iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59034

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Blockchain-Based Secure and Efficient Secret Image Sharing with Outsourcing Computation in Wireless Networks

Maha Siddiqui
BE in Computer Science and engineering, Presidency University, India

Abstract: ***We present a novel solution, the Blockchain-based Secure and Efficient Secret Image Sharing (BC-SESIS) scheme, designed to enhance the security and efficiency of secret image sharing in wireless networks. Traditional Secret Image Sharing (SIS) methods generate multiple shadow images to distribute a secret image, allowing retrieval with a subset of these shadows. However, existing SIS schemes suffer from vulnerabilities, particularly during communication, where shadow images are susceptible to tampering and corruption, compromising security. Leveraging blockchain technology, BC-SESIS encrypts and stores shadow images securely within the blockchain, mitigating risks of tampering and corruption. A smart contract, empowered with identity authentication, ensures the requisite threshold (k, n) for secret image restoration. To alleviate computational burdens on smart contracts and users, we propose an efficient outsourcing computation mechanism. This method delegates the restoration task to agent miners within the encryption domain, ensuring secure execution. The effectiveness of the BC-SESIS scheme is substantiated through theoretical analysis and extensive experimentation. Results underscore its capacity to uphold communication security while delivering high computational efficiency within wireless networks.***
Keywords: Blockchain, Secret image sharing, Wireless networks, Outsourcing computation.

I. INTRODUCTION

With the continuous advancement of wireless communication technology, ensuring the security of multimedia information transmitted over wireless networks is paramount due to vulnerabilities such as message alteration, tampering, and corruption [1]–[3]. Secret Image Sharing (SIS) emerges as a vital technology to safeguard secret images, achieved by generating n shadow images in a manner where any subset of k shadows can reconstruct the original image [4]–[13]. Initially proposed by Thien and Lin [4], the (k, n)-SIS scheme utilizes polynomial theory, where k secret pixels serve as coefficients for a (k−1)-degree polynomial function. This function generates n shadow pixels, each computed from f(xi), where xi is an integer within the range of [1, n]. Consequently, n shadow images are transmitted to corresponding participants, facilitating secret image restoration through Lagrange's interpolation algorithm.

This threshold-based cryptography scheme ensures that any combination of k shadow images can reveal the secret image, while (k−1) or fewer shadows remain insufficient.

Despite the security provided by (k−1) shadows, the susceptibility of these shadows to tampering or corruption within wireless networks poses a significant challenge [3], [9]–[13]. To address this concern, some SIS schemes incorporate image steganography [6], [7], [14]–[16], where each shadow image is discreetly embedded within a cover image, thereby reducing the risk of tampering or corruption. However, it's worth noting that even though these embedded shadows may remain imperceptible to human observation, sophisticated steganalysis tools can potentially detect them [17]–[19].

Blockchain, as a decentralized data structure, has gained widespread adoption across various domains [20]–[30] due to its ability to mitigate security risks associated with centralized systems. In the context of data communication and information security, blockchain not only safeguards against tampering and corruption but also addresses concerns related to malicious activities [27], [31]–[35].

Inspired by the potential of blockchain technology, we propose the Blockchain-based Secure and Efficient Secret Image Sharing (BC-SESIS) scheme, with an emphasis on outsourcing computation in wireless networks. In BC-SESIS, shadow images are initially generated from the secret image, encrypted using the Fully Homomorphic Encryption (FHE) algorithm, and stored within the blockchain to prevent tampering or corruption during wireless communication. For secret image restoration, an identity authentication-enabled smart contract is deployed to achieve the (k, n) threshold of SIS. Additionally, to alleviate computational burdens on smart contracts and users, we introduce an efficient outsourcing computation method.

©IJRASET: All Rights are Reserved

This approach delegates a significant portion of the secret image restoration task to agent miners within the encryption domain, ensuring secure execution.

The BC-SESIS scheme has been rigorously evaluated through theoretical analyses and extensive experiments, showcasing robust resilience against data tampering and corruption while maintaining high computational efficiency. Our contributions can be outlined as follows:

1) Introduction of a novel SIS scheme leveraging blockchain technology and the Fully Homomorphic Encryption (FHE) algorithm. This pioneering approach marks the first utilization of blockchain and FHE within the realm of SIS. By storing encrypted information on the blockchain, the BC-SESIS scheme ensures both secrecy and integrity, safeguarding the secret image from unauthorized access and preventing tampering or corruption of shadow images during wireless communication.

2) Implementation of automated participant identification and task initiation mechanisms. Through smart contracts, the proposed scheme streamlines the secret image restoration process by automatically identifying participating entities and initiating restoration tasks upon sufficient authorization. Furthermore, the incorporation of an Automatic Identity Authentication (AutoIDAuth)-enabled smart contract facilitates the realization of the (k, n) threshold required for SIS.

3) Development of an FHE-based outsourcing computation method for secret image restoration within the encryption domain. In BC-SESIS, shadow images undergo encryption using the FHE algorithm before storage on the blockchain. Leveraging the inherent properties of FHE, the outsourcing computation method enables polynomial computation tasks to be outsourced to miners within the blockchain network. This approach significantly alleviates computational burdens on smart contracts and users.

