


# Secure Image Retrieval and Sharing Technologies for Digital Inclusive Finance: Methods and Applications



Wei Wang 

Academic Affairs Office, Henan Open University, Zhengzhou 450046, China

Corresponding Author Email: [wangwei1@haou.edu.cn](mailto:wangwei1@haou.edu.cn)

<https://doi.org/10.18280/ts.400525>

## ABSTRACT

**Received:** 6 May 2023

**Revised:** 18 August 2023

**Accepted:** 26 August 2023

**Available online:** 30 October 2023

### Keywords:

*digital inclusive finance, secure image retrieval, secure image sharing, hash index method, reversible data hiding (RDH)*

In the evolving landscape of digital inclusive finance, securing voluminous user data and transaction information, predominantly image data, has emerged as a pivotal challenge in financial technology. Despite extensive research on secure image retrieval and sharing, the unique demands presented by digital inclusive finance remain largely unaddressed, leading to inefficiencies and potential vulnerabilities in large-scale, high-frequency financial transactions. In response to this gap, two novel image processing methods, tailored specifically for secure image retrieval and sharing applications, have been proposed. These methods endeavour to enhance efficiency in image data processing while fortifying its security, ensuring the safe integration of these technologies within the realm of digital inclusive finance. Emphasis has been placed on the innovative application of the hash index method and reversible data hiding (RDH) to address these concerns. It is anticipated that these advances will pave the way for more secure and efficient operations in the broader financial technology sector.

## 1. INTRODUCTION

In the intertwined realms of global financial markets and technological evolution, digital inclusive finance has emerged as a pivotal catalyst in the innovation and widespread adoption of financial services [1, 2]. This novel financial paradigm not only transcends the confines of traditional financial offerings but also facilitates unparalleled accessibility for individuals across diverse economic strata [3-6]. However, an exponential surge in data, especially image data pertinent to customer identity verification, electronic signatures, and transaction evidences, has been observed in financial institutions, primarily driven by advancements in big data and cloud computing technologies [7-9]. The dual challenge of bolstering the efficiency of financial services whilst safeguarding the integrity of this sensitive image data remains an unresolved quandary in the domain of financial technology [10, 11].

In contemporary digital settings, the significance of image data in financial transactions cannot be overlooked [12-15]. Secure image retrieval and sharing technologies hold paramount importance in fortifying the realm of digital inclusive finance. Firstly, such technological measures are pivotal in nurturing a trustworthy digital financial ecosystem, thereby amplifying users' confidence and propensity towards the adoption of financial technologies [16]. For financial institutions, these technologies not only mitigate the threats of substantial economic ramifications stemming from data breaches but also enhance their competitive standing and fortify their rapport with clientele [17, 18].

Despite a plethora of research endeavours focused on secure image retrieval and sharing, a discernible gap exists, with many methodologies overlooking the intricate challenges intrinsic to digital inclusive finance [19-23]. Certain retrieval

algorithms, it has been noted, inadequately address the nuanced sensitivity and privacy dimensions of financial data, culminating in potential unauthorized access or misuse of user information. Furthermore, many extant image sharing technologies have been observed to grapple with performance limitations, especially when deployed in intricate, large-scale, and high-frequency financial operations, rendering them unsuitable for catering to the real-world exigencies of the financial sector.

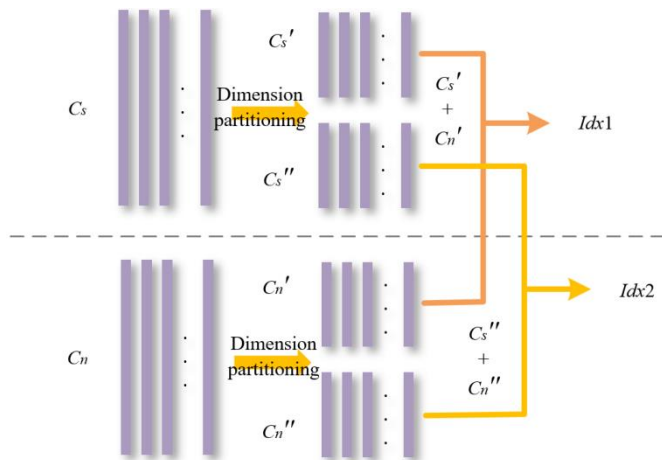
In light of these challenges, comprehensive research has been conducted. Emphasis has been laid on the proposition of secure image retrieval tailored for digital inclusive finance, wherein an avant-garde hash index method grounded in dimension partitioning was employed for the efficient and secure processing of finance-related image data, thus sidestepping potential security pitfalls. A subsequent discourse delved into secure image sharing specific to digital inclusive finance, introducing a clandestine image sharing algorithm rooted in RDH, achieving a balance between secure image sharing and ensuring image veracity and reversibility. The inception and empirical validation of these seminal technologies not only hold considerable academic merit but also promise to leave an indelible mark on the practical facets of the financial technology landscape.

## 2. SECURE IMAGE RETRIEVAL APPLICATION FOR DIGITAL INCLUSIVE FINANCE

The ascent of digital inclusive finance has led to the generation of substantial user data volumes. Such data, rather than being confined solely to textual information, encompasses a myriad of image types, encompassing user identification, banking instruments, manual signatures, and transaction certificates. Distinctively, numerous transactions

within the realm of digital inclusive finance necessitate immediate or near-immediate processing, demanding rapid data retrieval capabilities. Concurrently, the inherent sensitivity and privacy of financial data accentuate the ineffectiveness of conventional index methods in safeguarding such data. Thus, an innovative approach becomes imperative to adeptly manage and retrieve this data, ensuring the preservation of user data privacy, facilitating seamless transactions, and simultaneously ensuring efficient retrieval.

Within the digital inclusive finance framework, a novel hash index method predicated on dimension partitioning has been introduced in this study. This method was tailored to offer a unique data protection schema for this sector by harnessing the features extracted from convolutional neural networks (CNN). Through the dimension partitioning of CNN features, a segmented storage of these features was realized. When juxtaposed against holistic feature storage, this segmented approach poses greater challenges for potential attackers, hindering their ability to garner comprehensive or coherent information from singular hash buckets. The utilization of E2LSH (Euclidean LSH) for hash mapping ensured the assignment of proximate sub-features to identical hash buckets. By eschewing the direct storage of raw data or their immediate features and opting for this mapping strategy, the intrinsic structure of the original data is rendered more ambiguous, thus amplifying the challenges associated with illicit extraction of pertinent data. Figure 1 delineates a schematic representation of the index based on dimension partitioning.



