e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

BLOCKCHAIN TECHNOLOGY FOR SAFE AND EFFECTIVE SHARING OF SECRET IMAGES IN WIRELESS NETWORKS VIA OUTSOURCING COMPUTATION

Dr. Shashikala SV[*1], Likith R[*2]

[*1]Professor & HOD, Computer Science And Engineering, BGS Institute Of Technology, BG Nagara, Karnataka, India.

[*2]4th Year, 8th Sem Computer Science And Engineering, BGS Institute Of Technology, BG Nagara, Karnataka, India.

ABSTRACT

By creating and dispersing n shadow pictures in such a way that any subset of k shadow images may restore the secret image, a system known as Secret Image Sharing (SIS) allows the sharing of any given secret image. However, there are significant security risks since the shadow pictures in the current SIS systems are readily manipulated and altered during communication. Blockchain has become a promising paradigm in the fields of information security and data transmission in recent times. We provide a blockchain-based Secure and Efficient Secret picture Sharing (BC-SESIS) method with wireless network computation outsourcing to safely exchange and efficiently safeguard the secret picture data. The blockchain is used to store the encrypted shadow pictures in the proposed BC-SESIS method, keeping them safe from manipulation and corruption. We provide a blockchain-based Secure and Efficient Secret picture Sharing (BC-SESIS) method with wireless network computation outsourcing to safely exchange and efficiently safeguard the secret picture data. The blockchain is used to store the encrypted shadow pictures in the proposed BC-SESIS method, keeping them safe from manipulation and corruption. To reach the (k, n) threshold for recovering the secret picture, the identity authentication-enabled smart contract is introduced. In addition, an effective outsourcing computation approach is devised to outsource the restoration work, which is aimed to lessen the computational load on smart contracts and users. Agent miners in the encryption domain safely implement this. Comprehensive experiments and theoretical analysis show that the BC-SESIS system may achieve great computing efficiency and desired communication security in wireless networks.

Keywords: Blockchain, Wireless Networks, Outsourcing Of Compute, Covert Image Sharing.

I. INTRODUCTION

Multimedia information in wireless communication is particularly exposed to several security risks, such as message manipulation, tampering, and corruption in wireless networks, due to the broadcast nature of wireless media and the rapid advancement of wireless communication technologies[1]. As a result, it's essential to ensure that every hidden picture on wireless networks is secure. In light of this, the technique known as Secret picture Sharing (SIS) shares the secret picture by creating n shadow images in such a way that every subset of k shadow images has the ability to restore the secret image. Based on the idea of polynomials, Thien and Lin [4] initially presented the (k, n)-SIS approach. In this technique, a (k − 1)-degree polynomial f(x) has k coefficients made up of each of the k secret pixels. Then, by calculating f(xi), where xi is an integer and i ∈ [1, n], a dealer may create n shadow pixels. n shadow pictures are created and then sent to n matching participants on networks after the aforementioned procedure is repeated until all pixels of the secret image have been analysed. Any k shadow pictures may collectively recover the hidden image using Lagrange's interpolation process, but (k−1) or fewer shadow images cannot. As a result, one may consider the (k, n)-SIS system to be a threshold-based cryptography technique. Even though (k−1) or fewer shadows cannot reveal the secret picture information, it is quite likely that these shadows will be altered or damaged via wireless networks, making it impossible to accurately reconstruct the original secret image. Therefore, SIS systems are desperately needed to stop shadow pictures in wireless networks from being altered or damaged. Motivated by the great potential of blockchain, to securely communicate and effectively protect the secret image data distributed on the networks, we propose a Blockchain-based Secure and Efficient Secret Image Sharing (BC-SESIS) with outsourcing computation in wireless networks. In the proposed BC-SESIS scheme, the shadow images are first generated from a given secret image, and then they are encrypted by Fully Homomorphic Encryption (FHE) algorithm and stored in the blockchain to prevent them from being tampered and corrupted during the wireless communication. A smart contract that supports identity authentication is created and implemented during the secret image restoration step in order to meet the (k, n) SIS threshold. A significant portion of the secret image restoration operation, which is safely carried out by agent miners in the encryption domain, is also outsourced using an effective outsourcing computation mechanism in order to lessen the computational load on smart contracts and users. The BC-SESIS system exhibits significant resilience to data tampering and corruption, as well as good computing efficiency, as demonstrated by theoretical analysis and comprehensive testing.

