Sensing Data Concealment in NFTs: A Steganographic Model for Confidential Cross-Border Information Exchange

Ghassan Al-Sumaidaee * and Zeljko Zilic

Posted Date: 26 December 2023

doi: 10.20944/preprints202312.1891.v1

Keywords: NFTs; Blockchain; Steganography; Sensors

Article

Sensing Data Concealment in NFTs: A Steganographic Model for Confidential Cross-Border Information Exchange

Ghassan Al-Sumaidaee, Željko Žilić *

Department of Electrical and Computer Engineering, McGill University, Montréal, QC, Canada; ghassan.al-sumaidaee@mail.mcgill.ca

* Correspondence: zeljko.zilic@mcgill.ca

Abstract: In an era dominated by rapid digitalization of sensed data, the secure exchange of sensitive information poses a critical challenge across various sectors. Established techniques, particularly in emerging technologies like the Internet of Things (IoT), grapple with inherent risks in ensuring the confidentiality and integrity of transmitted data. Blockchain technology, known for its decentralized and tamper-resistant characteristics, stands as a reliable solution for secure data exchange. However, the persistent challenge lies in protecting sensitive information amidst evolving digital landscapes. This paper explores the potential of Non-Fungible Tokens (NFTs), a manifestation of blockchain technology, as dynamic carriers for diverse forms of sensitive information among businesses beyond their conventional association with art and collectibles. Our solution leverages the immutable NFT data to serve as a secure data pointer, while the mutable NFT data holds sensitive information protected by steganography. This dual approach ensures both data integrity and authorized access, even in the face of evolving digital threats. A performance analysis validates the efficacy of the approach, highlighting its reliability, robustness, and resistance to potential attacks on hidden information, ensuring secure data transmission across industries.

Keywords: NFTs; Blockchain; Steganography

1. Introduction

1.1. Background

An ever-increasing volume of data is being generated by IoT devices equipped with all kinds of sensors, including those embedded in smart medical devices, monitoring systems for industrial equipment, and environmental sensors for agricultural fields. This deluge of data necessitates a streamlined exchange across multiple organizations, as more and more IoT applications become global in scope. Take, for instance, a medical device company manufacturing pacemakers in Montreal that needs to securely share sensor data with a team of doctors in Japan for remote monitoring and analysis. Such cross-border data exchange, while enhancing the ease of collaboration and data utilization, presents formidable challenges in the realms of data security and privacy [1]. These challenges are particularly critical in sectors where sensitive data, in areas such as healthcare, supply chains, and financial services, forms the core of their operations and cannot be readily tolerated.

In the context of heightened global interconnectedness and technological progress, the phenomenon of cross-border data sharing has witnessed a rapid surge. The seamless global exchange of data requires the trust among entities. However, there is the lack of harmonized frameworks and shared principles between nations [2]. An additional challenge lies in ensuring the secure transmission of shared data from the source to the destination.

Blockchain has emerged as a significant enabling technology for trusted and secure data exchange. Derived from cryptographic principles and decentralized architectures, blockchain presents a secure and transparent framework for realizing global applicatiosn of IoTs. Its decentralized nature serves

 doi:10.20944/preprints202312.1891.v1

to alleviate the risks inherent in centralized control and potential single points of failure, thereby formulating a foundation of trust among entities involved in data exchange [3,4]. Blockchain addresses diverse needs such as data security, user privacy, and real-time sharing. Its substantial impact on cross-border communication is evident in its ability to overcome challenges associated with traditional systems and methodologies that include time-consuming processes [5].

Since its surge in adoption and popularity around 2016–2017, blockchain technology has demonstrated various applications, encompassing cryptocurrencies, smart contracts, and various emergent uses. One such example among these emerging applications is the rise of Non-Fungible Tokens (NFTs), recognized for their substantial purchase prices, occasionally reaching millions of dollars for ownership [6]. NFTs serve as digital representations of both physical and digital creative works or intellectual property, spanning various domains such as music, digital art, games, gifs, and video clips. The non-fungible nature of NFTs, in contrast to traditional fiat currencies where each unit is interchangeable, underscores the uniqueness of each token. This distinct quality ensures that each token is a singular entity, representing a specific object. These tokens encapsulate digital information, often in the form of media, with their value calculated in terms of cryptocurrencies [7].

The inception of NFTs in 2014 presents an attempt to establish a mechanism for artists to assert ownership over digital art [8]. However, it was in 2017 that non-fungible tokens materialized in the Ethereum blockchain. The Ethereum network, featuring smart contract functionality, facilitated token creation, programming, storage, and trading directly within the blockchain, establishing a more robust and accessible foundation for launching NFT projects. The year 2021 witnessed a significant surge in NFT popularity, as evidenced by a substantial increase in the average daily trading volume of the global NFT market, soaring from USD 180,000 in 2020 to an impressive USD 38 million. Despite this substantial increase, discussions have surfaced regarding a subsequent general decline in 2022 [9,10].

1.2. Related Work

The explosive growth of sensor technology and the subsequent decrease in the cost of wearable sensors have paved the way for transformative applications across various industries, with healthcare being one of the most significant beneficiaries. These sensors can be embedded in clothing, watches, and other everyday devices that enable continuous and cost-effective monitoring of the user's vital signs, such as body temperature, respiratory rate, and heart rate [11]. Within lifestyle and healthcare, sensor-generated data requires privacy and security. Several studies have proposed to address this need. One such example is the blockchain-based eHelathcare system proposed by [12]. This system leverages wireless body area networks (WBAN) to collect patient data from wearable sensors, which is then securely stored and transmitted using blockchain technology. This approach aims to ensure patient privacy and security through medical data immutability and traceability. Another work presented by [13], combines IoT, blockchain, and cloud technologies within the medical environment to offer healthcare and tele-medical laboratory services. The platform utilizes sensors to capture vital signs and physiological parameters, transmitting the data through a decentralized platform, built upon the Ethereum hybrid network certification system. The system's efficiency lies in its reduced response time and cost compared to alternative approaches. Focusing on energy and delay-aware healthcare monitoring, [14] a blockchain-assisted system for the WBAN-IoT is structured to facilitate three categories of communications: intra-WBAN, inter-WBAN, and beyond-WBAN. It utilizes both body and environment sensors, along with dual sinks for emergency and periodic packet transmission. The system [15] leverages a private Ethereum-based blockchain for communication between wearable sensors and smart devices (smartphones or tablets). IPFS is used to facilitate distributed storage of health data, while smart is used for data management and the association between doctors, patients, and the monitored data.

