14]	Lena	Original image				
		Encrypted image		0.0033	0.0025	-0.0041
Saba et al. 2024, [16]		Original image	Blue Green Red	0.9776 0.9668 0.9597	0.9759 0.9688 0.9711	0.9568 0.9402 0.9365
		Encrypted image	Blue Green Red	0.00007 0.0036 0.0009	0.0044 -0.0006 0.0064	-0.0019 -0.0030 -0.0027

4 Proposed encryption model

In this study, we applied the AES cryptographic algorithm, a symmetric encryption method that utilizes the same key for all encryption and decryption. AES operates on data in blocks, dividing it into 128-bit blocks (16 bytes). We will apply zero padding for data sizes that are not multiples of 16 bytes. We will use the Cipher Block Chaining (CBC) mode, which is known for producing different ciphertext blocks even when identical plaintext blocks are encrypted [17]. We will use the secrets module to generate the key and Initialization Vector (IV).

To manage data, including account authentication, passwords, related secrets, and security tokens, the secrets module generates cryptographically strong random numbers [18].

In blockchain applications, public blockchains are typically favored when involving cryptocurrency or engaging the entire community. However, for scenarios requiring privacy and restricted access [2]. In our case, private blockchains are often preferred, so we will utilize them. The proposed model encompasses various operational phases, including image encryption, blockchain validation, and image decryption.

4.1 Image encryption

A novel steganography method has been developed to conceal confidential messages within a host image while minimizing distortion of the stego images. During image encryption, the image is converted into a series of bytes to prevent access to its original form, enhancing digital content security. Digital images and text are encrypted using the AES algorithm in CBC mode. The encryption process involves generating a 32-byte key and a 16-byte initialization vector using the secrets module. The image is segmented into 32-byte blocks and encrypted, with the last block padded if its size is less than 32 bytes, ensuring that all blocks maintain the same size.

In addition to image encryption, a private blockchain is utilized where each block contains 32 bytes of data. Each block comprises the previous block hash, timestamp, block number, data, nonce, and hashes generated from the components. Two hash types, SHA-3-256 and SHA-256, are employed. The blockchain starts with the genesis block, followed by the key and initialization vector (IV) with a 16-byte padding to achieve a 32-byte size.

A dedicated block is allocated for textual data. Users can input up to 32 characters of text; if the text exceeds this limit, a message stating "Text is too long for a single block encryption" is displayed, whereas padding is added if the text is not long enough to ensure that all blocks are uniform in size. All blocks are stored in a JSON format file and serialized on the blockchain. Data is converted from bytes to hexadecimal before being appended to the file.

4.2 Validating of blockchain

Before decryption begins, the blockchain undergoes verification by recalculating the hash for each block in the chain. It ensures that the recalculated hash matches the hash stored in the file and verifies that the previous hash of each block correctly refers to the hash of the preceding block in the chain. A message confirming the blockchain's validity will be displayed if no tampering is detected. However, if an inconsistency is found, the block number and the recalculated hash will be shown, followed by a message indicating that the blockchain is "invalid".

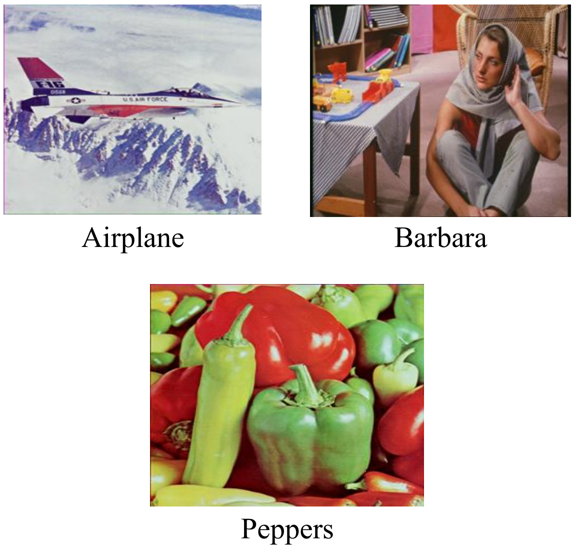
4.3 Image decryption

After verifying the validity of the blockchain, hexadecimal data is converted back into bytes, from which the key and initialization vector (IV) are extracted. The IV's padding is removed to initiate the decryption process. The block containing the text is decrypted first, and the padding is removed if included. Subsequently, the remaining blocks are decrypted, and the padding from the last block is removed if present. Encrypted bytes can be transferred to another system where they can undergo decryption to restore their original values. Ultimately, the data is compiled to reconstruct the image.

5 Performance evaluation metrics

Choosing datasets is extremely important for the experiment [19]. Images datasets can be present in three varying shapes: red–green–blue (RGB), binary (black and white), and greyscale images [4].