**Figure 1.** Schematic diagram of the index based on dimension partitioning

Given the inherent sensitivity of E2LSH, a relatively high probability, denoted as  $o_1$ , exists that any two points will be adjacent in the same region. Such adjacency suggests that a majority of images within a particular hash bucket bear similar content. Nevertheless, when observed across diverse dimensions, there is an absence of knowledge regarding feature classification on individual dimensions. Consequently, even if potential attackers gain access to a hash bucket, the reconstruction or comprehensive comprehension of the original images' entire content becomes challenging. This complexity arises since only select sub-features are stored within the bucket. As a result, the probability of two points being adjacent within the same bucket decreases, indicating that this decentralized storage methodology augments data security.

Furthermore, in terms of digital inclusive finance, transactions and operations are characteristically dynamic and multifaceted. Through the establishment of hash index tailored for sub-features separately, the method grounded on dimension partitioning is observed to adeptly address an array of intricate queries, simultaneously ensuring consistent protection across all queries. The vector average dimension partitioning equation employed within this methodology is articulated below:

$$\vec{c} = (\vec{c}', \vec{c}'') = \left( \left( \vec{c}'[1], \vec{c}'[2], \dots, \vec{c}'\left[\frac{f}{2}\right] \right), \left( \vec{c}''\left[\frac{f}{2}+1\right], \vec{c}''\left[\frac{f}{2}+2\right], \dots, \vec{c}''[f] \right) \right) \quad (1)$$

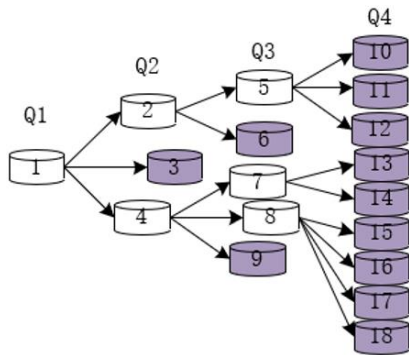
Amid the ongoing evolution of digital inclusive finance, substantial increases have been observed in user numbers, transaction frequencies, and transaction types. Concurrently, financial products and services within inclusive finance undergo constant innovation, leading to the introduction of newer products and services. As these advancements take place, the emergence of novel image data types and formats is witnessed, and a consequent accumulation of related image data is noted. To address the burgeoning volume of data, it is imperative for index methods to exhibit significant scalability, allowing for the seamless management of augmented data in forthcoming times. Service stability and sustainability, paramount in the financial realm, necessitate the inception of scalable index methods. If constant adjustments or replacements of index methods become essential due to data volume expansion, adverse implications on service stability might arise.

Characteristically, once data distribution within a hash bucket is established through E2LSH features, subsequent adjustments prove challenging. This insinuates that an initial hash bucket distribution might lose its optimality when shifts in data distribution or query patterns emerge. Contrarily, index methods imbued with scalability are discerned to adapt more adeptly to such changes, underpinning both the stability of indexing efficacy and outcomes. In considering two vectors,  $c^{\rightarrow}_1$  and  $c^{\rightarrow}_2$ , in a space, let  $d(y)$  represent the probability density function of stable distribution absolute values. With  $v$  symbolizing the Euclidean distance between said vectors and expressed as  $v = \|c^{\rightarrow}_1 - c^{\rightarrow}_2\|$ , for randomly chosen vectors  $s^{\rightarrow}$ ,  $s^{\rightarrow}c^{\rightarrow}_1$  and  $s^{\rightarrow}c^{\rightarrow}_2$  from the stable distribution, the collision probability between  $c^{\rightarrow}_1$  and  $c^{\rightarrow}_2$  is computed utilizing the subsequent equation:

$$o(v) = Oe_{s,n} \left[ g_{s,n}(\vec{c}_1) = g_{s,n}(\vec{c}_2) \right] = \int_0^v \frac{1}{v} d\left(\frac{y}{v}\right) \left(1 - \frac{y}{q}\right) f_y \quad (2)$$

In digital inclusive finance, a dynamic shift in user query requirements is observed, attributed to evolving market conditions. It is noted that certain hash buckets are subjected to frequent queries, while others garner diminished attention. For optimal efficiency in hash index operations, an equitable distribution of data across all hash buckets is deemed ideal. However, intrinsic data characteristics combined with the heterogeneity of user behaviour lead to certain hash buckets becoming overpopulated, whereas others remain underutilized.

To cater to the rapid response demands of high-frequency queries, the splitting of these saturated hash buckets is proposed. Through meticulous adjustments in bucket size and subsequent division, a more homogenized distribution of data is achieved, culminating in enhanced retrieval performance. Figure 2 shows the structure of bucket splitting.



**Figure 2.** Structure of bucket splitting

For the maintenance of hash index efficiency, the data volume within each hash bucket is periodically assessed. Regular audits are performed on the dataset quantities of individual hash buckets, and those surpassing pre-determined thresholds are designated as “overloaded buckets”. The selection of an optimal dimension for division is crucial, given the adoption of a dimension partitioning-based hash method. In cases of identified "overloaded buckets", the data distribution across each dimension is appraised. Subsequently, dimensions exhibiting the most skewed data distribution are earmarked for division. To effectuate bucket division, a rehashing of the data contained within the "overloaded bucket" is mandated. More specifically, predicated on the selected divisional dimension, the data contained within the "overloaded bucket" is segregated into two distinct subsets. Each subset is subjected to the E2LSH algorithm, spawning new hash buckets rooted in the sub-features of that particular dimension. Data from the original "overloaded bucket" are transitioned to these newly-formed hash buckets. Defining  $Q$  as the preset bucket shrinkage coefficient,  $\delta$  as the variation coefficient, and  $Q'$  as the re-selection of a smaller bucket width, with  $Q' = \delta \cdot N \cdot Q$ . A new locally sensitive hash function, represented as  $g_{s,n}(\cdot)$ , is derived through the computation of  $n' = n \cdot Q' / Q$ . Subsequent to the data migration process, updates are made to the hash index structure to encapsulate the bucket transformations. Indices of original "overloaded buckets" are purged, while those of the newly instantiated hash buckets are incorporated. Notably, though the bifurcation of "overloaded buckets" potentially mitigates data congestion, it might inadvertently instigate data imbalances in other hash buckets. As a remedial measure, a comprehensive assessment is conducted across all hash buckets to ascertain load equilibrium, ensuring the absence of emergent "overloaded buckets". In the event of their detection, the aforementioned divisional protocol is reiterated.

