Published by
NIGERIAN SOCIETY OF PHYSICAL SCIENCES
Available online @ https://journal.nsps.org.ng/index.php/jnsps

J. Nig. Soc. Phys. Sci. 7 (2025) 2560

Journal of the Nigerian Society of Physical Sciences

LWRNPIP: Design of a light weight restrictive non-fungible token based on practically unclonable functions via image signature patterns

Mahesh Kumar Singh[a], Pushpa Choudhary[b], Arun Kumar Singh[c], Pushpendra Singh[d,*]

[a]*Department of Computer Science and Engineering, Dronacharya Group of Institutions Greater Noida, Uttar Pradesh, India*
[b]*Department of Computer Science and Engineering, Galgotia College of Engineering and Technology, Greater Noida, Uttar Pradesh, India*
[c]*Department of Computer Science and Engineering, Greater Noida Institute of Technology Greater Noida, Uttar Pradesh, India*
[d]*Department of Computer Science and Engineering, SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, Ghaziabad, Uttar Pradesh, India-201204*

Abstract

Non-fungible tokens (NFT) have recently become a popular method of tokenizing & commercializing personal artifacts. Designing NFTs requires selecting different blockchain-based consensus models, encryption techniques, and distribution mechanisms. Existing NFT design techniques use computationally complex encryption models like Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), etc., which restricts their general-purpose usability, limiting their scalability for real-time use cases. To overcome this drawback, while maintaining high security, this text proposes a design of a lightweight, restrictive non-fungible token based on Practically Unclonable Functions (PuFs) via image signature patterns. The proposed model initially collects context-specific information sets about the entity that needs tokenization and uses this information to generate restrictive hash sets. These hash sets are passed through a customized PuF model, which generates image-like hash signatures. The generated hash signatures are iteratively embedded into unique images, which are fused via a dual visual encryption-decryption process. The encryption process generates 2 image sets, for distribution among the buyer & seller, while the decryption process aggregates these image sets to form a single file token. These tokens are passed through another encryption-decryption-based validation process while reselling operations. Due to use of PuFs and restrictive hash sets, the proposed model is capable of deployment for low-power IoT applications and can be scaled for general-purpose scenarios. The proposed model was tested on different NFT use cases, and showcased 10.4% lower processing delay, 8.3% lower energy consumption during selling, and 4.9% lower energy consumption during reselling processes. The tokens generated via this model were also tested under different attack types, and similar efficiency levels were observed under real-time scenarios.

DOI:10.46481/jnsps.2025.2560

Keywords: NFT, PuF, Cryptography, Dual, Delay

Article History :
Received: 05 December 2024
Received in revised form: 01 April 2025
Accepted for publication: 26 May 2025
Available online: 28 June 2025

Communicated by: Oluwatobi Akande

1. Introduction

The significance of NFT artwork extends beyond the monetary to the cultural as well. Art, from its very creation forward,

*Corresponding author Tel. No.: +91-965-088-6084.
Email address: `pushpendra.singh1@gmail.com` (Pushpendra Singh)

is the fruition of the intellectual effort of the artist; it represents the individual's unique perspective, aesthetic, and cultural upbringing. Not only that, but artists need to rethink their methods and create works that are influenced by online discourse rather than works on paper. This level of specificity gives birth to Internet art that enriches people's lives culturally. Most of the time, we attribute artistic creation to the era of contemporary technology's infancy and attribute its growth to the influence of online communities. Decentralization, represented by the end of blockchain-based storage, is now a feature of NFT artworks, allowing artists and collectors to conduct transactions directly with one another, without the need for middlemen according to Ante *et al*. [1]. A combination of technological innovation and creative expression has led to this. When compared to the standard collecting method, direct communication between artists and collection organizations has the potential to increase both the visibility of the creative process and the artist's public profile. Uniqueness is another feature, thanks to the fact that the NFT artwork identity is one-of-a-kind and that all of these details are incorporated using tamper-proof PROMETHEE (PMT) technology according to Baoet *et al*. [2].

Even though each transaction on a given blockchain is conducted independently, all data linkages on that blockchain are still linked to one another. A modification to one of them will have ripple effects across the other worksaccording to Pereiraet *et al*. [3]. Any changes to the blockchain's data systems need the approval of 50% of the collectors. This method ensures that NFT artworks remain scarce and recognizable throughout time, hence preserving their intrinsic value. This honest trading conduct may put an end to scams like selling fakes or stealing money from buyers and sellers, and it can protect the integrity of the art market. Perhaps most importantly, it includes resale rights via Solana Network (SNs) according to Zhai *et al*. [4], which were originally designed as a safety net to protect artists' interests; in otherwords, artists may acquire the right to profit anytime an artwork is sold to sustain their creative vigoro, but in fact, this system is difficult to execute. Due to the digital nature of NFT artworks, all ownership and creative rights of objects will apply to NFT artworks according to Aroraet *et al*. [5], and specialists may gain advantageous positions in the distribution of each artwork. This method provides a more open, fair, and equal regulatory framework.

Separation of ownership is another feature these systems must have. Despite the impossibility of physically dividing a piece of NFT art, ownership may be distributed to several recipients by exchanging monetary compensation. As tokens may be used to purchase completely owned artworks and to hold more ownership of artworks to minimize risks, this might increase the variety and number of transactions available to collectors according to Seifoddiniet *et al*. [6]. It might lower the bar to entry for collectors, reduce their need for liquid assets and exposure to market risk, and make it simpler for them to relocate their collections over the long term. An artwork's monetary value is a direct reflection of the technical difference between its purchase price and its current market value. Collectors of NFT works may place greater value on the works' market value than on its artistic or cultural significance.

In order to purchase or sell NFT artworks, collectors may use online trading platforms that provide a precise valuation of each item. NFT artworks may be realized by collectors using virtual currency, and lenders can acquire NFT artworks at reduced prices from defaulting borrowers according to Singh *et al*. [7]. This strategy might help the firm save money while increasing its economic worth by allowing it to acquire a wider variety of supplementary items. There is also a negative influence caused by the NFT's art collection. There is a lot of uncertainty about the cultural and monetary value of art, and the market for NFT art collections is now fragmented; depending on the time horizon, this might pose serious business risks. Whether five sheets are used as a virtual currency or NFT artworks are tools for making money in the business sector, users need to be cautious to avoid becoming victims of fraud. For those who own NFTs and also physical artwork, there is a system that goes against the rules of art. The benefits are negated by the collectors' mistakes in judgment and value judgments if the owner's NFT art is instantly destroyed and the collector's NFT art also experiences similar changes according to Chirtoacaet *et al*. [8].

The goal of art collecting is to protect and improve the value of the pieces throughout time. Such a large sum of money being spent on art is noteworthy. NFT artwork, on the other hand, may be traded like any other virtual product, much like digital currency. This kind of digital currency has a low rate of value retention, is very susceptible to market forces, and is subject to large price fluctuations. No works that can serve as market references owing to their wide cultural history and capacity to represent the essence of human civilization exist, and there is a lack of economic evaluation and associated systems for the relevant NFT artworks according to Kshetriet *et al*. [9]. The market for NFT art collecting is similarly unpredictable and chaotic, with prices set by a combination of market adjustment and the collectors' psychological conjecture. Even if we may reduce the amount of manual work involved, deep learning is data-driven and requires massive volumes of data for training.

Traditional artistic works according to Darshanet *et al*. [10]. are usually pleasing to the eye or even admirable, and only the artist is permitted to create works of art. As the popularity of digital art has grown according to Arthaet *et al*. [11]. many artists have shifted their attention away from engaging with their audience in favor of creating new works according to Nagpalet *et al*. [12]. As the public increasingly serves as the target demographic, it might be difficult for authors to effectively convey their ideas to their readers in different works. Because of the proliferation of NFT artwork production according to Mieszkoet *et al*. [13]. the public is now actively engaged in the creative process according to Yet *et al*. [14]. When an audience can create works of art, they may change the performance components at any time, enabling them to not only participate in the art but also express certain feelings via specific works of art. When it comes to depth and breadth of creative expression, NFT artworks often break through traditional boundaries between the artist and the work itself via social engagement and timely expression, enabling the audience to express their sentiments through the work according to Lennartet *et al*. [15].