II. OBJECTIVES

The objectives of the Blockchain-Based Secure and Efficient Secret Image Sharing (BC-SESIS) scheme with outsourcing computation in wireless networks can be summarized as follows:

1) *Enhanced Security:* Implement a robust security framework leveraging blockchain technology to protect secret image data from unauthorized access, tampering, or corruption during transmission over wireless networks.
2) *Efficient Secret Image Sharing:* Develop a mechanism for secret image sharing that ensures confidentiality and integrity while allowing authorized participants to securely access and reconstruct the original image from distributed shadow images.
3) *Utilization of Fully Homomorphic Encryption (FHE):* Employ FHE algorithm to encrypt shadow images before storing them on the blockchain, ensuring confidentiality while enabling secure computation on encrypted data.
4) *Automation of Identity Authentication:* Implement an automatic identity authentication mechanism to verify participants' identities and trigger the secret image restoration process seamlessly.
5) *Threshold-Based Secret Image Restoration:* Design and deploy smart contracts to enforce the (k, n) threshold requirement for secret image restoration, ensuring that a minimum number of authorized participants are required to reconstruct the original image.
6) *Outsourcing Computation:* Develop an efficient outsourcing computation method to offload computational tasks associated with secret image restoration to miners within the encryption domain, reducing the computational burden on smart contracts and users.
7) *Demonstrate Computational Efficiency:* Conduct theoretical analysis and extensive experiments to validate the computational efficiency of the BC-SESIS scheme, ensuring that it can operate effectively within the constraints of wireless networks
8) *Resistance to Tampering and Corruption:* Evaluate the scheme's resistance against data tampering and corruption through rigorous testing and demonstrate its ability to maintain data integrity even in the presence of malicious actors or network vulnerabilities.

III. LIMITATIONS

While the Blockchain-Based Secure and Efficient Secret Image Sharing (BC-SESIS) scheme with outsourcing computation in wireless networks offers significant advancements in securing secret image sharing, it does have limitations. These include potential scalability issues due to the computational overhead of blockchain operations and fully homomorphic encryption (FHE) algorithms, which could hinder the scheme's performance in high-volume scenarios. Additionally, the reliance on blockchain introduces dependencies on network consensus mechanisms, leading to potential latency and throughput challenges, especially in wireless environments with limited bandwidth and high latency. Furthermore, the outsourcing computation approach may introduce trust concerns, as reliance on miners within the encryption domain could raise questions regarding their reliability and integrity in executing secret image restoration tasks.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

IV. LITERATURE SURVEY

In [1] their study, Zhan, Yao, Gao, and Yu (2018) delve into the realm of Mobile Ad hoc Networks (MANETs) with a focus on enhancing key generation efficiency by leveraging the unique characteristics of wireless channels, particularly the concept of reciprocity.

The research addresses the critical challenge of secure key establishment in MANETs, crucial for ensuring the confidentiality and integrity of communication within these dynamic and self-organizing networks. Through a comprehensive literature survey, the authors investigate existing approaches and methodologies related to key generation in MANETs, aiming to identify gaps and opportunities for improvement. By proposing an efficient key generation scheme that capitalizes on wireless channel reciprocity, the study contributes valuable insights to the field of secure communication protocols for MANETs, offering potential advancements in key management practices for decentralized and resource-constrained network environments.

In [2] their survey titled "Survey on channel reciprocity based key establishment techniques for wireless systems," Wang, Liu, and Vasilakos (2015) provide a comprehensive overview of key establishment techniques that leverage channel reciprocity in wireless systems. The study focuses on exploring various approaches and methodologies for secure key establishment, considering the inherent reciprocity of wireless communication channels as a fundamental basis. By analyzing existing literature, the authors highlight the significance of channel reciprocity in facilitating efficient and reliable key establishment mechanisms across different wireless environments. Through a systematic review, the survey identifies key challenges, trends, and emerging research directions in the domain of channel reciprocity-based key establishment techniques, offering valuable insights for researchers and practitioners alike in the field of wireless networking and security.

In [3] their work "Wireless Network Security," authored by Karygiannis and Owens (2002) and published by the US Department of Commerce, Technology Administration, National Institute of Standards and Technology, the authors provide an extensive literature survey focusing on various aspects of wireless network security. This comprehensive survey covers a wide range of topics related to securing wireless networks, including authentication, encryption, access control, intrusion detection, and countermeasures against common attacks. By reviewing existing literature and industry standards, the authors aim to offer a holistic understanding of the challenges and solutions pertaining to wireless network security. This survey serves as a valuable resource for researchers, practitioners, and policymakers involved in the design, implementation, and management of secure wireless communication systems, providing insights into best practices, emerging technologies, and regulatory considerations in the field of wireless network security.