The proposed hash index method based on dimension partitioning was used for secure image retrieval in the following steps:

Step 1: Extracting CNN features of queried images. Images pertinent to digital inclusive finance - encompassing but not confined to users' ID photos, transaction vouchers, and other related financial materials - are inherently intricate, laden with salient details and features. Once an image is uploaded by the

user for querying, features from said image are extracted utilizing CNN in the deep learning domain. Various hierarchical features, spanning from rudimentary textures and colors to complex objects and structures, are captured by CNN. Thus, even with complex financial imagery, the critical attributes are duly extracted, facilitating ensuing retrieval processes.

Step 2: Bucket computing protocol. To bolster retrieval efficiency, it becomes imperative to hash feature vectors into designated buckets. The synergy of the E2LSH algorithm and a dimension partitioning stratagem facilitates the division of CNN-extracted features into sundry sub-features. Subsequent to this division, each sub-feature undergoes hash mapping to ascertain its affiliated hash bucket. Given the confidentiality demands of financial data, this step not only champions hash accuracy but simultaneously buttresses data privacy. The act of dimension partitioning is known to attenuate feature correlations, thereby diminishing potential data leakage risks.

Step 3: Obtaining candidate images. Predicated on hash bucket information, images bearing semblance in features to the queried image are rapidly identified. Features of these candidate images are then extracted from their respective buckets, congruent with the data derived from the bucket computing protocol. It is noteworthy that these procured candidate images could span diverse financial operations; for instance, a singular ID photo might have ties to an array of financial transactions. This step is, thus, pivotal in meticulously sieving the most pertinent candidates from a vast reservoir of financial images.

Step 4: Similarity calculation of images. Potential discrepancies in content or structure might surface between the procured candidate images and the queried image. Established methodologies, such as cosine similarity and Euclidean distance, are used to compute the similarity between attribute sets of every candidate image vis-à-vis the queried one. Based on the similarity results, candidate images are methodically ranked, culminating in the delivery of the most analogous results to the end-user. This meticulous process ensures users are furnished with financial images that resonate highly relevant to the queried image, aiding in the pinpointing of requisite financial information or supporting materials.

For CNN features  $c_w^{\rightarrow}$  of the queried image, denoted  $U_w$ , and those  $c^{\rightarrow}$  of the target image ( $U$ ), two distinct servers play pivotal roles. Server 1 is entrusted with the encrypted CNN features  $c_{ws}^{\rightarrow}$  and  $c_s^{\rightarrow}$ , while Server 2 is the repository for the vectors  $c_{wn}^{\rightarrow}$  and  $c_n^{\rightarrow}$ , quintessential for restoring the primordial CNN features. This bifurcation ensures that both servers compute distances on different sub-dimensions. An accompanying equation elucidates this mechanism.

$$DI^2(\bar{c}, \bar{c}_w) = DI^2(\bar{c}', \bar{c}'_w) + DI^2(\bar{c}'' , \bar{c}''_w) \quad (3)$$

### 3. SECURE IMAGE SHARING APPLICATION FOR DIGITAL INCLUSIVE FINANCE

In the sphere of digital inclusive finance, a vast array of sensitive financial data, ranging from personal loan records to identification documents and transaction vouchers, is frequently encountered. The significance of ensuring data security and privacy in such contexts cannot be overemphasized. Compounding this is the intricate nature of the financial domain, often characterized by collaborations among multiple institutions or partners. Thus, emerges the

imperative for a technology adept at securely disseminating information among these parties. To this end, an RDH-based algorithm has been proposed in this study. This algorithm is adept at deconstructing clandestine images (e.g., financial vouchers) into multiple shares. Only upon procurement of an adequate number of these shares can the original image be fully restored. By virtue of this methodology, distinct shares can be dispersed across varied locales or managed by diverse institutions, effectively obviating risks associated with singular points of vulnerability. Noteworthy is the fact that even in instances of unauthorized access to or deterioration of certain shares, the original data remains safely recovered, contingent upon possession of a requisite share quantum.

**Image Pre-processing and Block Segmentation:** Initially, the input image is subjected to a pre-processing regimen. Herein, the image at large is parsed into numerous diminutive blocks, each either of equal or near-equal dimensions. Typically, each such block encompasses a specified pixel count. Such categorization lays the groundwork for ensuing computations of pixel differences and registers auxiliary data, all the while preserving the algorithm's reversibility.

**Pixel Filtering within Designated Blocks:** Subsequent to block formation, pixel values encapsulated within each are sifted. Let the denotation  $z_u$  represent these pixel values. From this set, a labeled pixel, christened  $lo$ , is identified if it adheres to a specific equation. This pixel then undergoes a position exchange with the first pixel within the block.

$$\begin{cases} \text{MIN}(\text{MAX}|lo - z_u|) \\ |lo - z_u| \leq 127 \end{cases}, u = 1, 2, \dots, 16 \quad (4)$$

To embed secret information, the difference between a specific pixel (known as the "labeled" pixel) and other pixels in its group is determined. This difference's absolute value is referred to as  $f_u$ . Beyond simply embedding information, additional details, such as the exact position of the labeled pixel and any changes made to the differences, are also stored. This helps in perfectly reconstructing the original image later on. Consider  $Ea$  as a random binary value,  $BI$  as the binary bits of  $\text{MAX}(f_u)$ ,  $La$  as the type of pixel block,  $Mo$  as the position of  $lo$  in that block, and  $e$  as the relative size of  $lo$  compared to other pixels in the block. This research introduced an auxiliary pixel,  $Si$ , as represented in the given equation, to keep these extra details.