In this study, we will use RGB images. The size of the tested image is 256 × 256 pixels, and all images are stored in BMP format. The tests were accomplished on PC i5-12450H, 512GB SSD, and 8GB RAM. The simulation is conducted using Python 3.9.18. Three standard test images, including "Airplane", "Barbara", and "Peppers" are utilized. To evaluate the encryption algorithm, we will analyze the histogram to assess pixel dissemination in the original and ciphered images. We will also use NPCR and UACI as standards to assess resistance against differential hacks. The information entropy will be calculated to assess the unpredictability of the encrypted image, and the correlation coefficient will be used to measure the similarity between the encrypted and the original image. Figures 1 and 2 show the original and encrypted images.

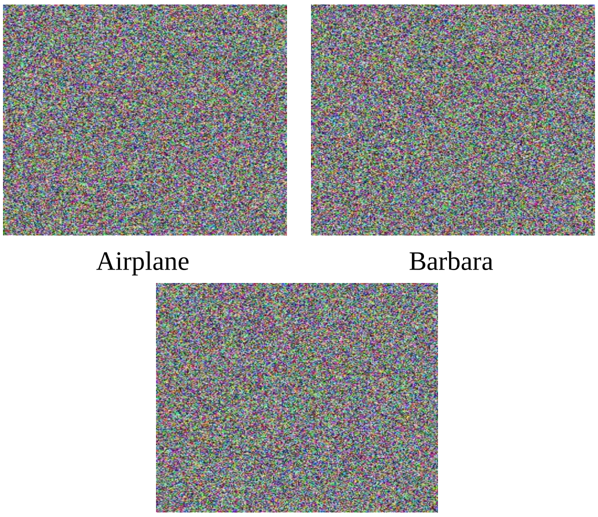


Airplane

Barbara

Peppers

Figure 1: The original images



Airplane

Barbara

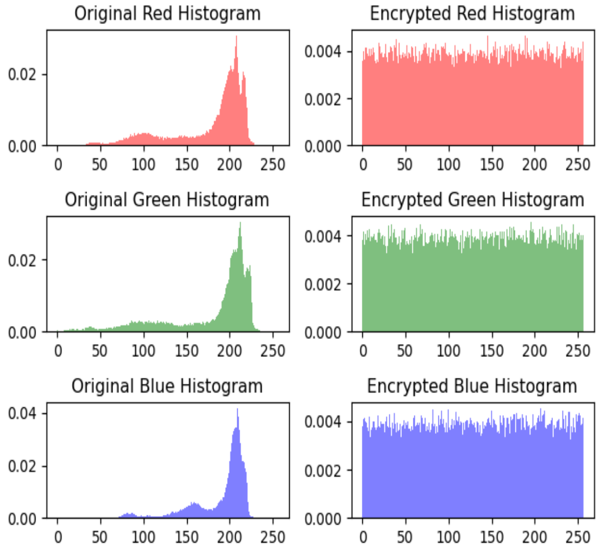
Peppers

Figure 2: The encrypted images

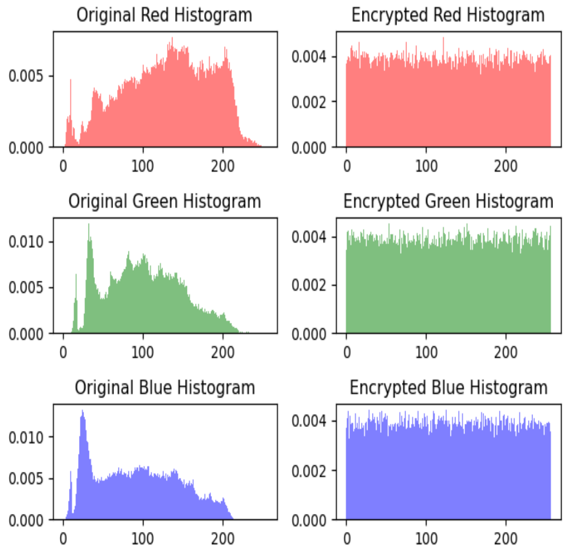
5.1 Histogram analysis

The image histogram holds significant importance in image analysis where the perfect ciphered image should have a uniform distribution frequency [20].

