ISSN: 2093-5374 / E-ISSN: 2093-5382

Assessing the Recreational Fishers and their Catches based on Social Media Platforms: Privacy and Ethical Data Analysis Considerations

Mingxin Xue[1*]

[1*]Master, Information Department, City University of Hongkong, Hongkong, China.
mingxixue2-c@my.cityu.edu.hk, https://orcid.org/0009-0007-7390-7155

Received: June 27, 2024; Revised: August 14, 2024; Accepted: September 09, 2024; Published: September 30, 2024

Abstract

Social Media (SM) can offer insights to track recreational Fishing (Rf); Many Limitations Hinder Its Practical Application. The proportion and characteristics of RFs that share their catches remain unidentified. The objective was to enhance the surveillance abilities of RF by utilizing SM information. This study focuses on the sharing economy information transmission, network optimization of SM platforms, and privacy protection issues during data transmission. The study starts with the data transmission characteristics in SM platforms, analyzes the data ethics in SM information transmission from the perspectives of natural and economic data attributes, and then focuses on the privacy protection principles in network information transmission. Then, a privacy protection scheme based on a locally sensitive hash algorithm is constructed, and finally, an information transmission scheme and method optimization based on a network optimization module are proposed. The research gathered data using physical (face-to-face) surveys and digital (email) surveys to define marine RF that post catches on online platforms ("sharers"), together with additional demographic and fishing data. A comparative analysis was conducted on the computational convergence and accuracy of different privacy protection methods, and the optimal rule framework for data privacy protection was discussed. The observation results show that the efficiency of information transmission using the Minhash-SSNR method is slightly inferior to that using the OSNR-SSNR method. Minhash technology is based on a similarity comparison of dimensionality-reduced data. This leads to data causing the initially highly similar two sets of lists to be misjudged as not having enough similarity, thereby reducing some potential information dissemination opportunities and affecting the efficacy of information transmission. It can be seen that the Minhash-SSNR strategy can effectively send information to nodes with high similarity, preventing excessive information duplication within the system. Although the Minhash-SSNR strategy has a certain degree of decline in information transmission efficiency, it accounts for only about 5% compared to the OSNR-SSNR strategy, ensuring the essential operational stability of SM opportunity networks without significant impact. With few learning and training times, the network information transmission optimization module proposed in this study quickly achieved a lower exponential error. As the number of training sessions gradually increases, the exponential error of

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 15, number: 3 (September), pp. 521-542. DOI: *10.58346/JOWUA.2024.I3.033*

*Corresponding author: Master, Information Department, City University of Hongkong, Hongkong, China.

the network information transmission optimization module in this study is small, and the prediction accuracy of the method is high. RFs who captured a prize, iconic, or symbolic species tended to discuss their catches more. This research signifies significant progress in incorporating SM information to oversee RFs.

Keywords: Social Media, Economic Information, Network Optimization, Privacy Data, Data Sharing.

1 Introduction

Recreational fishing (RF) is a widely favored pursuit internationally, from moderate to tropical waters, and ranks among the most prevalent marine leisure pursuits globally (Fowler et al., 2023). RFs constitute a substantial share of fisheries landings and hold significant socio-economic relevance in several nations. The expenditure produced by the 220 million RF is expected to be around US$ 190 billion. Despite its significance, RF sometimes needs more statistics, particularly in lower and middle-income countries (Zumpano et al., 2023).

Certain nations, including Brazil, exhibit minimal or nonexistent catch documentation, rendering the fishery's yield and financial worth unclear (Arostegui et al., 2021). Statistics from RF are challenging to acquire due to their spatial variability, the complexity of fishing practices, including many entry points, and unpredictable temporal periodicity. Despite little understanding, RF has been progressively acknowledged for exacerbating the decline of fish supplies.

To address the deficiency of data on RF, unconventional methodologies have garnered interest among researchers as a cost-effective means for data acquisition. Social Media (SM) can be a pertinent data source for examining individuals' behaviors and views around the environment (Zafar et al., 2021). Mining information on SM effectively contributes to scientific research by elucidating the social and human aspects of RF and resource extraction trends. Documentation of catches from pictures (pictures and videos) shared on SM has been demonstrated to be a substitute or supplementary method for evaluating species diversity, tactics employed, geographical structures, and assessment of RF catching activity (Allison et al., 2023).

With the rapid progress of internet technology and the rise of emerging methods like big data processing and cloud computing, network services have become indispensable for everyone's daily life. In the context of the fifth-generation communication era, much audio and video data and other multimedia information are rapidly spreading to various corners of the world through mobile devices (Olasumbo Afolabi et al., 2021; Arslan et al., 2022). Many emerging data are released in multiple forms through these devices every second and displayed to the public for viewing (Alowibdi et al., 2021; González-Padilla et al., 2022). Although the research can enjoy the benefits of using mobile phones and other portable electronic products to facilitate communication and interaction, the risks that come with it are an issue that cannot be ignored: the possibility of confidential information leakage is increasing, and the threat is rising. Due to the widespread application of smartphones, their powerful built-in features,

and the ability to send messages directly without review, they have become the most vulnerable target to hacker attacks. Therefore, as the digitization process accelerates, how to protect the security of this sensitive information has become particularly crucial. Researchers' exploration has shown that passing sensitive data information through a password processing process over the network is an efficient and operable strategy to enhance data information security, which can effectively address sensitive data information protection issues (Di Caprio et al., 2022; Bouarara, 2021).

The digital economy's rapid progress and vigorous growth are gradually becoming the primary driving force for improving financial growth and social change (Chopra et al., 2022; Arora & Bawa, 2022). A broad strategic vision - to accelerate monetary development, deepen integration with entities, and build a high-quality digital industry chain with global competitiveness (Lefèvre et al., 2022; Gu et al., 2022). As an essential economic form corresponding to the real economy, the digital economy is no longer limited to a simple combination of digital technology and financial industries. Instead, it comprehensively integrates economic forms, highlighting its essential position in national development strategies (Chawra & Gupta, 2022; Lehdonvirta et al., 2021). The past decade has been a golden period for China's digital economy to soar, with unprecedented scale, development speed, and influence trends. The significance of data security and safety in the macro narrative of the digital economy for personal protection, industry development, and even national economic security is self-evident. Strengthening the regulation and supervision of the digital economy and protecting consumer privacy have become critical issues (Abadi & Moallem, 2022).

Privacy generally refers to private activities, records, or information that natural persons are unwilling to share with the outside world. Scholars have long been exploring the protection and externalities of personal privacy from an economic perspective, analyzing the pros and cons of personal privacy liberalization. The safety or openness of privacy brings more benefits or costs to oneself or society. Since the 21st century, with the development of computer technology, scholars have begun to discuss the dual impact of personal privacy protection in the online age. For example, Garratt and Van argue that excessive recording and use of personal information can lead to data privacy abuse. Still, extreme privacy protection can limit the development opportunities of digital technology.

Recent research has identified data extraction applications on digital mediums to enhance knowledge of RF (Lennox et al., 2022). Data extracted from YouTube revealed that RF captures in Mediterranean EU nations predominantly target comparable species, with possible variations primarily attributable to the adoption of diverse fishing tactics. Sbragaglia et al., (2022) demonstrated that data extracted from YouTube can elucidate disparities in harvesting behaviors and SM characteristics among RF and fishermen (Sbragaglia et al., 2022). While data mining on digital SM is seen as a potential approach for monitoring RF, certain limitations and restrictions hinder the practical implementation of these approaches. This study was meant to mitigate constraints and enhance the incorporation and implementation of tracking RF employing SM information.

The primary restriction in tracking RF captures via SM information is the unknown fraction of RF who share their catches online; hence, extrapolating to the entire population of RF is inadvisable (Vitale et al., 2021). It is essential to ascertain if RF who disseminate their caught fish on SM vary in social features and fishing qualities from people who do not publish their captures.

RFs that broadcast their hauls on SM sites are anticipated to be fresher than those that do not, as SM consumers tend to be fresher than non-users (Gundelund et al., 2020). RF should enhance its online social networking presence, as their catches elicit more significant SM interaction. RF who document their activities on SM is likely to be more enthusiastic, dedicating a substantial portion of their leisure time to catching. Specialist fishermen are more likely to feature in traditional mediums, such as publications, which is a tendency SM consumers somewhat mirror. RFs who engage in SM allocate more financial resources to their pursuit due to their increased enthusiasm and expertise. RFs that showcase their catches on SM exhibit a greater specialization in fishing for trophies, iconic, or symbolic species since such postings tend to garner increased follower interaction (Eckhardt, 2024).