$$Si = Ea \| BI \| La \| Mo \| e \quad (5)$$

The same operation can be performed for the non-labeled pixel block. Let  $z_k$  represent the pixel values within sub-pixel block, a subsequent equation delineated the prerequisites for the sub-labeled pixel  $a\_lo$ :

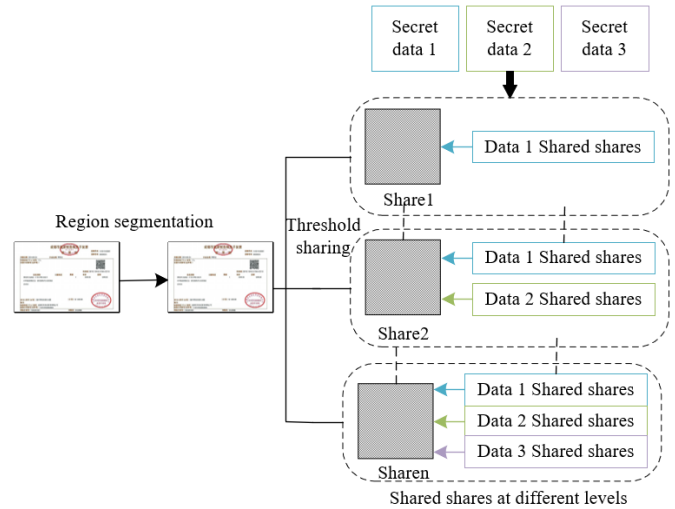
$$\begin{cases} \text{MIN}(\text{MAX}|a\_lo - z_k|) \\ |a\_lo - z_k| \leq 127 \end{cases}, k = 1, 2, \dots, 4 \quad (6)$$

Randomly generated binary numbers are represented by  $Ea$ ,  $Ea_1$  and  $Ea_2$ . Hence, the sub-auxiliary pixel  $a\_Si$  is denoted as:

$$a\_Si = \begin{cases} Ea \| e \| La \| Mo, o z \in a\_Lo \\ Ea_1 \| La \| Ea_2, o z \in a\_Bo \end{cases} \quad (7)$$

The RDH-based secret image sharing algorithm was used in the field of digital inclusive finance in the following steps:

First, the entire image was segmented based on content importance, with each region assigned a level. For example, regions containing personal identity or sensitive transaction information may be assigned a higher level. Let  $mp_1, mp_2, \dots, mp_l$  be the position coordinates of each region;  $P_1, P_2, \dots, P_l$  be the labels of corresponding image region;  $H_1, H_2, \dots, H_l$  be the assigned levels in the descending order.



**Figure 3.** Flowchart of generating the encrypted data shares

Then the information was encoded and classified based on the level of each region, which ensured that the information was processed at different levels based on the importance of each region in subsequent encryption and sharing steps. Let  $DA_1, DA_2, \dots, DA_l$  be the content classification, then the importance should be corresponding to  $P_1, P_2, \dots, P_l$ .

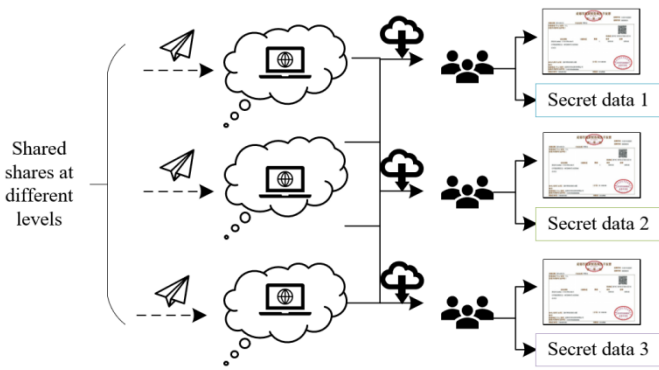
The secret sharing algorithm was further used to process each classified content and its position coordinates in the image, thereby generating corresponding encrypted data shares. The algorithm was used for  $DA_1, DA_2, \dots, DA_l$  and  $mp_1, mp_2, \dots, mp_l$  through their corresponding thresholds  $(y_1, b_1), (t_2, b_2), \dots, (y_l, b_l)$ , with  $y_1 \geq y_2 \geq \dots \geq y_l$ . The encrypted data shares  $DA_1, DA_2, \dots, DA_{u,2}, \dots, DA_{u,bu}$  were generated, with  $u=1, 2, \dots, l$ . Figure 3 shows the flowchart for generating the encrypted data shares.

The secret sharing algorithm was used to process the entire image or specific region to generate the so-called "shadow image". As an intermediate vector, the shadow image ensured that the content of the original image was not directly exposed during transmission or storage. In the condition of thresholds  $(y_1, b_1), (t_2, b_2), \dots, (y_l, b_l)$ , the algorithm was used for  $P_1, P_2, \dots, P_l$ , respectively, which generated  $b_1, b_2, \dots, b_l$  shadow images, respectively.

The encrypted data shares, which were generated in the third step, were embedded into the shadow image to generate sub-shared shares. In this way, both original financial data and the location and classification of these data were hidden, thereby further improving data security. Let  $DA_1, DA_2, \dots, DA_{u,2}, \dots, DA_{u,bu}$  be the encrypted data shares generated by embedding into the shadow image, and  $ap_{u,1}, ap_{u,2}, \dots, ap_{u,bu}$  be the generated sub-shared shares, with  $u=1, 2, \dots, l$ .

Finally, the generated sub-shared shares  $ap_{u,1}, ap_{u,2}, \dots, ap_{u,bu}$  ( $u=1, 2, \dots, l$ ) were sent to  $b_u$  storage points managed by authorizers with level  $H_u$ , such as security data centers of

financial institutions. Apart from data integrity and availability, it was ensured that only authorized entities could access and recover the original data. Figure 4 shows the flowchart of sending shared shares to storage points.



