# Proposal of Blockchain-Based Identity Information Hiding Image Sharing Mechanism for Building Image Sharing System

**Jinsu Kim[1], Eunsun Choi[2], Namje Park[3*]**

*[1]Department of Convergence Information Security, Graduate School, Jeju National University, Jeju, Republic of Korea*
*[2]Department Physics, Engineering and Technology, University of York, United Kingdom*
*[3]Department of Computer Education, Teachers College, Jeju National University, Jeju, Republic of Korea, namjepark@jejunu.ac.kr*

As SNS (Social Network Service) becomes popular, users are sharing their data on the platform. A large amount of data has been uploaded to the Internet at high speed by general users, and shared data is generally an image or video and includes personal identification information. In general, uploaded data includes facial information, and images containing facial information can be abused by third parties. Therefore, measures are required to prevent anyone other than the person who uploaded the data ledger from using the image without permission. In this paper, we propose a mechanism to share images through a block network by inserting user identity information into uploaded images to securely share images. To prevent indiscriminate use of images, user identification information is inserted into the LSB (Least Significant Bit) of the image based on the randomly generated key by the user, allowing for better management of the image information. In addition, to strengthen the integrity of image data, the hash of image data with hidden identity information is recorded and managed in the block network, thereby preventing excessive data from being inserted into the block network and authenticating the image ledger. Based on the random key, about 99.89% similarity was confirmed when 100 bytes of identity information was inserted into a 255*255 size image. To verify the insertion of image data into the blockchain network, block creation was executed on the private blockchain server.

**Keywords:** Identity information hiding image, block network, image sharing system, LSB, User identity information.

## 1. Introduction

SNS is a platform that is actively used by many users even today, and the main growth factor of SNS is that users can share their daily lives or experiences by using the platform. SNS users use images or video media that are easy to understand as a medium to share their

experiences (Tomas et al, 2021). The medium composed of images is an effective medium for sharing experiences because it can deliver visually and directly, and at the same time simplify and deliver complex information (Brooke et al, 2021).

However, it is becoming a social problem as the visual media used to share one's experience is used for crimes without the consent of the person concerned. In digital information, it is generally difficult to distinguish between original data and copied data, and even if the copied data is used by a third party, it is difficult for the originator of the data to recognize it(Umit et al, 2019). In addition, there is a problem that the reputation of the original author of the image data may be damaged, and privacy may be violated(Anna et al, 2020). Images containing facial information of general users can be used for scams that generate victims such as Romance Scam, Identity Theft, and Social Engineering Fraud by stealing identity(Spencer, 2019). Therefore, there is a need for a method of safely managing image data to protect user privacy.

In this paper, the author of the image is identified by hiding the user's identity information in the image using a random key, and the integrity of the image is strengthened by verifying the identity concealed image through a block network. We propose an image sharing mechanism that can be strengthened.

## 2. Related Works

### Digital Copyright Protection

Steganography refers to a technique of hiding data inside other data. The target of hiding includes general files, texts, audio, and images. A steganography file that hides data does not differ significantly from a general file in the transmission process (Kim et al, 2021). The bit plane embedding technique, which is one of the steganographic techniques, inserts its data by converting bits at positions that do not significantly affect the image (Sachinet al, 2020). At this time, a bit that does not significantly affect data is referred to as a least significant bit (LSB).

A watermark is a technique for displaying a visually identifiable identifier on an image or document (Mahbuda et al, 2020). The originality of the image or document including the identifier is guaranteed, and the copyright can be protected because the user's identity information is leaked when the user's identity information is inserted (Mohanarathinam et al, 2020). When a file is leaked to the outside, it can be used to track the leaked target based on the embedded watermark.

### Analysis of Related Research Trends

In general, security studies on images are focused on studies that strengthen the integrity of images so that they are not forged and altered by a third party. Forgery of images is not only a primary level problem of simply impersonating a specific individual, but also can cause social problems that may arise from impersonating an individual. Nandhini's research conducted research on the directionality of applying steganography, which hides data in images, to three areas: the traditional technique, the Convolutional Neural Network-based technique, and the General Adversarial Network-based technique (Nandhini et al, 2021). Pratap's research emphasized the influence of image steganography on application security, and conducted research on the application area of digital steganography (Pratap et al, 2022).

Ashwaq's research conducted a study on generating steganography using LSB and Secret map, and it was confirmed that it showed strength against differential and statistical attacks (Ashwaq et al, 2022).