In [4] their seminal work titled "Secret image sharing," Thien and Lin (2002) delve into the concept and techniques of secret image sharing, a critical aspect of secure multimedia communication. This literature survey provides a comprehensive overview of the principles, methodologies, and applications of secret image sharing, aiming to elucidate the underlying mechanisms and highlight the significance of this technology in safeguarding sensitive visual information. By analyzing existing literature and research findings, the authors explore various approaches to secret image sharing, including threshold-based schemes and cryptographic techniques, while discussing their strengths, limitations, and potential applications. Through this survey, Thien and Lin contribute valuable insights into the field of secure image communication, paving the way for further advancements and innovations in secret image sharing techniques and applications.

In [5] their paper titled "An image-sharing method with user-friendly shadow images," Thien and Lin (2003) present a novel approach to image sharing that emphasizes user-friendliness while maintaining security. This literature survey explores the methodology proposed by the authors, which aims to enhance the accessibility and usability of shadow images in the context of secret image sharing. By analyzing the key principles and techniques employed in the proposed method, the survey sheds light on the mechanisms underlying user-friendly image sharing and highlights its potential applications in multimedia communication systems.

Thien and Lin's contribution to the field of image sharing techniques with user-friendly shadow images provides valuable insights into addressing the usability challenges associated with traditional secret image sharing methods, offering new avenues for research and development in the realm of secure multimedia communication.

In [6] their paper titled "Secret image sharing with steganography and authentication," Lin and Tsai (2004) contribute to the field of secure image communication by proposing a method that integrates steganography and authentication techniques. This literature survey delves into the methodology outlined by the authors, which aims to enhance the security and integrity of secret image sharing processes. By examining the principles and mechanisms underlying steganographic techniques and authentication protocols, the survey elucidates how the proposed method combines these approaches to ensure confidentiality, authenticity, and integrity in secret image sharing. Lin and Tsai's work provides valuable insights into the integration of cryptographic and authentication techniques

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

within the context of secret image sharing, offering potential solutions to address security concerns in multimedia communication systems.

In [7] their paper "Improvements of image sharing with steganography and authentication," Yang et al. (2007) contribute advancements to the field of secure image sharing by proposing enhancements to existing methodologies that integrate steganography and authentication techniques. This literature survey delves into the authors' approach, which aims to address limitations and improve the security and effectiveness of image sharing processes. By analyzing the principles and mechanisms underlying steganographic methods and authentication protocols, the survey elucidates how the proposed improvements enhance confidentiality, authenticity, and integrity in image sharing. Yang et al.'s work provides valuable insights into refining and optimizing cryptographic and authentication techniques within the context of secure image sharing, offering potential solutions to bolster security in multimedia communication systems.

In [8] his survey titled "Secret-sharing schemes: A survey," Beimel (2011) provides a comprehensive overview of secret-sharing schemes, offering insights into their principles, methodologies, and applications. This literature survey delves into the diverse landscape of secret-sharing schemes, examining their theoretical foundations and practical implementations. By analyzing existing literature and research findings in the field of coding and cryptology, Beimel explores various secret-sharing schemes, including threshold-based and information-theoretic approaches, while discussing their properties, strengths, and limitations. Through this survey, Beimel contributes valuable insights into the field of secret-sharing schemes, shedding light on their significance in secure communication and data protection, and providing a valuable resource for researchers and practitioners in the field of coding and cryptology. In [9] their paper titled "Robust secret image sharing resistant to noise in shares," Yan et al. (2021) contribute to the field of secret image sharing by proposing a robust scheme designed to withstand noise interference in the shared images. This literature survey delves into the methodology presented by the authors, which aims to enhance the resilience of secret image sharing schemes against noise-induced errors. By analyzing the principles and techniques employed in the proposed method, the survey elucidates how robustness against noise interference is achieved, ensuring the integrity and reliability of shared images. Yan et al.'s work provides valuable insights into addressing the challenges posed by noise in secret image sharing schemes, offering potential solutions to enhance the robustness and effectiveness of multimedia communication systems.

In [10] their study titled "Robust secret image sharing scheme against noise in shadow images," Sun et al. (2021) contribute to the field of secure image sharing by proposing a scheme designed to mitigate the impact of noise on shadow images. This literature survey explores the methodology outlined by the authors, which aims to enhance the reliability and robustness of secret image sharing schemes in the presence of noise-induced errors. By examining the principles and techniques employed in the proposed method, the survey elucidates how the scheme effectively addresses noise interference, ensuring the integrity and accuracy of shared images. Sun et al.'s work provides valuable insights into addressing the challenges posed by noise in secret image sharing schemes, offering potential solutions to enhance the security and resilience of multimedia communication systems.