The market value of NFT artworks as a collectible fluctuates according to the regulations of the market and the collector's own preferences. As a consequence of continuous developments in science and technology, an endless variety of digital tools and new products keep popping up. Human creative output has grown more dependent on the free flow of information from a variety of sources. The traditional paper medium and passive acceptance have given place to more imaginative and distributing approaches according to Khati *et al*. [16] based on digital platforms according to Singh *et al*. [17]. Digital artworks according to Bamakan *et al*. [18], ”soundscapes”, according to Posavec *et al*. [19], and ”images” according to Bouraga *et al*. [20] have all supplanted traditional text-based modes of communication according to Rehmanet *et al*. [21]. The way people talk to one another and exchange ideas has been revolutionized by this new, all-encompassing style of communication.

Art trading rules according to Parket *et al*. [22] are unique and founded on internet commerce according to Weijerset *et al*. [23]. Artwork has both a monetary and an aesthetic value, with the former having a direct correlation to the latter according to Galal *at al*. [24]. Models proposed in, according to Meynset *et al*. [25]. discuss use of Decentralized Reputation System (DRS) and similar methods for optimization of NFT creation process. It's also the basis for the higher value of classical artworks when compared to the value of many other types of artworks. The proliferation of digital media according to Sestino *et al*. [26] has facilitated the dissemination of a wide variety of artistic practices. In most cases according to Hasan *et al*. [27]. manual transmission is still requiredwhen creating NFT artworks for digital platforms. This is a time-consuming and resource-intensive process that is highly dependent on the individual's skill set and experience. Intelligent NFT artwork creation based on deep learning algorithms according to Kimet *et al*. [28] is still challenging to implement in practice for real-time use cases.

Based on this discussion, it can be observed that existing NFT design techniques use computationally complex encryption models like Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), etc according to Alnuaimi *et al*. [29]. which restricts their general-purpose usability, thereby limiting their scalability for real-time use cases. To overcome this drawback, while maintaining high-security, next section of this text proposes design of a light weight restrictive non-fungible token based on Practically Unclonable Functions (PuFs) via image signature patterns.The model was evaluated on different NFT applications in section 3, where its efficiency was evaluated and compared with existing NFT generation techniquesaccording to Gebreab *et al*. [30]. Finally, this text concludes with some interesting observations about the proposed NFT generation & distribution model and also recommends methods to further extend its performance to different use cases.

2. Design of the proposed Fusion model to identify Fake Profiles from Multimodal Social Media Datasets

The discussion on existing NFT-based models reveals that these design techniques employ computationally complex encryption models such as Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), etc.according to Madine *et al*. [31], which limits their general-purpose usability and scalability for real-time use cases. This section discusses the design of the proposed lightweight restrictive non-fungible token based on Practically Unclonable Functions (PuFs) via image signature patterns in order to overcome this drawback while maintaining a high level of security according Battah *et al*. [32]. The model collects context-specific information sets about the entity requiring tokenization and uses this information to generate restrictive hash sets, as depicted in Figure 1. These hash sets are run through a customized PuF model that generates hash signatures that resemble images. The generated hash signatures are embedded iteratively into unique images, which are combined using a dual visual encryption-decryption procedure. The encryption process generates two image sets, which are distributed to the buyer and seller, whereas the decryption process combines these image sets into a single file token according to Renet *et al*. [33]. During reselling operations, these tokens undergo another encryption-decryption-based validation process. Due to the utilization of PuFs and restrictive hash-sets, the proposed model is deployable for low-power IoT applications and scalable for general-purpose use cases.

Thus, all input assets are initially represented by contextual parameter sets, which include,

1. Token Type (TT), which represents if the token is saleable re-saleable or reproduceableaccording to Gellman *et al*. [34].
   (a) Saleable tokens have immutable hash structures, and cannot be transferred to other users (TT=1)
   (b) Re-saleable tokens have internal sidechains, and can be transferred between users (TT=2)
   (c) Reproduceable tokens can be shared between different users via selective ownership mechanisms (TT=3)
2. Total Number of Tokens to be created for the asset (NT)
3. Cost Pattern of Tokens (CP), which can be either Fixed Price (CP=1), or Variable Price (CP=2)
4. Distribution Geographic Area (DA) for the tokens
5. Security Level (SL) for the tokens
   (a) This can be either Low (SL=1), Medium (SL=2) or High (SL=3)
   (b) Based on this level, encryption & hashing models will be modified during generation of tokens
   (c) Security Level is directly proportional to processing cost for generation & configuration of individual Tokens

Based on these parameter sets, a Genetic Algorithm (GA) is used for generation of restrictive hash sets. These hash sets assist in lowering the computational complexities during generation, verification and reconfiguration of tokens. To generate

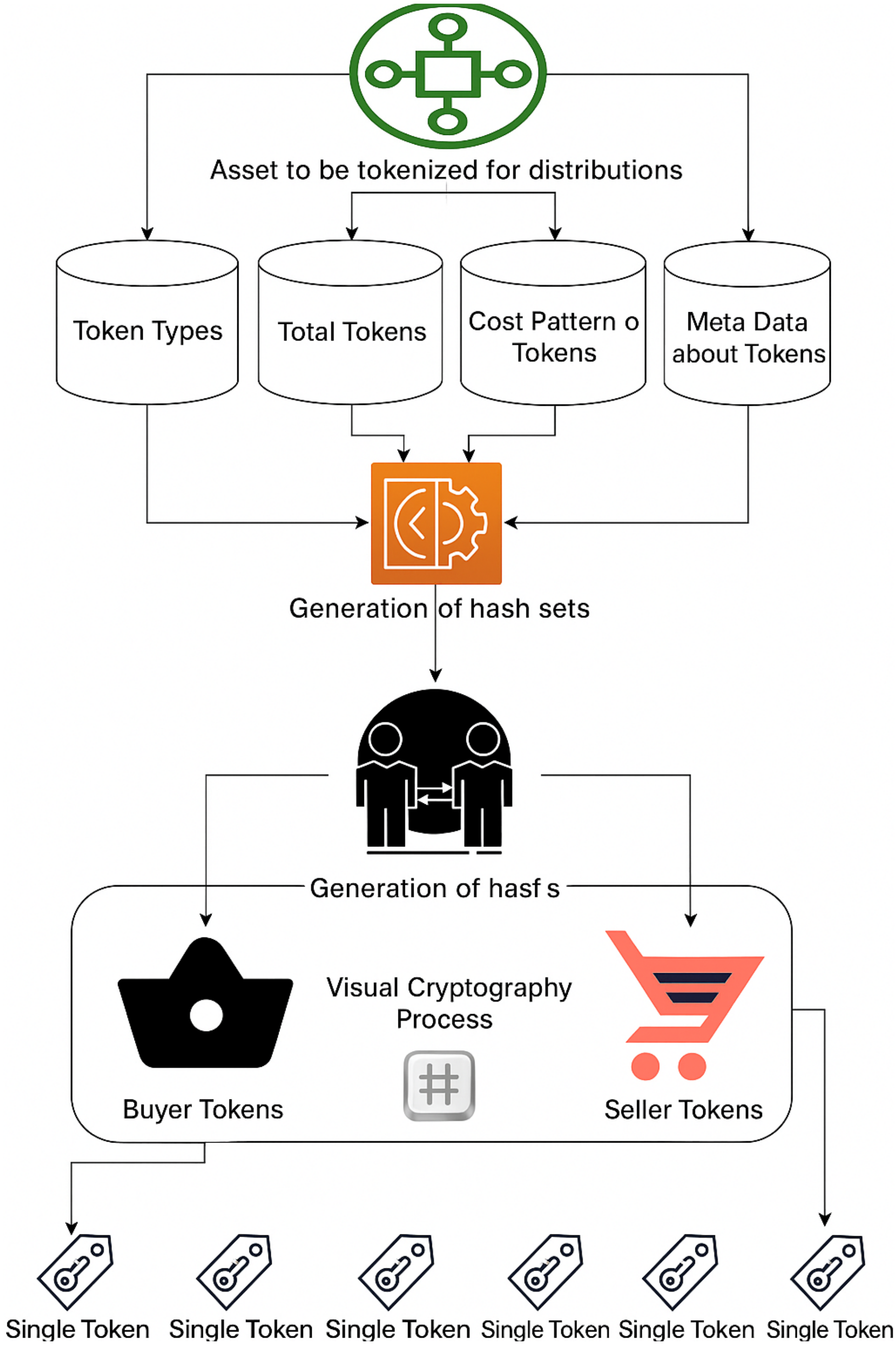

Figure 1. Design of the proposed NFT generation process.