The scope of NFT applications has transcended their initial association with digital art, now encompassing a variety of sectors including, but not limited to, collectibles, virtual worlds, and supply chain management. For instance, [16] presented an NFT-based model aimed at enhancing the

 doi:10.20944/preprints202312.1891.v1

copyright traceability of off-chain data, contributing to the sustainability of the NFT community. In a different application, [17] proposed a framework, KD-NFT, that integrates NFT security features with Knowledge Distillations to address security concerns. This model extends NFT security into machine learning, leveraging blockchain features to recover the training procedure. Another application, presented by [18], introduces an NFT-based framework for managing educational assets in the Metaverse. This framework utilizes blockchain technology to authenticate ownership, safeguard intellectual property, and prevent fraud in educational assets represented as NFTs within the Metaverse. In a distinctive approach, [19] suggests employing NFTs as an incentive mechanism tied to student assessments. This model reinforces positive behaviour by granting bragging rights and special access based on NFT holdings. Furthermore, [20] proposes a distributed intelligence networking scheme for autonomous vehicles using NFTs. In this context, NFTs tokenize intelligence, describing it through metadata to enhance understanding and search for intelligence in the complex and trust-lacking Internet of Vehicles. [21] proposes an NFT-based solution using blockchain smart contracts, tokenization protocols, and decentralized storage for an efficient medical device traceability and ownership management system. In this model, NFTs serve as digital twins, capturing essential attributes and metadata across the entire life cycle of the medical device, from production to current use.

1.3. Contribution

This research aims to offer an effective and secure framework for leveraging blockchain technology and NFTs for the secure exchange of sensitive information across diverse sectors. To our knowledge, this work marks the first implementation of NFTs as a mechanism for facilitating cross-border data sharing among diverse businesses. The contributions of this paper include:

- We propose using NFTs as carriers for sensitive data in cross-border transfers, ensuring secure and authorized access. Harnessing the unique properties of NFTs, we employ the immutable NFT data as a tamper-proof pointer, guaranteeing the authenticity and provenance of the sensitive information. Meanwhile, the mutable NFT data serves as a secure container for the sensitive content itself. This allows for dynamic updates to reflect changes in users' data, ensuring the information remains current and relevant.
- To address the public accessibility of NFT metadata, we propose leveraging the power of steganography. This enables us to both conceal sensitive information and enhance its protection, offering an effective solution for privacy-conscious users.
- To ensure secure and private user mobility across businesses, we propose an approach that prioritizes user data privacy and integrity during transitions. This objective is achieved through the application of a strong cryptographic technique, specifically OTP, which aligns with our model's security requirements.
- A structured performance analysis is conducted to assess the practicality and effectiveness of implementing this proposed methodology in real-world scenarios.

1.4. Paper Organization

This paper is organized as follows. Section 2 delves into the essential components enabling cross-border data sharing via NFTs. Each component is technically defined and outlined, alongside a detailed scenario illustrating the model's operational flow. Section 3 showcases the implementation environment and demonstrates the execution of the aforementioned scenario. The feasibility of NFTs as data-sharing mechanisms is evaluated in Section 4, presenting the obtained results and their subsequent discussion. Finally, Section 5 concludes the paper by highlighting key takeaways and outlining promising avenues for future research.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1891.v1

2. Materials and Methods

2.1. Technical Definitions

This section investigates the elements incorporated in our proposition for operating NFTs as a method for sharing data. The specific functions of each component within the framework will be outlined and explained.

2.1.1. Steganography

Steganography encompasses the insertion of private information into a regular and non-sensitive message or file, limiting awareness of the concealed message to solely the encoder and the intended decoder. In contrast to cryptography, which is dedicated to obfuscating data readability, steganography is oriented towards concealing the very existence of the data. Given the inherently public accessibility of data housed within NFTs, our endeavours are directed toward fortifying and safeguarding this information. Employing the steganography technique facilitates this objective. In our particular scenario, the data involves confidential information linked to various users requiring seamless transitions across multiple businesses. The essential role of steganography in our case is depicted in Figure 1.

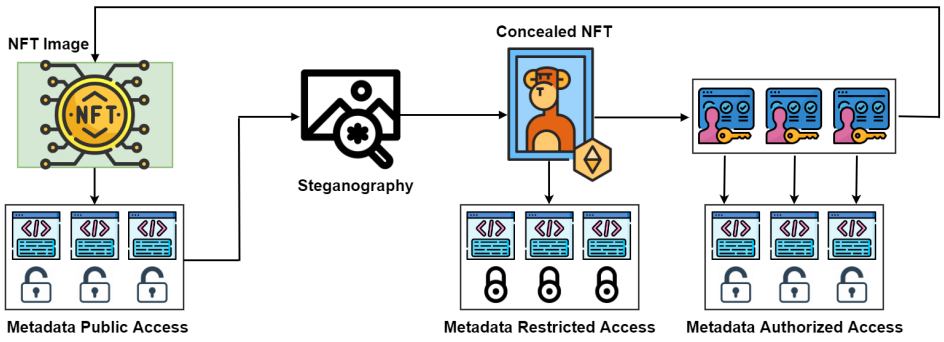

Figure 1. The role of steganography in protecting the NFT public metadata

2.1.2. One-Time Pad (OTP)

The one-time pad (OTP) is a cryptographically robust method, known for its theoretical invulnerability to ensure confidentiality. It relies on a simple yet highly secure principle using a key matching the message length, characterized by randomness and confidentiality. At its core, OTP involves generating a truly random key, often as a sequence of randomized bits or characters, equal to or surpassing the plaintext message length. Illustrated in Figure 2, OTP operations show the encryption process, combining each plaintext element with the corresponding key element through a bitwise XOR operation to produce ciphertext. The key, following the "one-time pad" principle, is for a single use and must be discarded securely afterward. Using this same one-time pad key, the recipient decrypts the message, guaranteeing confidentiality and randomness to reveal the original plaintext. We employed OTP for managing the transfer of steganography passwords between different businesses.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1891.v1