V. RELATED WORK

A. Secret Image Sharing

Naor and Shamir (1979) pioneered the concept of secret sharing schemes, where instead of directly transmitting the original secret data over the network, a set of random-like data, known as shares or shadows, is generated from the secret data and distributed to participants, ensuring each participant holds one shadow. In this scheme, the secret data elements are concealed within the constant coefficients of a (k - 1)-degree polynomial, and n shadows are generated by computing the polynomial at specific points. Thien and Lin (2002) extended Shamir's scheme for image data by embedding k secret pixels into the coefficients of the polynomial, resulting in smaller shadow sizes. Subsequent SIS schemes have focused on improving sharing efficiency, dependency on third parties, and the flexibility of image restoration. However, these schemes do not prevent shadow images from being tampered with or corrupted during transmission, potentially compromising the accurate restoration of the secret image. To address this issue, some SIS schemes incorporate image steganography to hide shadow images within cover images imperceptibly. Although this approach enhances security, statistical feature-based steganalysis methods may expose the hidden shadow images, thereby compromising secret communication security. Other schemes leverage integrity verification technology to detect tampering in shadow images.

TABLE I
COMPARISONS BETWEEN THE RELATED SECRET SHARING SCHEMES AND THE PROPOSED SCHEME. (VG: VISUAL CRYPTOGRAPHY, RG: RANDOM GRID, HE: HOMOMORPHIC ENCRYPTION)

	[38]	[39]	[40]	[41]	The proposed method
Security model	N/A	N/A	N/A	Secure	Semi-honest
Pixel expansion	Yes	Minimum	No	No	No
Hiding method	VC	RG	RG	VC	HE
Code book needed	Yes	Yes	No	No	No
Trusted third-part needed	Yes	Yes	No	Yes	Yes
Tamper resistance	No	No	No	No	Yes
Recovery type	Visible	Recognizable	Recognizable	Recognizable	Lossless

B. Blockchain Technologies

In contemporary literature, blockchain technology is widely acknowledged as a decentralized and distributed ledger system, where new information is appended to a block and made accessible to all users or nodes within a distributed network. Miners, responsible for generating new blocks via the Proof of Work (PoW) mechanism, play a pivotal role in maintaining the blockchain network's integrity. This mechanism not only enhances the cost of potential malicious attacks but also bolsters the overall security of the blockchain system. Recent research endeavors have increasingly focused on integrating blockchain technology into Internet of Things (IoT) systems to enhance their security and efficiency. For instance, scholars have proposed novel cooperative Mobile Edge Computing (MEC) blockchain computation offloading schemes and non-trustworthy MEC verification schemes to better allocate computing resources and optimize delay-limited computation offloading tasks. These approaches showcase the potential benefits of blockchain techniques in wireless network environments, inspiring the development of innovative solutions such as our proposed blockchain-based secure and efficient secret image sharing scheme. Compared to traditional secret sharing schemes lacking blockchain integration, our scheme boasts unique advantages, including anti-tampering capabilities for data validity verification, transparency allowing network nodes to access information, and multi-party security cooperation without reliance on third-party organizations. To facilitate the storage and retrieval of encrypted shadow image files, which often entail large sizes, within the BC-SESIS scheme, we leverage the InterPlanetary File System (IPFS), a peer-to-peer distributed file system. By storing the image files in IPFS and referencing their hash strings (file addresses) on the blockchain, we mitigate storage burdens and reduce latency. Furthermore, the integration of smart contracts, widely utilized in blockchain technology, enhances the BC-SESIS scheme's functionality. These contracts, executed on the blockchain's Ethereum Virtual Machine (EVM), automate predefined processes, reduce transaction costs, and mitigate abnormal or malicious actions. Specifically, within the BC-SESIS scheme, an AutoIDAuth-enabled smart contract is designed to achieve the (k, n) threshold of Secret Image Sharing, ensuring secure and efficient image restoration processes.

VI. THE PROPOSED BC-SESIS SCHEME

A. The Framework of Proposed BC-SESIS Scheme

1) *Security Model:* In our approach, we adopt the semi-honest model, where participants with fewer than k shares may collude with external users to tamper with or corrupt image shares. We assume that attackers cannot compromise the security of the blockchain network, meaning they lack the capability to dominate the network's computing power and resources. The BFV homomorphic encryption algorithm is introduced to ensure secure outsourcing of secret image restoration, known for its efficiency, feasibility, and strong security properties.
2) *Roles:* Key roles in our scheme include the Dealer, responsible for generating and distributing shadow images and encryption keys to participants; Participants, who receive a shadow image and encryption key, encrypt it, and upload it to the blockchain; the Applicant, a participant intending to restore the secret image; and Agent Miners, network nodes responsible for computing polynomials in the encryption domain for image restoration.