these hash sets, a Reference Hash Metric (RHM) is estimated via equation 1:

$$RHM = DA * NT * (TT + CP + SL) . \tag{1}$$

The GA Model works as per the following process:

1. To setup the hash optimization model, initialize the following GA constants,
   (a) Genetic iterations used reconfiguration of solutions (N_i)
   (b) Genetic Algorithm Solutions that will be generated and reconfigured (N_s)
   (c) Individual solution-level learning rates (L_r)
2. Based on these constants, the model initially generates N_s different hash sets as per the following process,

(a) Generate a total N number of tokens via the following process,

i. Aggregate information related to given assets into a single vector array

ii. Initialize N via equation 2:

$$N = STOCH(L_r, 1) * RHM, \tag{2}$$

where $STOCH$ generates stochastic values between the given range via Markovian optimizations.

iii. Segregate this information into M parts of stochastic lengths via equation (3):

$$M = \frac{N}{NT} \tag{3}$$

iv. To generate each of these M parts, use the following process:

3. Create a block for this part as per the block structure given in Table 1,
In this block structure, the following Meta Data information Sets are stored:

(a) TT Meta Data Sets, which consist of ownership information about the NFTs

(b) CP Meta Data Sets, which consists of current price of the NFTs

(c) DA Meta Data Sets, which consists of location of individualtokens

(d) SL Meta Data Sets, which contains information about the used Hashing & Encryption techniques

(e) Generate a stochastic Hashing Model (HM) & Encryption Model(EM) as per equations (4) & (5).

$$HM = STOCH(SL(H) * L_r,\ SL(H)), \tag{4}$$

$$EM = STOCH(SL(E) * L_r,\ SL(E)), \tag{5}$$

where $SL(H)$ & $SL(E)$ represent total number of hashing & encryption models available for current security levels.

4. Using the selected hash model, generate block hashes for each of the tokens as per equation (6).

$$BH = HM(TC,\ TS,\ nC,\ TTM,\ CPM,\ DAM,\ SLM), \tag{6}$$

where nC is a stochastic nonce, which is estimated via equation (7).

$$nC = STOCH\left(L_r * 2^{bHM},\ 2^{bHM}\right), \tag{7}$$

where bHM represents total number of bits that are supported by individual hashing models.

5. The value of nC is generated such that unique values of BH are generated for individual blocks

(a) Once these M parts are created, then solution fitness is estimated via equation (8):

$$f = \frac{1}{M}\sum_{i=1}^{M}\frac{S(nC_i)}{d_i}, \tag{8}$$

where $S(nC)$ & d represents the size of generated nonce, and delay needed for hashing operations.

i. Generation of N_s different solutions is done as per the same process

ii. Once all solutions are generated, then a solution fitness threshold is estimated as per equation 9:

$$f_{th} = \frac{1}{N_s}\sum_{i=1}^{N_s} f_i * L_r. \tag{9}$$

iii. After evaluation of this fitness, solutions with $f < f_{th}$ are regenerated (or mutated) in next iteration, while other solutions are crossover to consecutive iterations.

Once all iterations are completed, then solutions with $f > f_{th}$ are combined, and their solutions are aggregated to form a restrictive set of hashes. New tokens are generated by taking consecutive hashes from this set, which reduces the time needed for generation of these tokens.

Once these tokens are generated, then a Practically Unclonable Function (PuF) is used for generation of hashed image sets. This PuF uses a trapdoor function, which is estimated via equation (10).

$$E_{gn}(x, y) = g^x n^y \ MOD\ n^2, \tag{10}$$

where $n = p * q$, which are two large prime numbers, g represents an effective unique integral value of x that belongs to (0, n), such that two numbers w_1 & w_2 when generated via equation (11), are able to regenerate the same value sets.

$$\left[w_1 * w_2 \ \%\ n^2\right] = \left[(w_1 + w_2) * g\ \right] \ \%\ n, \tag{11}$$

while, $x,\ y$ are represented via equations (12) & (13) as follows:

$$x = \frac{L\left(w_1 \% n^2\right)}{L(g \% n^2)} mod\ n, \tag{12}$$

$$y = \left(g^{-x}\right)^{\frac{1}{n}} \ mod\ n, \tag{13}$$

where L is a Lagrange's Polynomial, which is represented via equation (14).

$$\begin{aligned} L(x) = HM(x_1) * &\left[\frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)}\right] + \\ HM(x_2) * &\left[\frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)}\right] + \\ HM(x_3) * &\left[\frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)}\right], \end{aligned} \tag{14}$$

where $x_1,\ x_2,\ \&\ x_3$ represents 3 stochastic nonce values from the generated set of restrictive hashes. Thus, every NFT is passed through equations (10) – (14) to generate 2 sets of PuFs (x & y), which can be used for buying and selling operations.

These operations are facilitated via Shamir's secret sharing mechanisms, which can be observed from Figure 2a, and Figure 22b, where share generation (selling) & reconstruction (buying) operations can be visualized for different share types.

To generate shares, the seller decides how many sub-tokens (k) are needed by them for selling, and the system generates

Table 1. Block structure of the NF Tokens.

Token Contents (TC)	Timestamp (TS)	Nonce (nC)	Block Hash (BH)
TT Meta Data Sets (TTM)	CP Meta Data Sets (CPM)	DA Meta Data Sets (DAM)	SL Meta Data Sets (SLM)

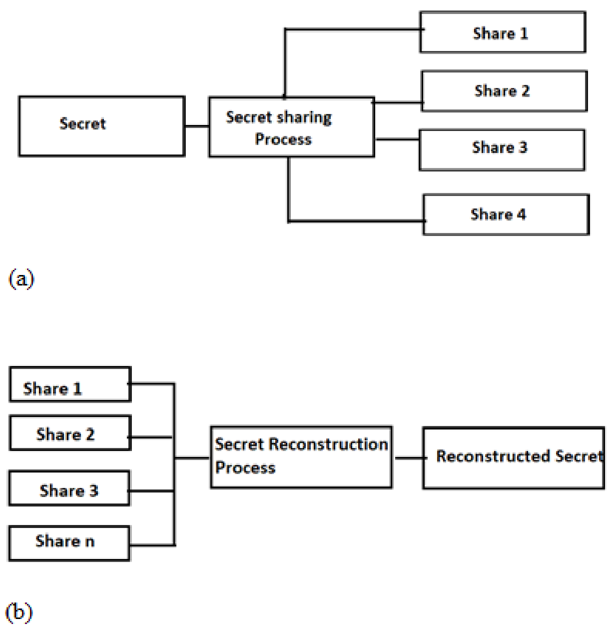

Figure 2. (a) Shamir share creation process (b) Shamir share reconstruction process.