II. RELATED WORK

Firstly, we examine the standard SIS systems. Next, we also explain the blockchain technologies that are very relevant to the proposed BC-SESIS scheme, such as smart contracts and the Inter Planetary File System (IPFS).

A. Secret Image Sharing.

The technique for secret sharing was initially presented in 1979 by Naor and Shamir. The secret sharing scheme essentially creates a set of random-like data, known as shares or shadows, from given secret data and then distributes them to the participants to ensure that each participant has one shadow, rather than directly communicating the original secret data on the network. The secret data components in this method are concealed within the constant coefficient of a polynomial of degree (k − 1), called f(x). Then, by computing f(xi), where xi is a real number and xi ∈ [0, p − 1], i ∈ [1, n], one may produce n shadows. Following the previously mentioned process for each of the k data items in the secret image, n shadows are created and distributed to the n participants on the networks that correspond to them. Consequently, throughout the previous few decades, numerous SIS methods were put forth. They concentrate on enhancing sharing efficiency through various concealment techniques [5], examining the extent of reliance on reliable third parties [6], and assessing the adaptability and durability of picture restoration [7], [8]. Following a thorough examination of these references, Table I presents a thorough comparison between the suggested system and the associated SIS designs. It should be noted that while all of the SIS systems mentioned above are capable of preventing the secret picture from being accessed by others without sufficient shadows, they are not able to stop the shadow images from being altered and damaged in communication networks, which will make it impossible to precisely recover the secret image.

B. Blockchain Technologies

1) Blockchain: Generally speaking, blockchain is understood to be a distributed, decentralized data ledger in the literature [10]. New data is uploaded to a block and made accessible to all users or nodes in a distributed network by utilizing blockchain technology. The network nodes known as miners, who are in charge of maintaining the blockchain, are primarily in charge of creating new blocks using the Proof of Work (Pow) technique [11].When it comes to offloading computations, the cooperative strategy may support a greater number of IoT devices than noncooperative approaches. For block chained IoT systems, which may more sensibly distribute computing resources to IoT nodes, the non-trustworthy MEC verification technique was developed. An alternating iterative technique based on Continuous Relaxation and Greedy Rounding (CRGR) was presented to efficiently accomplish optimal delay-limited computation offloading for all users in the delay-limited mining job based on PoW, which was described as a non-cooperative game. We are motivated to suggest a blockchain-based secure and effective secret image sharing system with outsourced computing for wireless networks after the aforementioned methods have shown the security and efficacy of blockchain techniques in this setting.

2) IPFS: An interplanetary distributed file system, or peer-to-peer IPFS, has been suggested. It is inspired by the decentralized nature of blockchain technology. In contrast to conventional distributed file systems, which rely on a centralized server for file administration and storage, IPFS does not require a central server in order to store and exchange file data among many network nodes. By employing Distributed Hash Tables (DHT), IPFS may provide a high-throughput storage methodology.

III. THE PROPOSED BC-SESIS SCHEME

A. The BC-SESIS Scheme's proposed framework

The first security model Throughout the entire study, we took the semi-honest model into consideration. More specifically, any number of participants with less than k would work together with other users in the wireless network to try and get, alter, or corrupt other people's image sharing. Furthermore, we believe that attackers are unable to breach the blockchain network's security.

Stated differently, since the majority of nodes in the blockchain network are seen to be trustworthy and dependable, the attackers are unable to control the majority of the network's computational power and resources. Furthermore, we present the BFV homomorphic encryption scheme to guarantee the safe outsourcing of secret image restoration.

1. Roles: We first outline the principal roles, which are as follows, in order to make the introduction of the BC-SESIS system easier.

Dealer: As the owner of the secret image, the Dealer is in responsibility of creating and providing the group of Participants with an encryption key and a collection of shadow.

