Authentication Approach for Sensitive Data in Block Chain –non -fungible token Environment based on Simon Encryption and Steganography Techniques

Zainab Hassan Katoof[1]
cs.24.14@grad.uotechnology.edu.iq

Prof. Hala Bahjat Abdul Wahab [2]
Hala.b.abdulwahab@uotechnology.edu.iq

Abstract: Due to the increasing growth of data sent and received between parties, and how to protect it and keep it safe from tampering and theft, this led to the necessity of using and innovating techniques and algorithms that enhance the security of this data, especially sensitive data. Blockchain technology provides a reliable option for transferring data, especially sensitive data, securely due to its decentralized properties. However, there is still a challenge in how to maintain it in the face of continuous digital development. Non-fungible tokens (NFTs), one of the growing uses of blockchain technology, have evolved as digital ownership certificates that safely store a variety of data on a distributed ledger, This study offered a strategy for protecting a valuable, sensitive image and prove that a certain person is the rightful owner of it, The image encrypted, and then uploaded to the interplanetary file system (IPFS), hidden within a carrier image for added security, and then stored on the blockchain. This strategy would mitigate the issue of counterfeit photographs and nefarious individuals attempting to mimic the rightful owners of images or sensitive data. The results regarding encryption and embedding, which were as follows: PNG images retained higher quality after encoding than JPEG images. (PSNR: inf dB, MSE:0.0).

Keywords: Blockchain technology, non-fungible tokens (NFTs), steganography, Encryption ,image encrypted.

[1] M.Sc. Student, Computer Sciences Department, Technology University, Baghdad

[2] Prof, Computer Sciences Department, Technology University, Baghdad, Iraq

1. Introduction

As the scope of Internet applications expands, a massive amount of data is being transferred, which, it turns, requires streamlined exchange across multiple organizations. An example of this is a medical system that needs to securely share sensitive data with a team of doctors elsewhere. This cross-border data exchange, along with enhanced ease of collaboration and data usage, poses significant challenges in the areas of data security and privacy. These challenges are particularly critical in data-sensitive sectors, such as healthcare and supply chains. Emerging technologies such as blockchain have emerged, along with the challenges they face, including interplanetary file systems and their security challenges. Addressing these challenges through the use of multi-level security has become crucial.

Blockchain technology is a collection of documents, known as blocks, linked (chained) with a unique number for each block. A block includes a cryptographic hash of the previous block, a timestamp, and transaction information [1]. Blockchain technology has emerged as a revolutionary invention for decentralizing record-keeping and transaction processing within digital networks. For example, electronic medical records using non-fungible tokens (NFTs) rely on a custom permissioned blockchain built with secret-sharing technology to reduce key management costs and provide a readable extension of the record to ensure it is easily readable and accessible from any type of computer [2]. There are also studies using blockchain to securely transfer physical election votes digitally, relying on blockchain technology. This system takes into account anticipated challenges and technical and operational considerations, enhancing transparency and integrity, and ultimately building citizens' trust in democratic systems [3].

To enhance the reliability and ownership of data, including digital photographs and sensitive information, NFT technology has developed in the technological landscape. A non-fungible token (NFT) is a digital asset stored on a blockchain characterized by unique identifying information and codes that differentiate it from other assets. NFTs can deter counterfeiting as each token possesses uniqueness attributed to the owner's digital signature. [4]

data security has become a fundamental necessity. Through networks like the internet, several entities can communicate with one another. As a result, secure connection must be provided. One way to prevent unwanted access to data is encryption [5]. The Simon cipher is a lightweight cryptographic algorithm that balances security, performance, and cost in contexts with limited resources [6].

The internet regulates every aspect of life, making cutting-edge security mechanisms indispensable for confidential communication. Because of this, steganography, the art and science of concealing information from people who should not have access to it, has gained a lot of attention lately [7].

The research proposes a new approach that relies on block encryption capabilities to increase the security of sensitive data in a blockchain environment. We take multiple security steps to ensure that sensitive data is not compromised during transmission.

2. Research Gap

Although recent research that integrates encryption, anonymization, and non-fungible tokens (NFTs) has made significant progress [8,13], there are still numerous research gaps to be addressed. First, most approaches are limited to certain platforms or data types, e.g., Solana-specific solutions or 2D image NFTs, and thus cannot be used on other blockchain platforms and multimedia types. Second, existing approaches primarily address data protection, which is not enough to defend against larger attacks such as Sybil attacks, denial-of-service attacks, and large-scale hacking attacks. The implementation of OTP keys necessitates stringent key management protocols, potentially complicating their practical application.

The challenges of scalability in networks like Ethereum, together with the complexities of smart contracts and decentralized storage solutions such as IPFS, remain substantial obstacles to widespread adoption.