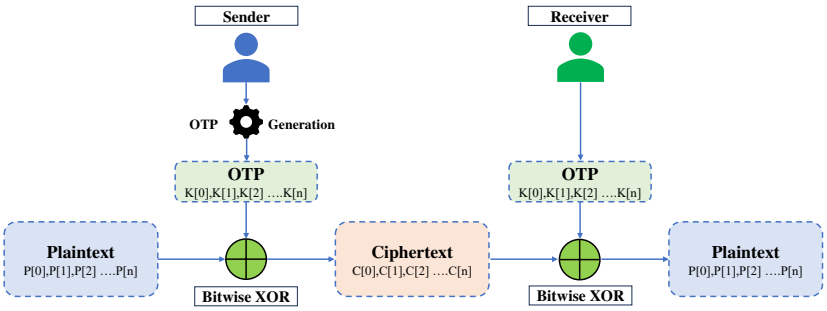

Figure 2. One-time pad encryption and decryption processes

2.1.3. NFTs

Cryptocurrencies, mirroring physical currency, demonstrate fungibility, where units within the same currency are interchangeable, such as one Bitcoin for another. In contrast, non-fungible assets, like event tickets, are unique and lack one-to-one exchangeability. NFTs, developed to digitize and trade such assets, represent diverse physical or digital items like art and music. Each NFT possesses a distinct identifier linked to a public blockchain address, ensuring uniqueness among multiple minted NFTs. In our context, we employ NFTs for cross-border data sharing, enabling the secure transfer of sensitive user data across diverse networks. Operating NFTs ensures privacy and security while boosting interoperability among various businesses.

2.1.4. Smart Contract

A smart contract is a specialized program designed to enforce predetermined conditions established by participants within a network. Its primary function revolves around the initiation and oversight of the ledger state within a blockchain framework, achieved through the processing of transactions submitted by users. These contracts are deployable across diverse blockchain networks, enabling the automated and secure execution of contractual agreements.

2.2. Tracing Model Operations

2.2.1. Sensing Data Collection

We develop the experiments on the Mobile Health Human Behavior dataset from Kaggle, a prominent online repository for diverse datasets. This dataset comprises body motion and vital signs recordings from ten volunteers of varying demographics performing various physical activities. Sensors positioned on the chest, right wrist, and left ankle captured the movement of different body parts, specifically acceleration, gyroscopic rate of turn, and magnetic field orientation. Data collection employed Shimmer2 wearable sensors. All modalities were recorded at a 50 Hz sampling rate, deemed sufficient for capturing human activity. The activity set encompasses diverse actions, including standing, sitting, relaxing, walking, running, jogging, and more. We consider a subset of these records, generated through sensor data, to be embedded within the NFT image. Figure 3 depicts a sample of these embedded records.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1891.v1

Subject	Activity	alx	aly	alz	glx	gly	glz	arx	ary	arz	grx	gry	grz
subject1	0	2.1849	-9.6967	0.63077	0.1039	-0.84053	-0.68762	-8.6499	-4.5781	0.18776	-0.44902	-1.0103	0.034483
subject1	0	2.3876	-9.508	0.68389	0.085343	-0.83865	-0.68369	-8.6275	-4.3198	0.023595	-0.44902	-1.0103	0.034483
subject1	4	5.3524	-8.0329	0.67271	0.60853	-0.57599	0.43418	-3.0312	-5.6574	2.2588	-0.53529	-0.67146	0.74353
subject2	0	0.49965	-9.668	1.5216	-0.47866	-0.53471	0.53438	-4.6451	-8.2508	1.9208	-0.98039	-0.41889	0.18966
subject2	5	0.18314	-9.4906	-6.4831	-0.26716	-0.38649	0.17485	-3.4535	-10.677	2.3412	-0.41176	-0.40452	0.012931
subject2	6	-1.2973	-9.4702	-2.4656	-0.57514	-0.67355	-0.67976	-7.6246	-9.3805	-1.0524	-0.30784	-0.80903	-0.55172
subject3	2	2.8136	-9.4215	-2.5471	0.718	-0.5122	-0.73281	0.45637	-9.4938	1.6191	0.6451	-0.72074	-0.00431
subject3	0	-2.2805	-9.2326	1.4947	-0.141	-0.71295	0.56385	-4.4007	-9.3386	-0.86276	-0.91569	-0.47639	0.27155
subject3	8	0.18191	-9.2596	0.768	-0.39703	-0.82176	-0.53045	-2.4333	-5.3411	2.8892	-0.63922	-0.846	-0.21121
subject4	0	1.5792	-9.7001	1.2808	-0.28015	-0.85741	-0.68173	0.71452	-10.095	3.5474	0.43725	-1	-0.33836
subject4	10	7.1498	-3.5358	-11.001	-0.2987	-0.85366	-0.56385	-10.181	-10.378	-0.84184	-0.88039	-0.24846	-0.49138
subject4	9	-1.0187	-6.7477	-2.4934	0.55659	-0.76735	-0.10609	5.5066	-1.6068	0.31549	0.87255	-0.23819	0.75216
subject5	4	0.16488	-7.6876	-2.4244	-0.46011	-0.15572	-1.0413	-2.1751	-9.4501	0.98583	0.46078	-1.0185	-0.28448
subject5	0	1.1971	-9.5346	0.99357	-0.64564	-0.78424	0.1945	-7.9562	-3.0478	4.2226	-0.91373	-0.46201	0.48276
subject5	8	0.7007	-9.6216	-0.77616	-0.7013	-0.75985	-0.01572	-0.36621	-4.9215	-0.15233	-0.74706	-0.76797	0.002155

Figure 3. Sample of MHEALTH dataset.