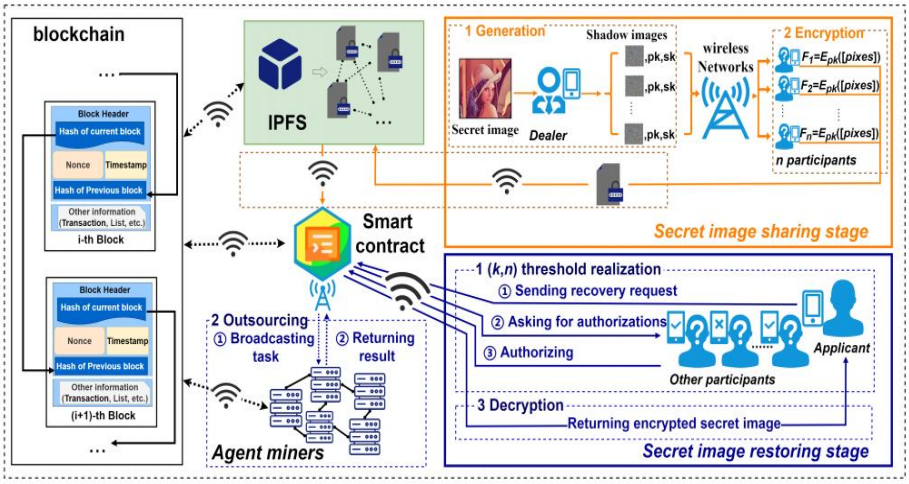


Fig. 1. The framework of proposed BC-SESIS scheme

3) *Trust Setup Phase:* The trust setup phase involves the Dealer securely distributing n secret shares to participants, ensuring that any k or more participants can recover the original secret, while groups with less than k shares cannot.
4) *Framework:* Our framework encompasses the secret image sharing and restoring stages. In the sharing stage, the Dealer generates and distributes shadow images and encryption keys to participants securely. Participants encrypt their shadows using the FHE algorithm, store encrypted shadows in IPFS, and upload their addresses to the blockchain.
5) *Secret Image Restoring Stage:* The process begins with the Applicant initiating a request for image restoration, providing their identity information to the AutoIDAuth-enabled smart contract. Upon receiving the request, the smart contract validates the Applicant's identity and solicits authorizations from Participants to access their shadow images. Upon collecting k authorizations, the smart contract outsources a portion of the secret image restoration task - specifically, computing polynomials in the encryption domain - to the blockchain. Agent Miners then carry out the computation and relay the polynomial coefficients back to the smart contract. After verifying the coefficients, the smart contract forwards them to the Applicant, who then utilizes them to compute the secret image.

This comprehensive process ensures secure and efficient secret image restoration within the proposed BC-SESIS scheme, utilizing blockchain technology and smart contracts to facilitate the restoration process while maintaining security and integrity.

B. *Secret Image Sharing Stage*

1) *Step 1:* Shadow Image Generation: In this step, shadow images are generated from the given secret image SI using a (k−1)-degree polynomial, similar to existing polynomial-based Secret Image Sharing (SIS) schemes. The polynomial is defined based on positive integers k and n, with coefficients (a1, a2, ..., ak−1) and a prime number p. The Dealer inputs a set of n random numbers (x1, x2, ..., xn) into the polynomial to compute corresponding shadow pixels $\{f(xi)|1 \le i \le n\}$. This process is repeated until all pixels of the secret image have been traversed, resulting in n shadow images. To maintain fidelity, we set the prime number p as 257, ensuring all pixels of generated shadows are within the range of [0, 255].
2) *Step 2:* Shadow Image Encryption: To enable secure outsourcing computation of secret image restoration, the shadow images are encrypted using Fully Homomorphic Encryption (FHE) before uploading to the blockchain. The Brakerski-Fan-Vercauteren (BFV) algorithm is chosen for its efficiency and feasibility. A batch encryption strategy is employed to encrypt a set of vectors representing pixels in the shadow image. By encrypting multiple pixels in one encryption operation, efficiency in encryption and decryption processes is enhanced, saving considerable computing time.
3) *Step 3:* Shadow Image Uploading: Due to storage constraints and latency concerns, directly storing large encrypted files on the blockchain is impractical. Instead, Participants upload encrypted files to the InterPlanetary File System (IPFS), which returns a unique hash string as the file's address. This address is then sent to the blockchain, ensuring efficient storage and retrieval of shadow images without overburdening the blockchain network.

C. *Secret Image Restoring Stage*

1) *Step 1:* (k, n) Threshold Realization: In this step, the AutoIDAuth-enabled smart contract is designed to authenticate the identities of Participants and ensure the (k, n) threshold of SIS. When an Applicant seeks to restore a secret image, they submit a restoration request along with their identity and gas reward to the smart contract via the HTTP SSL protocol. The smart contract then authenticates the Applicant's identity and broadcasts the restoration request to all Participants, requesting their authorizations to access the encrypted shadow image files. Participants who agree to authorize send their identity information to the smart contract for authentication. If the number of authorizations exceeds k, indicating there are enough Participants for restoration, the smart contract proceeds to trigger the encrypted domain polynomial computation. Otherwise, the Applicant is informed that restoration cannot proceed due to insufficient authorizations.

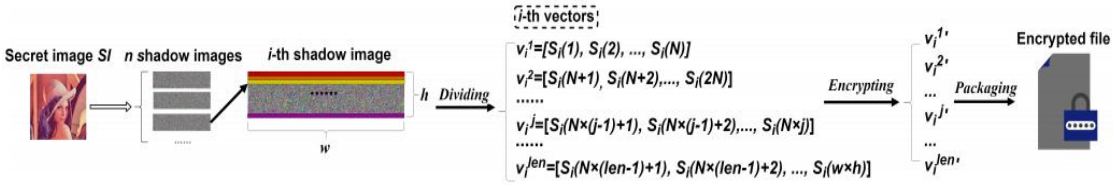


Fig. 2. The process of batch encryption.