3. Related Work

There are studies that have researched and presented methods in this field and combined techniques, for example in [8] The authors suggest using NFT data that can't be changed as a safe point of reference and information hiding techniques to hide sensitive data in NFT data that can be changed, This guarantees data integrity and regulated access **,**There is also a lot of research addressed topics encryption, steganography ,and (NFT)technologies, for example in the following article. In [9] presents a security-enhanced NFT transaction scheme integrating compression, encryption, and steganography, It uses chaotic color multi-image compression to combine and encrypt several images, then uses a better multi-cover LSB steganography method to hide them in 3D models, This method makes encryption, steganography, and attack resistance better, and it lets you hide 2D NFT images in 3D models to make them even safer. The method ensures robustness against noise, cutting, and statistical threats, making NFT handling more secure and efficient. In another [10] This research combines conventional steganography with deep learning to improve NFT security against cybercrime. Notwithstanding authentication protocols, NFTs continue to be susceptible to theft and deception. The suggested method combines crypto-steganography with deep learning to improve authentication. This makes sure that creating, validating, and predicting the price of NFTs are all safe. It focuses on establishing a robust, user-friendly NFT minting platform that smoothly integrates with blockchain technology, employing deep learning to combat data theft in NFT marketplaces. in [11] The document offers a self-defense copyright protection strategy (SDCP-IE) for NFT image art by inserting imperceptible ownership information into digital images prior to minting. This guarantees that even if an illegal entity mints an NFT, the original creator can retrieve the contained information to substantiate ownership. The approach utilizes adversarial perturbations and a binary quantization network to improve security while preserving image quality. in [12] A method is suggested that is hard to find using stealth analysis tools: hide the encrypted image after encrypting it with the (OTP) algorithm on the blockchain. The Solana platform was chosen for the demonstration of the proposed method, and a hidden image was downloaded from a chosen cover image to hide the data. This image was then made public as (stego-nft). We complete the data transfer process by extracting the hidden data and then burning the transferred NFT.

Authors in [13] propose a novel approach to enhance the security of Aadhar cards generated by the unique identification authority of India (UIDAI) using blockchain technology implemented with steganography. Here we use steganographic techniques to embed a certain immutable, encrypted secret image on the pre-existing Aadhar card template with the Aadhar data that is collected while first issuing the card to produce a new “Steg-Aadhar” (steganographic Aadhar) which can then be converted into an NFT which will be uploaded onto the IPFS for storage. On doing so, a unique identifier, content identifier (CID) is generated which can be used to verify the Aadhar card later on. This method will help tackle the issues of fake Aadhar cards and malicious people trying to impersonate Aadhar individuals thus ensuring the smooth implementation of banking and government welfare schemes for the masses.

In Table (1) illustrated the studies provided cover various aspects. These works focused on enhancing the security of NFTs using various approaches. All of these studies seek to enhance the security and reliability of NFTs against cyber-attacks and breaches.

Table 1: Illustrated previous studies

Ref	Year	Methodes/work	Advantage	Limitation
[6]	2024	to encrypted and Used One time pad(OTP) and used AES(advanced encryption standard(LSB(least scnificant Bit) and DCT(discrete cosine transfer) DWT(discrete wavelet transfer)	The (OTP) algorithm provides data integrity during transfer, and (LSB) provides almost acceptable visual quality SSIM = 0.99, PSNR > 85), JPEGs affecting imperceptibility in contrast to PNGs.	The use of big data had the effect of increasing execution times and reducing incomprehension. Password complexity and encryption type had little effect on visual quality and performance.
[7]	2023	Utilized A sequence of chaotic patterns is generated through the iteration of a chaotic map, while compression sensing (CS) is employed to compress several secret images and amalgamate the compressed images into a singular large secret image. Subsequently, this secret image is encrypted and concealed within multiple cover images using steganography.	The devised technique possesses a suitably expansive key space and steganographic capacity, while simultaneously demonstrating commendable performance regarding reconstruction efficacy, resilience against statistical assaults, resistance to differential attacks, and overall robustness.	When numerous photos with inconsistent dimensions are amalgamated into a single huge image, the quality of the compressed reconstructed image is slightly compromised. The running time constitutes a significant portion of the overall duration of the entire scheme.
[9]	2024	The defensive mechanism is In advance NFT/used SDCP-IE, the original author or authorized publisher	1. Making hidden data safer, since adversarial perturbations used offer a lot of protection against	Due to the utilization of deep learning models such as SR Net, substantial processing power is necessitated for both

		can incorporate the copyright information into the published digital image art without compromising its visual impact.	being found. 2. Do not substantially diminish the visual quality.	training and testing.

4. lightweight Block Cipher Algorithms

Lightweight block ciphers are symmetric-key algorithms optimized to operate under severe resource constraints; they provide confidentiality with small memory, low power, and reduced area requirements in hardware implementations. When a block of plain text is used to create a cipher text block of the same length, it is referred to as a block cipher. most common block sizes are 64 or 128 bits [14]. The NSA developed the Simon cipher in 2013 as a lightweight block cipher used to encrypt data in fixed-size blocks [15]. Characteristics of the Simon Cipher Algorithm Key include lightweight design and minimized computational complexity using simple bitwise operations (XOR, AND, and circular shifts) instead of complex S-boxes, thus providing good security while being efficient on micro-controllers and low-power devices [16,17]. It offers effective encryption with minimal energy and computational needs, which makes it appropriate for protecting online identities in environments with constrained resources [18]. Figure 1 shows a diagram of Simon's algorithm.

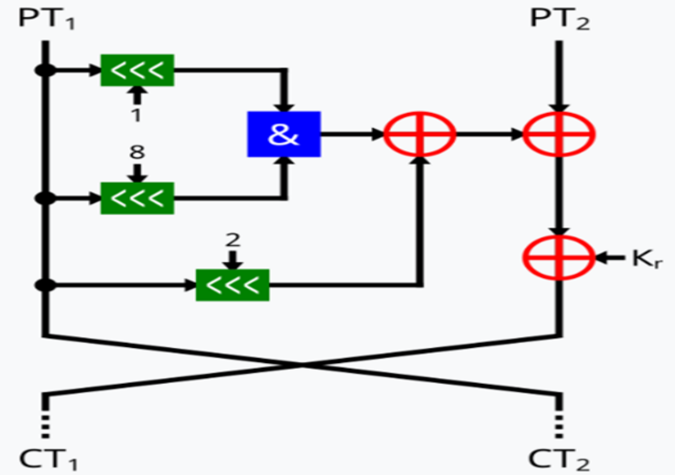


Figure 1: Simon diagram

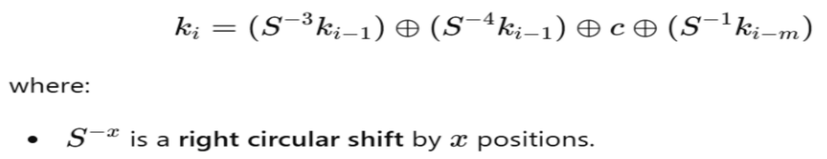
4.1 Simon Cipher Algorithm [19]