Those in attendance: Each participant receives one shadow image and the encryption key from the Dealer at the secret picture sharing stage. He then uploads the encrypted shadow picture to the blockchain after encrypting it with the key.

During the stage of hidden image restoration, each participant chooses whether to provide the applicant access to their shadow.

2. Phase of Trust Establishment: Designates a mutual-trust entity (dealer), who computes n secret shares based on the initial secret picture and disburses them to n participants in a safe manner, ensuring that any k or more participants who share their image shares may readily retrieve the original secret, but whatever A group that possesses just k − 1 shares or less is unable to retrieve the secret.

3. Framework: Next, as seen in 1, we present the framework. Both the secret picture restoration step and the secret image sharing stage are included. TABLE II is a collection of the principal notations used in the suggested scheme. stage of secret image sharing: Starting with a secret picture SI, the Dealer creates n shadow images {Si} |1 ≤ i ≤ n}, then securely distributes the shadows and the FHE algorithm private key, shown as (Si, sk), to n Participants. The FHE technique is then used by the Participants to encrypt their own shadows. Ultimately, the participants store the encrypted shadow pictures S ′ i on IPFS and upload the file's address that has been returned encrypted from IPFS to the blockchain.

4. Secret image restoring stage: Initially, when the applicant wants to recover the secret picture, he sends the AutoIDAuth-enabled smart contract a request for image restoration together with his identification details. The smart contract then requests permission to see the participants' shadow pictures after confirming their identities. The calculation of polynomials in the encryption domain on the blockchain is one of the tasks that the smart contract outsources when it has gathered k authorizations. Afterwards, a few Agent Miners calculate the polynomials inside the encryption domain and subsequently transmit the polynomial coefficients to the smart contract. Ultimately, the applicant computes the secret picture using these coefficients once the smart contract confirms them and provides them to them.

B. Stage for Covert Image Sharing

The process of sharing a hidden image has three primary stages: creating a shadow image encrypting the shadow image, and uploading the shadow image. Here are the specifics for each phase.

Step 1 Creating shadow images: We also use the polynomial (k − 1)-degree polynomial, which is defined as follows, to produce the shadow pictures from a given secret image SI with the size of w × h, similar to the current polynomial-based SIS systems.