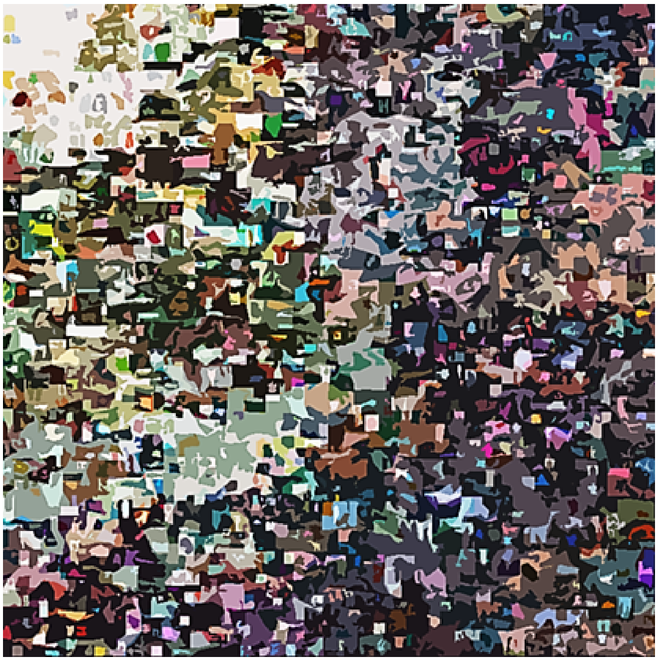

Figure 3. Sample of generated NFTs from the visual cryptography process.

($n = k^2$), different sub-tokens for the purpose of extended distributions. To perform this task, all PuF seller values are given to equation (15) for generation of n different shares.

$$S(x) = \sum_{i=1}^{n} \left[s(x_i) \prod_{j=1,\ j \neq i}^{k} \frac{x - x_j}{\left(x_i - x_j\right)} \right] mod\ p, \tag{15}$$

where p is generated by the PuF process, while $s(x)$ is the input data which needs to shared, and x represents nonce values which are selected stochastically from the restrictive hash sets. Once these shares are generated, then they are aggregated to form a single image, which is represented via equation (16):

$$I = \bigcup_{i=1}^{n} S(x)_i. \tag{16}$$

A sample NFT generated by this process is depicted in Figure 3, where it can be observed that individual rows represent single visual shares.

While selling, the seller has to perform decoding operations on any k parts of this image via equation (17).

$$s(x) = \left(1 + s_1 * x + s_2 * x^2 + \cdots + s_{n-1} * x^{k-1}\right). \tag{17}$$

Which will assist regeneration of the original token hashes, that can be used for viewing & redistribution purposes. Due to which, the model is able to improve its sharing, re-distribution, and security characteristics according to Manzoor *et al.* [35]. These characteristics are compared in terms of delay needed during distribution, delay needed for re-distribution, and energy needed during formation of shares. A comparison of these metrics is done in the next section of this text.

3. Result evaluation & comparison

The proposed NFT generation model initially collects contextual information about different token sets, and uses this information to generate restrictive hash setsaccording to Bellagardaet *et al.* [36]. These hash sets are created via a Genetic Algorithm (GA), which assists in reducing the delay needed for evaluation of hash values while generating different tokens, Hash sets generated by the GA process are used for generation of buyer and seller PuF values, which internally uses Lagrange's polynomial for generation of share distribution matrices. These polynomials are given to a Shamir Secret Sharing process, that generates squared arrays, which are used for creation of seller-NFTs according to Maksymyuket *et al.* [37]. These seller-NFTs can be commercially sold, and verified via an inverse secret sharing regeneration process. The regenerated tokens can be re-distributed via the same operations, which will

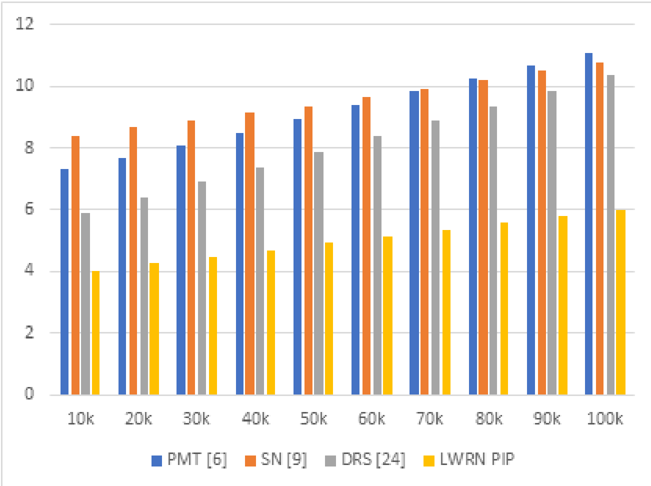

Figure 4. Delay needed for buying different NFTs.

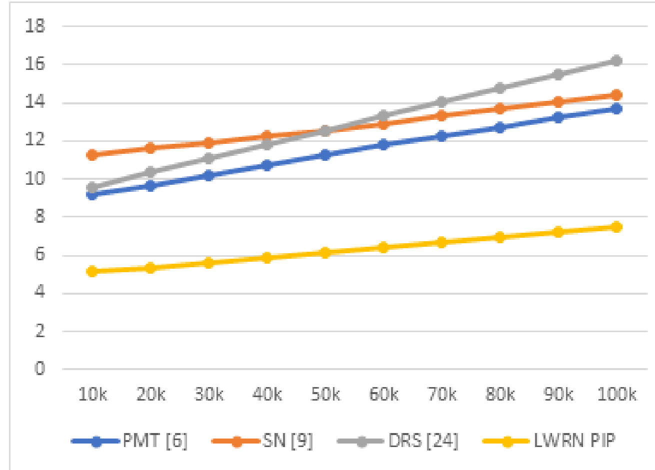

Figure 5. Energy needed for buying different NFTs.

assist buyers and sellers to modify & tune their costs.

To evaluate the performance of this model, it was validated on Ethereum NFTs https://www.kaggle.com/datasets/simiotic/ethereum-nfts, Zenodo NFTs, (https://zenodo.org/record/6967048#.Y528tHZBy3A), NFT Collections https://www.kaggle.com/datasets/hemil26/nft-collections-dataset, Snowflake NFTs https://www.snowflake.com/datasets/allocaterite-nft-dataset/.

All these collections were combined to form a total of 150k asset samples, which were divided into multiple NFTs ranging between 10k to 100k for individual assets according to Elmay *et al.* [38]. NFT generation and regeneration performance was estimated via simulating the model on Network Simulator (NS3), via the parameter sets observed from Table 2.

As per this evaluation strategy, the average delay needed for selling N NFTs is estimated via equation (18),

$$D_{sell} = \frac{1}{N}\sum_{i=1}^{N} t_{end_i} - t_{start_i}, \tag{18}$$

where t_{start}&t_{end} represent the timestamps for initiating and completing the NFT transfer process. This delay was estimated for PMT according to Seifoddini *et al.* [6], SN according to Kshetri ȇt al. [9], Galal *at al.* [24], and compared with the proposed model in Table 3.

As per this evaluation and Figure 4, it can be observed that the proposed model is able to achieve 10.5% faster performance when compared with PMT according to Seifoddini *et al.* [6], 9.4% faster than SN according to Kshetri *et al.* [9], and 8.5% when compared with Galal *at al.* [24], which makes it highly useful for large-scale scenarios. The reason for this improvement is use of Genetic Algorithm (GA) which assists in identification of restrictive hash sets. These hash sets reduce the need of instantaneous computations during generation of tokensaccording to Antelmiet *et al.* [39]. Due to which, the model is useful for high-speed NFT generation use cases.

Similarly, energy consumption was evaluated via equation (19), as follows:

$$E = \frac{1}{N}\sum_{i=1}^{N} E_{start_i} - E_{end_i} \tag{19}$$

where E_{start}&E_{end} are energy levels of nodes during start and completion of NFT generation operations. These levels can be observed from Table 4.