1. Initialization

- Choose **block size (n)** and **key size (m × n)**.
- Define the number of **rounds (T)** based on the block size:
  - 32-bit: 32 rounds
  - 48-bit: 36 rounds
  - 64-bit: 42 rounds
  - 96-bit: 52 rounds
  - 128-bit: 68 rounds

2. Key Expansion

- Split the key into **m words** of **n/2 bits each**.
- Generate **T round keys** using the formula:



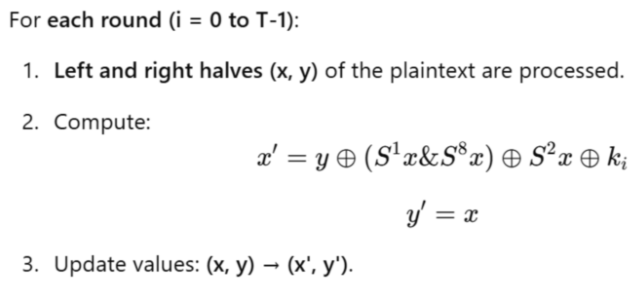
$$k_i = (S^{-3}k_{i-1}) \oplus (S^{-4}k_{i-1}) \oplus c \oplus (S^{-1}k_{i-m})$$

where:

- S^{-x} is a **right circular shift** by x positions.

  - c is a constant (0xFFFFFFFFFFFFFFFC).
  - m is the number of key words.

3. Encryption Process



For **each round** (**i = 0 to T-1**):

1. **Left and right halves** (**x, y**) of the plaintext are processed.
2. Compute:

$$x' = y \oplus (S^1x \& S^8x) \oplus S^2x \oplus k_i$$

$$y' = x$$

3. Update values: **(x, y) → (x', y')**.

4. Decryption Process

- Perform the encryption steps **in reverse order**, applying the **round keys in reverse**.

5. Output

- After all rounds, **(x, y)** represents the encrypted (ciphertext) or decrypted (plaintext) value.

5. Interplanetary File System (IPFS)

The goal of the Interplanetary File System (IPFS) project is to create a completely decentralized platform for the storing and retrieval of content-addressable media objects. IPFS is a community-driven, open-source initiative essential for fostering community engagement and establishing an open platform for design innovation [20].

IPFS is a basis for many other Decentralized Web apps, such as social networking and discussion platforms (Discussify, Matters News), data storage solutions (Space, Peergos, Temporal), content search (Almonit, Deece), messaging (Berty), content streaming (Audius, Watchit), and e-commerce (Ethlance, dClimate). This indicates confirmed ownership of a unique digital or physical item on the blockchain [21].

Additionally, IPFS access has been incorporated into popular browsers like Opera and Brave, facilitating its easy and broad adoption. [21].

The principal characteristics of IPFS comprise:

1- Each file is distinctly identifiable by its content hash, guaranteeing data integrity and enabling rapid retrieval.

2- A decentralized network of nodes enables direct file sharing without reliance on centralized
servers.

3- Facilitates file versioning and enables users to monitor changes over time.

4- IPFS interacts effortlessly with decentralized applications (dApps), providing a resilient storage layer for blockchain and Web3 ecosystems.

6. Proposed approach

Sensitive data Although blockchain has features, the user doesn't want to reveal his data, so we suggested encrypting it with Simon. Then we upload the encrypted image to IPFS. IPFS is a decentralized file storage system that uses content addressing to ensure data integrity using a unique content hash. Then we get the CID to generate an NFT containing the CID data. Then we hide the NFT data inside a cover image using LSB technology. Then we store the carrier image in the blockchain. Then we can retrieve the carrier image from the blockchain and then decrypt it.