Information extracted from SM can only be a reliable surveillance instrument if the demographic of RF sharing their captures is sufficiently characterized. This study seeks to address the current lack of understanding by offering instrumental insights to enhance the surveillance abilities of RF using SM.

This study focuses on the sharing economy information transmission, network optimization of SM platforms, and privacy protection issues during data transmission. The study starts with the data transmission characteristics in SM platforms, analyzes the data ethics in SM information transmission from the perspectives of natural and economic data attributes, and then focuses on the privacy protection principles in network information transmission. Then, a privacy protection scheme based on a locally sensitive hash algorithm is constructed, and finally, an information transmission scheme and method optimization based on a network optimization module are proposed. A comparative analysis was conducted on the computational convergence and accuracy of different privacy protection methods, and the optimal rule framework for data privacy protection was discussed.

The research utilized data from a continuous monitoring initiative in Catalonia (north-western the Mediterranean Ocean, Spain). The study used information gathered from in-person face-to-face discussions and via the internet surveys distributed via email to assess the percentage of RF disseminating their catches across various online channels, in conjunction with other variables such as their ages, fishing method, avidity, capture per unit labor, financial spending, and organisms obtained.

2 Data Transmission Characteristics in SM Platforms

2.1 Data Ethics in SM Information Transmission

SM related to financial information disclosure, dissemination, and sharing can be divided into three categories: microblogging, such as Weibo and Twitter of RF. Its characteristic is that enterprises can

directly push information to users who follow the enterprise. Users can interact with each other and share user-generated content. With the widespread application of machine learning and other technologies in big data, people's understanding of the ethical issues brought about by the design, openness, and use of data systems is constantly deepening on RF (Boudiaf et al., 2022). In addition to proposing sufficient legislative norms and guidelines for data development, government departments, enterprises, and other entities must consider ethical rules when designing digital economy mechanisms and products (Liang et al., 2021). The data ethics rules should be set for financial growth, and the data transmission characteristics in SM platforms are shown in Figure 1.

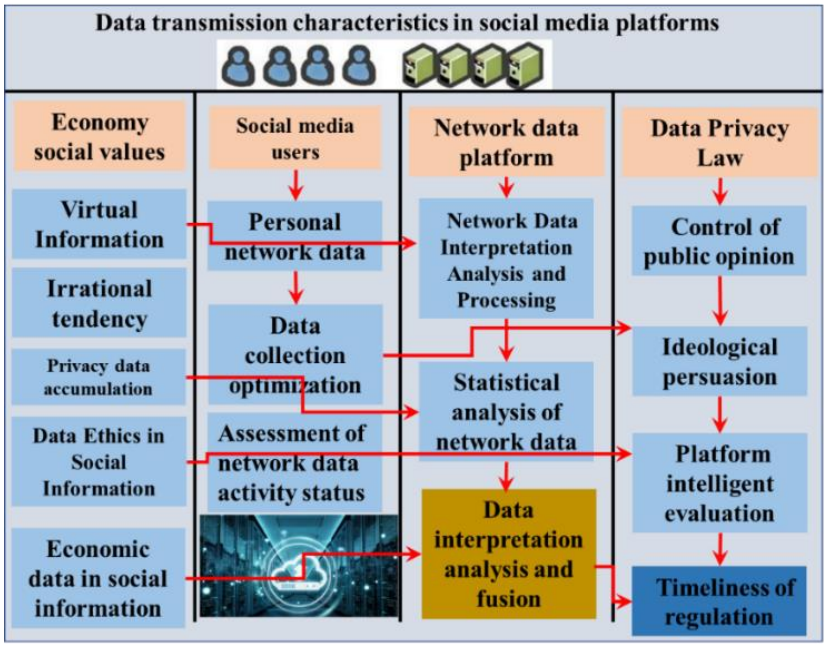

Figure 1: Data Transmission Characteristics in SM Platforms

2.1.1 Natural Attributes of Data

With the widespread application of machine learning and other technologies in big data, people's understanding of the ethical issues brought about by the design, openness, and use of data systems is constantly deepening. The rules of data ethics should be set for the financial growth of RF. In the digital economy era, data has increasingly become an essential factor of production (Ma et al., 2022). The value of data ultimately manifests in becoming a usable data product, and the production of data products includes consumer raw data and digital enterprises' processing and integration labor. According to the principles of Marx's labor theory of value, data value comes from the data processing labor of data engineers, and only this labor can create value. Digital enterprises occupy the surplus value of data engineers. That is to say, data ownership belongs to RF, but its value is created by data engineers who put in labor.

2.1.2 The SM and Economic Attributes of Data

Processing a large amount of data recorded by human activities has become increasingly common and robust, and human, financial operations, and SM operations have been converted into multiple dimensions. Information from RF has vital SM and economic parameters, whether from the record collection or usage perspective. From the standpoint of data users, firstly, the government relies on extensive data collection to maintain SM operation and order and perform necessary SM management of RF (Ding et al., 2022). The most typical case is the collection of personal information, such as health and travel codes used by the government for prevention and control during the COVID-19 epidemic. Secondly, there are significant technology companies where data becomes a necessary input resource for controlling SM, online sales, and other activities (Gong et al., 2022). Technology companies can accurately deliver information through algorithmic calculations to increase consumer stickiness. Most countries use the "pick it up for me" method. The dissemination of private data on SM is shown in Figure 2.