As per this evaluation and Figure 5, it can be observed that the proposed model is able to achieve 8.3% lower energy consumption when compared with PMT according to Seifoddini *et al.* [6] ,12.4% lower energy consumption than SN according to Kshetri *et al.* [9], and 15.5% lower energy consumption than Galal *at al.* [24], which makes it highly useful for high lifetime scenarios. The reason for this improvement is use of Genetic Algorithm (GA) with PuFswhich assists in identification of restrictive hash sets. These hash sets eliminate the need for continuous hashing during generation of tokens. Due to which, the model is useful for low energy NFT generation use cases. Similarly, average levels of throughput were evaluated as seen in equation (20).

$$TDR = \frac{1}{N}\sum_{i=1}^{N} \frac{T_{rx_i}}{T_{tx_i}}, \tag{20}$$

where T_{rx}& Drepresent total tokens received and the delay during reception of these tokens. Based on this evaluation, the throughput levels can be observed from Table 5.

As per this evaluation and Figure 6, it can be observed that the proposed model is able to improve the throughput during buying NFTs by 8.3% when compared with PMT according to Seifoddini *et al.* [6], 8.5% when compared with SN according to Kshetri *et al.* [9], and 9.4% when compared with Galal *at al.* [24], which makes it useful for high date rate scenarios. The reason for this improvement in throughput is use of PuFs with secret sharing which assists in identification of restrictive hash sets. These hash sets reduce computational delays, and

Table 2. Network parameters used for communication of NFTs.

Distributed Network Parameter Sets	Instance Values of these Sets
Total nodes for sharing the NFTs	500 to 2000
Protocol used for Routing these NFTs	DSR
Geographical size of the network scenarios	10km x 10km
Energy Model Details	Power consumed during transmission of NFTs = 1mJ Power consumed during reception of NFTs = 0.2 mJ Power consumed when nodes are performing NFT calculations= 0.1 mJ Initial level of energy for participating nodes = 2 W Energy needed by nodes when shifting from buyer to seller = 0.01 mW

Table 3. Delay needed for buying different NFTs.

N	D (ms) PMT [6]	D (ms) SN [9]	D (ms) DRS [24]	D (ms) LWRN PIP
10k	7.32	8.36	5.90	4.04
20k	7.69	8.67	6.39	4.26
30k	8.06	8.91	6.89	4.47
40k	8.48	9.14	7.38	4.68
50k	8.94	9.37	7.88	4.91
60k	9.38	9.63	8.37	5.13
70k	9.83	9.92	8.87	5.36
80k	10.24	10.21	9.37	5.59
90k	10.64	10.49	9.86	5.81
100k	11.05	10.76	10.35	6.02

Table 4. Energy needed for buying different NFTs.

N	E (mJ) PMT [6]	E (mJ) SN [9]	E (mJ) DRS [24]	E (mJ) LWRN PIP
10k	9.23	11.27	9.59	5.11
20k	9.69	11.61	10.33	5.37
30k	10.19	11.92	11.07	5.63
40k	10.72	12.23	11.81	5.89
50k	11.26	12.57	12.56	6.16
60k	11.78	12.93	13.30	6.43
70k	12.26	13.35	14.04	6.70
80k	12.75	13.72	14.78	6.96
90k	13.22	14.09	15.52	7.23
100k	13.71	14.45	16.26	7.49

increases the data rates for generation of tokens. Due to which, the model is useful for high throughput NFT generation use cases. Similarly, token delivery ratio (TDR) was evaluated via equation (21).

$$TDR = \frac{1}{N}\sum_{i=1}^{N}\frac{T_{rx_i}}{T_{tx_i}}, \tag{21}$$

where T_{tx} is the number of tokens that are generated during each of the communications. Based on this strategy, the TDR (T) was tabulated in Table 6.

Table 5. Throughput needed for buying different NFTs.

N	T (kbps) PMT [6]	T (kbps) SN [9]	T (kbps) DRS [24]	T (kbps) LWRN PIP
10k	413.54	490.66	387.22	549.56
20k	434.30	506.91	418.11	578.09
30k	456.26	520.70	449.05	606.11
40k	479.86	534.17	479.87	634.66
50k	504.81	548.56	510.76	664.24
60k	528.95	563.95	541.66	693.90
70k	552.81	580.54	572.56	723.96
80k	575.56	596.52	603.46	753.26
90k	597.81	612.07	634.36	782.16
100k	620.41	627.10	665.25	810.98

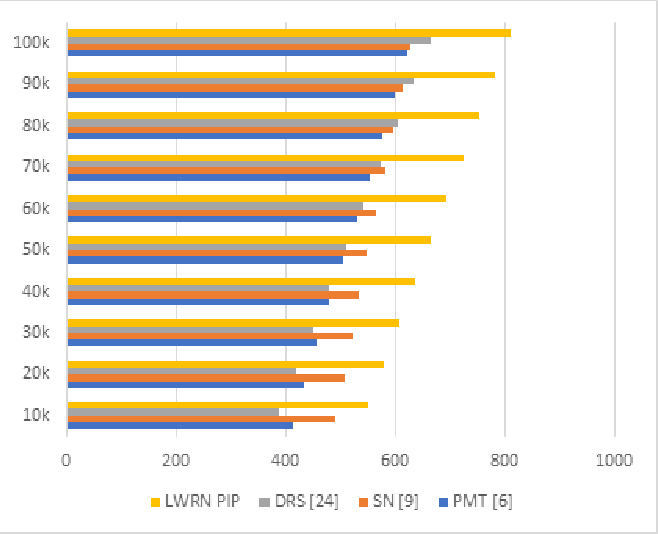

Figure 6. Throughput needed for buying different NFTs.

As per this evaluation and Figure 7, it can be observed that the proposed model is able to improve the TDR during buying NFTs by 9.4% when compared with PMT according to Seifoddini *et al.* [6], 5.9% when compared with SN according to Kshetri *et al.* [9], and 10.5% when compared with Galal *at al.* [24], which makes it useful for high-acceptancetoken com-

Table 6. Token Delivery Ratio obtained for buying different NFTs.

N	T (%) PMT [6]	T (%) [9]	T (%) DRS [24]	T (%) LWRN PIP
10k	93.10	92.19	93.25	98.09
20k	92.25	91.51	92.02	97.57
30k	91.35	90.93	90.78	97.06
40k	90.38	90.36	89.54	96.54
50k	89.36	89.76	88.31	96.00
60k	88.37	89.11	87.07	95.46
70k	87.39	88.41	85.84	94.92
80k	86.46	87.74	84.60	94.39
90k	85.54	87.08	83.36	93.86
100k	84.61	86.45	82.13	93.34

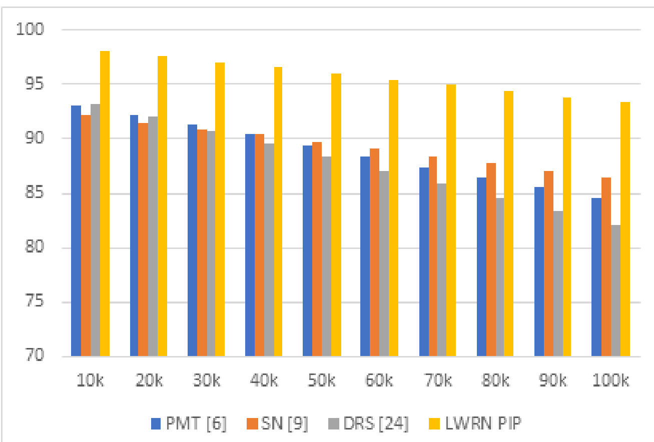

Figure 7. Token Delivery Ratio obtained for buying different NFTs.

Table 7. Energy needed for re-selling different NFTs.