**Figure 4.** Flowchart of sending shared shares to storage points

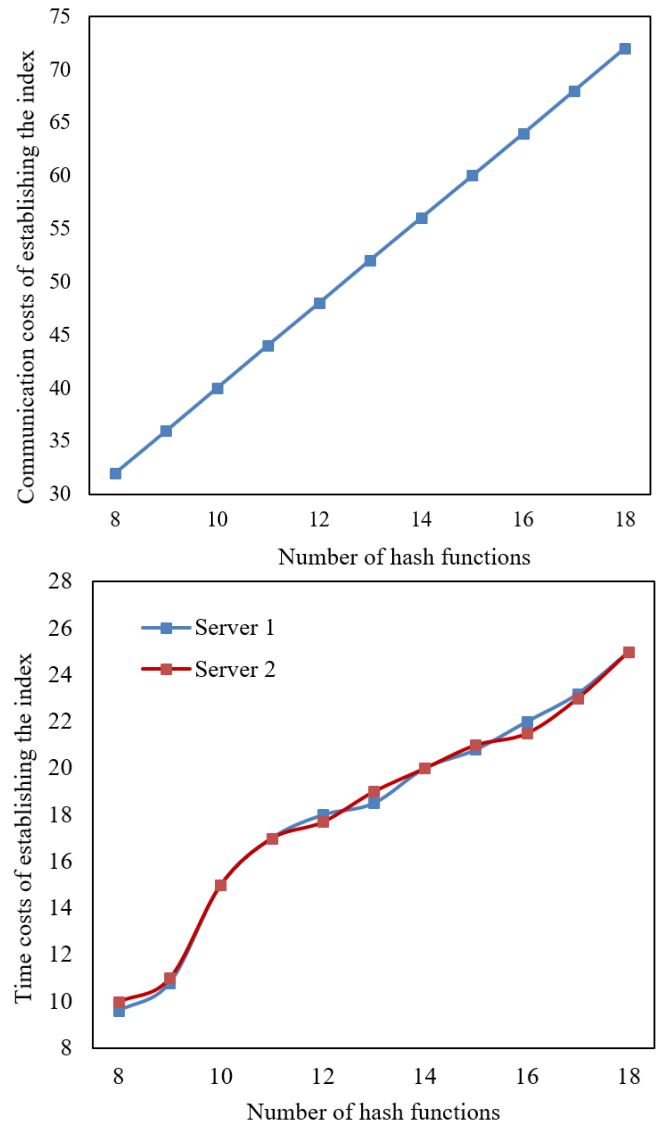
To achieve hierarchical image restoration and information extraction, necessary sub-shared shares were first obtained from the storage points managed by the authorizers, which is the foundation of the restoration and extraction process, given that access and initiation of the reconstruction procedure were strictly restricted to approved entities. At least  $y_j$  authorizers with level  $H_j$  received the shared shares  $AP_{j,k}$  ( $k=UF_1, UF_2, \dots, UF_{y_j}$ ) managed by them, and data  $DA_{j,U,F_1}, DA_{j,U,F_2}, \dots, DA_{j,U,F_{y_j}}$  were extracted from the shared shares.

Then previously embedded encrypted data shares were extracted from the shadow image using specialized tools. The level of image region to be restored was determined according to requirements and permissions. The secret sharing algorithm was used to decrypt the extracted encrypted data shares, thereby restoring the original classified content and location coordinates. The Lagrange interpolation algorithm was used in this study to recover the extracted data into secret data  $DA_j$  and position coordinates  $mp_j$ . When  $j=l$ , corresponding information was extracted from the image based on the decrypted position coordinates. In addition, the information was assembled according to classification, that is, the image region  $P_l$  was restored using the position coordinates  $mp_j$ . Finally, the reverse operation of RDH was performed for the extracted information, such as restoring the difference between the labeled pixel and other pixels in the block, thereby obtaining the original unmodified image. When  $j \neq l$ , at least  $y_{j-1}$  necessary participants were required among the authorizers, which aimed to restore the image region  $P_j$  using the shared shares while extracting additional  $ap_{u,UD1}, ap_{u,UD2}, \dots, ap_{u,UD_{y_u}}$  ( $u \in [j, l]$ ) from the shared shares, thereby reconstructing image regions  $P_{j-1}, \dots, P_l$  and secret data  $DA_{j-1}, \dots, DA_l$ .

#### 4. EXPERIMENTAL RESULTS AND ANALYSIS

In the pursuit of secure image retrieval applications tailored for digital inclusive finance, this study presented an advanced hash index method anchored on dimension partitioning. The primary objective was to process financial image data both efficiently and securely, thereby mitigating potential security vulnerabilities. As delineated in Figure 5, a discernible trend was noted: as the number of hash functions escalates, the

communication costs associated with index establishment concomitantly rise. Generally, augmenting the number of hash functions is perceived to refine the retrieval's accuracy and precision. However, this augmentation simultaneously amplifies both communication and computational overheads. A parallel observation was made concerning the temporal costs associated with index establishment on two distinct servers, namely Servers 1 and 2. Notably, these costs exhibited a direct relationship with the increasing number of hash functions, a trend congruent with prior expectations and discussions.