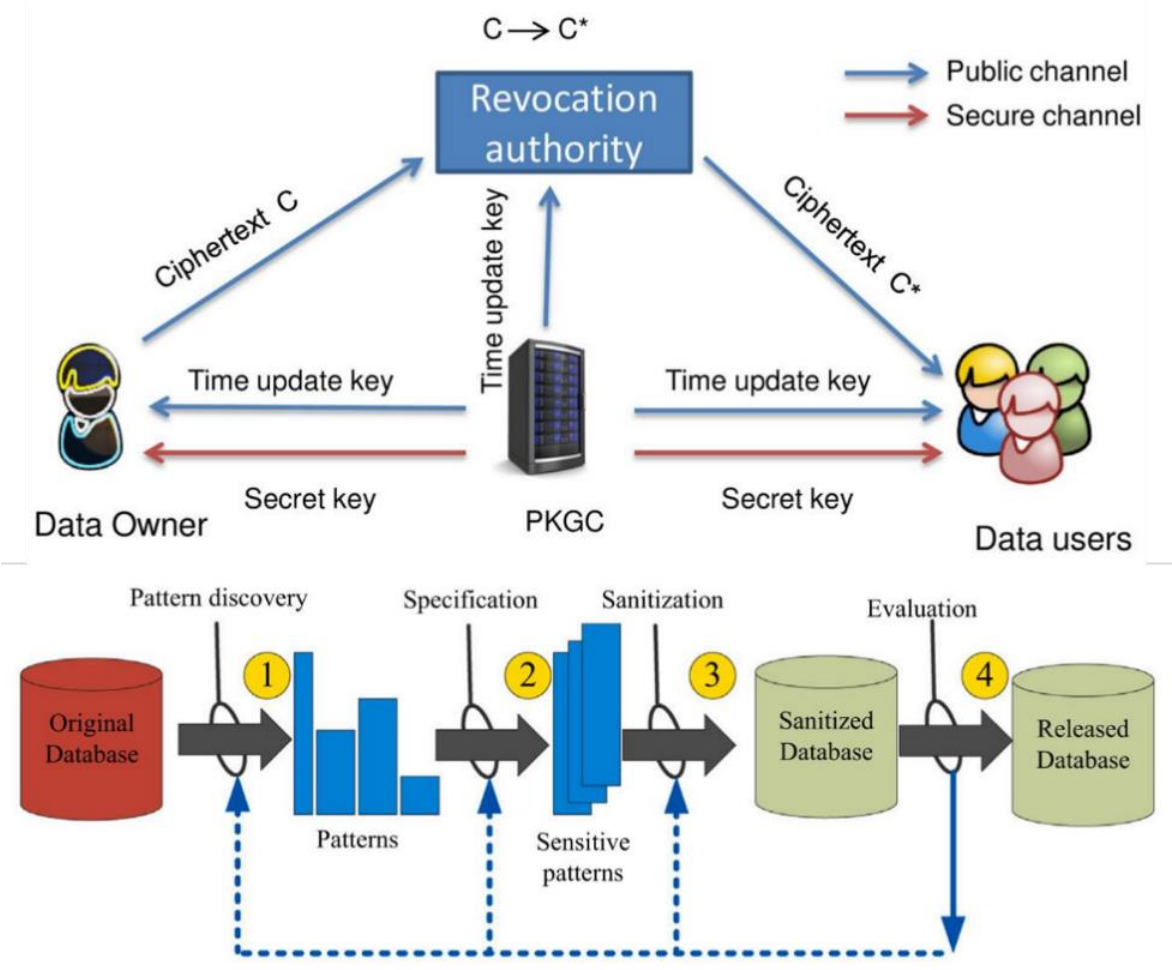

Figure 2: Privacy Data Dissemination in SM

Observing data collection, personal information is illegally obtained, stored, and transmitted, which includes lifelong characteristic details such as the face, fingerprints, and iris. Because this information is unique for a lifetime, if leaked, it means a lifetime of loss, with severe consequences. Secondly, data exchange did not fully consider the cost of privacy breaches. Consumers face many hidden dangers, including collecting and illegally transferring data from RF beyond the prescribed scope and allowing illegal actors to obtain and engage in illicit transactions through improper means.

2.2 Data Ownership of Economic Data Creators

The financial growth has brought two problems. Firstly, the data must be more transparent and frequently violate personal security. The second is that big data is saved in a private (organizational) repository. Unlike ordinary property, data from RF has its invisibility and inherent physical aspects. Data advocacy in the digital economy is indispensable for advocating individual fundamental rights and freedoms.

On the other hand, more than emphasizing the importance of privacy protection is needed. As an information entity, individuals are deeply intertwined with their personal information and their embedding in the information circle. Due to individuals weaving information bonds within the information circle, controllable and localized information openness enables them to participate in community interactions and SM operations. The information entities and data ownership of RF are not enough; sometimes, they seek to share it with others.

2.3 Materials and Methods

The information used for this study was supplied by the Catalan Institute of Studies for Ocean Administration, which recently initiated an extensive aquatic RF tracking scheme. The initiative gathers information from on-site surveys on the Catalan coastline (the southwest coast of Spain) and web-based surveys distributed to license owners. The two procedures are employed concurrently to mitigate data quality concerns based on a prior understanding of their methodological advantages and limitations. The integrated technique was initially tested in a pilot study 2021 and expanded in 2023 to establish a long-term surveillance platform. Data obtained from both Internet and physical questionnaires were freely submitted by participants and maintained in a database in compliance with the EU 2016/679 private information protection law. The information collected from each poll is anonymized; the web-based surveys could not identify the licensed customer replying to the survey.

3 Optimization of Economic Information Transmission and Encryption Mode in SM

3.1 Privacy Protection Principles for Information Transmission on SM

Determine a statistical source entropy by establishing a model for statistical sources and a model for statistical sinks. Then, it is integrated into the privacy conditional entropy and average privacy mutual

information and calculated to protect the privacy rights of internet transmission during the artificial intelligence era of RF. The transformation mode of economic data privacy information sources is shown in Figure 3.

If thieves have no means to obtain personal data, they can only rely on observation channels to reveal the personal information of RF. Therefore, the following is a mathematical modeling of private information source X ':

$$\begin{matrix} X' \\ P(X') \end{matrix} = \begin{pmatrix} x_1' & x' & \cdots & x_{i'}' & \cdots & x_{n'}' \\ p'(x_1') & p'(x_2') & \cdots & p'(x_{i'}') & \cdots & p'(x_{n'}') \end{pmatrix} \quad (1)$$

Among them, Y 'represents a private sink, 0 ≤ p' (y'j) ≤ 1, ∑ wj=1p '(y'j)=1. For the above mathematical model, define a privacy source entropy H (X '):

$$H(X') = -\sum_{i'=1}^{n'} p'(x_{i'}')\log_2 p'(x_{i'}')$$
$$H(Y') = -\sum_{j=1}^{w} p'(y_j')\log_2 p'(y_j') \quad (2)$$

H (X ') is the origin privacy data, and H (Y') is the sink privacy data. The more prominent H (X ') and H (Y'), the less likely the security data of RF will be leaked. In the absence of external conditions, this value is determined.

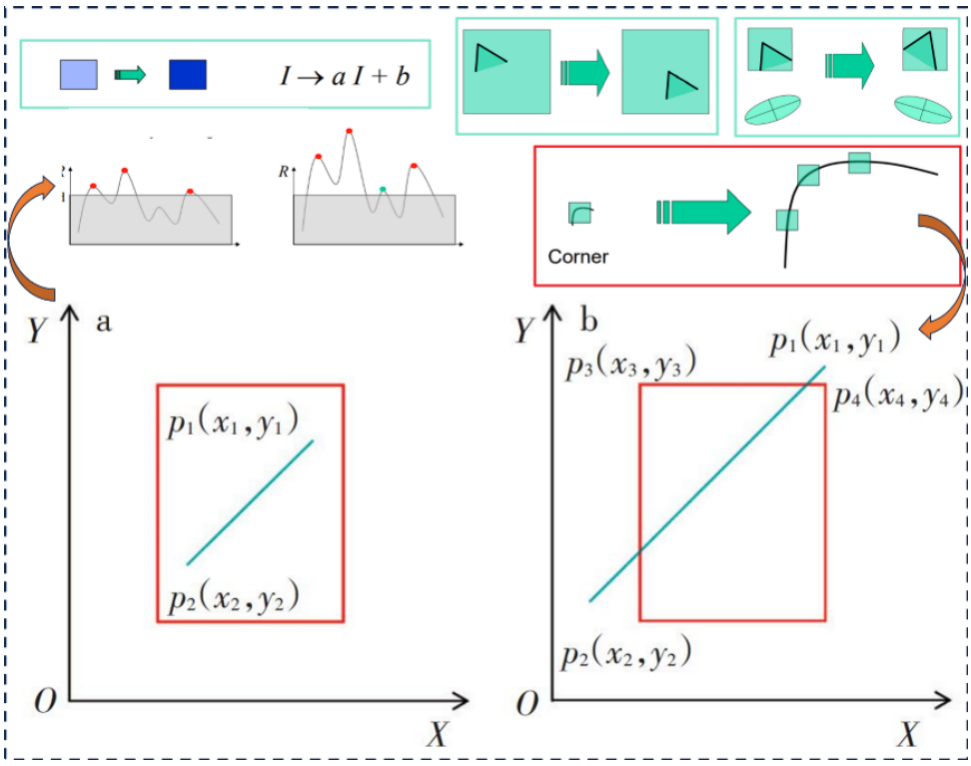

Figure 3: Conversion Mode of Economic Data Privacy Information Sources

Once a certain amount of private data of RF is collected by the privacy target Y ', the research can describe and measure the accuracy of the private source information by using the privacy conditional entropy H (X'/Y '), which is shown as:

$$H(X`/Y`)=-\sum_{j=1}^{w}\sum_{i`=1}^{n}p`(x`_i,y`_j)\log_2 p`\left(x_i/y_j\right) \quad (3)$$

According to the explanation of formula (3), when the recipient of the personal information receives Y ', even the sender X' of the private information of RF still has a slight possibility of being recognized. This study uses the mean privacy mutual data I (X '; Y') to measure the level of privacy exposure on the channel and constructs a network data transmission confidentiality model using equations (1) to (4). The following is a description of the calculation formula for mutual data:

$$I(X`/Y`)=\sum_{j=1}^{w}\sum_{i`=1}^{n}p`(x`_i,y`_j)\log_2\frac{p`\left(x_i/y_j\right)}{p`\left(x_i\right)} \quad (4)$$

In this process, I (X '; Y') represents the mean value of interactive data between the private data source X 'and the recipient Y' and is used to measure the depth of personal privacy exposure of RF. By comparing absolute differences and their squared errors, this study can effectively ensure the secure transmission of personal information in SM.