N	D (ms) PMT [6]	D (ms) SN [9]	D (ms) DRS [24]	D (ms) LWRN PIP
10k	10.52	10.96	9.16	5.63
20k	11.06	11.28	9.84	5.91
30k	11.62	11.58	10.52	6.19
40k	12.21	11.89	11.21	6.48
50k	12.80	12.23	11.89	6.77
60k	13.36	12.58	12.58	7.06
70k	13.92	12.93	13.26	7.35
80k	14.47	13.27	13.94	7.63
90k	15.03	13.59	14.62	7.92
100k	15.59	13.92	15.30	8.20

munication scenarios. The reason for this improvement in TDR is use of secret sharing which assists in reducing errors during communication of tokens. Due to which, the model is useful for high TDR NFT generation use cases.

Under similar use cases, the delay needed for re-selling the tokens (purchasing tokens and then regeneration of tokens for further distributions), can be observed from Table 7.

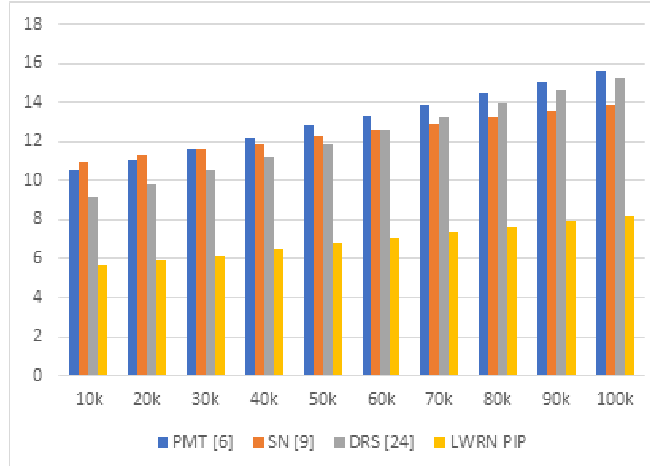

Figure 8. Delay needed for re-selling different NFTs.

Table 8. Energy needed for re-selling different NFTs.

N	E (mJ) PMT [6]	E (mJ) SN [9]	E (mJ) DRS [24]	E (mJ) LWRN PIP
10k	13.28	14.70	14.76	7.10
20k	13.95	15.10	15.78	7.44
30k	14.65	15.52	16.81	7.78
40k	15.34	15.96	17.83	8.12
50k	16.02	16.43	18.86	8.47
60k	16.67	16.90	19.88	8.81
70k	17.31	17.38	20.90	9.15
80k	17.98	17.82	21.92	9.50
90k	18.64	18.26	22.94	9.84
100k	19.32	18.70	23.96	10.18

As per this evaluation and Figure 8, it can be observed that the proposed model is able to achieve 8.5% faster performance when compared with PMT according to Seifoddini *et al.* [6], 6.4% faster than SN according to Kshetri *et al.* [9], and 5.3% when compared with Galal *at al.* [24], which makes it highly useful for large-scale scenarios. The reason for this improvement is use of Genetic Algorithm (GA) which assists in identification of restrictive hash sets. These hash sets reduce the need of instantaneous computations during generation of tokens. Due to which, the model is useful for high-speed NFT re-selling use cases. Similarly, energy consumption can be observed from Table 8.

As per this evaluation and Figure 9, it can be observed that the proposed model is able to achieve 7.5% lower energy consumption when compared with PMT Seifoddini *et al.* [6], 10.5% lower energy consumption than SN according to Kshetri *et al.* [9], and 12.4% lower energy consumption than DRS H. S. Galal *at al.* [24], which makes it useful for high lifetime scenarios. The reason for this improvement is use of Genetic Algorithm (GA) with PuFs which assists in identification of restrictive hash sets. These hash sets eliminate the need for continuous hashing during re-selling of tokens. Due to which, the

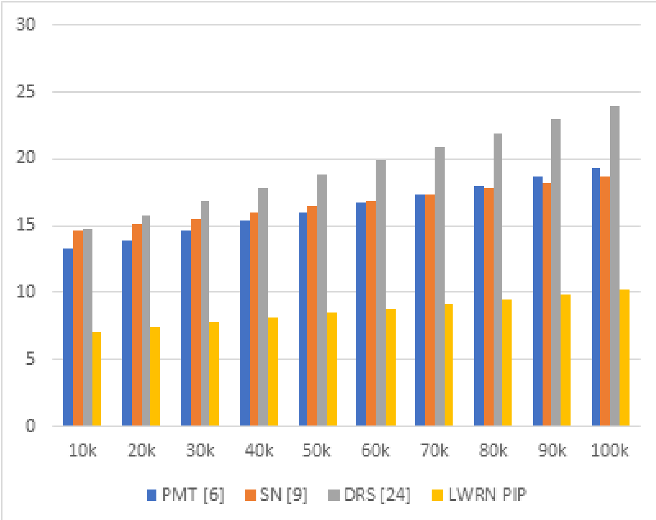

Figure 9. Energy needed for re-selling different NFTs.

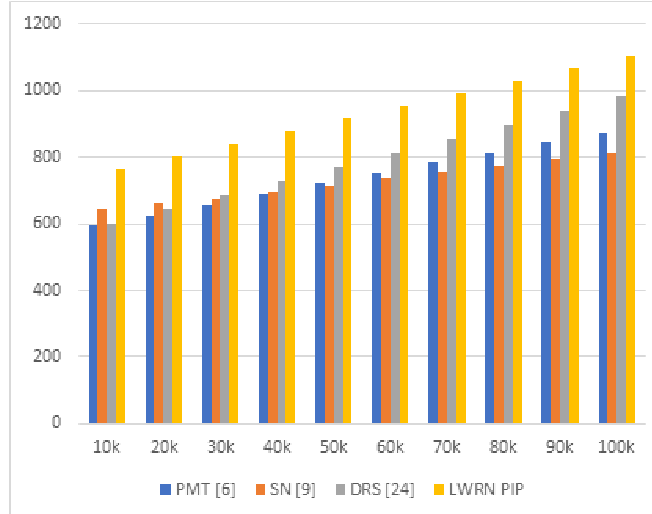

Figure 10. Throughput needed for re-selling different NFTs.

Table 9. Throughput needed for re-selling different NFTs.

N	T (kbps) PMT [6]	T (kbps) SN [9]	T (kbps) DRS [24]	T (kbps) LWRN PIP
10k	594.65	641.39	598.02	764.01
20k	625.08	659.48	640.62	801.00
30k	656.63	677.31	683.22	838.36
40k	688.81	696.01	725.81	876.37
50k	720.71	715.49	768.43	914.63
60k	751.71	735.34	811.05	952.67
70k	782.20	755.07	853.67	990.44
80k	812.80	774.08	896.28	1027.93
90k	843.59	792.83	938.88	1065.38
100k	874.74	811.45	981.49	1102.92

Table 10. Token Delivery Ratio obtained for re-selling different NFTs.

N	T (%) PMT [6]	T (%) SN [9]	T (%) DRS [24]	T (%) LWRN PIP
10k	81.57	84.88	91.40	96.11
20k	80.74	84.32	90.16	95.60
30k	79.88	83.76	88.93	95.08
40k	79.00	83.17	87.69	94.55
50k	78.13	82.56	86.46	94.02
60k	77.28	81.94	85.22	93.49
70k	76.44	81.32	83.98	92.97
80k	75.61	80.73	82.75	92.44
90k	74.76	80.14	81.51	91.92
100k	73.91	79.56	80.27	91.40

model is useful for low energy NFT re-selling use cases. Similarly, average levels of throughput can be observed from Table 9.

As per this evaluation and Figure 10, it can be observed that the proposed model is able to improve the throughput during re-selling NFTs by 7.5% when compared with PMT Seifoddini *et al*. [6], 6.3% when compared with SN according to Kshetri *et al*. [9], and 8.5% when compared with Galal *at al*. [24], which makes it useful for high date rate scenarios. The reason for this improvement in throughput is use of PuFs with secret sharing which assists in identification of restrictive hash sets. These hash sets reduce computational delays, and increases the data rates for re-selling of tokens. Due to which, the model is useful for high throughput NFT re-selling use cases. Similarly, token delivery ratio (TDR) was tabulated in Table 10.