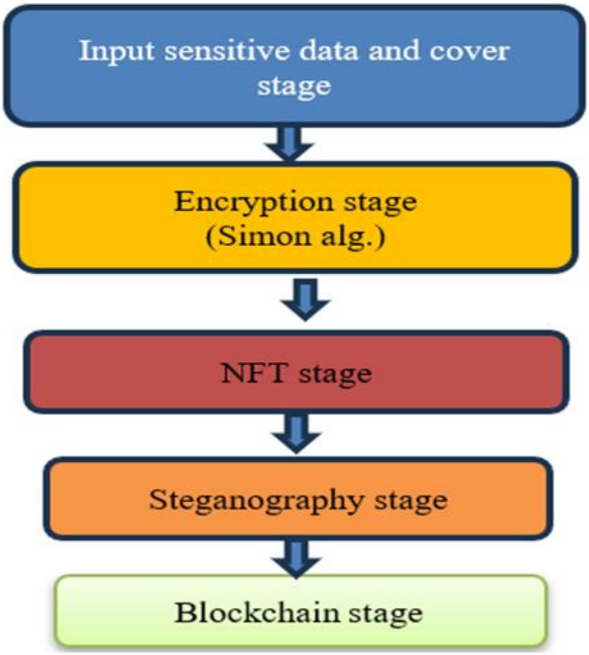
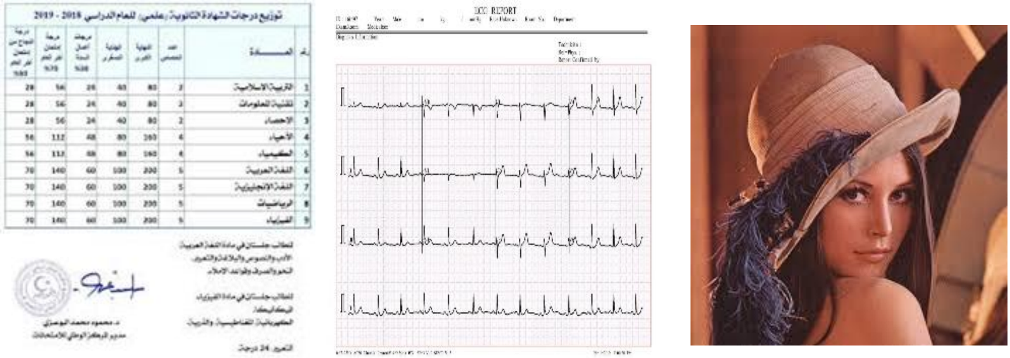

Input sensitive data and cover stage
Encryption stage (Simon alg.)
NFT stage
Steganography stage
Blockchain stage

Figure 2: Stages of the proposed system

The details of the five main stages reference Improve NFT-blockchain and IPFS environment for sensitive data are as follows:

Stage 1: Input sensitive data and cover stage

The user here needs to enter sensitive data from his point of view, and depending on the type of application that will be applied, for example, the possibility of using (personal photos - medical examination - a photo of Estate) Depending on the user's decision; all these data are considered sensitive data. Examples of this are shown in Figure 3.



توزيع درجات الشهادة الثانوية (علمي) للعام الدراسي 2018 - 2019

رقم	المادة	عدد الحصص	النهاية الكبرى	النهاية الصغرى	درجة أعمال السنة %30	درجة امتحان آخر العام %70	درجة النجاح من امتحان آخر العام %50
1	التربية الاسلامية	2	80	40	24	56	28
2	تقنية المعلومات	2	80	40	24	56	28
3	الاحصاء	2	80	40	24	56	28
4	الأحياء	4	160	80	48	112	56
5	الكيمياء	4	160	80	48	112	56
6	اللغة العربية	5	200	100	60	140	70
7	اللغة الانجليزية	5	200	100	60	140	70
8	الرياضيات	5	200	100	60	140	70
9	الفيزياء	5	200	100	60	140	70

للطالب جلستان في مادة اللغة العربية
الأدب والنصوص والبلاغة والتعبير
النحو والصرف وقواعد الإملاء

للطالب جلستان في مادة الفيزياء
الميكانيكا
الكهربائية المغناطيسية والذرية

التعبير 24 درجة

د. محمود محمد [illegible]
مدير المركز الوطني للامتحانات

(a) (b) (c)

Figure 3: Sensitive data types (a) Degree image; (b) medical image; (c)personal image

Stage 2: Encryption stage

This section is dedicated to describing the encryption by using Simon algorithm, which consists of four main components, each of which performs a specific function in the encryption process. The encryption uses parameters such as block size and key size. The method is responsible for splitting the master key into multiple 16-bit words and generating round keys using the SIMON key scheduling algorithm. These round keys are essential for secure encryption and decryption. The method applies SIMON encryption to 64-bit plaintext using a Feistel-like structure over 44 rounds. Each round modifies the data using bitwise operations and round keys to ensure confidentiality. The images that the user selects after reading them enter this stage, and according to his/her choice of image, the following Figure 4, shows Sensitive data may include personal photos, medical images, or grades, it also demonstrates how to convert sensitive images into an encrypted image using the Simon algorithm.

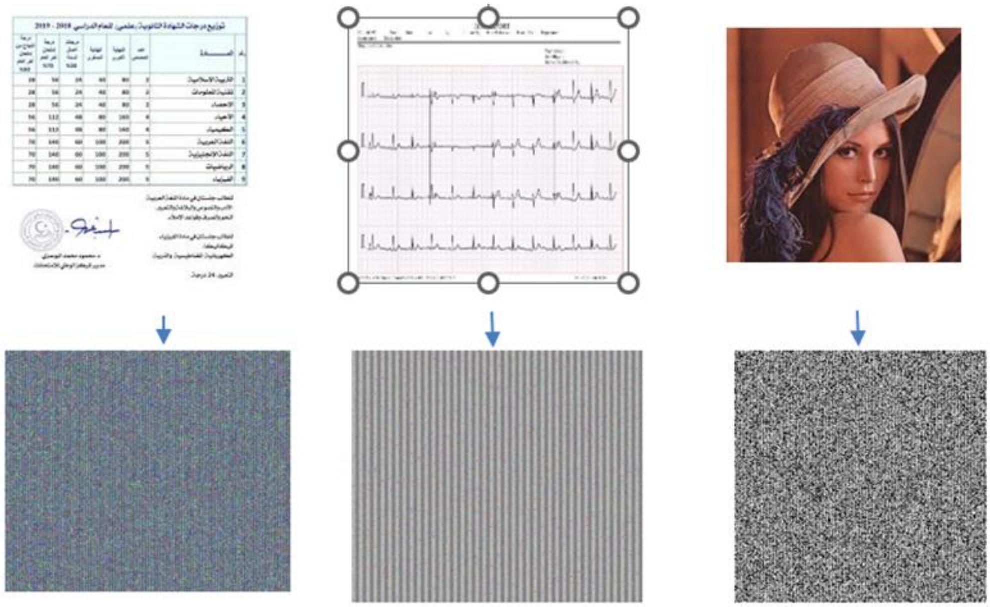


Figure 4: Encryption of sensitive images

Stage 3: Non-Fungible Token (NFT)