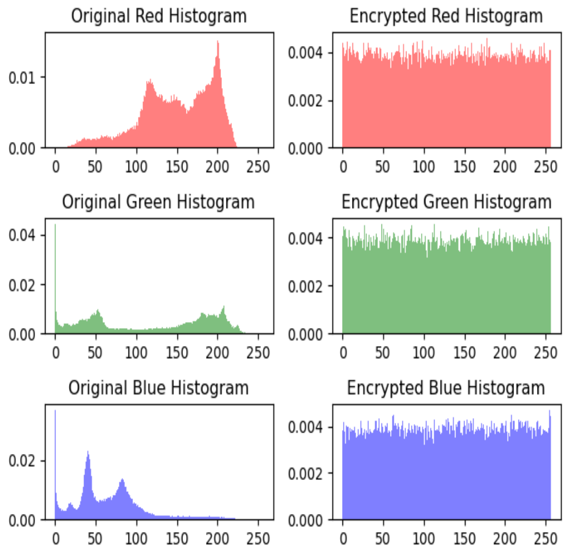
Figure 3 (a, b, and c) shows the histogram analysis of the RGB original and ciphered image channels. It is clear that the histograms of an encrypted image are uniform and random, it can be concluded that the recommended method lacks any useful statistical information about the encrypted image. Furthermore, because the text is hidden as a block in the blockchain, it does not affect the histogram analysis of the image.



(a) The Airplane Image



(b) The Barbara Image



(c) The Peppers Image

Figure 3: Histogram Analysis in red, green, and blue for original and encrypted images

5.2 Differential attack

To determine if the suggested encryption algorithm is capable of withstanding differential attacks, Unified Average Changing Intensity (UACI) and Number of Pixels Changing Rate (NPCR) exist as two crucial assessment metrics to conduct analyses of differential attacks

$$\text{UACI} = \frac{1}{m*n}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right]*100\ \% \qquad (1)$$

$$\text{NPCR} = \frac{\sum_{i,j}D(i,j)}{m*n}*100\ \% \qquad (2)$$

where for the image, the height is M and the width is N, when values in C1 and C2 are similar, $D\ (i.\ j)$ = 0, and when they differ, it equals 1, accordingly, the ciphered images, before and after one pixel of the plain image is changed, are denoted through $C1(i, j)$ and $C2(i, j)$ [21].

The encryption algorithm should not be affected by minor adjustments to the original image. To verify the sensibility of the image, we changed only one pixel in the original image and encrypted the original and modified image. Tables 2 and 3 show UACI and NPCR values for both encrypted images. The resultant NPCR is near the ideal percentage of 99.6094%, and UACI is near the ideal percentage of 33.4653% [21]. These outcomes illustrate that the encryption approach used is responsive toward minor changes, resistant to differential attacks, and has an elevated degree of safety. Additionally, because the text is hidden as a block in the blockchain, it does not affect the UACI and NPCR results.

Table 2: Result of UACI

Images	Color	Proposed	ZAID et al. [22]	Osama et al. [23]
Airplane	Red	33.5536		33.38
	Green	33.5100		33.39
	Blue	33.5578		33.55
	Average	33.5405	33.55539	33.44
Barbara	Red	33.6211		33.24
	Green	33.5674		33.29
	Blue	33.5773		33.37
	Average	33.5886	33.46354	33.3
Peppers	Red	33.4312		33.54
	Green	33.6079		33.34
	Blue	33.5911		33.28
	Average	33.5434	33.83490	33.3867

Table 3: Result of NPCR

Images	Color	Proposed	Bhaskaran et al. [15]	ZAID et al. [22]	Osama et al. [23]
Airplane	Red	99.6185			99.6215
	Green	99.6429			99.6704
	Blue	99.6048			99.6536
	Average	99.6221	99.340	99.61344	99.6485
Barbara	Red	99.6262			99.5819
	Green	99.6201			99.4552
	Blue	99.6292			99.4293
	Average	99.6251	97.260	99.62158	99.4888
Peppers	Red	99.5682			99.5941
	Green	99.6216			99.6429
	Blue	99.6231			99.2492
	Average	99.6043		99.60937	99.4954

5.3 Information entropy

Entropy determines the image uniformity by quantifying image randomness, and it can be calculated for a message source (s) by the formula below:

$$\mathrm{H(s)} = \sum_{i=1}^{2^{i}-1} p(s_i)\log_2\frac{1}{p(s_i)} \qquad (3)$$

where entropy is stated in bits, while the H(s) represents the s_i character probability, and for the best encryption to be achieved, the entropy quantity must reach 8 [24].

Table 4 presents the three encrypted images' entropy.

The entropy of this image is close to the target value, indicating that the encrypted images are random. This suggests that the proposed encryption scheme can withstand statistical attacks. Moreover, because the text is hidden as a block in the blockchain, it does not affect the randomness of the encrypted image.