3.2 Privacy Protection Scheme based on Local Sensitive Hash Algorithm

Locality Sensitive Hash LSH is the most popular approximate nearest neighbor search algorithm. It can effectively extract a large amount of similar information from it and be used in various scenarios such as text matching and web page retrieval of RF. The local sensitive hash algorithm data interaction mode is shown in Figure 4. Its basic concept is similar to a spatial concept called "regional transformation." Suppose two pieces of data already have a certain degree of correlation or similarity. In that case, the results processed by a specific hash function will show high correlation and consistency. If there is no apparent link or differentiation between the two, the output information generated through this process should not show significant changes or related situations.

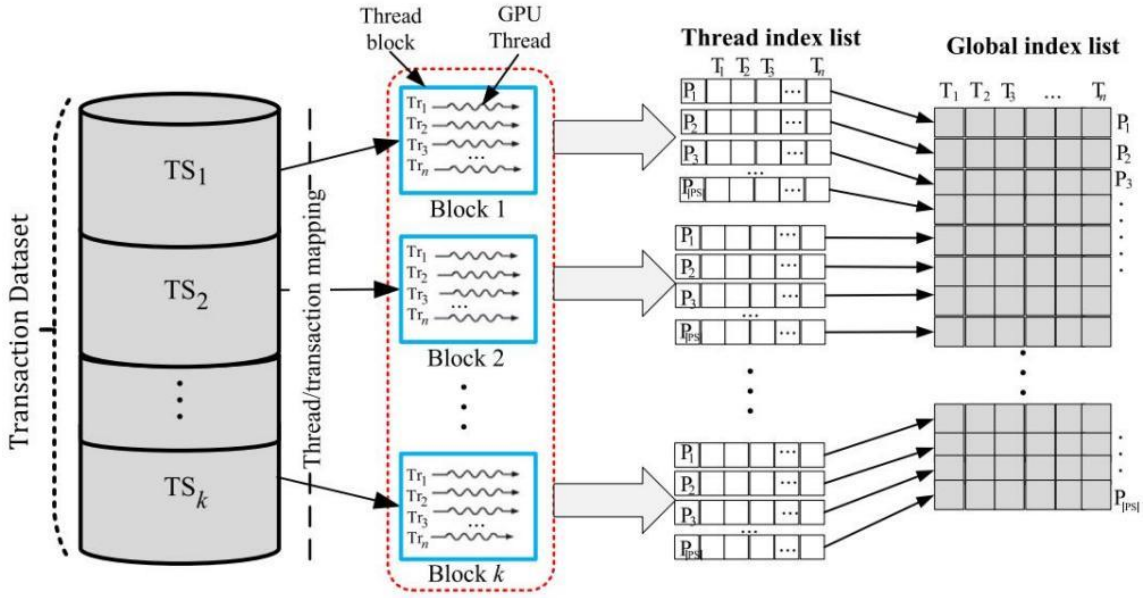

Figure 4: Local Sensitive Hash Algorithm Data Interaction Mode

The Minsha algorithm is widely used in large-scale data comparison processes, and its time and memory consumption issues have become key factors. In terms of measuring the similarity between clusters, this technology can effectively measure their similarity relationships. In the SNS system, this study used the Jacaranda index to measure the difference between the two and made accurate and distortionless predictions. The range of this indicator varies from zero to one: if the two are very close, then its score tends towards "one." The opposite situation is that the score will get lower and lower. The equation (5) is given as,

$$Jaccard(A,B)=\frac{|A\mathrm{I}\ B|}{|A\mathrm{U}B|} \quad (5)$$

Due to the consistent random likelihood of each row during the random arrangement, an essential conclusion of the Minhash algorithm can be drawn: the probability of Minhash value collision between any two users is equal to the Jaccard coefficient, and the equation (6) is given as,

$$P\left[h(A)=h(B)\right]=\frac{|A\mathrm{I}\ B|}{|A\mathrm{U}B|}=Jaccard(A,B) \quad (6)$$

The basic principle of the Minhash algorithm mentioned above can be used to calculate and obtain the Minhash signature of each user. Numerous hash functions can be used to simulate random permutations when calculating the Minhash signature to avoid multiple random permutations of the feature matrix. If k hash functions are used initially, the minimum value of the feature matrix can be calculated for each user's friend list. If there are n users in the network, after k hashing operations, the

signature matrix M_{k*n} of each user's feature matrix can be obtained. After obtaining the signature matrix M_{k*n}, the similarity between users can be calculated based on the validity of the signature. For sufficiently large k-values, the similarity of Minhash values between two users equals the similarity between the original data from RF. The privacy data processing mode of the local sensitive hash method is represented in Figure 5.

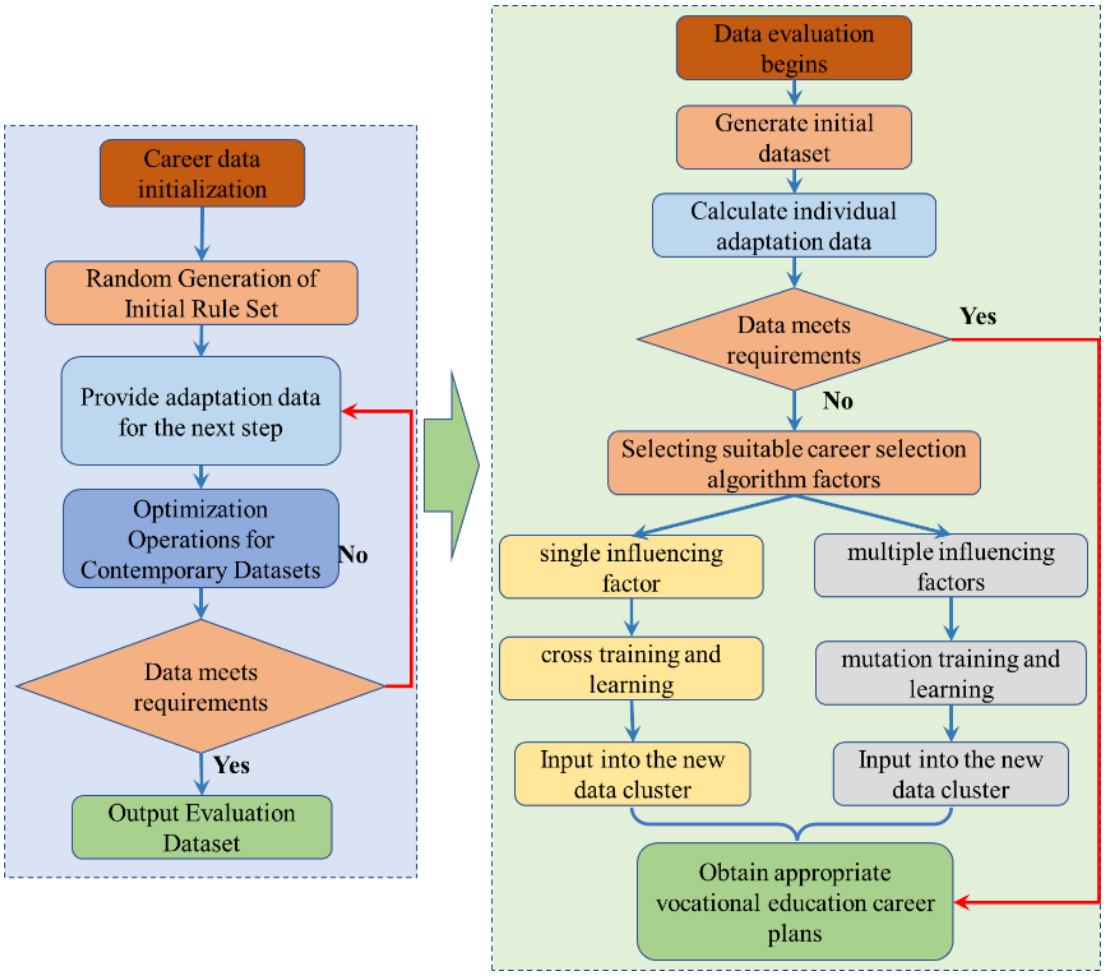

Figure 5: Private Data Processing Mode of Local Sensitive Hash Method

Based on the core mechanism of the Minhash algorithm, this study can apply the Minhash algorithm to user circles in SM opportunity networks to obtain the Minhash value of each user. Then, these Minhash values are used to evaluate the similarity of friend circles between the intermediary node and the target node to prevent the risk of users' friend circle information being publicly leaked on the network. The decision accuracy of the Minhash SSRN privacy protection scheme is shown in Figure 6. Using Minhash technology, each user's friend list can be transformed into Minhash identifiers, which can be used to calculate the similarity between friends instead of directly retrieving the original friend list to obtain resemblance. Minhash technology can reduce data volume and adopt diverse hash functions for

processing, preventing the risk of RF dictionary attacks. To study the difference between Minhash privacy policy and OSNR and to simulate the comparison of Minhash SSNR and OSNR SSNR, the friend list adjustment rate under the SSRN scheme ranges from -80% to 80%. Under the Minhash policy, the Minhash algorithm generates Minhash labels, which are used as supplementary information for routing protocols in network environments.