In this stage, the image is uploaded to the IPFS file system after being encrypted in the previous stage to obtain a content identifier (CID) and create a non-fungible token (NFT). Files are stored in the IPFS file system across a distributed network, and each file is assigned a unique identifier known as a content identifier (CID), which is derived using a hash algorithm such as SHA-256. This ensures that any modification to the file results in a change to the CID. When a sensitive image (such as a selfie) is uploaded to the IPFS file system via tools like Pinata, a series of important steps are automatically implemented to ensure data security and integrity. These steps include:

1. Splitting the file into parts:

The file is not stored as a single part, but rather divided into small, fixed-sized parts.

2. Creating a hash for each part:

A hash value is calculated for each part, forming a unique digital fingerprint.

3- Building a hierarchical structure using a Directed Acyclic Merkle Graph:

The parts are connected via a Directed Acyclic Merkle Graph (DAG), a directed acyclic graph structure where each part of the file is represented as a node containing its hash value, and all root nodes are linked to represent the entire file. The file previously stored on IPFS (encrypted data) is converted into CID, after that creates unique digital token known as an NFT (non-fungible token), a JSON file is created containing descriptive information about the token. JavaScript Object Notation (JSON) is a lightweight, text-based, language-independent data exchange format. It is derived from the ECMAScript programming language and is used to represent structured data as human-readable text, such as:

- Token_ID: - Unique code to NFT.
- CID: -Content ID of the file on IPFS.
- Name: - Name of image or artwork.
- Description: - Brief description.
- Creator: - Name of the token creator or owner.
- Timestamp: -Creation time.

These steps are explained according to the following algorithm (1).

```
Algorithm (3.1) NFT generation
Input: Encrypted image
Step1 : calculate CID to encrypted image
 Step2: Create a metadata dictionary with the following fields:-
    • token_id:-current blockchain length.
    • CID :- content identifier.
    • name: -name of NFT
    • description: -textual description
    • creator: -creator's name
    • time stamp: - current date and time as string
Output: Metadata for NFT
```

Stage 4: Steganography stage

This stage is an important security step in the crypto system, where the NFT data (containing the CID and information associated with the original image) as A JSON is hidden inside a cover image using a technique called steganography, specifically using the LSB (Least Significant Bit) algorithm. The main goal is to hide NFT data in a visually indistinguishable way within a natural-looking image, protect proprietary data and content from tampering or spying, and ensure that only the user who owns the cover image can extract NFT data from it later.

Stage 5: Blockchain stage

After hiding NFT data (such as CID and metadata) within a cover image using the LSB stego algorithm, the resulting image (called a stego-image) is stored within the blockchain. This means that the system not only hides the data but also records the stego-image within the blockchain to ensure traceability, verification, and tamper-proof protection

1-Encrypt the Secret Image by Using Simon Cipher

Inputs: secret image, Encryption key,
Output: The encrypted image is saved as (encrypted_image.png)

- Steps:
  1- Open the image and convert it into byte data.
  2- Apply padding to make data length compatible for encryption.
  3- Divide the data into 8-byte blocks.
  4- Encrypt each block using Simon Cipher.

2- Upload the Encrypted Image to IPFS

Inputs: The encrypted image.
Output: The encrypted image is stored on IPFS, and the CID is returned
Steps:

1. Send an API request to Pinata to upload the image to IPFS.
2. Extract the CID (Content Identifier) .
3. Return the CID for later use.

3- Create an NFT for Encrypted Image

Inputs: CID of the image, NFT name and description ,Creator details, Blockchain. Output: A new NFT has been created containing the encrypted image details
Steps:

1- Determine the NFT Token ID based on the number of blocks in the blockchain.
2- Create NFT metadata in JSON format, including CID, name, and description.

4 -Hide NFT Metadata Inside a Cover Image

Inputs: the cover image, NFT metadata
Output: A cover image containing hidden NFT metadata
Steps:

1. Convert NFT metadata into a JSON string.
2. Hide the metadata inside the cover image using Stegano.
3. Save the new stego-image.

5-Store the Stego Cover Image in Blockchain

- Inputs: Blockchain, the stego-image. Output: The stego-image is stored in the blockchain.
- Steps:
  1- Read the cover image data and convert it to hexadecimal format.
  2- Add the cover image data to the blockchain.
  3- The stego-image is stored in the blockchain

7. Implementation and Experimental Results

The procedures required to implement the approach will be outlined, first with the acquisition of a sensitive image, followed by its encryption, and then continuing through the subsequent stages detailed in the suggested method.

Let’s take image (3) and show the encryption and decryption process demonstrated in Figure 5. We will use the plain images Lenna 225*225, ECG image 909*1280, and Degree 208*242. The results of all tests are color images.