Table 4: Information entropy result

Images	Color	Proposed	ZAID et al. [22]	Osama et al. [23]
Airplane	Red			7.3256
	Green			7.2838
	Blue			7.1599
		7.9992	7.99904	7.2564
Barbara	Red			7.7358
	Green			7.6303
	Blue			7.5681
		7.9992	7.99910	7.6447
Peppers	Red			7.6663
	Green			7.7452
	Blue			7.1788
		7.9992	7.99890	7.5301

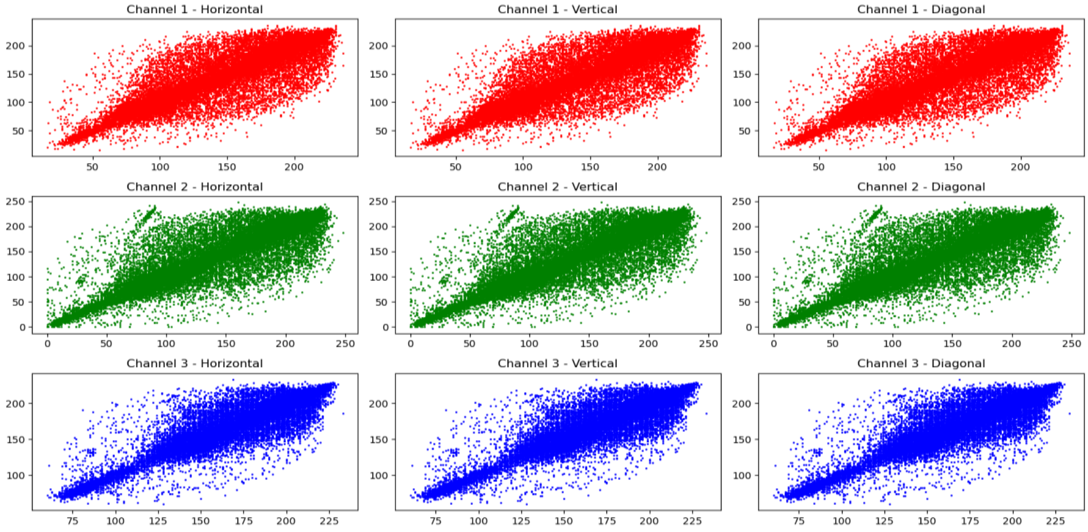
5.4 Correlation coefficient analysis

An original image regularly shows a definite degree of correlation among all two adjoining pixels, so an efficient encryption method must diminish the correlation among adjoining pixels to zero [21].

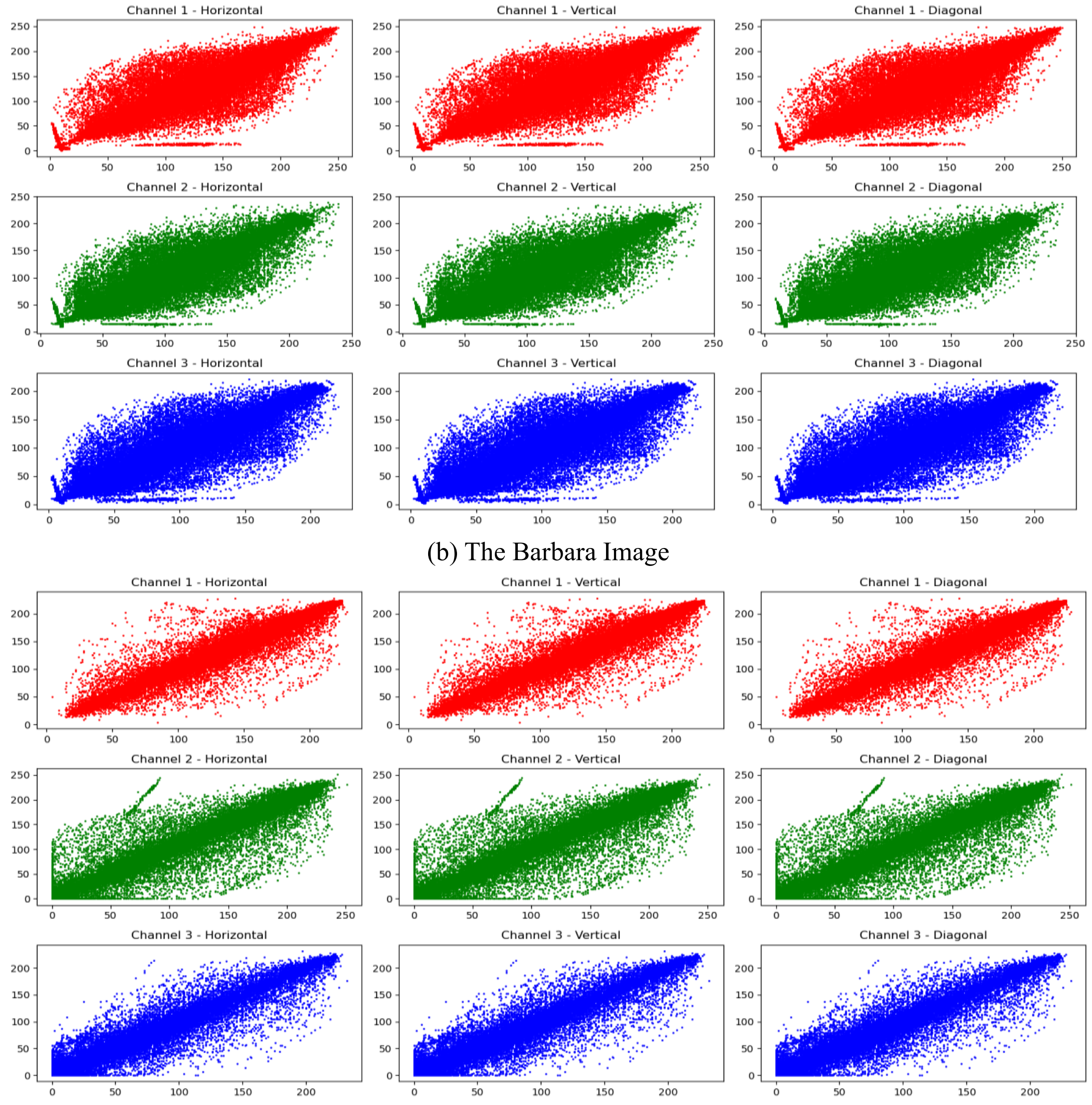
Figures 4 (a, b, and c) and 5 (a, b, and c) show the correlation coefficient of the original input image and the encrypted image. They demonstrate that the correlation coefficient is extremely elevated in the original image, while it is zero in the encrypted image, which shows a close correlation between pixels within the vertical, horizontal, and diagonal direction of the original image, this correlation becomes extremely low in encrypted images.