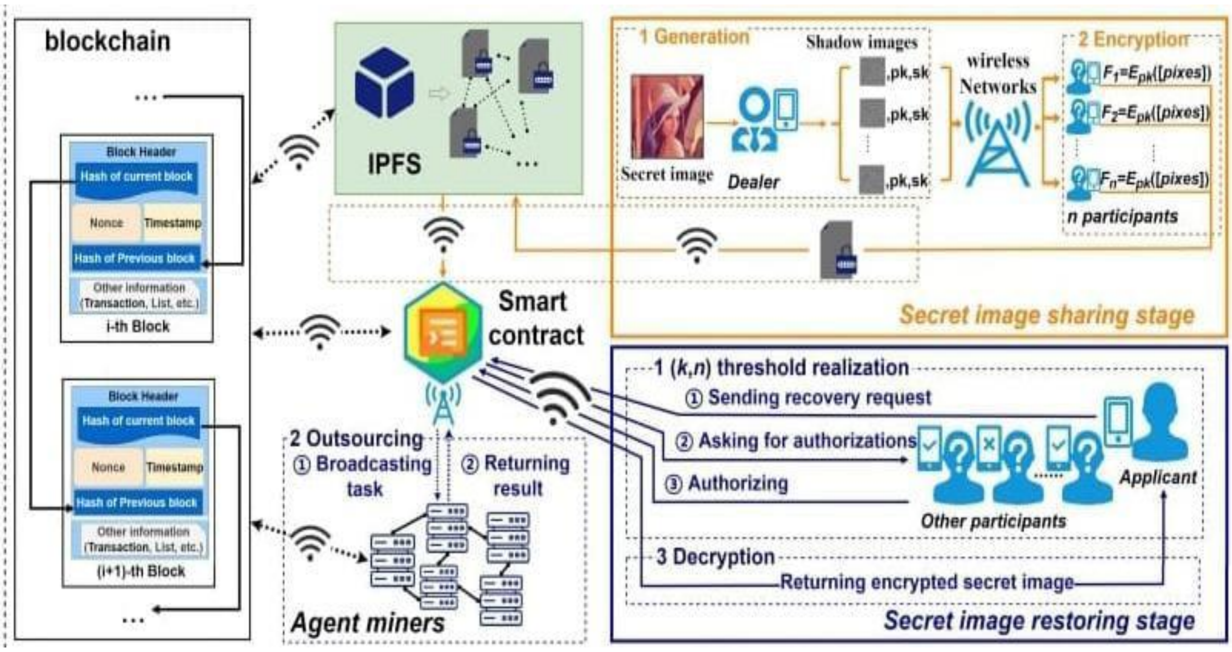

Fig 1. Framework proposed BC-SESIS scheme.

Step 2: Shadow image encryption: We use the FHE algorithm to encrypt the shadow images before uploading them to the blockchain in order to facilitate the outsourcing of the computation of secret image restoration. This is because the FHE algorithm allows secure computations on encrypted data without the need to decrypt it. In comparison to other FHE algorithms, the BFV algorithm performs better in terms of efficiency and feasibility because of its smaller relinearization key. For these reasons, we have selected the BFV algorithm as the FHE algorithm in the proposed BC-SESIS scheme for shadow image encryption.

Step 3: Uploading a shadow image: It is important to note that the blockchain would experience significant delay and storage overhead if these huge encrypted data are directly stored on the blockchain.

IV. EXPERIMENTAL RESULT AND ANALYSES

A. Parameters

There are two important factors in the proposed BC-SESIS scheme: k and N. Here, N is the number of pixels split into each batch during the batch encryption for shadow pictures, and k denotes the minimal number of shadow photos required to restore the original secret one. We quantify the effects of the settings on the accuracy and time required to restore the suggested BC-SESIS method in this section. Noise is typically present throughout the encryption process in the BFV method, and the noise in the decrypted output will be amplified

by addition and multiplication. More pixels encrypted during the computation of a single polynomial may result in more noise in the encryption output.

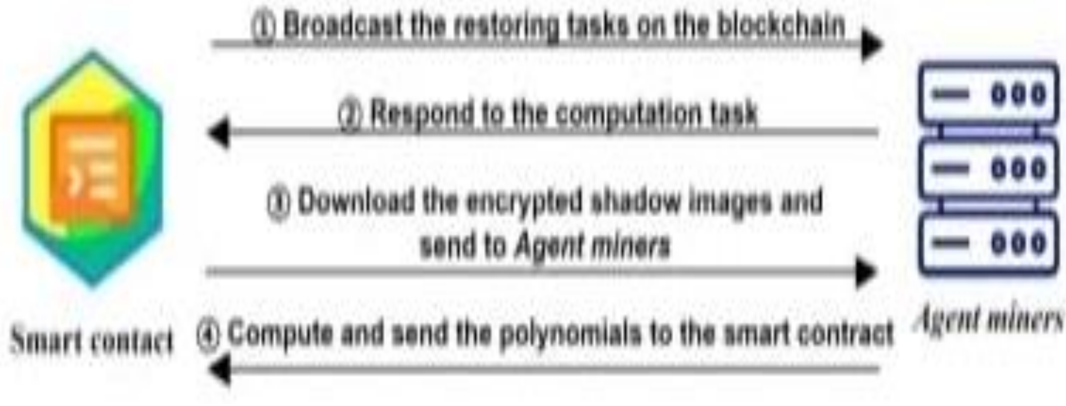
① Broadcast the restoring tasks on the blockchain
② Respond to the computation task
③ Download the encrypted shadow images and send to Agent miners
④ Compute and send the polynomials to the smart contract
Smart contact
Agent miners

Fig 2. Secret image computation

Furthermore, the parameter k controls the multiplication's depth and affects both the accuracy and restoration time. It’s important to assess the effects of the two factors on the restoration time consumption in order to strike a fair balance between accuracy and efficiency.