2) *Step 2:* Encrypted Domain Polynomial Computation: Once the smart contract collects authorizations from at least k Participants, it initiates the encrypted domain polynomial computation. Due to the significant computing burden and latency involved, the task is outsourced to Agent Miners on the blockchain using the FHE-based outsourcing computing method. The BFV algorithm is chosen for its efficiency and feasibility. The process begins with the smart contract broadcasting the computation task to Agent Miners. After collecting the necessary encrypted shadow image files from IPFS, the smart contract distributes them to a subset of Agent Miners for computation. Each Agent Miner independently computes the polynomials in the encrypted domain and sends the coefficients to the smart contract. Upon receiving the coefficients, the smart contract compares them to ensure consistency. If all computed results match, the smart contract accepts the coefficients, pays the gas reward to the Agent Miners, and proceeds with the restoration process. Otherwise, the computation task is repeated to ensure accuracy and security.

3) *Step 3:* Secret Image Decryption: Following the completion of the outsourcing computation, the smart contract obtains the coefficients of the computed polynomials. Subsequently, these coefficients are transmitted to the Applicant. Upon receiving the computed polynomials, the Applicant decrypts the coefficients and transforms them into vectors. These vectors are then processed to obtain pixel values, which undergo a modulus operation with respect to p to restore the original secret image, denoted as SI.

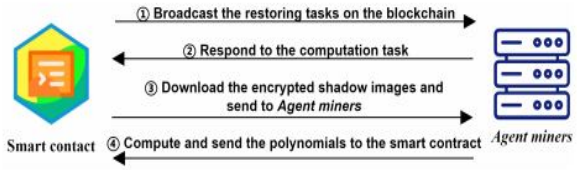


Fig. 3. The illustration of outsourcing process, in which the smart contract outsources the task of secret image computation to the *Agent miners*.

VII. EXPERIMENTAL RESULTS AND ANALYSIS

A. *Parameter Selection*

In the proposed BC-SESIS scheme, two key parameters, namely k and N, play crucial roles. Here, k represents the minimum number of shadow images required for restoring the original secret image, while N denotes the number of pixels divided into each batch during batch encryption for shadow images. In this section, we analyze the impact of these parameters on the scheme's performance in terms of restoring time consumption and accuracy. In the BFV algorithm [77], the encryption process introduces noise, which gets amplified during addition and multiplication, potentially affecting the accuracy of decryption results. When encrypting a single polynomial, encrypting more pixels can lead to increased noise and impact the accuracy of image restoration.

Consequently, if N exceeds a certain threshold, the accuracy of image restoration may be compromised. Additionally, the parameter k influences the depth of multiplication, thereby affecting both the time consumption and accuracy of the restoration process.

To strike a balance between restoration efficiency and accuracy, it's essential to evaluate the impact of these parameters on the BC-SESIS scheme's performance. Table III illustrates the effects of k and N on restoration time consumption and accuracy. The minimum \(N \) signifies the smallest value of \(N \) necessary to ensure 100% restoration of the secret image. From the table, it's observed that to maintain a 100% restoration accuracy, \(N \) is set to 16,384 when \(k = 2 \) or \(3 \), and 32,768 when \(k \geq 4 \). Furthermore, it's evident that the time consumption for computing a single polynomial remains below 2 seconds when \(N = 16,384 \), but increases significantly when \(N = 32,768 \).

B. Quality of Restored Secret Image

We present experimental results showcasing the restoration capability of secret images using the BC-SESIS scheme. Figure 4 illustrates an experimental outcome displaying both the original version and the restored version of a 256 × 256 image using the proposed scheme. For this experiment, a (4, 6)-threshold case of our scheme is employed. Figure 4(a) exhibits the original image with dimensions of 256 × 256. Figures 4(b) to 4(g) depict the six generated shadow images, which appear as noisy images and are 1/4 the size of the original secret image. Finally, Figure 4(h) displays the restored secret image, reconstructed from any four of the generated shadow images.

To assess the quality of the restored secret image by the BC-SESIS scheme, various statistical metrics including Root Mean Square Error (RMSE) and Peak Signal to Noise Ratio (PSNR) are employed.

C. Validity of Batch Encryption Strategy on Efficiency

To enhance the efficiency of generating shadow images, we introduced and adopted the batch encryption strategy in Section III-B. The process of secret image restoration involves multiple operations of computing polynomials using Lagrange's interpolation algorithm. In traditional schemes, each coefficient of the polynomial hides one pixel, and each polynomial computation can restore k pixels. In our proposed BC-SESIS scheme, the batch encryption strategy significantly improves the efficiency of secret image restoration. This strategy allows for hiding N pixels into each coefficient, enabling each polynomial computation to restore N × k pixels simultaneously.

In this section, we conduct experiments to compare the time consumption and the number of restored pixels per polynomial computation using both traditional and batch encryption strategies. Additionally, we compare the efficiency of the two strategies by observing the time consumption of restoring an image with dimensions of 512 × 512.