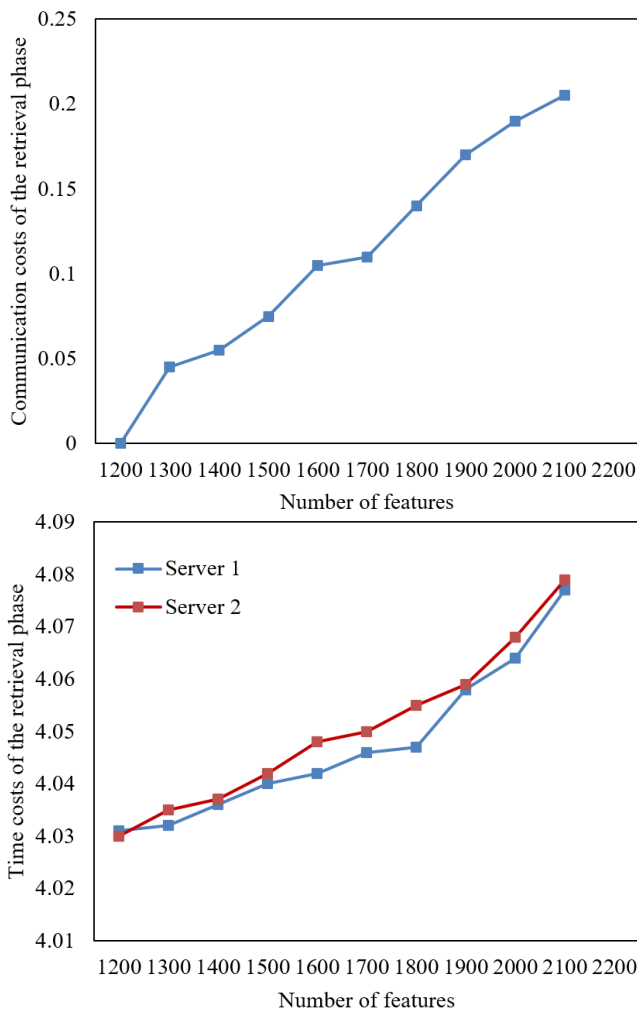


**Figure 5.** Impact of the number of hash functions on index performance

In scenarios demanding elevated accuracy and security standards, a greater ensemble of hash functions may be deemed appropriate, albeit at the expense of increased temporal overheads. Conversely, when expedited responses are paramount, opting for a reduced set of hash functions might be more prudent. Such observations underscore the inherent adaptability and potential applicability of the proposed algorithm.

As delineated in Figure 6, a rise in communication costs during the retrieval phase was observed in tandem with an increase in the number of features. Typically, a more extensive feature set is hypothesized to confer enriched information,

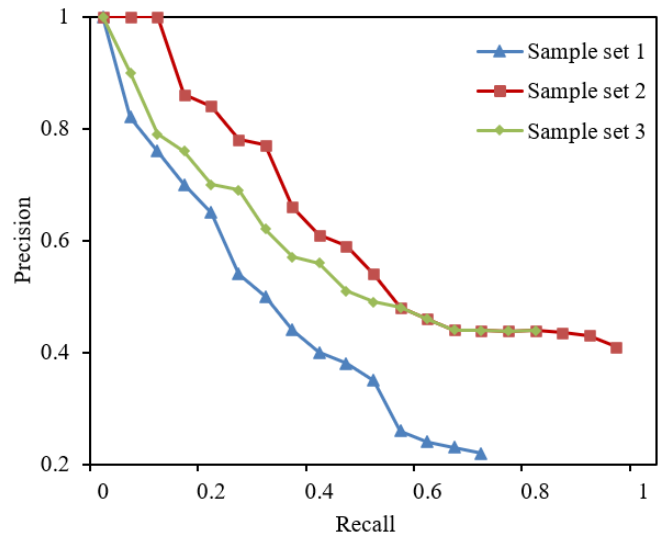
potentially heightening retrieval accuracy. Nonetheless, this expansion invariably necessitates elevated communication overheads, attributable to the augmented volume of data being transmitted and processed. Concurrently, an association between the quantity of features and the time costs incurred during the retrieval phase was discerned. The data illustrated in the figure indicated a consistent yet modest ascent in the retrieval time costs for both servers commensurate with the escalating feature count. Whilst these temporal overheads exhibited a gradual increment with the burgeoning number of features, their rate of growth remained comparatively restrained, suggestive of the algorithm's efficiency. This implies that even when confronted with a surge in information processing demands, results can still be yielded within a time frame deemed acceptable, a criterion of paramount significance in the financial domain.



**Figure 6.** Secure image retrieval performance with different numbers of features

In information retrieval, the relationship between recall and precision serves as a pivotal metric for assessing the efficacy of retrieval systems. As depicted in Figure 7, a discernible decline in precision for the financial transaction image set (Sample set 1) was observed as recall approached unity, with a more pronounced decrease evident around a recall value of 0.8, where precision plummeted to 0.38. Conversely, the personal identity verification image set (Sample set 2) exhibited a steadfast precision of 1 until recall neared 0.4, suggesting remarkable efficiency of the proposed method for this dataset in identifying pertinent images. The precision for

the financial product advertisement image set exhibited a rapid decline, converging to 0.439 at a recall value around 0.8, marginally inferior to Sample set 2. From this analysis, it was inferred that the advocated hash index method predicated on dimension partitioning manifests exemplary retrieval proficiency across diverse financial image datasets.



**Figure 7.** P-R curves of the secure image retrieval method in different sample sets

Further exploration was conducted into secure image sharing technology for digital inclusive finance, where an RDH-based secret image sharing algorithm was introduced. This innovative approach ensured image integrity and reversibility whilst facilitating secure image sharing. Embedding rate was judiciously chosen as a pivotal index for gauging the algorithm's effectiveness, stemming from its direct correlation with the algorithm's information capacity and its role in mediating between information capacity and image quality.

**Table 1.** Shared embedding rate of different test images (2,3)

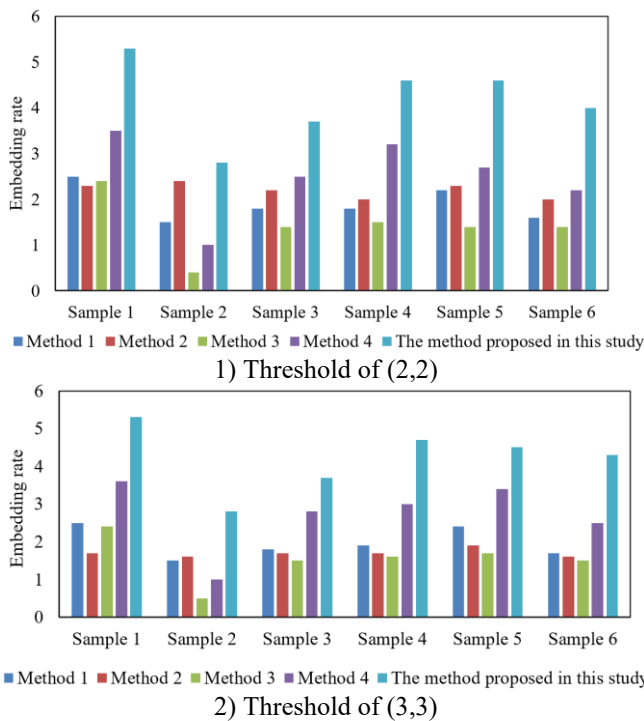
Images	Effective Embedded Data Volume	Embedding Rate (%)
Sample 1	1,215,849	4.35
Sample 2	482,561	1.92
Sample 3	712,546	2.63
Sample 4	912,549	3.14
Sample 5	842,316	3.36
Sample 6	812,639	3.28