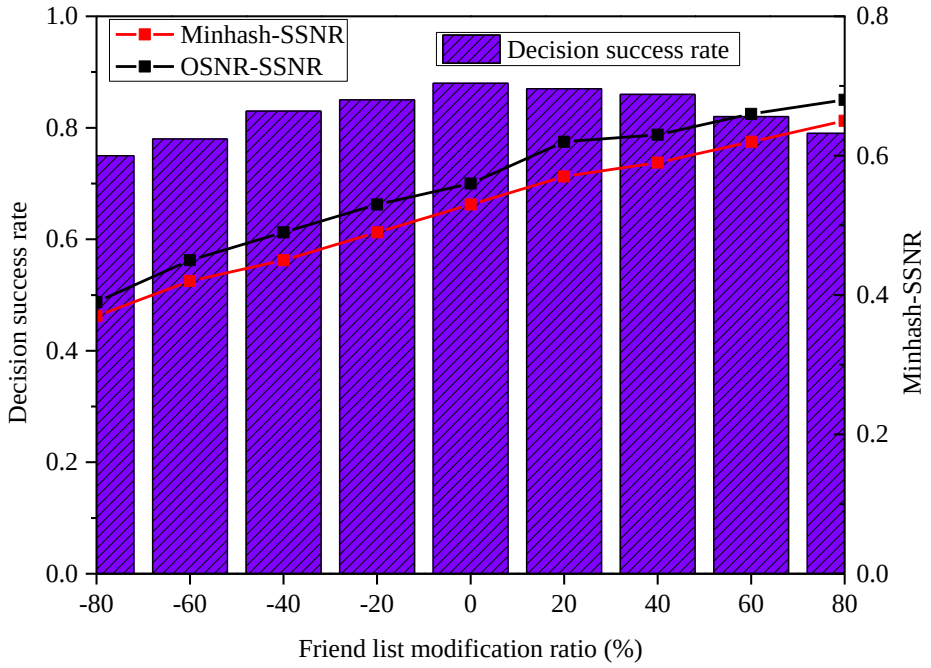

Figure 6: Decision Accuracy of Minhash-SSRN Privacy Protection Scheme

Although the information transmission efficiency of Minhash-SSNR and OSNR-SSNR methods is similar, the former still needs to be improved. This is because the Minhash algorithm compares the similarity of dimensionality-reduced data of RF, which results in a loss of some information, causing the two sets of lists that were initially high in parallel to be misjudged as low in similarity, thereby reducing the opportunity for some original information to spread and ultimately affecting the efficacy of information transmission. When the information transmission effect weakens, the average cost of the entire system decreases, indicating that Minhash-SSNR can effectively send information to nodes with high similarity and prevent excessive duplicate data within the system.

Although the message delivery efficiency of the Minhash-SSNR method has slightly decreased compared to the OSNR-SSNR method, its reduction is only 5% or less, which ensures the stable operation of the SM opportunity network and avoids significant degradation of network performance. At the same time, using Minhash technology can maintain personal privacy while maintaining efficient network operation.

4 Information Transmission Scheme and Optimization based on Network Optimization Module

4.1 Privacy Protection Scheme based on SSNR

In the SSRN privacy protection strategy, each information exchange process includes users adjusting their SM circle - adding or removing friends and then using the same hash algorithm to encrypt each piece of data from RF on these modified friend lists in a one-way manner. Because the hash algorithm is non-reversed, this approach can provide excellent privacy protection. The SSNR privacy data algorithm architecture pattern is shown in Figure 7. Under the SRSNR protocol, once two nodes meet, they must know whether the target friend exists on their friend list to make communication decisions. In response to this situation, this study needs to consider the following possible scenarios:

If this study decides to expand the list of friends in this study by adding new members, then this study can consider selecting m potential new candidates from the existing network, and the number of these candidates should be at least equal to the number of new members multiplied by the ratio P. In this way, the total number of newly added friends will be n+n * P, and this process will be influenced by the random selection of n * P among m individuals in this study. This adjustment and update of the friend list changed the path planning selection.

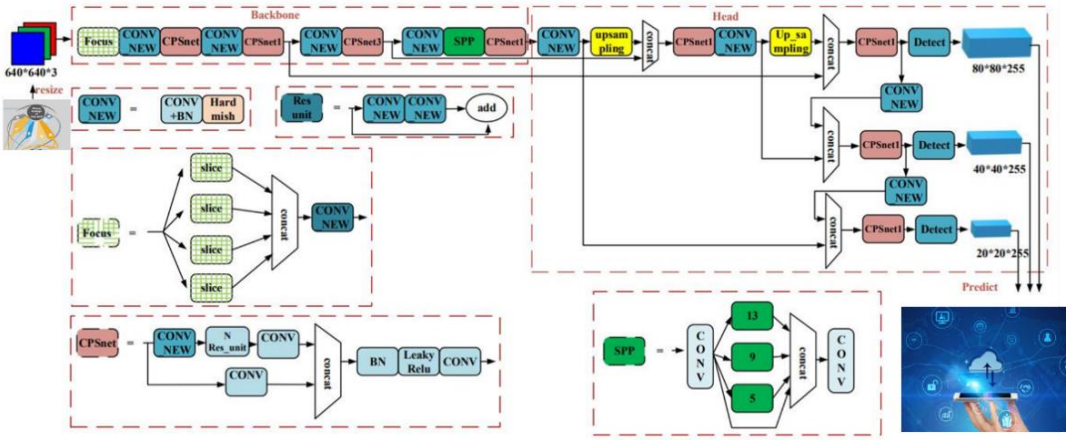

Figure 7: SSNR Privacy Data Algorithm Architecture Pattern

If m=n * p, then error=100%, meaning misjudgment will occur. Customers can choose any method and ratio to change their friend list in real-world scenarios of RF. In the simulation testing phase, this study selected a fixed friend list update method and ratio to simplify the protocol process. For example, if you choose to increase by 50%, the user has added 50% to their friend list, and all network nodes will perform the same operation to update their friend list. Generally speaking, the number of shared friends in an SM group reflects the strength of their connection. According to the SM opportunity path SRSNR and SSN protocols of the SSNR scheme, the selection accuracy of the information transmission rate and privacy protection plan of RF can be referred to in Figure 8.

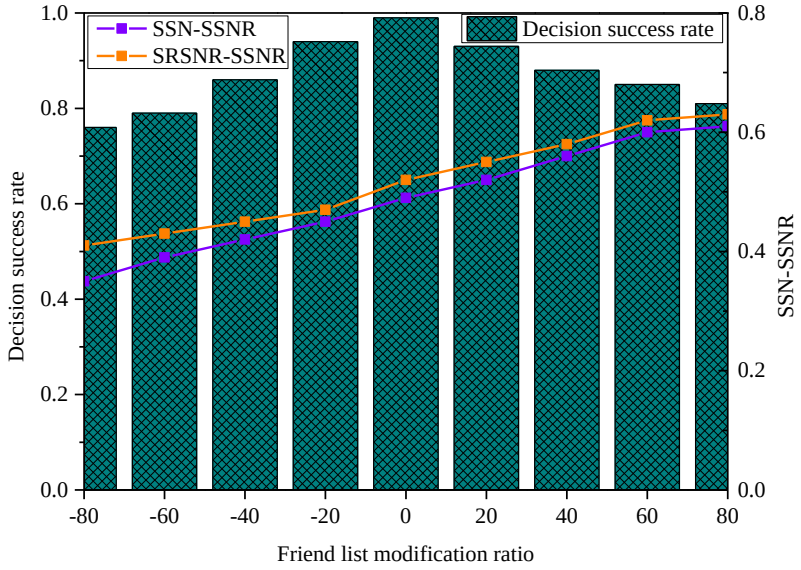

Figure 8: Message Delivery Rate and Decision Accuracy of Privacy Protection Scheme

When the user has not implemented privacy protection policies, the accuracy of the decision is 100%, and no errors have occurred. As this study begins to remove some individuals or add new ones to its friend list, the accuracy of the decisions made in this study will rapidly decrease with these changes. Regardless of adjusting the friend list, it leads to incorrect choices, and the likelihood of such decisions is directly proportional to the changes made. If this study adds new names to the list of friends or reduces the names of specific individuals, it can guarantee at least a 90% chance of making the right decision. Similarly, using the SSNR method to handle the deletion problem on the friend list can maintain the accuracy of the decision in this study at around 80%, indicating that this method is very stable and effective.