Table 5 (a, b, and c) presents the values for each direction for encrypted and original images. Table 6 reveals the outcomes of analyzing the correlation between encrypted and original images and the correlation between original and decrypted images. For original and decrypted images, the correlation value is 1, this means that we could recover the original image without any loss of pixels.

For the text, we used a set of sentences consisting of a set of letters and calculated the correlation between the original and encrypted text and also between the original and the decrypted text. Table 7d illustrates the text results of the correlation analysis. The result demonstrates that the zero-correlation coefficient is also satisfied, and the original text could be recovered without any loss.



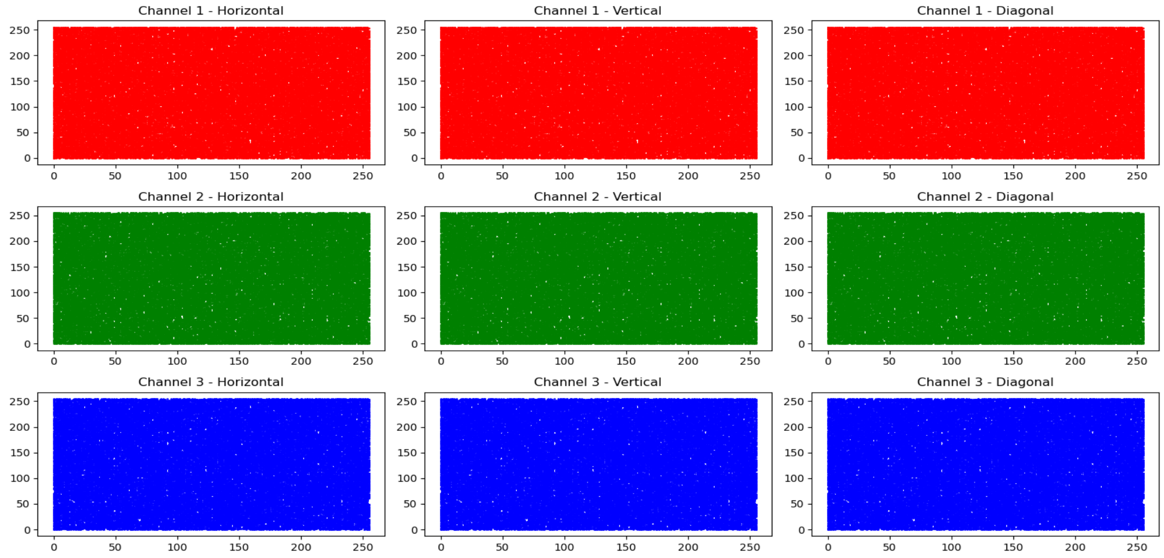
(a) The Airplane Image



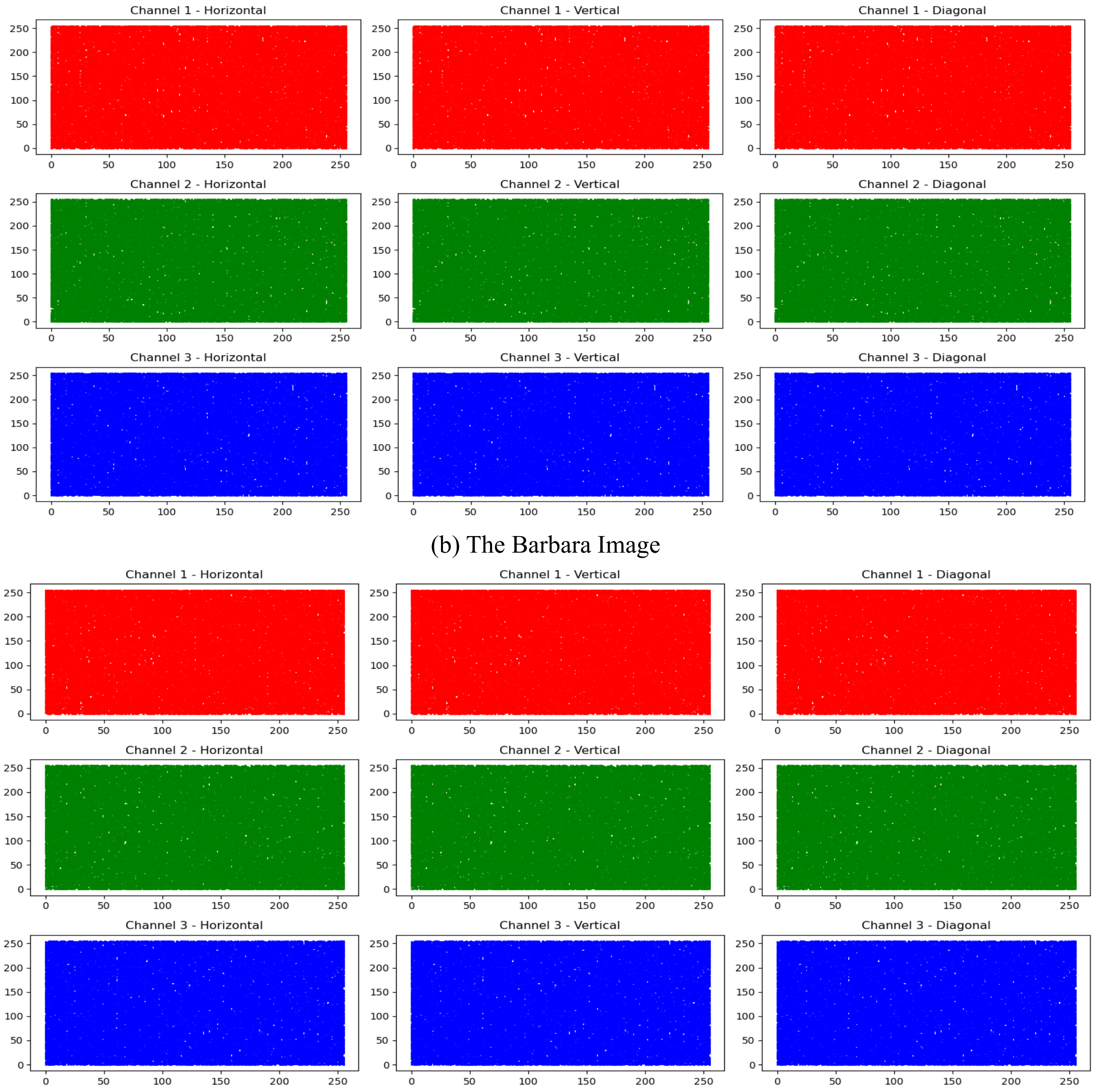
(b) The Barbara Image

(c) The Peppers Image

Figure 4: Correlation Analysis for the original image for each channel



(a) The Airplane Image



(b) The Barbara Image

(c) The Peppers Image

Figure 5: Correlation Analysis: (a) Airplane, (b) Barbara, (c) Peppers for the encrypted image for each channel

Table 5-A: Results of horizontal

Images		Horizontal			
		Red	Green	Blue	Average
Airplane	Original	0.9327	0.9220	0.9453	0.9333
	Encrypted	0.0057	0.0016	0.0004	0.0026
Barbara	Original	0.9011	0.8970	0.9125	0.9036
	Encrypted	-0.0053	0.0023	0.0014	-0.0005
Peppers	Original	0.9606	0.9670	0.9533	0.9603
	Encrypted	-0.0045	-0.0056	0.0042	-0.00196