2.2.2. Priming NFTs for Use

Unique NFTs are assigned to users throughout the business ecosystem. Before assignment, multiple steps prepare them for deployment. First, data generation occurs. Each generated NFT holds data for various purposes. In our case, mutable data enables the transfer of sensitive information. This data is carefully reviewed before being generated by each business. Minting NFTs requires a dedicated smart contract. In our scenario, a custom contract is built and deployed. Typically, the user's original business's admin unit is responsible for creating, auditing, and verifying this contract. Upon creation, the contract starts assigning NFTs to business users, linking their data to these NFTs. These NFTs with associated data secure users' sensitive information as they move between businesses. Figure 4 shows the sequential stages through which NFT progresses to achieve the data exchange.

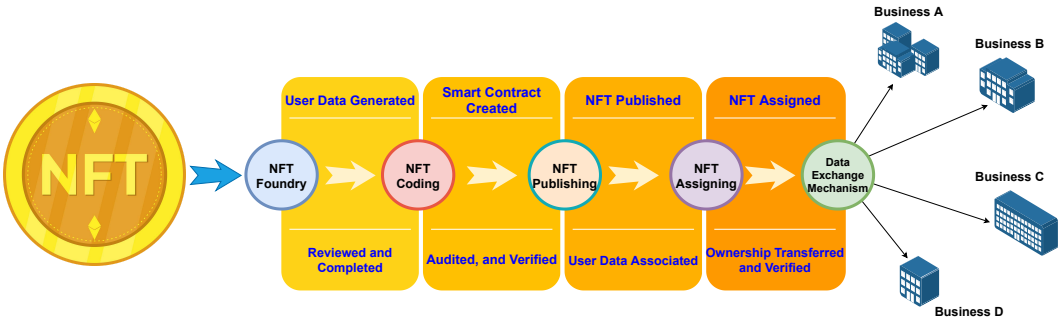

Figure 4. The processes associated with using NFTs for facilitating data exchange.

2.2.3. Scenario

A consortium of businesses is establishing a secure data exchange system for their users. Sensitive user data samples, collected via sensors and sourced from the MHEALTH dataset, are stored in a human-readable format, typically a text file. This information is then concealed within an ordinary image I_{norm} using steganography and creating an encrypted image I_{enc} with no visible signs of hidden data. Extracting the concealed information requires decrypting I_{enc} using a password. The NFT creation process enables the incorporation of unique identifiers generated by IPFS, establishing a direct reference to the original data stored within the IPFS system. IPFS (InterPlanetary File System) is a decentralized storage system designed to create a peer-to-peer mechanism of storing and sharing data in a distributed manner. I_{enc} is then uploaded to IPFS to function as an NFT image. The resulting unique identifier becomes a reference in the NFT metadata file, containing details like name, age, and description, specified by the business. The metadata file is also uploaded to IPFS and the obtained unique identifier is used in the NFT smart contract to link I_{enc} with the metadata. Each user is assigned an NFT, serving as both an ownership mechanism and a holder of sensitive data for cross-border

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1891.v1

sharing. To transition to a new business, a user's descriptive data is embedded within the NFT image for transfer. A smart contract on the Ethereum blockchain controls access, ensuring only authorized administrators can update the NFT's metadata. The updatable metadata allows changes to the user's NFT, supporting minting for users to connect with their updated metadata on IPFS using their wallet address. Figure 5 provides the procedures involved in employing NFTs as a means for data exchange.

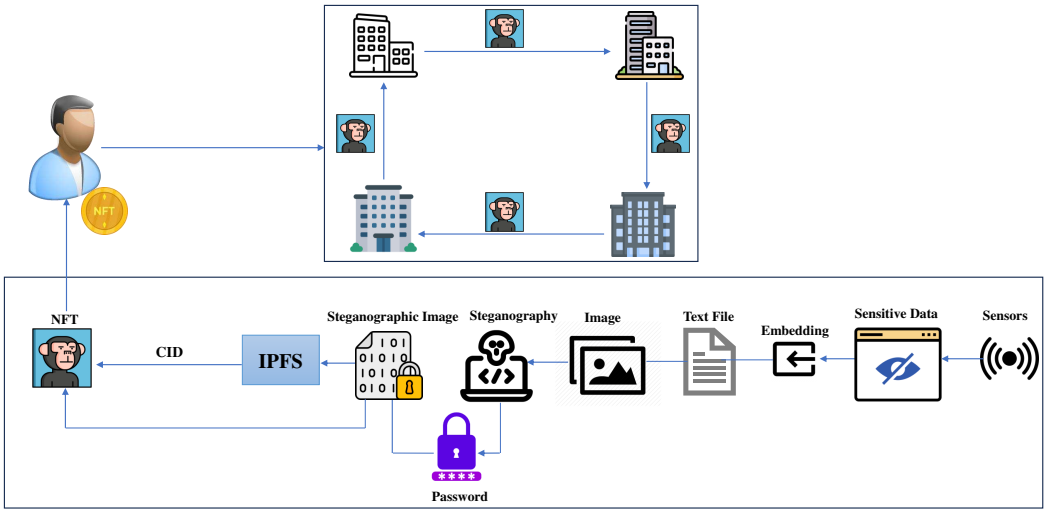

Figure 5. The processes associated with using NFTs for facilitating data exchange.

2.2.4. User Mobility

Our model tackles user mobility across diverse businesses, where user data is concealed within steganographic NFT images. As previously mentioned, accessing this data requires a password. Secure and unaltered transmission of this password is crucial, while also actively involving the user. For this, we leverage the power of One-Time Passwords (OTPs).