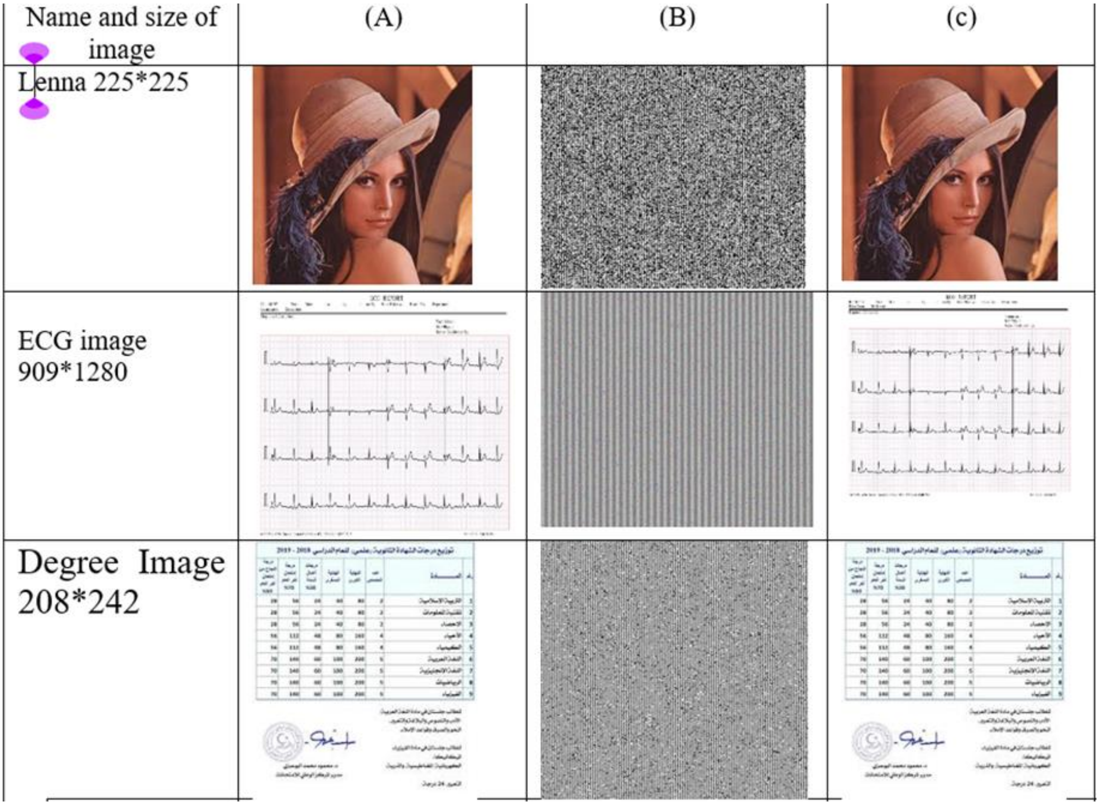


Figure 5: A) sensitive image; B) encrypted image; and C) decrypted image

7.1 Picture Quality Evaluation (PQE) Metrics

The Picture Quality Assessment (PQE) must be used for displaying experimental, encoded, decoded image quality measurements, as shown below with our images in Table 2, A low SSIM and a Correlation close to zero or negative means that the encryption is strong (i.e., the cipher image does not retain a clear structure from the original).

Table 2: PQE Metrics for the difference between the original image and encrypted image

Name and size of image	MSE	PSNR	SSIM	correlation	TIME Second
Lenna 225*225	104.43	27.94	0.0088	-0.0059	2.1589
ECG image 909*1280	83.64	28.91	0.0237	0.0009	50.2383
Degree image 208*242	84.77	28.85	0.0146	-0.0006	0.6526

In the above table, a low SSIM and a correlation close to zero or negative mean that the encryption is strong (i.e., the cipher image does not retain a clear structure from the original).

Table (3) PQE Metrics between the original image and decrypted image

Name	MSE	PSNR	SSIM	Correlation
Lenna 225*225	0.00	Inf dB	1.0000	1.0000
ECG image 909*1280	0.00	Inf dB	1.0000	1.0000
Degree image 900*1346	0.00	Inf dB	1.0000	1.0000

The efficacy of the restored images post-algorithm application was assessed utilizing four principal metrics: mean square error (MSE), peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), and correlation coefficient. The results exhibited a high degree of accuracy in reconstructing the original images across all evaluated samples. The MSE value for all photos was zero (0.00), signifying no disparity between the original and recovered images at the pixel level, showing that all pixel color values remained constant without any variation. Given that MSE = 0, the PSNR value was infinite (∞ dB), indicating the utmost quality achievable in lossless image processing. The SSIM index always got a perfect score of 1.0000, which means that the restored images were exactly the same as the originals in terms of structure, brightness, contrast, and overall look. This outstanding match is rare and shows that the way masking and retrieving are done does not harm the data (lossless).

If the correlation coefficient is 1.0000, it means that the original and restored pictures were perfectly linearly linked. This shows that the changes did not change what was in the picture. Based on the above, it is evident that the suggested method is a superior approach to keep the quality of images after they have been hidden or encrypted. This makes it ideal for jobs that need to be very precise and keep things confidential without damaging the source material.

7.2 Comparison between using PNG image and JPEG image in SIMON encoding

Table 4: Illustrates Comparison Between (JPEG & PNG)

Measures	Encrypted (PNG)	Encrypted (JPEG)
PSNR	∞ - 30.07	30.67 - 27.99
MSE	0.0-64.0	55.68 - 103.11
SSIM	1.0 - 0.79	0.446 – (-0.0007)
Correlation	1.0- 0.98	0.803 – (-0.068)

The results above indicate that PNG images perform significantly better in encryption and decryption compared to JPEG images.

Steganography Stage:

The cutting-edge security mechanism is indispensable for confidential communication in every walk of life that is regulated by the internet. Therefore, steganography, which is one of the arts and sciences of concealing information from unauthorized access, has acquired a lot of consideration, recently [22].