Table 5-B: Results of vertical

Images		Vertical			
		Red	Green	Blue	Average
Airplane	Original	0.9151	0.9278	0.8983	0.9137
	Encrypted	-0.0013	0.0003	-0.0041	-0.0017
Barbara	Original	0.9445	0.9405	0.9504	0.9451

	Encrypted	0.0007	-0.0036	0.0017	-0.0004
Peppers	Original	0.9646	0.9722	0.9598	0.9655
	Encrypted	0.0015	-0.0020	0.0004	-0.00003

Table 5-C: Results of diagonal

Images		Diagonal			
		Red	Green	Blue	Average
Airplane	Original	0.8611	0.8688	0.8673	0.8657
	Encrypted	-0.0052	0.0005	0.0027	-0.0007
Barbara	Original	0.8584	0.8484	0.8718	0.8595
	Encrypted	-0.0000	0.0035	-0.0017	0.0006
Peppers	Original	0.9306	0.9416	0.9200	0.9307
	Encrypted	0.0048	-0.0026	-0.0021	0.00004

Table 6: Correlation coefficient analysis

Images		Proposed
Airplane	Original + Encrypted	-0.0004
	Original + Decrypted	1.0000
Barbara	Original + Encrypted	0.0003
	Original + Decrypted	1.0000
Peppers	Original + Encrypted	-0.0005
	Original + Decrypted	1.0000

Table 7: Correlation coefficient

Text		Proposed
Data hidden in an image	Original + Encrypted	-0.0102
	Original + Decrypted	1.0000
Image steganography	Original + Encrypted	-0.0020
	Original + Decrypted	1.0000
Message embedding	Original + Encrypted	0.0127
	Original + Decrypted	1.0000

6 Discussion

The results for UACI (%) and NPCR (%) shown in Table 2 and Table 3 are practically equal or greater than the other techniques mentioned in the related work, especially the techniques proposed by Bhaskaran et al. [15], ZAID et al. [22], and Osama et al. [23] studies that use the same images used in this study. This is also applied to the information entropy result as shown in Table 4. This demonstrates that the encrypted images are random, and this recommended encryption scheme can resist statistical attacks. The reason for that is the use of the AES algorithm with CBC mode which has the advantage of not creating identical ciphertext blocks even if the plaintext blocks are identical [17].

Additionally, the text is stored within the encrypted image blocks and not within the image pixels which might otherwise affect the quality of the image or necessitate the use of more than one image [4]. So, the text is encrypted and stored with the rest of the image blocks ensuring that there is no need to manipulate the image pixels to store the text.

Additionally, this study uses a symmetric key that is generated and stored not as an external key, but as a block within the encrypted image. This approach ensures that the key block is the same size as the other blocks, making the key undetectable.

The overhead of this encryption approach is influenced by both the size of the image and the complexity of the encryption process. While integrating blockchain adds additional computational overhead, it improves the security of encrypted images and hidden texts. Moreover, it can detect any tampering in the encrypted images, making the integration more cost-effective.

7 Conclusion

This study focuses on maintaining the integrity of hidden text through a novel steganography-based blockchain method. The approach utilizes symmetric encryption and cryptographic hash functions, yielding favorable results in image encryption. Moreover, the model ensures seamless integration of text without impacting image pixels, thus effectively meeting the imperceptibility (undetectability) requirement. Standardizing block sizes were applied to achieve this goal, resulting in 99.6221% for NPCR, 33.5886 for UACI, and 7.9992 for the entropy value. Both statistical measures and differential metrics confirm the algorithm's effectiveness. The blockchain component further ensures the detection of any tampering, as changes to blockchain transactions affect the associated hashes, thereby maintaining data integrity.

References

[1] A. Sabir, H. A. Ali, and M. A. Aljabery, "ChatGPT Tweets Sentiment Analysis Using Machine Learning and Data Classification," *Inform.*, vol. 48, no. 7, pp. 103–112, 2024, doi: 10.31449/inf.v48i7.5535.

[2] M. Takaoğlu, A. Özyavaş, N. Ajlouni, A. Alshahrani, and B. Alkasasbeh, "A novel and robust hybrid blockchain and steganography scheme," *Appl. Sci.*, vol. 11, no. 22, 2021, doi: 10.3390/app112210698.

[3] A. Jan, S. A. Parah, M. Hassan, and B. A. Malik, "Double layer security using crypto-stego techniques: a comprehensive review," *Health Technol. (Berl).*, vol. 12, no. 1, pp. 9–31, 2022, doi: 10.1007/s12553-021-00602-1.

[4] A. H. Mohsin *et al.*, "PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralized hospitals intelligence architecture," *Multimed. Tools Appl.*, vol. 80, no. 9, pp. 14137–14161, 2021, doi: 10.1007/s11042-020-10284-y.