As per this evaluation and Figure 11, it can be observed that the proposed model is able to improve the TDR during re-selling NFTs by 18.3% when compared with PMT Seifoddini *et al*. [6], 10.5% when compared with SN according to Kshetri *et al*. [9], and 8.5% when compared with DRS H. S. Galal *at al*. [24], which makes it useful for high-acceptance token communication scenarios. The reason for this improvement in TDR is use of secret sharing which assists in reducing errors

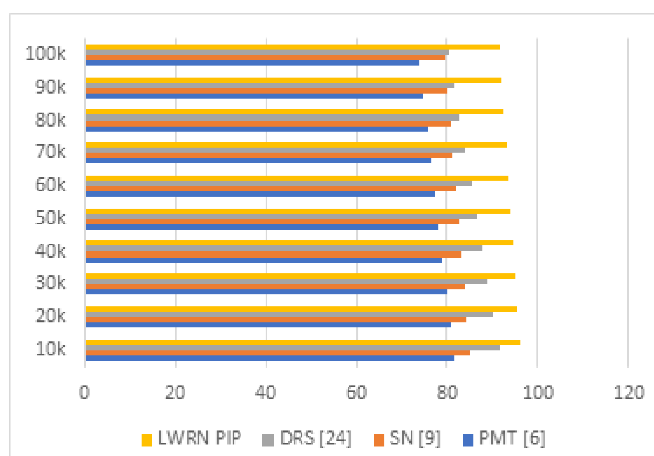

Figure 11. Token Delivery Ratio obtained for re-selling different NFTs.

during communication of tokens. Due to which, the model is useful for high TDR NFT re-selling use cases. As per these results, it can be observed that the proposed model is highly useful for a wide variety of NFT generation and reselling use cases, with high performance levels.

4. Conclusion and future scope

The proposed NFT generation model collects contextual information about various token sets, then uses this data to generate restrictive hash sets. These hash sets are generated using a Genetic Algorithm (GA), which reduces the time required to evaluate hash values while generating distinct tokens. Hash sets generated by the GA process are used to generate buyer and seller PuF values, which uses Lagrange's polynomial internally to generate share distribution matrices. These polynomials are provided to a Shamir Secret Sharing procedure, which generates squared arrays that are utilized in the generation of seller-NFTs. These seller-NFTs can be sold commercially and verified through an inverse secret sharing regeneration procedure. Tokens that have been regenerated can be redistributed using the same operations, allowing buyers and sellers to modify and tune prices.

In terms of delay required for generation and reselling, it was determined that the proposed model achieves 10.5% faster performance than PMT Seifoddini *et al.* [6], 9.4% faster performance than SN according to Kshetri *et al.* [9], and 8.5% faster performance than Galal *at al.* [24], making it extremely useful for large-scale scenarios. This improvement is due to the application of Genetic Algorithm (GA), which aids in the identification of restrictive hash sets. These hash sets reduce the need for immediate computations during token generation. Due to this, the model is useful for use cases involving rapid NFT generation. Compared to PMT Seifoddini *et al.* [6], SN according to Kshetri *et al.* [9], and DRS H. S. Galal *at al.* [24], the proposed model consumes 8.3% less energy than PMT J. Seifoddini *et al.* [6], 12.4% less energy than SN according to Kshetri *et al.* [9], and 15.5% less energy than Galal *at al.* [24], making it an excellent choice for high lifetime scenarios. This improvement is a result of the use of Genetic Algorithm (GA) with PuFs, which aids in identifying restrictive hash sets. These hash sets eliminate the need for repeated hashing during token generation. As a result, the model is applicable to low-energy NFT generation use cases.

Estimated in terms of throughput levels, it was found that the proposed model improves the throughput of purchasing NFTs by 8.3% when compared to PMT Seifoddini *et al.* [6], 8.5% when compared to SN according to Kshetri *et al.* [9], and 9.4% when compared to Galal *at al.* [24], making it useful for high date rate scenarios. This improvement in throughput is due to the utilization of PuFs with secret sharing, which facilitates the identification of restrictive hash sets. These hash sets decrease computational delays and increase token generation data rates. Due to this, the model is useful for NFT generation use cases with a high throughput. In terms of consistency levels, it was found that the proposed model can improve the TDR during the purchase of NFTs by 9.4% when compared to PMT Seifoddini *et al.* [6], 5.9% when compared to SN according to Kshetri *et al.* [9], and 10.5% when compared to Galal *at al.* [24], making it useful for high-acceptance token communication scenarios. This improvement in TDR is due to the use of secret sharing, which helps reduce errors during token communication. Consequently, the model is useful for use cases involving high TDR NFT generation. Based on these results, it can be seen that the proposed model is extremely useful for a wide range of NFT generation and reselling use cases, with high levels of performance.

The performance of this model must be validated on larger scale NFT generation and distribution use cases in the future, and it can be enhanced through the incorporation of bioinspired techniques for the generation of dynamic hashes and encryption key sets. This performance can also be enhanced through the incorporation of low-complexity deep learning models that can be applied to IoT-based networks for the pre-emptive transfer of tokens in response to various attack scenarios.

Data availability

The data used in this study were gethered from Ethereum NFTs https://www.kaggle.com/datasets/simiotic/ethereum-nfts, Zenodo NFTs https://zenodo.org/record/6967048#.Y528tHZBy3A, NFT Collections https://www.kaggle.com/datasets/hemil26/nft-collections-dataset, and Snowflake NFTs https://www.snowflake.com/datasets/allocaterite-nft-dataset/

References

[1] L. Ante, "The Non-Fungible Token (NFT) Market and Its relationship with Bitcoin and Ethereum", FinTech **1** (2022) 216. https://doi.org/10.3390/fintech1030017.

[2] H. Bao & D. Roubaud, "Non-fungible token: a systematic review and research agenda", Journal of Risk and Financial Management **15** (2022) 215. https://doi.org/10.3390/jrfm15050215.

[3] E. Pereira, P. Ferreira & D. Quintino "Non-fungible tokens (nfts) and cryptocurrencies efficiency and comovements", FinTech **1** (2022) 310. https://doi.org/10.3390/fintech1040023.

[4] Wenbin Zhai, "Innovation and research of digital artwork design based on big data and integrated media", Journal of Function Spaces **2022** (2022) 6333688. https://doi.org/10.1155/2022/6333688.

[5] A. Arora, Kanisk & S. Kumar, "Smart Contracts and NFTs: Non-Fungible Tokens as a Core Component of Blockchain to Be Used as Collectibles", in *Lecture notes on data engineering and communications technologies*, Springer, Singapore, 2021, pp. 401–422. https://doi.org/10.1007/978-981-16-3961-6_34.

[6] J. Seifoddini, "A multi-criteria approach to rating Metaverse games", Journal of Metaverse **2** (2022) 42. https://doi.org/10.57019/jmv.1053778.

[7] P. Singh, S. Khan, Y. V. Singh & R. S. Singh, "A secure and stable humanoid healthcare information processing and supervisory method with IoT-Based sensor network", Journal of Sensors **2022** (2022) 8568540. https://doi.org/10.1155/2022/8568540.

[8] D. Chirtoaca, J. Ellul,& G. Azzopardi, "A framework for creating deployable smart contracts for non-fungible tokens on the ethereum blockchain", *IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, Oxford, UK, 2020, pp. 100-105. https://doi.org/10.1109/DAPPS49028.2020.00012.

[9] N. Kshetri, "Economics of nonfungible tokens", Computer **55** (2022) 94. https://doi.org/10.1109/MC.2022.3192701.

[10] M. Darshan, S. R. Raswanth & P. Kumar, "Data analysis of Non Fungible Tokens (NFTs) pricing using brokerage firm data", in *IEEE Global Conference on Computing, Power and Communication Technologies (GlobConPT)*, New Delhi, India, 2022, pp. 1-5. https://doi.org/10.1109/GlobConPT57482.2022.9938298.