The first critical step involves the user's originating network generating an OTP. This OTP acts as a unique binary key, equal or greater in length to the steganography password. It's a random binary sequence of equal length, denoted as (K = K[0], K[1], ..., K[L-1]), where (K[i]) represents the (ith) bit. Essentially, the generation process can be summarized as:

$$K[i] \xleftarrow{R} \{0,1\} \tag{1}$$

Each bit $K[i]$ is sampled uniformly and independently from 0,1 using a random process operator $\xleftarrow{R}$, guaranteeing unbiased selection. The fundamental operation for confidentiality is bitwise XOR $(\oplus)$, applied to each corresponding bit pair from P and the K. The resulting ciphertext (C) is obtained by applying $(\oplus)$ to each bit, generating a new sequence based on the combined values.

$$C[i] = P[i] \oplus K[i] \tag{2}$$

where $C[i]$ represents the ith bit of the ciphertext. The OTP, a one-and-done key, is never used twice, ensuring absolute secrecy. The user receives this key to unlock the steganography password in the receiving business or network when the need arises.

With the OTP safely in the user's hands, the originating network can send the encrypted password C through any insecure channel such as the internet. Even if compromised, C is just random noise without the user's OTP. The receiving network is helpless without it as they have the encrypted password, but it means nothing without the user's decryption code. The user's exclusive possession of

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1891.v1

the OTP guarantees password control and security every step of the way, even in the face of potential threats. The following algorithm outlines the password transmission process.

Algorithm 1: Secure Password Transmission

Input: Steganography password P, User's OTP K
Output: Decrypted password P for sensative data access

$C_P \leftarrow P \oplus K$;
$C_P \rightarrow$ Transmit (B1 $\rightarrow$ B2);
$B2 \leftarrow$ Wait;
$P \leftarrow C_P \oplus K$;
$\Rightarrow$ Access sensative data;

Upon secure reception of the ciphertext C by any receiving business, the decryption process requires close collaboration with the user to obtain the steganography password P. This decryption process is detailed as follows:

Each bit $P[i]$ of P is calculated using a bitwise XOR operation between the corresponding bits of the C and the OTP (K). This operation can be expressed mathematically as:

$$P[i] = C[i] \oplus K[i] \quad \text{for } i = 0, 1, \ldots, L-1 \tag{3}$$

The validation for the decryption process can be represented as follows:

$$F_{\text{Decryption}}(C[i], K[i]) = \begin{cases} \text{Error} & \text{if } C[i] \oplus K[i] \neq P[i] \\ P[i] & \text{if } C[i] \oplus K[i] = P[i] \end{cases} \tag{4}$$

The application of the XOR operation serves to reverse the encryption process and retrieve the original password. The following algorithm explains the migration scenario between two different businesses.

Algorithm 2: User Data Migration from B_1 to B_2

Input: User's NFT in B_1, Steganography Password
Output: User's Sensative Data on B_2

foreach *User* **do**
    PresentNFT(User, Steganography Password);
    VerifyUserIdentity(User, NFT);
    RetrieveFile(User, NFT);
    ExtractFData(User, Steganography Password);
    LocateUserData(User, Sensitive data);
    RetrievelData(User);
    StoreNewData(User);
    RepeatSteps3To8(User);

3. Setup and Implementation

Within this section, our focus lies on evaluating the performance of the steganography. The objective is to assess the efforts to protect sensitive data associated with individual users. This analysis aids in estimating the reliability and resilience of the technique in concealing confidential information, all while upholding the quality of the cover NFT images. Moreover, it validates the technique's ability to withstand potential attacks seeking to reveal concealed data. Additionally, it affirms the high similarity between the original and encrypted image, dispelling any uncertainties regarding including sensitive data within the NFT image.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1891.v1

3.1. Environment Setup

The evaluation takes place on a local Python 3.8 environment, using specific libraries and tools dedicated to Steganography tasks. Development and debugging are carried out within the Pycharm IDE. The analysis is executed on a Windows system operating at 64-bit with 16GB of RAM and an Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz. Various parameters and configurations are examined to evaluate Steganography performance and identify potential avenues for improvement.

3.2. Performance Metrics

In this phase, we assess the performance of Steganography, focusing on two key metrics: the Structural Similarity Index (SSIM) and the Peak Signal-to-Noise Ratio (PSNR). SSIM provides insights into the quality of hidden information by measuring the similarity between the original and modified images. Higher SSIM values mean seamless embedding of sensitive data, ensuring minimal perceptible alterations to the NFT image's visual appearance. On the other hand, PSNR quantifies the level of distortion introduced during the steganography process, offering an overall evaluation of the modified image's fidelity. Preserving the accuracy and reliability of the NFT image is paramount, as any distortion may compromise the privacy and integrity of the embedded data.

SSIM extracts three essential characteristics from an image: luminance, contrast, and structure. The luminance attribute is calculated by averaging all pixel values [22]. In mathematical terms, this computation can be expressed as:

$$\bar{\kappa} = \frac{1}{N}\sum_{i=1}^{N}\kappa_i \tag{5}$$

Here a_i denotes the pixel value of the image a, and N signifies the total count of pixel values within the image. As mentioned earlier, SSIM evaluates similarities between images by considering their luminance, contrast, and structure. Therefore, a comparison function is needed to assess two given images based on their luminance. This luminance comparison function can be mathematically expressed as follows:

$$l(\kappa,\nu) = \frac{2\bar{\kappa}\bar{\nu}+\eta_1}{\bar{\kappa}^2+\bar{\nu}^2+\eta_1} \tag{6}$$

Here, η_1 serves as a crucial numerical constant ensuring stability by preventing division by zero. The computation of the contrast feature entails determining the standard deviation of all pixel values. Mathematically, the contrast can be expressed as follows:

$$\sigma = \left(\frac{1}{N-1}\sum_{i=1}^{N}(\kappa_i-\bar{\kappa})^2\right)^{\frac{1}{2}} \tag{7}$$