Upon analysis of Table 1, it was discerned that the effective embedded data volume for Sample 1 (identity certificates) stood at 1,215,849, accompanied by an embedding rate of 4.35%. In contrast, Sample 2 (financial reports) exhibited an effective embedded data volume of 482,561 and an embedding rate of 1.92%. Further, the effective embedded data volumes and embedding rates for Samples 3 through 6 were identified as follows: for Sample 3 (asset certificates), 712,546 (2.63%); for Sample 4 (signature samples), 912,549 (3.14%); for Sample 5 (transaction records), 842,316 (3.36%); and for Sample 6 (human faces or biometric images), 812,639 (3.28%). It was observed that embedding rates demonstrated variance across the diverse samples, a phenomenon attributable to the intrinsic content and structural characteristics of the respective images. Particularly, Sample 1 was noted to manifest the apex

embedding rate, underscoring the prowess of the RDH-based secret image sharing algorithm in adeptly processing images rich in content. On the other hand, Sample 2's embedding rate, albeit the nadir among the datasets, registered a commendable 1.92%, bolstering the assertion of the algorithm's expansive adaptability across a plethora of financial image categories.

**Table 2.** Embedding rate of different test images with different shared thresholds

Images	Threshold of (3,3)	Threshold of (3,4)	Threshold of (4,4)
	Embedding Rate (%)	Embedding Rate (%)	Embedding Rate (%)
Sample 1	5.14	5.17	6.17
Sample 2	2.78	2.76	3.92
Sample 3	3.69	3.66	4.62
Sample 4	4.52	4.35	5.31
Sample 5	4.18	4.31	5.33
Sample 6	4.23	4.28	5.28



**Figure 8.** Comparison of embedding rate using different image sharing methods with different thresholds

Upon examination of Table 2, it was discerned that the embedding rate across all samples exhibited an escalating trend as the threshold progressed from (3,3) to (3,4), and subsequently to (4,4). This trend suggests an augmentation in the volume of embedded information with the elevation of the shared threshold. A consistent trend was identified across various samples: identity certificates, financial reports, asset certificates, signature samples, transaction records, and human faces or biometric images. The inference drawn is that the embedding rate incrementally ascends with the increase of the shared threshold, thereby corroborating the algorithm's consistent efficacy across diverse financial image types. Notably, even among variances in shared thresholds, the embedding rate across samples remained remarkably stable, reinforcing the algorithm's consistent performance under myriad scenarios. Divergent embedding rates were observed within fluctuating shared thresholds, offering a modulated

approach to harmonize the juxtaposition between embedded information quantity and image quality.

Figure 8 delineates a comparative analysis of embedding rates across various thresholds utilizing disparate methods: the secure image sharing methodology postulated in this study, juxtaposed with Shamir's secret sharing algorithm, Visual Cryptography Scheme (VCS), and the secret sharing paradigms of both Krawczyk and Blakley. Across all the scrutinised samples, the proposed methodology's embedding rate was consistently observed to surpass that of the other four esteemed algorithms, specifically at thresholds of (2,2) and (3,3). A high embedding rate implies an enhanced capacity for the incorporation of secret information within the same image—a salient feature for secure image sharing within digital inclusive finance, allowing a more voluminous data transmission while preserving image security. Concurrently, it was noted that the embedding rate of the proposed methodology exhibited minimal variance across both thresholds. In contrast, rates of alternative methodologies demonstrated pronounced fluctuations, indicating the proposed methodology's relative stability irrespective of threshold settings.

## 5. CONCLUSION

In the realm of secure image sharing technology for digital inclusive finance, particular attention was given to the RDH-based secret image sharing algorithm within this study. The primary objective was to facilitate secure image sharing, concurrently maintaining the integrity and reversibility of images. A variation in the number of hash functions, distinct features, and diverse thresholds were introduced to ascertain the method's efficacy.

Empirical analysis indicated that increasing the number of hash functions influences the temporal and communicative costs associated with index establishment, albeit this escalation remains within acceptable bounds. Secure retrieval performance of images was found to be contingent on varying feature quantities, establishing a link between feature count and both temporal and communicative retrieval expenses. When juxtaposed with different recall values, three distinct sample sets manifested varying precision levels, underscoring the influence of sample typologies on image retrieval efficacy. Upon evaluating with assorted samples and thresholds, the embedding rate of the proposed technique consistently surpassed that of four classical counterparts, accentuating the preeminence of the recommended approach.

Digital inclusive finance's secure image sharing technology has emerged as a domain of burgeoning significance. The RDH-based secret image sharing algorithm, as elucidated within this study, has been positioned as a potent instrument in this context. Post meticulous experimental scrutiny, the proposed approach exhibited steadfastness and preeminence across myriad scenarios, with a pronounced emphasis on embedding rate, endorsing its practicality and trustworthiness in the digital finance milieu. In summation, an efficacious, unwavering, and safeguarded methodology for the application of secure image sharing within the digital inclusive finance landscape has been proffered by this study.