[5] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial internet of things," *Entropy*, vol. 22, no. 2, 2020, doi: 10.3390/e22020175.

[6] A. K. Bermani, T. A. K. Murshedi, and Z. A. Abod, "A hybrid cryptography technique for data storage on cloud computing," *J. Discret. Math. Sci. Cryptogr.*, vol. 24, no. 6, pp. 1613–1624, 2021, doi: 10.1080/09720529.2020.1859799.

[7] K. Koptyra and M. R. Ogiela, "Imagechain—application of blockchain technology for images," *Sensors (Switzerland)*, vol. 21, no. 1, pp. 1–12, 2021, doi: 10.3390/s21010082.

[8] S. A. Yousiff, R. A. Muhajjar, and M. Al-Zubaidie, "Designing A Blockchain Approach to Secure Firefighting Stations Based Internet of Things," *Inform.*, vol. 47, no. 10, pp. 9–26, 2023, doi: 10.31449/INF.V47I10.5395.

[9] M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[10] M. Y. Jabarulla and H. N. Lee, "Blockchain-based distributed patient-centric image management system," *Appl. Sci.*, vol. 11, no. 1, pp. 1–20, 2021, doi: 10.3390/app11010196.

[11] P. Ms.Jahanvi, Navtej, Medini H, Mamisha, "Blockchain Technology Based Image Steganography," *Int. J. Creat. Res. Thoughts*, vol. 11, no. May, pp. 82–87, 2023.

[12] 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, 2022, doi: 10.1007/s11042-022-12617-5.

[13] J. H. Horng, C. C. Chang, G. L. Li, W. K. Lee, and S. O. Hwang, "Blockchain-Based Reversible Data Hiding for Securing Medical Images," *J. Healthc. Eng.*, vol. 2021, 2021, doi: 10.1155/2021/9943402.

[14] M. Acharya and R. S. Sharma, "A novel image encryption based on feedback carry shift register and blockchain for secure communication," *Int. J. Appl. Eng. Res.*, vol. 16, no. 6, pp. 466–477, 2021.

[15] R. Bhaskaran, R. Karuppathal, M. Karthick, J. Vijayalakshmi, S. Kadry, and Y. Nam, "Blockchain Enabled Optimal Lightweight Cryptography Based Image Encryption Technique for IIoT," *Intell. Autom. Soft Comput.*, vol. 33, no. 3, pp. 1593–1606, 2022, doi: 10.32604/iasc.2022.024902.

[16] S. Inam, S. Kanwal, R. Firdous, and F. Hajjej, "Blockchain-based medical image encryption using Arnold's cat map in a cloud environment," *Sci. Rep.*, vol. 14, no. 1, pp. 1–22, 2024, doi: 10.1038/s41598-024-56364-z.

[17] M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, "Symmetric encryption algorithms: Review and evaluation study," *Int. J. Commun. Networks Inf. Secure.*, vol. 12, no. 2, pp. 256–272, 2020.

[18] "secrets — Generate secure random numbers for managing secrets." https://docs.python.org/3/library/secrets.html (accessed Feb. 17, 2024).

[19] S. Kurnaz and M. A. H. Aljabery, "Predict the type of hearing aid of audiology patients using data mining techniques," *ACM Int. Conf. Proceeding Ser.*, pp. 2–6, 2018, doi: 10.1145/3234698.3234755.

[20] G. K. Shraida and H. A. Younis, "An Efficient Diffusion Approach for Chaos-Based Image Encryption and DNA Sequences," *Iraqi J. Electron. Electron. Eng.*, vol. 18, no. 2, pp. 69–74, 2022, doi: 10.37917/ijeee.18.2.9.

[21] Z. Man, J. Li, X. Di, and O. Bai, "An Image Segmentation Encryption Algorithm Based on Hybrid Chaotic System," *IEEE Access*, vol. 7, pp. 103047–103058, 2019, doi: 10.1109/ACCESS.2019.2931732.

[22] Z. A. Abduljabbar *et al.*, "Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map," *IEEE Access*, vol. 10, pp. 26257–26270, 2022, doi: 10.1109/ACCESS.2022.3151174.

[23] O. S. Faragallah, H. S. El-Sayed, A. Afifi, and W. El-Shafai, "Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform," *Opt. Lasers*

Eng., vol. 137, no. May 2020, 2021, doi: 10.1016/j.optlaseng.2020.106333.

[24] G. K. Shraida, H. A. Younis, T. A. Al-Amiedy, M. Anbar, H. A. Younis, and I. H. Hasbullah, “An Efficient Color-Image Encryption Method Using DNA Sequence and Chaos Cipher,” *Comput. Mater. Contin.*, vol. 75, no. 2, pp. 2641–2654, 2023, doi: 10.32604/cmc.2023.035793.