## 3. Proposal of blockchain-based identity information hiding image sharing mechanism

The blockchain-based identity information hiding image-sharing mechanism proposed in this paper can prove that it is the data ledger by hiding the user's identity information in an image based on a random key. blockchain technology offers innovative solutions for identity information hiding, authenticity verification, and data integrity across diverse industries (Kusuma Kumari et al., 2022; Kim and AlZubi, 2024). By leveraging blockchain's decentralized and tamper-resistant properties, organizations can enhance privacy, security, and trust in digital transactions and interactions. In addition, when used for a crime, the leaker or theft victim can be found based on the data hidden in the image. In the process of data sharing, the image information in which the user's identity information is hidden is recorded in the block network through a hash operation to distribute and store verification data for future images. The hash value distributed and stored through the block network is used to verify image data and check duplicate data.

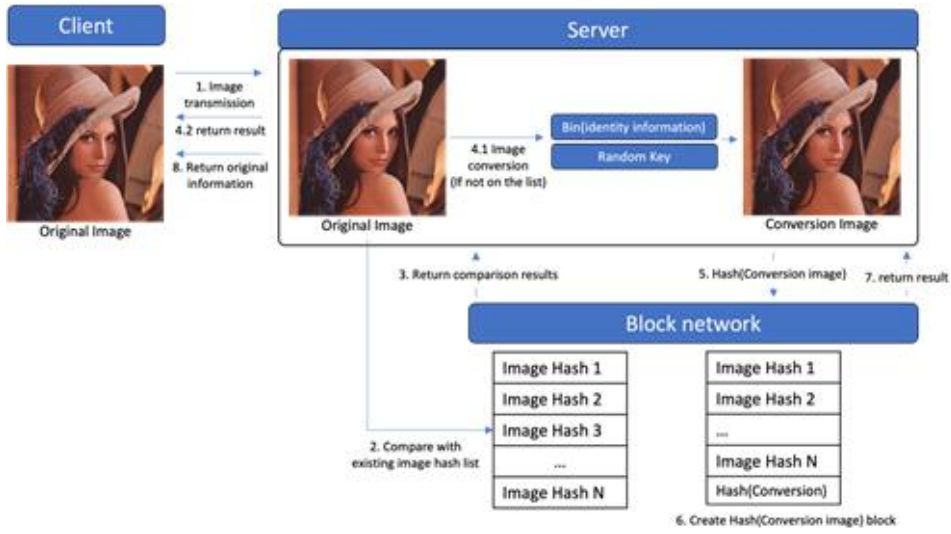


Fig. 1: Proposal Mechanism Conceptual Diagram

[Figure 1] explains the overall concept of the proposed mechanism. When image data is requested to be recorded by a client, the server primarily performs a hash operation on the image received from the client to determine whether the hash value is a recorded image on the block network. If it is a hash value recorded on the block network, it notifies the user that upload is not possible and ends. However, if it is not recorded, the user's identity information is hidden in the image based on the random key, and the hash value of the newly created image is generated as a new block to perform registration. Finally, when the hash value of the converted image recorded on the block network is confirmed, the original information that can be restored by the random key is transmitted to the user. Only the random key is stored on the server, and the original information transmitted to the user is deleted. In this

case, it means the LSB of the original image dropped in the process of converting the original information. Therefore, since the server does not record the LSB information of the original image, arbitrary restoration is impossible.

The proposed mechanism consists of two key functions. Firstly, a data validation module that determines whether the image to be uploaded is valid. Secondly, an image conversion module that inserts identity information based on a random key into new images.

Data Validation Module

The data discrimination module performs the process of receiving an image from a user and storing it in a block network. The image received from the user requires a conversion process in which identity information is inserted by a random key, and image conversion is performed by the image conversion module. [Table 1] summarizes the data and data abbreviations used in the proposed mechanism.

Table 1: Abbreviation

| Data structure | Function |
|---|---|
| Target image ($IM_T$) | Ledger of images requested to be shared by users. |
| Image metadata ($MD_I$) | Metadata such as the image's EXIF data, image size, resolution, etc. |
| User identification ($ID_U$) | Identification information to perform user authentication. |
| Random key ($K_R$) | Key required to insert or restore user identification information into an image. |
| Convert Image ($IM_C$) | An image in which identity information is inserted into a target image by a random key. |
| Convert Image LSB ($LSB_C$) | LSB set of ledger images dropped due to identity embedding. |
| Image License ($L_I$) | About setting a user's license permissions for image sharing. |
| Hash List ($H_L$) | A hash list of converted images stored on the block network |
| Block Data ($B_D$) | Identification information of the block in which data is stored. |