The security performance of privacy and confidentiality policies in cryptography depends on how they can resist these threats when maliciously violated. When using SSNR privacy protection methods, one of the primary means of destruction is dictionary attacks. Once the hacker obtains the modified friend list of the target user, they can use this ratio and dictionary search method to restore the original friend list of the target user.

4.2 Comparative Analysis of Privacy Protection Schemes

To analyze the differences between two user security schemes based on local sensitive hash algorithms, Minhash and Simhash, and security based on hash function encryption one by one, this section applies four plans, SSNR, OSNR, Minhash, and Simhash, to the SM opportunity network protocol SSN, respectively.

Many studies and simulations on SM opportunity networks rely on existing real-world human behavior trajectory datasets and input them into simulation models to better understand the situation. This dataset was collected on university campuses, with 40 participants from students and teachers. The most critical part includes their SM platform's personal information, which is used as the basis for SM relationships. Some encounter events were not recorded due to equipment issues, resulting in a relatively small dataset. At the same time, this study constructed a similar environment to test the performance indicators of SM opportunity networks based on the privacy protection policies of RF.

To assess the impact of various privacy protection measures on network performance. This study conducted simulation experiments on four privacy and confidentiality methods on the ONE platform: SSNR, OSNR, Minhash, and Simhash. To simulate initial data, this study set SSNR to add 0% of new friends to the friend list; OSNR adopts the Bloom filter algorithm and sets its parameter M to 20. In the Minhash algorithm, the number of hash functions is defined as 64 to facilitate multiple rounds of extracting the minor hash result from the friend list to improve accuracy. Finally, in the Simhash algorithm, the length of the Simhash signature is determined to be 64 bits, ensuring accurate results in the final similarity comparison. The comparative analysis of message delivery rates between different network optimization algorithms is shown in Figure 9.

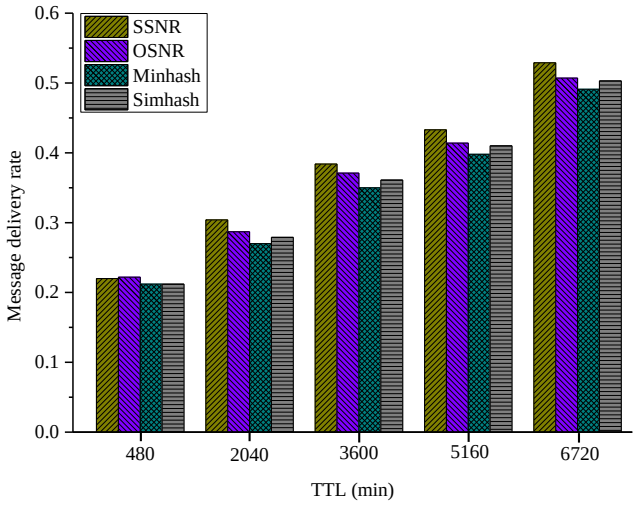

Figure 9: Comparative Analysis of Message Delivery Rates among different Network Optimization Algorithms

Because there is no possibility of error execution or reduced information volume, the SSNR method can provide the highest message delivery efficiency. Using SSNR to ensure the functionality of the original SM opportunity network, zero changes to the SSNR scheme are equivalent to the information transmission effect of the actual opportunity network. The other four strategies are similar regarding RF

information transmission speed, with Simhash providing a higher information transmission rate and shorter delay time than the other two. Minhash's method can maintain network performance similar to OSNR.

To test the computational accuracy and convergence of this study's network information transmission optimization module, it was compared and analyzed with the privacy protection scheme mentioned above in the same sample of RF. In standardized test sample inputs, a network model is used to simulate operations without setting target expected values, and the output values of the model are compared with the sum to check the accuracy of the simulation. Figure 10 shows the number of machine learning times and exponential error distribution for different models.

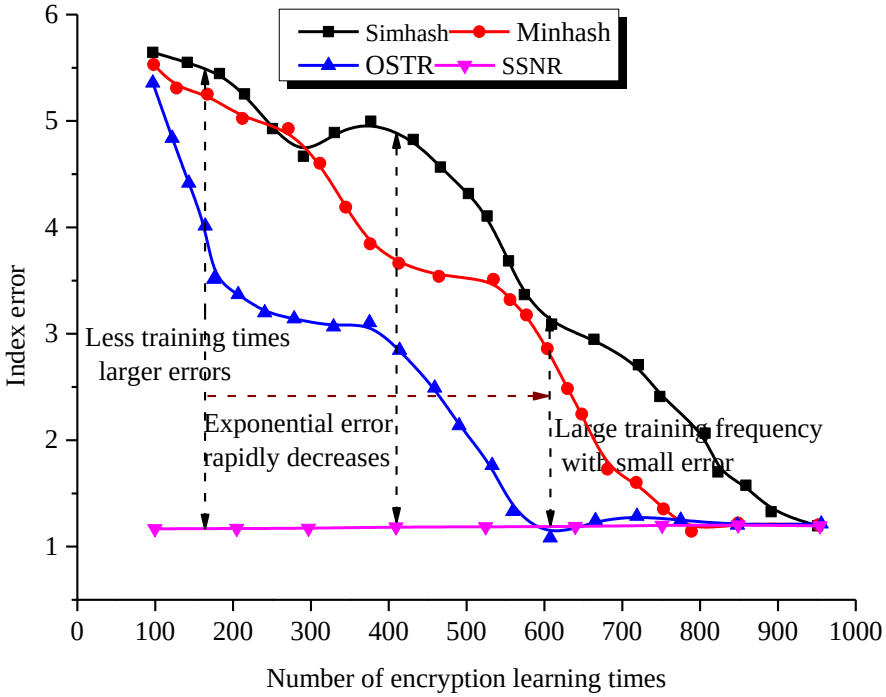

Figure 10: Learning Times and Exponential Error Distribution of Different Methods

From Figure 10, it can be seen that the Simhash privacy protection method requires 912 steps to reach the accuracy requirement. The Minhash privacy protection method requires 742 degrees to achieve the accuracy target. With few learning and training times, the network information transmission optimization module proposed in this study quickly gained a lower exponential error. Compared to other methods, the convergence of the Simhash privacy protection method is poor, requiring more training sessions to achieve a sure convergence accuracy. The above experimental data is divided into two RF, A and B datasets. The training errors for different privacy protections on two other datasets, A and B, are shown in Figure 11.