Just as with luminance, the contrast comparison function for images κ and ν can be mathematically expressed as follows:

$$c(\kappa,\nu) = \frac{2\sigma_\kappa\sigma_\nu+\eta_2}{\sigma_\kappa^2+\sigma_\nu^2+\eta_2} \tag{8}$$

The third attribute extracted by SSIM is known as structure. It entails a process where the input image undergoes division by its standard deviation, leading to the creation of a normalized image with a unit standard deviation. This normalization step is crucial to ensure that the resultant image maintains a unit standard deviation, thereby enhancing the reliability of comparisons. The mathematical representation for the structure of the κ image can be expressed as follows:

$$K = \frac{\kappa-\bar{\kappa}}{\sigma} \tag{9}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1891.v1

Just as with both luminance and contrast, the structure comparison function for κ and ν images can be mathematically expressed as follows:

$$S(\kappa,\nu) = \frac{\sigma_{\kappa\nu} + \eta_3}{\sigma_\kappa \sigma_\nu + \eta_3} \tag{10}$$

$\sigma_{\kappa\nu}$ can be defined as follows:

$$\sigma_{\kappa\nu} = \frac{1}{N-1}\sum_{i=1}^{N}(\kappa_i - \bar{\kappa})(\nu_i - \bar{\nu}) \tag{11}$$

Then the SSIM score can be expressed as follows:

$$S(\kappa,\nu) = [l(\kappa,\nu)]^\alpha [c(\kappa,\nu)]^\beta [s(\kappa,\nu)]^\gamma \tag{12}$$

Using parameters α , β , and σ allows for the precise adjustment of the relative importance of the three aforementioned features, each assigned a value > 0. To streamline the expression, a simplification can be made by assuming that $\alpha = \beta = \gamma = 1$, and $\eta_3 = \eta_2/2$. This simplification results in a specific formulation of the SSIM index:

$$SSIM(\kappa,\nu) = \frac{(2\bar{\kappa}\bar{\nu} + \eta_1)(2\sigma_{\kappa\nu} + \eta_2)}{(\bar{\kappa}^2 + \bar{\nu}^2 + \eta_1)(\sigma_\kappa^2 + \sigma_\nu^2 + \eta_2)} \tag{13}$$

PSNR relies on the Mean Squared Error (MSE) as a foundational element. Both PSNR and MSE stand out as significant metrics broadly used for evaluating and assessing image quality. The process of determining the PSNR value begins with the measurement of MSE for a specific original and distorted image. Mathematically, the MSE is calculated as follows:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[\kappa(i,j) - \nu(i,j)]^2 \tag{14}$$

$\kappa(i,j)$ denotes the original image, $\nu(i,j)$ stands for the distorted image, and m, n represent the number of rows and columns in the image. Once the MSE is calculated, determining the PSNR value becomes straightforward through this mathematical equation:

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \tag{15}$$

Here, MAX symbolizes the maximum possible pixel value within the image. When representing pixels with 8 bits per sample, this value is commonly set to 255. A smaller MSE value signifies a reduced level of error, consequently resulting in a higher PSNR value. This higher PSNR value serves as an indicator of enhanced image quality [23].

3.3. Parameter Settings and Configurations

In this section, we explore the effects of the key parameters on the efficiency of the steganographic NFT image. Our examination centers on examining how these parameters impact the predefined metrics mentioned previously. The parameters encompass the embedding algorithm, data size, image type and size, password complexity, and encryption mode.

3.3.1. Embedding algorithm

The choice of the embedding algorithm is a key factor that significantly influences the steganography technique. Although our current configuration uses the Least Significant Bit (LSB) technique, we explore alternative embedding algorithms, including Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Our analysis extends to understanding their impact on steganography performance. While LSB conceals data by modifying the least significant bit of

 doi:10.20944/preprints202312.1891.v1

pixel values with minimal visual alterations, DWT analyzes image frequency components, enabling data embedding in various frequency bands. DCT, on the other hand, facilitates hiding data in less perceptually significant regions by transforming the image into frequency coefficients. These algorithms present diverse trade-offs in terms of data hiding, resistance to attacks, and image quality.

3.3.2. Data size

Our objective during this phase is to assess the impact of varying data sizes on the performance of steganographic images used for NFTs. We will specifically embed user-sensitive data provided by the MHEALTH dataset. Since the data is stored in a text file, we will evaluate three distinct file sizes. Initially, we will embed a small piece of sensitive data, resulting in a 1KB file size. Next, we will increase the file size to 10KB by incorporating more sensitive data. Finally, we will further expand the volume of descriptive data to investigate the possibility of embedding larger data, resulting in a 20KB file size. This investigation seeks to establish a clear understanding of the relationship between data size and steganographic image performance.

3.3.3. Image type and size

To evaluate the impact of image format on steganographic image quality in NFTs, we are conducting an experiment involving two widely used formats: JPEG and PNG. The selection of the image format can impact the visual quality of the steganographic data concealed within the NFT image. Analyzing both formats can assist in providing insights into optimizing steganographic image quality and security within the NFT ecosystem.

3.4. Password complexity

To further enhance the security of sensitive data concealed using steganography, this experimental phase is dedicated to examining the relationship between password strength and its impact on steganographic image integrity. We are categorizing passwords into three different levels: weak, moderate, and strong (complex). Each password category is subjected to a series of steganography code tests to assess its influence on the steganographic image's quality and resilience against unauthorized access.

3.4.1. Encryption mode

To accommodate data larger than its native 128-bit block size, the Advanced Encryption Standard (AES) employs various block cipher modes. These modes define how AES encrypts or decrypts data by treating it as individual blocks of the same size. AES supports multiple block cipher modes, including the Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter (CTR), and Galois/Counter (GCM) modes. In our experimental setup, we are evaluating the impact of each of these modes on steganography performance.

4. Results and Discussion

In this section, we present the outcomes derived from the conducted parameters outlined earlier. Additionally, we analyze their influence on the steganographic NFT image and assess their implications for the efficacy of the presented concept in facilitating cross-border data sharing.