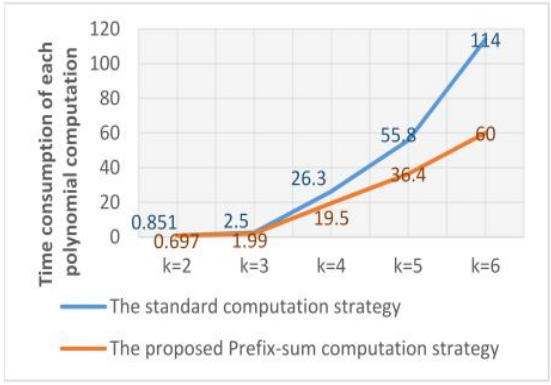


Fig. 5. Efficiency comparison between the standard computation strategy and the proposed *Prefix-Sum* computation strategy.

The efficiency of restoration using the batch encryption strategy far surpasses that of the traditional method, where pixels are encrypted one by one. To maintain a restoration accuracy of 100%, different values of N are selected for different values of k. For instance, when k = 6, the time consumed per pixel for restoration using the batch encryption scheme is nearly 800 times faster than that of the traditional encryption strategy. Since each polynomial computation can restore N × k pixels, the time required to restore

the entire image using the batch encryption strategy is significantly less compared to the traditional strategy. It is evident that the batch encryption strategy can substantially improve the efficiency of our scheme, particularly when k is a large value.

VIII. CONCLUSION

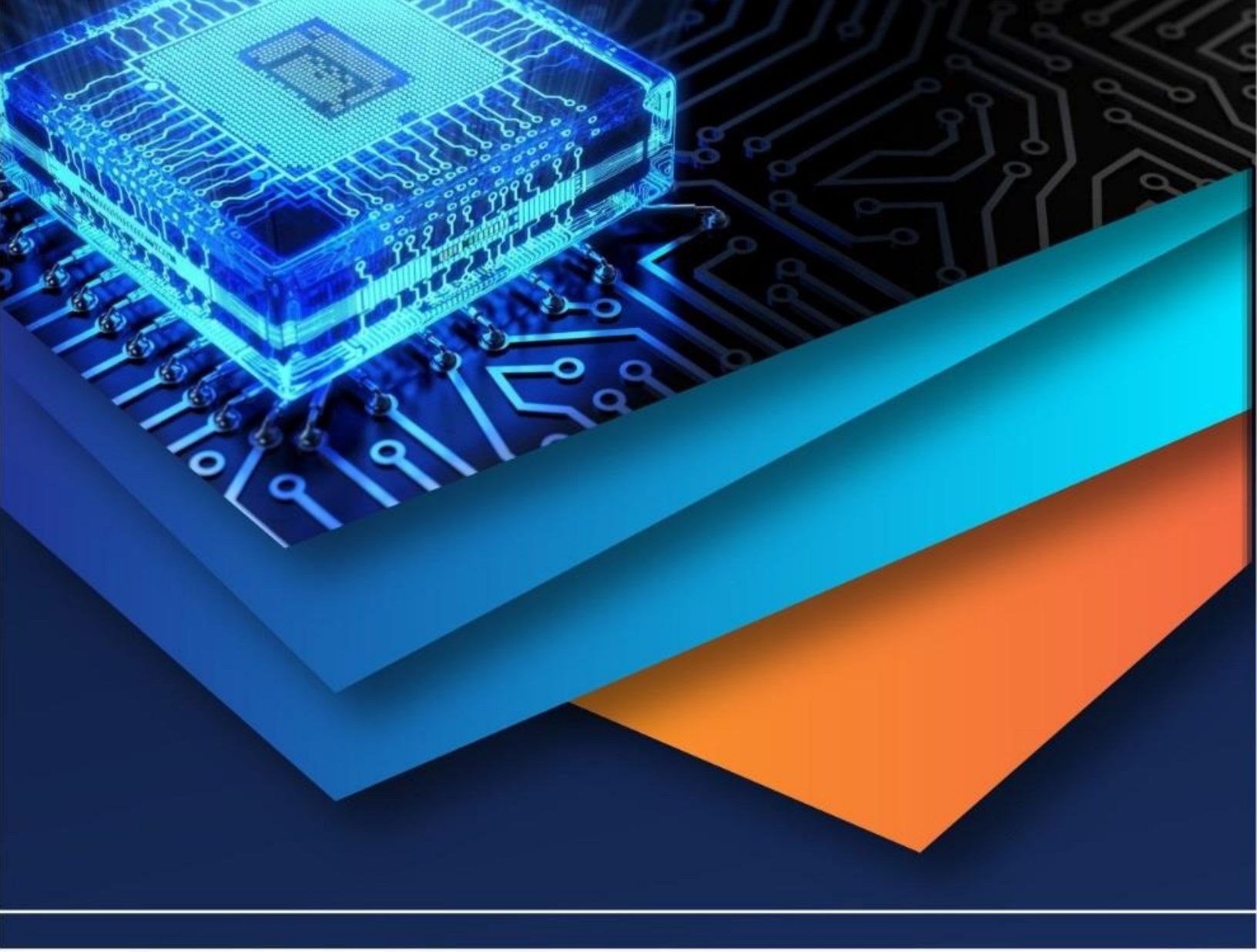
In this paper, we introduce the BC-SESIS scheme, a novel approach designed to securely communicate and safeguard secret image data within wireless networks. Our scheme employs blockchain technology to encrypt and store generated shadows, thus preventing tampering and corruption. Additionally, we deploy an identity authentication-enabled smart contract on the blockchain to facilitate the (k, n) threshold of Secret Image Sharing (SIS) for image restoration. Furthermore, we propose an outsourcing computation method based on Fully Homomorphic Encryption (FHE) to alleviate the computational burden on smart contracts and users during image restoration. Theoretical analyses and extensive experiments confirm the effectiveness of the BC-SESIS scheme in achieving robust security and high computational efficiency.