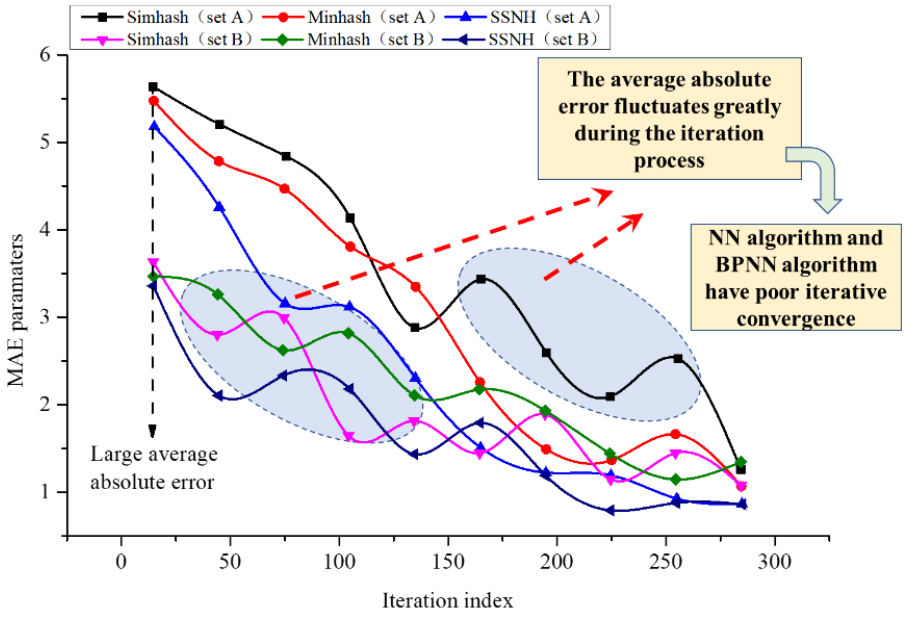

Figure 11: Distribution of Iterative Exponential Mean Absolute Error (MEA) Values for Different Methods

Figure 11 shows that the MAE values (average absolute error) of the Network Information Transmission Optimization Module (SSNR) in this study are relatively low on different datasets. Compared with other methods, the error is relatively small, indicating that this method has a certain degree of accuracy. This study established initial weights, learning weights, training datasets, test datasets, application datasets, and other RF data as files for program calls.

4.3 Exploration of the Optimal Rule Framework for Protecting Economic Data Privacy

In recent years, China has rapidly proposed maintaining a balanced development in the digital economy, which requires promoting and regulating its growth. At the same time, corresponding regulatory frameworks have been established, and necessary boundaries and warning lines have been set, all of which aim to build a solid legal foundation to support the sustained and stable development of the digital economy. The core lies in establishing and gradually optimizing data ethics systems and artificial intelligence ethics systems and developing professional, ethical guidelines for data collection, storage, and analysis to meet the needs of China's digital development and ensure the good use of science and technology. The optimal rule framework for protecting economic data privacy is shown in Figure 12.

According to the basic principles of welfare economics, an ideal SM management model should simultaneously achieve two significant goals: firstly, society's overall well-being is the highest; secondly, sharing wealth and SM resources somewhat is essential. Although these two principles sometimes conflict due to their short-term or partial impact, they should complement and support each other from a long-term and comprehensive perspective. In terms of the digital process, the main task of this study is to utilize effective mechanisms to generate more revenue for the entire industry and improve the

quality of life for the public. Therefore, to achieve this goal, this study must strive to create an environment where all roles can benefit, especially those who have been overlooked and should receive appropriate support and services.

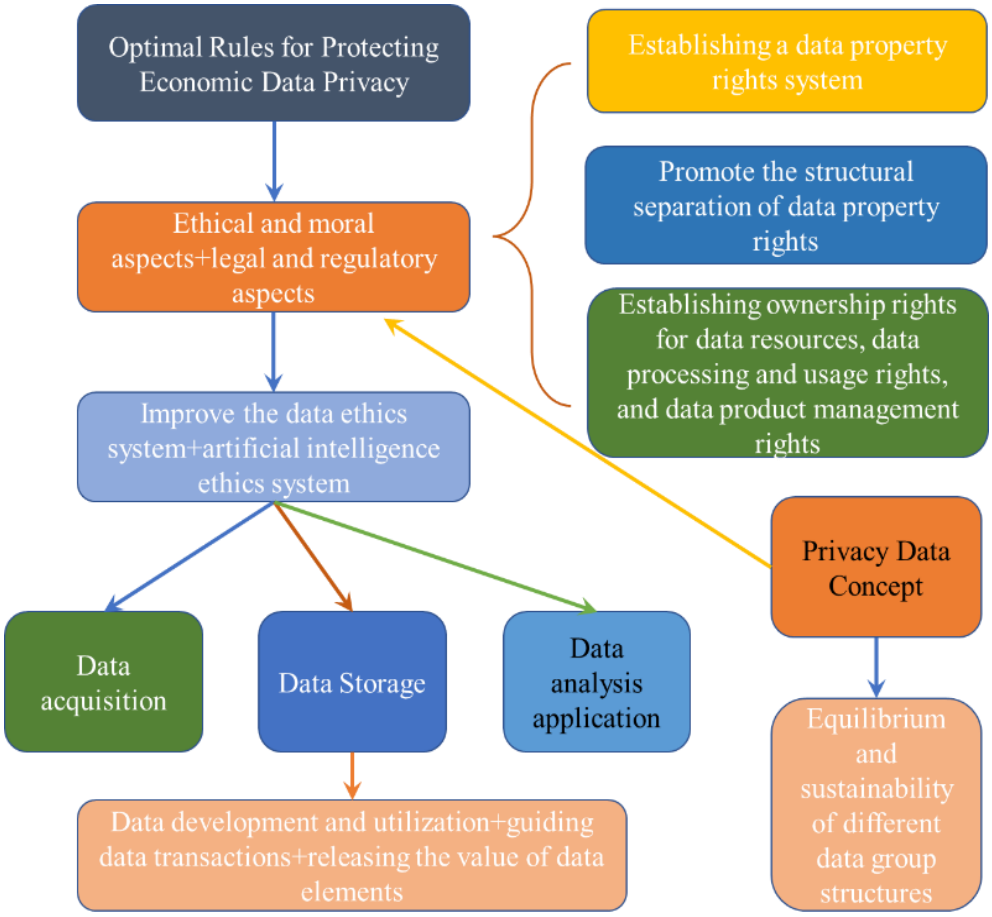

Figure 12: Optimal Rule Framework for Economic Data Privacy Protection

Firstly, this study needs to construct a system of data privacy and confidentiality principles for consumers in China's digital economy. Then, this study aims to actively promote the decentralization of data ownership architecture, break free from the constraints of a single ownership concept, and enable all roles to participate in collecting, managing, analyzing, and applying consumer data. By dividing the ownership rights of data assets, data processing, and usage rights, and data commodity operation rights, this study can provide necessary legal support for promoting the orderly flow of data, stimulating innovative use of data of RF, guiding the purchase and sale of data products, and exerting the role of data elements. This study can only stimulate relevant interest entities to find ways to generate reasonable profits from data operations in a protected environment while ensuring personal information rights, enabling them to carry out data-driven work of RF.

5 Conclusion

This study focuses on the sharing economy information transmission, network optimization of SM platforms, and privacy protection issues during data transmission of RF. The study starts with the data transmission characteristics in SM platforms, analyzes the data ethics in SM information transmission from the perspectives of natural and economic data attributes, and then focuses on the privacy protection principles in network information transmission. Then, a privacy protection scheme based on a locally sensitive hash algorithm is constructed, and finally, an information transmission scheme and method optimization based on a network optimization module are proposed. A comparative analysis was conducted on the computational convergence and accuracy of different privacy protection methods for RF, and the optimal rule framework for data privacy protection was discussed.

1. If the list of friends on SM has not changed (i.e., the modification rate is zero), then the accuracy of the decision is 100%, and no errors will occur. Once deleting or changing a friend list is implemented, decision-making accuracy will be decreased. Increasing or decreasing the friend list leads to decision failure; the more significant the increase or decrease, the lower the probability of a successful decision. When adding new behavior to the friend list, the accuracy of its decision-making can always be maintained at over 90%. When performing deletion operations, using the SSNR strategy can stabilize the decision accuracy within a range of about 80%, demonstrating the efficiency and trustworthiness of the strategy.
2. Although the interaction efficiency of Minhash-SSNR is lower than that of OSNR-SSNR, the reason is that the Minhash method compares the similarity of dimensionality-reduced data, which causes information loss, leading to the possibility of two sets of SM relationships with high similarity being misjudged as low similarity, thereby affecting the effective information transmission and interaction effect in SM opportunity networks, and ultimately leading to a decrease in message delivery rate for RF.
3. When the efficiency of information transmission decreases, the overall cost of the network decreases, indicating that the Minhash-SSNR strategy effectively sends information to nodes with high similarity, thereby preventing the repetition of information within the network. Although the information transmission efficiency of the Minhash-SSNR strategy is slightly lower compared to the OSNR-SSNR strategy, its reduction is only about 5%, ensuring that the essential functions of the SM opportunity network are not affected and there is no possibility of a significant decline in network performance for RF. Using the Minhash algorithm while ensuring personal privacy, regular operation can be maintained in SM opportunity networks.
4. In the case of few learning and training times, the network information transmission optimization module proposed in this study quickly achieved a lower exponential error. When the number of training sessions is small, there is a difference between the exponential mistake of the other three algorithms and the exponential error of the network information transmission optimization module in this study. As the number of training sessions gradually rises, the exponential error of the network information transmission optimization module for RF in this study is relatively small, and the prediction accuracy of the method is high. Compared to other methods, the convergence

of the Simhash privacy protection method is poor, and more training sessions are needed to achieve a sure convergence accuracy.