4.1. Impact of embedding algorithm

A comparison of various embedding algorithms for steganography within our model is presented in Table 1. Among the tested algorithms, LSB outperformed DWT and DCT in terms of image quality, as evidenced by its superior SSIM and PSNR values. This indicates that LSB can effectively embed sensitive information into NFT images while minimizing quality degradation. However, LSB exhibited

 doi:10.20944/preprints202312.1891.v1

a higher encryption execution time (0.089 seconds) compared to DCT (0.022 seconds) and DWT (0.058 seconds). Despite this, LSB's decryption execution time (0.025 seconds) remained reasonable.

Based on the observed performance, we opted for the LSB algorithm for embedding data into NFT images. This decision was driven by LSB's superior image quality, as measured by SSIM and PSNR, which were critical considerations for us, along with its acceptable execution speed.

Table 1. Results of embedding algorithms and their corresponding parameters.

	PSNR(dB)	SSIM	Encryption Execution Time(Sec)	Decryption Execution Time(Sec)
LSB	85.36	0.99	0.089	0.025
DCT	32.92	0.97	0.022	0.001
DWT	30.72	0.94	0.058	0.007

4.2. Impact of data size

Our findings, as illustrated in Table 2, reveal a negative correlation between embedded data size and PSNR value. This inverse relationship stems from the intensifying distortion inflicted upon the cover image as the data payload expands within it. Similarly, the execution time for encryption and decryption exhibits a proportional increase with the burgeoning embedded data size. This escalating demand on computational resources arises from the necessity to process a larger volume of data during both encryption and decryption. In our specific case, where we solely embedded some sensitive information for each user, a data size of 10 KB proved to be the optimal point of balance. This selection strikes a delicate balance between preserving satisfactory SSIM and PSNR values, maintaining feasible execution times for encryption and decryption, and ensuring the NFT image retains high visual fidelity.

Table 2. Results of data sizes and their corresponding parameters.

	PSNR(dB)	SSIM	Encryption Execution Time(Sec)	Decryption Execution Time(Sec)
1 KB	82.009	0.999	0.053	0.021
10 KB	62.872	0.999	0.163	0.119
20 KB	59.747	0.999	0.273	0.209

4.3. Image type

Table 3 demonstrates that PNG images outperform their JPEG counterparts in terms of PSNR values. This disparity stems from the inherent lossless nature of PNGs, ensuring minimal to no data degradation during the steganographic process. Conversely, JPEGs are inherently lossy, leading to data loss during embedding and compromising PSNR values. Encryption and decryption execution time, however, paints a different picture. JPEG images exhibit significantly shorter processing times compared to PNGs. This can be attributed to the inherent simplicity of JPEGs, which translates to reduced computational demands during encryption and decryption operations.

Considering these trade-offs, our decision leaned towards adopting PNG images for embedding sensitive data into NFT images. This choice was driven by the superior PSNR performance of PNGs and their ability to maintain acceptable encryption and decryption execution times despite their higher computational requirements.

Table 3. Results of data sizes and their corresponding parameters.

	PSNR(dB)	SSIM	Encryption Execution Time(Sec)	Decryption Execution Time(Sec)
JPEG	79.669	0.999	0.059	0.021
PNG	93.845	0.999	0.262	0.054

4.4. Impact of password complexity

Table 4 reveals the minimal influence of password complexity on both NFT image quality and encryption/decryption times. Regardless of the chosen mode (weak, moderate, or strong),

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1891.v1

image quality remains consistently high (SSIM of 0.999) with only negligible variations in PSNR. Similarly, encryption and decryption execution times exhibit remarkable uniformity across all password complexities, differing only by milliseconds. This suggests that, within the confines of this steganographic setup, prioritizing robust security measures should take precedence over password complexity. Image fidelity and computational efficiency remain unperturbed by password strength, rendering complex passwords unnecessary for maintaining acceptable image quality. Therefore, we opted for a strong password, acknowledging its alignment with best security practices while still achieving an acceptable PSNR value.

Table 4. Results of password modes and their corresponding parameters.

	PSNR(dB)	SSIM	Encryption Execution Time(Sec)	Decryption Execution Time(Sec)
Weak	81.941	0.999	0.052	0.029
Moderate	82.483	0.999	0.053	0.020
Strong	81.836	0.999	0.054	0.020

4.5. Impact of encryption mode

The results presented in Table 5 reveal minimal influence of encryption mode on NFT image quality. All tested modes show remarkably high SSIM values of 0.999, and PSNR values hover around a consistent 82 dB, demonstrating negligible quality degradation across the board. Furthermore, encryption and decryption execution times show comparable performance with slight, millisecond-range variations across all modes. This consistency suggests that image quality remains virtually unaltered regardless of the chosen encryption mode.

Based on these findings, we opted for CFB mode in our implementation due to its superior PSNR performance. While other modes achieved statistically comparable results, CFB's slight edge in preserving image fidelity ultimately informed our decision.

Table 5. Results of encryption mode and their corresponding parameters.

	PSNR(dB)	SSIM	Encryption Execution Time(Sec)	Decryption Execution Time(Sec)
CBC	82.027	0.999	0.053	0.019
CFB	82.379	0.999	0.051	0.018
CTR	82.070	0.999	0.052	0.019
OFB	82.050	0.999	0.049	0.017
GCM	81.949	0.999	0.051	0.020
ECB	82.035	0.999	0.050	0.018

5. Conclusions

The challenge of secure and confidential data exchange has not received the level of attention it deserves in existing research, with proposed solutions often plagued by practical complexities or insecure mechanisms. Non-fungible tokens (NFTs), a burgeoning blockchain application, have recently gained widespread interest for their potential beyond their traditional association with digital art and collectibles. This paper contributes to ongoing NFT exploration by investigating their potential for embedding sensing data within NFTs, enabling confidential and cross-border data exchange.