The BC-SESIS scheme demonstrates effective management and protection of images distributed across networks, offering significant practical value in various applications. Looking ahead, we aim to further reduce the computational load on smart contracts and users while enhancing the outsourcing computation method. Our future efforts will focus on completely outsourcing all verification and computation operations related to SIS tasks in wireless networks, thereby advancing the scheme's capabilities in real-world scenarios.

REFERENCES

[1] F. Zhan, N. Yao, Z. Gao, and H. Yu, “Efficient key generation leveragingwireless channel reciprocity for manets,” Journal of Network andComputer Applications, vol. 103, pp. 18–28, 2018.
[2] T. Wang, Y. Liu, and A. V. Vasilakos, “Survey on channel reciprocitybased key establishment techniques for wireless systems,” Wireless Networks, vol. 21, no. 6, pp. 1835–1846, 2015.
[3] T. Karygiannis and L. Owens, Wireless Network Security:. US De┐ partment of Commerce, Technology Administration, National Institute of . . . , 2002.
[4] C.-C. Thien and J.-C. Lin, “Secret image sharing,” Computers & Graphics, vol. 26, no. 5, pp. 765–770, 2002.
[5] “An image-sharing method with user-friendly shadow images,” IEEE Transactions on circuits and systems for video technology, vol. 13, no. 12, pp. 1161–1169, 2003.
[6] C.-C. Lin and W.-H. Tsai, “Secret image sharing with steganography and authentication,” Journal of Systems and software, vol. 73, no. 3, pp. 405–414, 2004.
[7] C.-N. Yang, T.-S. Chen, K. H. Yu, and C.-C. Wang, “Improvements of image sharing with steganography and authentication,” Journal of Systems and software, vol. 80, no. 7, pp. 1070–1076, 2007.
[8] A. Beimel, “Secret-sharing schemes: A survey,” in International confer┐ ence on coding and cryptology. 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 Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 17, no. 1, pp. 1–22, 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. 23 284–23 300, 2021.
[11] M. K. Sardar and A. Adhikari, “A new lossless secret image sharing scheme for grayscale images with small shadow size,” in Proceedings of International Conference on Frontiers in Computing and Systems. Springer, 2021, pp. 701–709.
[12] S. Charoghchi and S. Mashhadi, “Three (t, n)-secret image sharing schemes based on homogeneous linear recursion,” Information Sciences, vol. 552, pp. 220–243, 2021.
[13] X. 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,” Journal of Information Security and Applications, vol. 51, p. 102452, 2020.
[14] P.-Y. Lin and C.-S. Chan, “Invertible secret image sharing with steganog┐ raphy,” Pattern Recognition Letters, vol. 31, no. 13, pp. 1887–1893, 2010.
[15] X. Wu, D. Ou, Q. Liang, and W. Sun, “A user-friendly secret image shar┐ ing scheme with reversible steganography based on cellular automata,” Journal of Systems and Software, vol. 85, no. 8, pp. 1852–1863, 2012.
[16] G. Prema and S. Natarajan, “Steganography using genetic algorithm along with visual cryptography for wireless network application,” in 2013 International Conference on Information Communication and Embedded Systems (ICICES). IEEE, 2013, pp. 727–730.
[17] N. F. Johnson and S. Jajodia, “Steganalysis: The investigation of hidden information,” in 1998 IEEE Information Technology Conference, Information Environment for the Future (Cat. No. 98EX228). IEEE, 1998, pp. 113–116.
[18] J. Fridrich and M. Goljan, “Practical steganalysis of digital images: state of the art,” security and Watermarking of Multimedia Contents IV, vol. 4675, pp. 1–13, 2002.
[19] J. Fridrich and J. Kodovsky, “Rich models for steganalysis of digital images,” IEEE Transactions on information Forensics and Security, vol. 7, no. 3, pp. 868–882, 2012.
[20] M. Poongodi, A. Sharma, V. Vijayakumar, V. Bhardwaj, A. P. Sharma, R. Iqbal, and R. Kumar, “Prediction of the price of ethereum blockchain cryptocurrency in an industrial finance system,” Computers & Electrical Engineering, vol. 81, p. 106527, 2020.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)