This section concentrates on assessing the efficacy of steganography. The aim is to evaluate the measures implemented to safeguard sensitive data linked to particular users. This analysis assists in evaluating the dependability and robustness of the method in safeguarding confidential information.

Table 5: illustrate comparison

Original Image	Comparison	
	Original Image & Retrieved Image	Cover Image Before and After Hiding
	MSE: 0.00 PSNR: inf dB SSE: 0.00 SME: 0.00 Correlation: 1.0000	MSE: 0.20 PSNR: 55.07 dB SSE: 164064.00 SME: 0.45 Correlation: 1.0000

Comparison of the Original Image with the Retrieved Image ,When MSE is zero, PSNR becomes infinite, which means that the retrieved image is exactly identical to the original ,and where SSE=0.00 There is no cumulative error between the two images, confirming that the retrieved image is a perfect match, SME =0.00 No difference is detected between the two images when analyzing pixel values, **Correlation = 1.0000** ,A value of **1.0000** means that the retrieved image is completely identical to the original, confirming that the process preserved all details accurately .This mean The hiding process did not introduce any noise into the hidden image, and the retrieved image was restored without any loss in quality.

Comparison of the Cover Image Before and After Hiding, when **MSE = 0.20** A very small difference between the original cover image and the modified cover image, indicating minimal alterations, **PSNR = 55.07 dB** A very high value, which means that the difference between the original and modified images is extremely small and not visible to the human eye, **SSE = 164064.00** The cumulative sum of pixel differences, which is relatively small considering the image size , An image with a size of 900 x 900 pixels is considered large, **SME = 0.45** The difference between images is minimal but present, confirming that the hiding process slightly modified the image, **Correlation = 1.0000** The modified cover image is almost identical to the original, indicating that the process was highly efficient with minimal distortion.

8. Blockchain and NFT Environments.

Blockchain technology and NFTs (Non-Fungible Tokens) are closely linked, but they serve different purposes. Blockchain is the foundation of decentralized transactions and data security, while NFTs are unique digital assets that exist on the blockchain, proving ownership and authenticity. Below is a detailed comparison of the two concepts. In Table 6, it is shown that Blockchain technology and NFTs are interconnected but serve different purposes. Blockchain provides a secure and immutable ledger for transactions, while NFTs utilize blockchain to prove ownership and authenticity of unique digital or physical assets.

Table 6: compare between Blockchain –NFT

Feature	**Blockchain**	**NFT (Non-Fungible Token)**
Fungibility	On the blockchain, cryptocurrencies like Ethereum and Bitcoin are fungible, or interchangeable.	Each NFT token is distinct and cannot be substituted since they are non-fungible.
Use Case	Smart contracts, decentralized apps (dApps), and safe transactions all use it.	used for identity verification, digital art, virtual assets, collectibles, and real estate.
Structure	consists of an immutable ledger made up of blocks with transaction data.	blockchain-based coin containing distinct metadata, such as Ethereum or Solana.
Ownership	Transactions are recorded, but they don't indicate exclusive ownership of digital goods.	Denotes authenticated ownership of a distinct digital or physical asset on the blockchain.

9. Conclusion

The exchange of secure and confidential data has received much attention from researchers; the proposed solutions still suffer from practical complexities or insecure mechanisms. The proposed approach successfully integrates three essential components of digital security: information hiding, lightweight block encryption (Simon's algorithm), and non-fungible tokens (NFTs) within a decentralized blockchain framework with the distributed file system IPFS. Experiments have shown that this integration maintains data security and privacy, while maintaining high image quality after encryption and information hiding. PNGs had much higher PSNR and SSIM values and much lower MSE values than JPEG images. The results also showed that the recovered image was exactly the same as the original (MSE = 0, PSNR → ∞). This means that the model can do lossless steganography without changing how things look. Also, using IPFS helped provide each file a unique ID, which made it easier to track and verify digital ownership through NFT technology without slowing down the system.

10. References:

[1] Shareef, Sarah Mohammed and Hassan, Rehab Flaih (2025) "Enhancing Cybersecurity based on Blockchain Technology: A Systematic Review," Journal of Soft Computing and Computer Applications: Vol. 2: Iss. 1, Article 1015. DOI: https://doi.org/10.70403/3008-1084.1015 .

[2] Mohammed, M. A., & Abdul Wahab, H. B. (2023). A Novel Approach for Electronic Medical Records Based on NFT-EMR. International Journal of Online & Biomedical Engineering, 19(5).

[3] Mohammed, Mohanad A. and Wahab, Hala B. Abdul (2025) "Blockchain-based Physical Election Votes Digitally Secure Transfer," Journal of Soft Computing and Computer Applications: Vol. 2: Iss. 1, Article 1018.

[4] Taherdoost, H. (2022). Non-fungible tokens (NFT): A systematic review. Information, 14(1), 26.

[5] Rana M. Zaki, Zaed S. Mahdi,and Matheel E. Abdulmunim "Survey: A Study on Image Encryption Using DNA in Bioinformatics" Journal of Soft Computing and Computer Applications" DOI: https://doi.org/10.70403/3008-1084.1013

[6] Neve, R. P., & Bansode, R. (2024). Attack Analysis on Hybrid-SIMON-SPECKey Lightweight Cryptographic Algorithm for IoT Applications. *Indian Journal of Science and Technology*, *17*(10), 932-940.