To achieve this, the proposed solution leverages both the immutable and mutable attributes of NFTs. Immutable data serves as a secure pointer and establishes data ownership, while mutable data acts as a secure container for sensitive information. Steganography safeguards the confidentiality of data embedded within the NFT, addressing the inherently public nature of NFT metadata. User mobility across multiple businesses is maintained through the employment of a robust cryptographic technique, in our case, a one-time password (OTP) that prioritizes user data privacy and integrity during transitions.

Our experiments demonstrated several insights into embedding sensor data within NFTs using steganography. The type of embedding algorithm was the most crucial factor impacting

imperceptibility, with LSB offering near-flawless visual quality (SSIM = 0.99, PSNR > 85) but slower execution times, while DCT and DWT sacrificed some imperceptibility with lower SSIM (< 0.99) and lower PSNR (< 33 dB). Data size also mattered, as larger data loads decreased imperceptibility and significantly increased execution times. Image type played a minor role, with JPEGs impacting imperceptibility compared to PNGs. Password complexity and encryption mode had negligible effects on both visual quality and performance.

Future work in this area should focus on developing advanced and standardized implementation tools to streamline the OTP generation and encryption processes, which fall outside the scope of this work. For example, current cryptocurrency wallets lack functionalities for users to encrypt/decrypt data using their public/private keys. Such tools and features would not only enhance the adaptability of the proposed solution but also facilitate user-friendly and effortless adoption.

References

1. Jin, H.; Luo, Y.; Li, P.; Mathew, J. A review of secure and privacy-preserving medical data sharing. *IEEE Access* **2019**, *7*, 61656–61669.
2. Liu, Z.; Li, Z. A blockchain-based framework of cross-border e-commerce supply chain. *International Journal of Information Management* **2020**, *52*, 102059.
3. Kim, S.; Kim, D. Securing the Cyber Resilience of a Blockchain-Based Railroad Non-Stop Customs Clearance System. *Sensors* **2023**, *23*, 2914.
4. Zhao, H. A cross-border E-commerce approach based on blockchain technology. Mob. *Inf. Syst* **2021**, *2006082*.
5. Zhang, L.; Xie, Y.; Zheng, Y.; Xue, W.; Zheng, X.; Xu, X. The challenges and countermeasures of blockchain in finance and economics. *Systems Research and Behavioral Science* **2020**, *37*, 691–698.
6. Cornelius, K. Betraying blockchain: accountability, transparency and document standards for non-fungible tokens (nfts). *Information* **2021**, *12*, 358.
7. Rehman, W.; e Zainab, H.; Imran, J.; Bawany, N.Z. NFTs: Applications and challenges. 2021 22nd International Arab Conference on Information Technology (ACIT). IEEE, 2021, pp. 1–7.
8. Baker, B.; Pizzo, A.; Su, Y. Non-fungible tokens: a research primer and implications for sport management. *Sports Innovation Journal* **2022**, *3*, 1–15.
9. Teplova, T.; Kurkin, A.; Baklanova, V. Investor sentiment and the NFT market: prediction and interpretation of daily NFT sales volume. *Annals of Operations Research* **2023**, pp. 1–25.
10. Tahmasbi, N.; Shan, G.; French, A.M. Identifying Washtrading Cases in NFT Sales Networks. *IEEE Transactions on Computational Social Systems* **2023**.
11. Kang, J.Y.; Bae, Y.S.; Chie, E.K.; Lee, S.B. Predicting Deterioration from Wearable Sensor Data in People with Mild COVID-19. *Sensors* **2023**, *23*, 9597.
12. Wang, J.; Han, K.; Alexandridis, A.; Chen, Z.; Zilic, Z.; Pang, Y.; Jeon, G.; Piccialli, F. A blockchain-based eHealthcare system interoperating with WBANs. *Future Generation computer systems* **2020**, *110*, 675–685.
13. Wang, D.H. IoT based clinical sensor data management and transfer using blockchain technology. *Journal of IoT in Social, Mobile, Analytics, and Cloud* **2020**, *2*, 154–159.
14. Anbarasan, H.S.; Natarajan, J. Blockchain Based Delay and Energy Harvest Aware Healthcare Monitoring System in WBAN Environment. *Sensors* **2022**, *22*, 5763.
15. Taralunga, D.D.; Florea, B.C. A blockchain-enabled framework for mhealth systems. *Sensors* **2021**, *21*, 2828.
16. Chen, Y.; Wang, Z.; Liu, X.; Wei, X. A New NFT Model to Enhance Copyright Traceability of the Off-chain Data. 2022 International Conference on Culture-Oriented Science and Technology (CoST). IEEE, 2022, pp. 157–162.
17. Wang, N.; Sajjanhar, A.; Xiang, Y.; Gao, L. A Robust NFT Assisted Knowledge Distillation Framework for Edge Computing. International Conference on Testbeds and Research Infrastructures. Springer, 2022, pp. 20–31.
18. Hocaoğlu, M.; HABBAL, A. NFT based model to manage educational assets in Metaverse. *Avrupa Bilim ve Teknoloji Dergisi* **2022**, pp. 20–25.

19. Elmessiry, A.; Elmessiry, M.; Bridgesmith, L. NFT student teacher incentive system (NFT-stis). *Available at SSRN 4120879* **2021**.
20. Ren, Y.; Xie, R.; Yu, F.R.; Huang, T.; Liu, Y. NFT-based intelligence networking for connected and autonomous vehicles: A quantum reinforcement learning approach. *IEEE Network* **2022**, *36*, 116–124.
21. Gebreab, S.A.; Hasan, H.R.; Salah, K.; Jayaraman, R. NFT-based traceability and ownership management of medical devices. *IEEE Access* **2022**, *10*, 126394–126411.
22. Wang, Z.; Bovik, A.C.; Sheikh, H.R.; Simoncelli, E.P. Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing* **2004**, *13*, 600–612.
23. Saladi, S.; Amutha Prabha, N. Analysis of denoising filters on MRI brain images. *International Journal of Imaging Systems and Technology* **2017**, *27*, 201–208.