The research initially assessed the profiles of ocean RF who share their catches on digital channels, encompassing accessible SM and fishing applications. This information is essential for effectively incorporating SM data in overseeing RF. The increasing proliferation of digital data research methodologies yields quantitative instruments that enhance RF administration based on ecological and SM viewpoints. The research addressed significant information gaps regarding the accuracy of SM data for the surveillance of RF, advancing this potential monitoring methodology toward developing new programs, including large-scale, real-time, and cost-effective surveillance.

References

[1] Abadi, R. Y., & Moallem, P. (2022). Robust and optimum color image watermarking method based on a combination of DWT and DCT. *Optik*, *261*, 169146. https://doi.org/10.1016/j.ijleo.2022.169146

[2] Allison, C., Winkler, A. C., Childs, A. R., Muller, C., & Potts, W. M. (2023). Can social media platforms be used to foster improved environmental behavior in recreational fisheries? *Fisheries Research, 258*, 106544. https://doi.org/10.1016/j.fishres.2022.106544

[3] Alowibdi, J. S., Alshdadi, A. A., Daud, A., Dessouky, M. M., & Alhazmi, E. A. (2021). Coronavirus pandemic (COVID-19): Emotional toll analysis on Twitter. *International Journal on Semantic Web and Information Systems (IJSWIS)*, *17*(2), 1-21.

[4] Arora, S., & Bawa, A. (2022). Response to personalized marketing communication: an empirical investigation comparing users and non users of surrogate shoppers. *Journal of Internet Commerce*, *21*(2), 246-269.

[5] Arostegui, M. C., Anderson, C. M., Benedict, R. F., Dailey, C., Fiorenza, E. A., & Jahn, A. R. (2021). Approaches to regulating recreational fisheries: Balancing biology with angler satisfaction. *Reviews in Fish Biology and Fisheries, 31*(3), 573-598.

[6] Arslan, O., Xing, W., Inan, F. A., & Du, H. (2022). Understanding topic duration in Twitter learning communities using data mining. *Journal of Computer Assisted Learning*, *38*(2), 513-525.

[7] Bouarara, H. A. (2021). Recurrent neural network (RNN) to analyse mental behaviour in social media. *International Journal of Software Science and Computational Intelligence (IJSSCI)*, *13*(3), 1-11.

[8] Boudiaf, M., Mueller, R., Ben Ayed, I., & Bertinetto, L. (2022). Parameter-free online test-time adaptation. *In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 8344-8353.

[9] Chawra, V. K., & Gupta, G. P. (2022). Optimization of the wake-up scheduling using a hybrid of memetic and tabu search algorithms for 3D-wireless sensor networks. *International Journal of Software Science and Computational Intelligence (IJSSCI)*, *14*(1), 1-18.

[10] Chopra, M., Singh, S. K., Gupta, A., Aggarwal, K., Gupta, B. B., & Colace, F. (2022). Analysis & prognosis of sustainable development goals using big data-based approach during COVID-

19 pandemic. *Sustainable Technology and Entrepreneurship*, *1*(2), 100012. https://doi.org/10.1016/j.stae.2022.100012.

[11] Di Caprio, D., Santos-Arteaga, F. J., & Tavana, M. (2022). An information retrieval benchmarking model of satisficing and impatient users' behavior in online search environments. *Expert Systems with Applications*, *191*, 116352. https://doi.org/10.1016/j.eswa.2021.116352

[12] Ding, N., Xu, Y., Tang, Y., Xu, C., Wang, Y., & Tao, D. (2022). Source-free domain adaptation via distribution estimation. *In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 7212-7222.

[13] Eckhardt, Y. (2024). Fishing for compliments: Legitimate illegality and institutional signaling in the case of recreational fishing in Germany. *Geoforum*, *155*, 104082. https://doi.org/10.1016/j.geoforum.2024.104082

[14] Fowler, A. M., Dowling, N. A., Lyle, J. M., Alós, J., Anderson, L. E., Cooke, S. J., & Chick, R. C. (2023). Toward sustainable harvest strategies for marine fisheries that include recreational fishing. *Fish and Fisheries, 24*(6), 1003-1019.

[15] Gong, T., Jeong, J., Kim, T., Kim, Y., Shin, J., & Lee, S. J. (2022). Note: Robust continual test-time adaptation against temporal correlation. *Advances in Neural Information Processing Systems*, *35*, 27253-27266.

[16] González-Padilla, P., López, A. F., & Lacárcel, F. J. (2022). Main government-related data extraction techniques: a review. *Handbook of research on artificial intelligence in government practices and processes*, 142-160.

[17] Gu, J., Vo, N. D., & Jung, J. J. (2022). Contextual Word2Vec model for understanding chinese out of vocabularies on online social media. *International Journal on Semantic Web and Information Systems (IJSWIS)*, *18*(1), 1-14.

[18] Gundelund, C., Arlinghaus, R., Baktoft, H., Hyder, K., Venturelli, P., & Skov, C. (2020). Insights into the users of a citizen science platform for collecting recreational fisheries data. *Fisheries Research*, *229*, 105597. https://doi.org/10.1016/j.fishres.2020.105597

[19] Lefèvre, P., Carré, P., Fontaine, C., Gaborit, P., & Huang, J. (2022). Efficient image tampering localization using semi-fragile watermarking and error control codes. *Signal Processing*, *190*, 108342. https://doi.org/10.1016/j.sigpro.2021.108342

[20] Lehdonvirta, V., Oksanen, A., Räsänen, P., & Blank, G. (2021). Social media, web, and panel surveys: using non-probability samples in social and policy research. *Policy & Internet*, *13*(1), 134-155.

[21] Lennox, R. J., Sbragaglia, V., Vollset, K. W., Sortland, L. K., McClenachan, L., Jarić, I., & Twardek, W. M. (2022). Digital fisheries data in the Internet age: emerging tools for research and monitoring using online data in recreational fisheries. *Fish and Fisheries, 23*(4), 926-940.

[22] Liang, J., Hu, D., & Feng, J. (2021). Domain adaptation with auxiliary target domain-oriented classifier. *In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 16632-16642.

[23] Ma, N., Bu, J., Lu, L., Wen, J., Zhou, S., Zhang, Z., ... & Yan, X. (2022). Context-guided entropy minimization for semi-supervised domain adaptation. *Neural Networks*, *154*, 270-282.

[24] Olasumbo Afolabi, O., Ozturen, A., & Ilkan, M. (2021). Effects of privacy concern, risk, and information control in a smart tourism destination. *Economic research-Ekonomska istraživanja*, *34*(1), 3119-3138.

[25] Sbragaglia, V., Espasandín, L., Coco, S., Felici, A., Correia, R. A., Coll, M., & Arlinghaus, R. (2022). Recreational angling and spearfishing on social media: insights on harvesting patterns, social engagement and sentiments related to the distributional range shift of a marine invasive species. *Reviews in Fish Biology and Fisheries, 32*(2), 687-700.

[26] Vitale, G., Dedeu, A. L., Pujol, M., & Sbragaglia, V. (2021). Characterizing the profile of recreational fishers who share their catches on social media. *Frontiers in Marine Science*, *8*, 768047. https://doi.org/10.3389/fmars.2021.768047.

[27] Zafar, A. U., Shen, J., Ashfaq, M., & Shahzad, M. (2021). Social media and sustainable purchasing attitude: Role of trust in social media and environmental effectiveness. *Journal of Retailing and Consumer Services, 63*, 102751. https://doi.org/10.1016/j.jretconser.2021.102751

[28] Zumpano, F., Copello, S., Favero, M., & García, G. O. (2023). Research trends and future perspectives of recreational fisheries in South America. *Fisheries Research, 258*, 106546. https://doi.org/10.1016/j.fishres.2022.106546