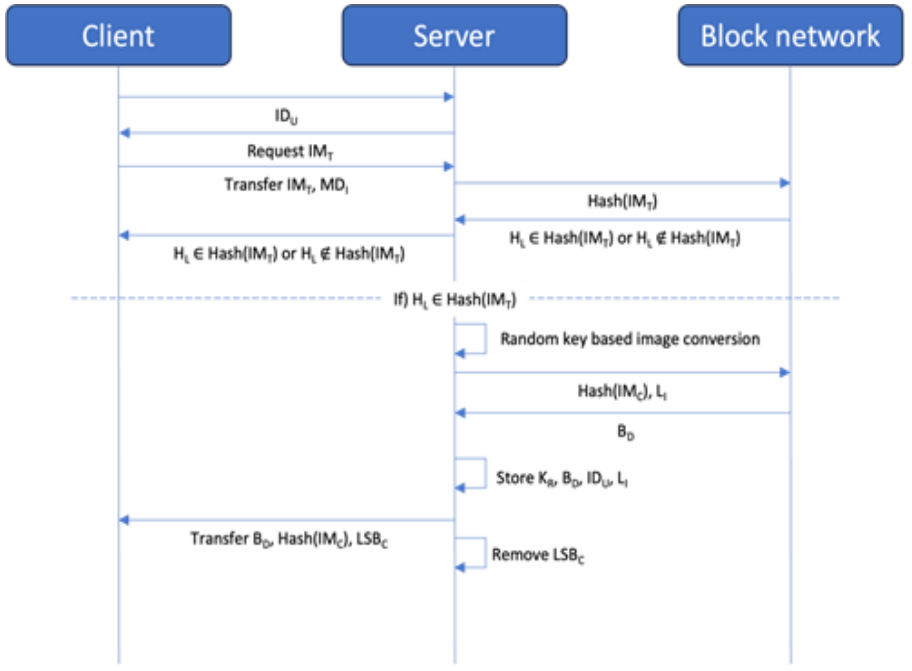


Fig. 2: Data validation module flowchart

[Figure 2] shows the flow of the data validation module. The client sends its identification information ($ID_U$) to the server to prove its identity and save the image to the sharing system. The server requests an image according to the request of the client, and the user delivers the image ($IM_T$) and the metadata ($MD_I$) of the image to the user. The server compares the hash of the image received from the user with the hash list ($H_L$) stored on the block network. Currently, if the hash of the requested image is included in the hash list, the result is returned to the client and the process is terminated.

If the image requested by the user is not included in the hash list, the user's identification information is hidden in the image based on the random key. Concealment of identification information may not be performed according to the user's license authority setting. The server records the hash of the converted image ($IM_C$) in which the user's identification information is inserted and the license authority setting ($L_I$) in the block network. Thereafter, the random key, block data, user identification information, and license authority setting information including the identification information of the generated block data ($B_D$) are stored in the server. The identification information for checking block data, the hash value of the converted image, and finally the LSB state value ($LSB_C$) of the ledger image that can restore the converted image are transmitted to the user, and the LSB state value is removed on the server.

**Image Conversion Module**

The image conversion module refers to a module that hides identity information based on a random key in image information received from a user. In the process of inserting user identification information ($ID_U$) into an image, a hash operation ($D_{hash}$) is performed on the identification information primarily so that a specific individual cannot be inferred. The hash value is converted to binary ($D_{Bin}$) for insertion into the LSB. [Formula 1] and [Formula 2] show the process of hashing the identity information and converting it into binary numbers, respectively.

$$D_{Hash} = Hash(ID_U) \quad (1)$$

$$D_{Bin} = Bin(D_{Hash}) \quad (2)$$

The insertion of the binarized identity information is performed by using a random key ($R_K$) in the matrix ($I_H$, $I_W$) of the image. In order to change the LSB state value of a specific location, the size of the entire image is divided by the length of the binary value of the identity information so that all identity information can be entered in the image. Based on the position, move as much as the remainder divided by the random key. As the constant value of the random key increases, the range of location selection widens. [Formula 3] shows the process of selecting a random location.

$$Px = \frac{I_H * I_W}{Len(D_{Bin}) - R_K} + (Px_{n-1} \,\%\, R_K)$$

If image conversion is performed through the above process, the result shown in [Figure 3] can be obtained. [Figure 3.a] shows the position of the LSB selected during the image conversion process, and [Figure 3.b] randomly changes the pixel at the LSB position selected in the converted image to (255,255,255) for visual confirmation. will show results.