B. Validity of Batch Encryption Strategy on Efficiency

The batch encryption approach is developed and used to increase the productivity of creating shadow pictures. The various polynomial computation steps involved in the Lagrange interpolation technique are what make up the hidden picture restoration procedure. According to the conventional plan, every polynomial computation may restore k pixels, and each coefficient is employed to conceal one pixel. The batch encryption technique in the suggested BC-SESIS method can significantly improve the secret image restoration efficiency. Each polynomial computation may concurrently restore N × k pixels, and it can hide N pixels inside each coefficient. This part will involve studies comparing the time consumption and the amount of recovered pixels for each polynomial computation using batch and conventional encryption strategies. Finally, we will assess how effective the two solutions are by looking at how long it takes to restore a 512 × 512 image.

C. Validity of Prefix-Sum Strategy on Efficiency

To calculate the coefficients of continuous multiplication polynomials Qk (t=1,$\not{t}$=i) (x− Xt) quickly, we provide a Prefix-Sum method. We will contrast the time consumption of each polynomial calculation between the usual computation. strategy and the suggested Prefix-Sum computation strategy. The Prefix-Sum computation strategy drastically reduces the computational complexity of our scheme from O(2k)O(k2). The regular calculation strategy takes somewhat less time than the Prefix-Sum computation strategy when k is two or three, as seen in figure 5 by comparing the two computation techniques' respective levels of efficiency. It is evident that the time consumption of the Prefix-Sum computing strategy develops considerably more slowly than that of the regular calculation strategy when k is bigger than 3.

D. Time Saved in Users’ Side

The Agent miners are contracted by the Applicant to compute polynomials in the encrypted domain. The original secret picture must then be restored by the applicant by decrypting the calculated polynomial coefficients as vectors, transforming them into pixel values, and performing a modulus operation by p on the pixel values.

We examine the time that the outsourced computation saves the users as a result.

The users' time consumption T1 with outsourcing calculation, the time consumption T2 for recovering the secret picture, and the rate of time consumption savings α = (T2−T1) T2 will all be tested in the section that follows. TABLE VI displays the time usage. Based on this table, it can be seen that when the value of k falls between 2 and 6, the saving rate for users can range from 62.7% to 74.9% because the complex polynomial computation process is outsourced by the applicant. Additionally, as k increases, the complexity of the polynomial computation process increases and the proportion of modular operations in the overall restoring task decreases.

E. Probability of Cracking the Secret Image

This subsection presents the likelihood of successfully deciphering the hidden picture using a random guess. Assume that because of the participants' strong defenses, an attacker is unable to gain the decryption key, sk.

$$Pc = 1/256^{k2}$$

May be used to calculate the chances of the successfully deciphering the secret picture concealed within the encrypted coefficients of polynomials. To sum up, the Prefix-Sum computing technique has the potential to significantly increase the efficiency of the proposed system, particularly in cases when k is big where the number of polynomials in the suggested BC-SESIS scheme is denoted by Len, and k is the threshold value. The calculated Pc values for various values of k are presented. Given how unlikely it is that the secret image would be successfully cracked, the suggested method appears to be sufficiently safe.

V. CONCLUSION

We have introduced the BC-SESIS technique with outsourcing computation in wireless networks in this study in order to safely communicate and efficiently safeguard secret picture data in wireless communication. To guard against manipulation and/or corruption, the created shadows in this method are encrypted and kept on the blockchain. To reach the (k, n) threshold of SIS for secret image restoration, the identity authentication-enabled smart contract is implemented on the blockchain. To lessen the computational load on smart contracts and users, the FHE-based outsourcing computation approach is intended to outsource the secret image restoration work. Theoretical investigations and comprehensive testing demonstrate that the BC-SESIS system has a high computing efficiency in addition to achieving satisfactory security. It has been demonstrated that the suggested BC-SESIS technique is capable of managing and protecting the pictures that are dispersed over the networks. It is therefore extremely important in real-world applications. In the current and future digital world, we intend to further lessen the computational load on smart contracts and users. We also want to enhance the method of outsourcing computation so that all verification and computation operations related to the SIS task in wireless networks can be fully outsourced.