## REFERENCES

[1] Yin, L., Xin, H. (2023). An empirical study on the impact

- of digital inclusive finance on China's cultural industry. *Smart Innovation, Systems and Technologies*, 358: 761-769. [https://doi.org/10.1007/978-981-99-3416-4\\_61](https://doi.org/10.1007/978-981-99-3416-4_61)
- [2] Lin, S., Ma, W. (2023). Digital inclusive finance and industrial structure upgrade—Based on nonlinear relationship perspective. *Journal of Advanced Computational Intelligence and Intelligent Informatics*, 27(2): 251-258. <https://doi.org/10.20965/jaciii.2023.p0251>
- [3] Wang, S., Yuan, L., Xiong, Z., Liu, Y. (2023). The impact of digital inclusive finance on enterprise financing in Fujian Province. *ACM International Conference Proceeding Series*, 93-101. <https://doi.org/10.1145/3599609.3599623>
- [4] Rahman, M.R., Rahman, M.M. (2023). Impact of digital financial services on customers' choice of financial institutions: A modified UTAUT study in Bangladesh. *International Journal of Safety and Security Engineering*, 13(3): 409-421. <https://doi.org/10.18280/ijss.130304>
- [5] Zhang, X., Zhang, C. (2023). The empirical research of digital inclusive finance on the coordinated development of regional economy. *Smart Innovation, Systems and Technologies*, 358: 685-696. [https://doi.org/10.1007/978-981-99-3416-4\\_55](https://doi.org/10.1007/978-981-99-3416-4_55)
- [6] Wang, X., Chen, X. (2023). An empirical study on financing constraints of digital inclusive finance development on small and medium-sized technology-based enterprise. *Kybernetes*, 52(2): 585-600. <https://doi.org/10.1108/K-01-2022-0095>
- [7] Yan, W., Wang, Y., Zheng, S., Xing, L., Zhang, L. (2023). Nonlinear impact of the digital inclusive finance on enterprise technological innovation based on the AK model and PSTR empirical analysis. *Journal of Global Information Management (JGIM)*, 31(3): 1-23. <https://doi.org/10.4018/JGIM.320191>
- [8] Simoneau, A., Aubé, M. (2023). Methods to calibrate a digital colour camera as a multispectral imaging sensor in low light conditions. *Remote Sensing*, 15(14): 3634. <https://doi.org/10.3390/rs15143634>
- [9] Guo, M., Song, L., Ilyas, M. (2021). Research on practical intelligent mode of digital image economy based on improved genetic multilayer neural network. *Computational Intelligence and Neuroscience*, Article ID: 3113584. <https://doi.org/10.1155/2021/3113584>
- [10] Gonçalves, T.M., Campos Bianchi, A.G., Gazel Yared, G.F. (2023). Digital image processing in the diagnosis of cracks in steel sheet. *Enterprise Information Systems, ICEIS - Proceedings*, 1: 623-629.
- [11] Hasan, M.K., Kamil, S., Shafiq, M., Yuvaraj, S., Kumar, E.S., Vincent, R., Nafi, N.S. (2021). An improved watermarking algorithm for robustness and imperceptibility of data protection in the perception layer of internet of things. *Pattern Recognition Letters*, 152: 283-294. <https://doi.org/10.1016/j.patrec.2021.10.032>
- [12] Marwan, M., Kartit, A., Ouahmane, H. (2018). A cloud-based framework to secure medical image processing. *Journal of Mobile Multimedia*, 14(3): 319-344. <https://doi.org/10.13052/jmm1550-4646.1434>
- [13] Cone, S.W., Carucci, L.R., Yu, J., Rafiq, A., Doarn, C.R., Merrell, R.C. (2005). Acquisition and evaluation of radiography images by digital camera. *Telemedicine Journal & e-Health*, 11(2): 130-136. <https://doi.org/10.1089/tmj.2005.11.130>
- [14] Al-Husainy, M.A.F., Al-Sewadi, H.A., Masadeh, S.R. (2022). Using a DNA tape as a key for encrypt images. *International Journal of Electronic Security and Digital Forensics*, 14(4): 373-387. <https://doi.org/10.1504/IJESDF.2022.123868>
- [15] Almamoori, A.A., Bhaya, W.S. (2023). Hybrid deep learning approach utilizing RNN and LSTM for the detection of DDoS attacks within the Bitcoin ecosystem. *Ingénierie des Systèmes d'Information*, 28(4): 931-937. <https://doi.org/10.18280/isi.280413>
- [16] Wang, W., Liu, X., Zhang, Y., Liu, J., Jiang, P. (2022). Study on the detection and recovery algorithm of important financial information tampering. *International Journal of Information and Communication Technology*, 21(3): 317-332. <https://doi.org/10.1504/IJICT.2022.125558>
- [17] Shiraishi, M., Aida, H. (2022). Money transfer on transaction signature-based ledger. In *International Symposium on Foundations and Practice of Security*, Ottawa, ON, Canada, pp. 338-354. [https://doi.org/10.1007/978-3-031-30122-3\\_21](https://doi.org/10.1007/978-3-031-30122-3_21)
- [18] Luo, Y. (2023). Financial data security management method and edge computing platform based on intelligent edge computing and big data. *IETE Journal of Research*, 69(8): 5187-5195. <https://doi.org/10.1080/03772063.2021.1973596>
- [19] Padma Vijetha Dev, B., Venkata Prasad, K. (2023). An adaptive lightweight hybrid encryption scheme for securing the healthcare data in cloud-assisted internet of things. *Wireless Personal Communications*, 130(4): 2959-2980. <https://doi.org/10.1007/s11277-023-10411-6>
- [20] Yalla, S.P., Uriti, A., Sethy, A. (2022). GUI implementation of modified and secure image steganography using least significant bit substitution. *International Journal of Safety and Security Engineering*, 12(5): 639-643. <https://doi.org/10.18280/ijss.120513>
- [21] Signing, V.F., Mogue, R.T., Kengne, J., Kountchou, M., Saïdou. (2021). Dynamic phenomena of a financial hyperchaotic system and DNA sequences for image encryption. *Multimedia Tools and Applications*, 80(21-23): 32689-32723. <https://doi.org/10.1007/s11042-021-11180-9>
- [22] Zhang, N. (2022). Accounting computerization data adjustment method on account of artificial intelligence algorithm. In *International Conference on Cyber Security, Artificial Intelligence, and Digital Economy (CSAIDE 2022)*, 12330: 248-253. <https://doi.org/10.1117/12.2646279>
- [23] Fujiwara, N., Yokoyama, S. (2022). Ownership protection of specified image data using blockchain technology. In *Proceedings of the 14th International Conference on Management of Digital EcoSystems*, Venice, Italy, pp. 56-63. <https://doi.org/10.1145/3508397.3564843>