(a)

(b)

Fig. 3: Image conversion result

## 4. CONCLUSION

As communication technology develops, a network with increased accessibility provides a lot of information to users and acquires a lot of data from users at the same time. In particular, in the case of SNS, as image data is actively used, new images are uploaded to the server to share experiences. In SEMRUSH, which analyzes traffic on the network side and provides search volume, keyword research, and online ranking data, etc., it can be seen that the traffic rankings of Twitter, Facebook, and Instagram, three representative SNS applications, are included in the top 10(Semrush, 2023).

However, SNS, which is actively used, is causing many problems with shared images at the same time. In particular, as it is used for scams such as romance scams that impersonate others by stealing image information, image information is more secure in that it mass-produces not only victims who directly suffer financial damage from images but also victims who have their personal information stolen. A way to share is required.

Therefore, in this paper, to safely share image information, we hide identity information in images based on random keys to prevent indiscriminate use by third parties and to track the target through identity information in images when using images. In addition, in the process of storing or using images, the hash of the image can be used limitedly according to the user's authority through the hash list recorded in the block network and the license permission setting.

**Acknowledgments**

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2022S1A5C2A04092269).

**References**

Anna, C., Andrea, P., Fabio, F., Fulvio, C., Alessandra, M., & Giacomo, G. (2020). Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review. Clin Pract Epidemiol Ment Health, 16, 24-35, https://doi.org/10.2174/1745017902016010024

Ashwak, A., Maisa'a, A.A.K.A., & Adnan, S. (2020). Image steganography using least significant bit and secret map techniques. International Journal of Electrical and Computer Engineering (IJECE), 10(1), 935-946. https://doi.org/10.11591/ijece.v10i1.pp935-946

Brooke, A. & Monica, A. (2021). Social Media Use in 2021: A majority of Americans say they use YouTube and Facebook, while use of Instagram, Snapchat and TikTok is especially common among adults under 30. Pew Research Center.

Jinsu, K., & Namje, P. (2022). De-identification mechanism of user data in video systems according to risk level for preventing leakage of personal healthcare information. Sensors, 22(7), 2589. https://doi.org/10.3390/s22072589

Kim, S.Y. and AlZubi, A.A. (2024). Blockchain and Artificial Intelligence for Ensuring the Authenticity of Organic Legume Products in Supply Chains. Legume Research. https://doi.org/10.18805/LRF-786.

Kusuma K., B. M., Arora, M., AlZubi, A. A., Verma, A., & Andrze, S. (2022). Application of Blockchain and Internet of Things (IoT) in the Food and Beverage Industry. Pacific Business Review (International. 15(10), 50-59.

Mahbuba, B., & Mohammad, S.U. (2020). Digital Image Watermarking Techniques: A Review. Information, 11(2), https://doi.org/10.3390/info11020110

Mohanarathinam, A., Kamalraj, S., Prasanna Venkatesan, G.K.D., Renjith, V.R., & Manikandababu, C. S. (2019). Digital watermarking techniques for image security: a review. Journal of Ambient Intelligence and Humanized Computing. 11, 3221-3229. https://doi.org/10.1007/s12652-019-01500-1

Nandhini, S., Omar, E., Somaya, A.M., & Ahmed, B. (2019). Image Steganography: A Review of the Recent Advances. IEEE Access, 9, 23409-23423. https://doi.org/10.1109/ACCESS.2021.3053998

Pratap, C.M., Imon, M., Goutam, P., Chatterji, B.N. (2020). Digital image steganography: A literature survey. Information Sciences, 609, 1451-1488. https://doi.org/10.1016/j.ins.2022.07.120

Sachin, D., & Rashmi, G. (2020). Analysis of various data security techniques of steganography: A survey. Information Security Journal: A Global Perspective, 30(2), 63-87, https://doi.org/10.1080/19393555.2020.1801911

Semrush, https://ko.semrush.com/?l=ko&1692591443 [Accessd : 2023/08/21]

Spencer, H. (2019). Getting to Know You: Welfare Fraud Investigation and the Appropriation of Social Ties. American Sociological Review, 84(1), 171-196. https://doi.org/10.1177/0003122418818198

Thomas, A., Matthias, G., Oswin, M., & Deni, J. (2021). Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019. Cyberpsychology, Behavior, and Social Networking, 24(4), https://doi.org/10.1089/cyber.2020.0134

Umit, C., & Bilal, A. (2019). A new direction in social network analysis: Online social network analysis problems and applications. Physica A: Statistical Mechanics and its Applications. 535, https://doi.org/10.1016/j.physa.2019.122372