[7] Rahman, S., Uddin, J., Zakarya, M., Hussain, H., Khan, A. A., Ahmed, A., & Haleem, M. (2023). A comprehensive study of digital image steganographic techniques. *IEEE Access*, *11*,

[8] Al-Sumaidaee, G., & Žilić, Ž. (2024). Sensing data concealment in nfts: A steganographic model for confidential cross-border information exchange. *Sensors*, *24*(4), 1264.

[9] Zhang, Z., Cao, Y., Jahanshahi, H., & Mou, J. (2023). Chaotic color multi-image compression-encryption/LSB data type steganography scheme for NFT transaction security. *Journal of King Saud University-Computer and Information Sciences*, *35*(10), 101839

[10] Divya, N., Dhawan, E., Sundar, H. S., Jain, H., & Dinakar, R. (2024, March). NFTGenesis-An NFT Generation and Authentication System with Market Intelligence Using Deep Learning Based Steganography. In *2024 IEEE International Conference on Contemporary Computing and Communications (InC4)* (Vol. 1, pp

[11] Wang, F., Fu, Z., & Zhang, X. (2024). A Self-Defense Copyright Protection Scheme for NFT Image Art Based on Information Embedding. ACM Transactions on Multimedia Computing, Communications and Applications, 21(2), 1-23.

[12] Takaoğlu, M., Takaoğlu, F., & Dursun, T. (2023, July). NBS: An NFT-Based Blockchain Steganography Method. In *International Conference on Computing, Intelligence and Data Analytics* (pp. 192-201). Cham: Springer Nature

[13] Vivek, S., & Kamath, B. S. (2022, December). Enhancing the Security of Aadhar Cards using Blockchain and Steganography. In *2022 International Conference on Artificial Intelligence and Data Engineering (AIDE)* (pp. 177-181). IEEE.

[14] William Stallings, (2006) Cryptography and Network Security: Principles and Practice, ISBN 978-0-13-670722-6, published by Pearson Education © 2020.

[15] Hiba, B., & Abderrahim, A. (2024). Design of a new DNA Encryption Algorithm based on Simon Algorithm. Procedia Computer Science, 238, 428-435.

[16] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015, June). The SIMON and SPECK lightweight block ciphers. In Proceedings of the 52nd annual design automation conference (pp. 1-6).16).

[17] Susanti,B.H., Permana, O.J.,Amiruddin, 2021.RobustnessTest ofSIMON-32, SPECK-32, andSIMECK-32AlgorithmsUsing Fixed-PointAttacks.J.Phys.: Conf.Ser.1836,012006.

[18] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 2013;29(7):1645-1660. DOI: 10.1016/j.future.2013.01.010.

[19] Trautwein, D., Raman, A., Tyson, G., Castro, I., Scott, W., Schubotz, M., ... & Psaras, Y. (2022, August). Design and evaluation of IPFS: a storage layer for the decentralized web. In *Proceedings of the ACM SIGCOMM 2022 Conference* (pp. 739-752).

[20] https://en.wikipedia.org/wiki/InterPlanetary_File_Syste

نهج المصادقة للبيانات الحساسة في بيئة الرموز غير القابلة للاستبدال في سلسلة الكتل استنادًا إلى تقنيات التشفيرسايمون والتخفي

أ. د . هالة بهجت عبد الوهاب[2]
Hala.b.abdulwahab@uotechnology.edu.iq

زينب حسن كطوف[1]
cs.24.14@grad.uotechnology.edu.iq

المستلخص: نظرًا للنمو المتزايد للبيانات المرسلة والمستلمة بين الأطراف، وكيفية حمايتها والحفاظ عليها آمنة من العبث والسرقة، أدى ذلك إلى ضرورة استخدام وابتكار تقنيات وخوارزميات تعزز أمن هذه البيانات، وخاصة البيانات الحساسة. توفر تقنية البلوك تشين خيارًا موثوقًا به لنقل البيانات، وخاصة البيانات الحساسة، بشكل آمن نظرًا لخصائصها اللامركزية. ومع ذلك، لا يزال هناك تحدٍ في كيفية الحفاظ عليها في مواجهة التطور الرقمي المستمر. تطورت الرموز غير القابلة للاستبدال (NFTs)، وهي أحد الاستخدامات المتزايدة لتقنية البلوك تشين، كشهادات ملكية رقمية تخزن مجموعة متنوعة من البيانات بأمان على دفتر أستاذ موزع. قدمت هذه الدراسة استراتيجية لحماية صورة قيمة وحساسة وإثبات أن شخصًا معينًا هو المالك الشرعي لها. يتم تشفير الصورة، ثم تحميلها إلى نظام الملفات بين الكواكب (IPFS)، وإخفاؤها داخل صورة ناقلة لمزيد من الأمان، ثم تخزينها على البلوك تشين. من شأن هذه الاستراتيجية أن تُخفف من مشكلة الصور المزيفة والأفراد المُضللين الذين يحاولون تقليد المالكين الشرعيين للصور أو البيانات الحساسة. وكانت النتائج المتعلقة بالتشفير والتضمين، والتي كانت كما يلي: حافظت صور PNG على جودة أعلى بعد التشفير مُقارنةً بصور JPEG. (PSNR: inf dB, MSE: 0.0).

الكلمات المفتاحية: تقنية Blockchain، الرموز غير القابلة للاستبدال (NFTs)، التخفي، التشفير، الصورة المشفرة.

[1] طالبة ماجستير؛ قسم علوم الحاسوب – الجامعة التكنولوجيا– بغداد - العراق

[2] الدكتورة: قسم علوم الحاسوب – الجامعة التكنولوجيا– بغداد - العراق