[11] K. A. R. Artha, S. N. Zain, A. A. Alkautsar & M. H. Widianto, "Implementation of smart contracts for e-certificate as non-fungible token using solana network, in *IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA)*, Yogyakarta, Indonesia, 2022, pp. 1-6. https://doi.org/10.1109/ICITDA55840.2022.9971423.

[12] Yashika Nagpal, "Non-Fungible Tokens (NFT's): The Future of Digital Collectibles", International Journal of Law Management and Humanities **4** (2021) 758. https://doij.org/10.10000/IJLMH.111984.

[13] Mazur, Mieszko, "Non-Fungible Tokens (NFT). The analysis of risk and return", 2021. [Online]. https://dx.doi.org/10.2139/ssrn.3953535.

[14] Y. Chandra, "Non-fungible token-enabled entrepreneurship: A conceptual framework", Journal of Business Venturing Insights **18** (2022) e00323. https://doi.org/10.1016/j.jbvi.2022.e00323.

[15] A. Lennart, "The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum", 2021. [Online]. https://dx.doi.org/10.2139/ssrn.3861106.

[16] P. Khati, A. K. Shrestha & J. Vassileva, "Non-Fungible Tokens Applications: A Systematic Mapping Review of Academic Research", in IEEE13thAnnualInformationTechnology, ElectronicsandMobileCommunicationConference(IEMCON), Vancouver, BC, Canada, 2022, pp. 0323-0330. https://doi.org/10.1109/IEMCON56893.2022.9946500.

[17] M. K. Singh, O. P. Rishi, A. K. Singh, P. Singh & P. Choudhary, "Implementation of knowledge based collaborative filtering and machine learning for e-commerce recommendation system", Journal of Physics: Conference Series **2007** (2021) 012032. https://iopscience.iop.org/article/10.1088/1742-6596/2007/1/012032/meta.

[18] S. M. H. Bamakan, N. Nezhadsistani, O. Bodaghi & Q. Qu, "Patents and intellectual property assets as non-fungible tokens; key technologies and challenges", Scientific reports **12** (2022) 2178. https://doi.org/10.1038/s41598-022-05920-6.

[19] A. B. Posavec, K. Aleksić-Maslać & M. Tominac, "Non-Fungible tokens: might learning about them be necessary?", in *45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, Opatija, Croatia, 2022, pp. 700-705. doi: 10.23919/MIPRO55190.2022.9803425.

[20] S. Bouraga, "On the popularity of non-fungible tokens: preliminary results, *3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Paris, France, 2021, pp. 49-50. https://doi.org/10.1109/BRAINS52497.2021.9569792.

[21] W. Rehman, H. E. Zainab, J. Imran & N. Z. Bawany, "NFTs: applications and challenges, in *22nd International Arab Conference on Information Technology (ACIT)*, Muscat, Oman, 2021, pp. 1-7. https://doi.org/10.1109/ACIT53391.2021.9677260.

[22] A. Park, J. Kietzmann, L. Pitt & A. Dabirian, "The Evolution of Nonfungible Tokens: Complexity and Novelty of NFT Use-Cases", IT Professional **24** (2022) 9. https://doi.org/10.1109/MITP.2021.3136055.

[23] D. Weijers & H. J. Turton, "Environmentally smart contracts for artists using non-fungible tokens", in *IEEE International Symposium on Technology and Society (ISTAS)*, Waterloo, ON, Canada, 2021, pp. 1-4. https://doi.org/10.1109/ISTAS52410.2021.9629203.

[24] H. S. Galal & A. M. Youssef, "Aegis: privacy-preserving market for Non-Fungible tokens", IEEE Transactions on Network Science and Engineering **10** (2022) 92. https://doi.org/10.1109/TNSE.2022.3205428.

[25] S. C. Meyns & F. Dalipi, "What users tweet on NFTs: mining twitter to understand nft-related concerns using a topic modeling approach, IEEE Access **10** (2022) 117658. https://doi.org/10.1109/ACCESS.2022.3219495.

[26] A. Sestino, G. Guido & A. M. Peluso, "The concept and technicalities of NFTs", *Non-Fungible Tokens (NFTs)*, Springer International, Switzerland, 2022, pp. 11–22. https://doi.org/10.1007/978-3-031-07203-1.

[27] H. R. Hasan, K. Salah, A. Battah, M. Madine, I. Yaqoob & R. Jayaraman "Incorporating Registration, Reputation, and Incentivization Into the NFT Ecosystem", IEEE Access **10** 2022 76416. https://doi.org/10.1109/ACCESS.2022.3192388.

[28] H. Kim, H. -S. Kim & Y. -S. Park, Perpetual Contract NFT as Collateral for DeFi Composability, in IEEE Access **10** (2022) 126802. https://doi.org/10.1109/ACCESS.2022.3225884.

[29] N. Alnuaimi, A. Almemari, M. Madine, K. Salah, H. A. Breiki & R. Jayaraman, "NFT certificates and proof of delivery for fine jewelry and gemstones", IEEE Access **10** (2022) 101263. https://doi.org/10.1109/ACCESS.2022.3208698.

[30] S. A. Gebreab, H. R. Hasan, K. Salah & R. Jayaraman, "NFT-Based traceability and ownership management of medical devices", IEEE Access **10** (2022) 126394. https://doi.org/10.1109/ACCESS.2022.3226128.

[31] M. Madine, K. Salah, R. Jayaraman, A. Battah, H. Hasa & I. Yaqoob, "Blockchain and NFTs for Time-Bound access and monetization of private data, IEEE Access **10** (2022) 94186. https://doi.org/10.1109/ACCESS.2022.3204274.

[32] A. Battah, M. Madine, I. Yaqoob, K. Salah, H. R. Hasan & R. Jayaraman, Blockchain and NFTs for Trusted Ownership, Trading, and Access of AI Models, IEEE Access **10** (2022) 112230. https://doi.org/10.1109/ACCESS.2022.3215660.

[33] Y. Ren, R. Xie, F. R. Yu, T. Huang & Y. Liu, "Green Intelligence Networking for Connected and Autonomous Vehicles in Smart Cities", IEEE Transactions on Green Communications and Networking **6** (2022) 1591. https://doi.org/10.1109/TGCN.2022.3148293.

[34] P. Gellman, "Blockchain: The new art house", ITNOW **63** (2021) 18. https://doi.org/10.1093/itnow/bwab070.

[35] A. Manzoor, M. Samarin, D. Mason & M. Ylianttila, "Scavenger Hunt: Utilization of Blockchain and IoT for a Location-Based Game", IEEE Access **8** (2020) 204863. https://doi.org/10.1109/ACCESS.2020.3037182.

[36] J. S. Bellagarda & A. M. Abu-Mahfouz, "An updated survey on the convergence of distributed ledger Technology and Artificial Intelligence: Current State, Major Challenges and Future Direction, IEEE Access **10** (2022) 50774. https://doi.org/10.1109/ACCESS.2022.3173297.

[37] T. Maksymyuk, J. Gazda, G. Bugár, V. Gazda, M. Liyanage & M. Dohler, "Blockchain-empowered service management for the decentralized metaverse of things", IEEE Access **10** (2022) 99025. https://doi.org/10.1109/ACCESS.2022.3205739.

[38] F. K. Elmay, K. Salah, R. Jayaraman & I. A. Omar, "Using NFTs and blockchain for traceability and auctioning of shipping containers and cargo in maritime industry, IEEE Access **10** (2022) 124507. https://doi.org/10.1109/ACCESS.2022.3225000.

[39] A. Antelmi, G. D'Ambrosio, A. Petta, L. Serra & C. Spagnuolo, "A volunteer computing architecture for computational workflows on decentralized web", IEEE Access **10** (2022) 98993. https://doi.org/10.1109/ACCESS.2022.3207167.