VI. REFERENCES

[1] F.Zhan, N. Yao, Z. Gao, and H. Yu, “Efficient key generation leveraging wireless channel reciprocity for MANETs,” J. Netw. Comput. Appl., vol. 103, pp. 18–28, Feb. 2018.

[2] T. Wang, Y. Liu, and A. V. Vasilakos, “Survey on channel reciprocity based key establishment techniques for wireless systems,” Wireless Netw., vol. 21, no. 6, pp. 1835–1846, Aug. 2015.

[3] T. Karygiannis and L. Owens, Wireless Network Security. Gaithersburg, MD, USA: National Institute of Standards and Technology

[4] C.-C. Thien and J.-C. Lin, “Secret image sharing,” Comput. Graph., vol. 26, no. 5, pp. 765–770, Oct. 2002.

[5] C.-C. Thien and J.-C. Lin, “An image-sharing method with user-friendly shadow images,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 12, pp. 1161–1169, Dec. 2003.

[6] C.-C. Lin and W.-H. Tsai, “Secret image sharing with steganography and authentication,” J. Syst. Softw., vol. 73, no. 3, pp. 405–414, Nov. 2004.

[7] C.-N. Yang, T.-S. Chen, K. H. Yu, and C.-C. Wang, “Improvements of image sharing with steganography and authentication,” J. Syst. Softw., vol. 80, no. 7, pp. 1070–1076, Jul. 2007.

[8] A. Beimel, “Secret-sharing schemes: A survey,” in Proc. Int. Conf. Coding Cryptol. Cham, Switzerland: Springer, 2011, pp. 11–46.

[9] X. Yan, L. Liu, L. Li, and Y. Lu, “Robust secret image sharing resistant to noise in shares,” ACM Trans. Multimedia Comput., Commun., Appl., vol. 17, no. 1, pp. 1–22, Feb. 2021.

[10] Y. Sun, Y. Lu, X. Yan, L. Liu, and L. Li, “Robust secret image sharing scheme against noise in shadow images,” IEEE Access, vol. 9, pp. 23284–23300, 2021.

[11] M. K. Sardar and A. Adhikari, “A new lossless secret image sharing scheme for grayscale images with small shadow size,” in Proc. Int. Conf. Frontiers Comput. Syst. Cham, Switzerland: Springer, 2021, pp. 701–709.

[12] S. Charoghchi and S. Mashhadi, “Three (t, n)-secret image sharing schemes based on homogeneous linear recursion,” Inf. Sci., vol. 552, pp. 220–243, Apr. 2021.

[13] Wu, C.-N. Yang, and Y.-Y. Yang, “A hybrid scheme for enhancing recovered image quality in polynomial based secret image sharing by modify-and-recalculate strategy,” J. Inf. Secur. Appl., vol. 51, Apr. 2020, Art. no. 102452.

[14] P.-Y. Lin and C.-S. Chan, “Invertible secret image sharing with steganography,” Pattern Recognit. Lett., vol. 31, no. 13, pp. 1887–1893, Oct. 2010.

[15] X. Wu, D. Ou, Q. Liang, and W. Sun, “A user-friendly secret image sharing scheme with reversible steganography based on cellular automata,” J. Syst. Softw., vol. 85, no. 8, pp. 1852–1863, Aug. 2012.

[16] Prema and S. Natarajan, “Steganography using genetic algorithm along with visual cryptography for wireless network application,”.

[17] N. F. Johnson and S. Jajodia, "Steganalysis: The investigation of hidden information," in Proc. IEEE Inf. Technol. Conf., Inf. Environ. Future, Sep. 1998, pp. 113–116.

[18] J. Fridrich and M. Goljan, "Practical steganalysis of digital images: State of the art," Proc. SPIE, vol. 4675, pp. 1–13, Apr. 2002.

[19] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 868–882, Jun. 2012.

[20] P. Poongodi et al., "Prediction of the price of Ethereum blockchain cryptocurrency in an industrial finance system," Comput. Electr. Eng., vol. 81, Jan. 2020, Art. no. 106527.