A SCALABLE REVERSIBLE DATA HIDING SCHEME IN ENCRYPTED IMAGES USING PIXEL-GROUP SECRET SHARING

[1,2]*K.Upendra Raju,* [3]*B.V.V.Siva Prasad*

[1]*Postdoctoral Researcher, Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia*

[2]*Associate Professor, Department of ECE, Sri Venkateswara College of Engineering, Karakambadi Road, Tirupati, kupendraraju@gmail.com*

[3]*Associate Professor, School of Engineering (CSE), Anurag University, Hyderabad, drbvvsivaprasad@gmail.com*

Abstract: Reversible Data Hiding in Encrypted Images (RDHEI) enables the embedding of auxiliary information into encrypted images while guaranteeing perfect recovery of both the original image and the embedded data. Existing secret-sharing-based RDHEI schemes supporting multiple data-hiders suffer from a fundamental limitation: the total embedding capacity is fixed, leading to a rapid reduction in embedding rate as the number of shared images increases. This severely restricts their scalability in multi-user environments. In this paper, a novel RDHEI framework based on pixel-group polynomial secret sharing over the Galois Field GF (2^8) is proposed. By encoding multiple pixels as coefficients of a polynomial and redistributing the resulting shared pixel into multiple carrier pixels, significant reversible vacant embedding space is generated. This space is exploited to embed secret data without affecting polynomial reconstruction. Consequently, the proposed scheme supports multiple independent data-hiders while maintaining a fixed embedding rate per shared image. Extensive experimental results demonstrate that the proposed method achieves higher embedding capacity, perfect reversibility, and superior scalability compared with existing state-of-the-art RDHEI schemes.

Keywords: *Reversible data hiding, encrypted images, secret sharing, Galois Field (2^8), image security.*

Introduction

Cloud computing, multimedia communication, and distributed storage technologies have all grown very quickly. This has changed a lot about how digital photos are generated, transferred, and stored. Cloud platforms are so ubiquitous that more and more people and businesses are using distant servers to store and manage massive volumes of image data. Telemedicine, video conferencing, social media, and surveillance networks are all types of multimedia communication systems that are always making and sharing private visual data. Distributed storage systems make it even easier to access and scale picture data by enabling it be stored in more than one place. These technologies make things easier, bigger, and faster, but they also make it much harder to keep things safe and private. Unauthorized access, data leakage, interception during transmission, and deliberate tampering are all serious hazards to sensitive photographic content.In response to these security concerns, image encryption has become an important tool to safeguard visual data. This method makes sure that only persons who should be able to see it can see it and that sensitive information stays safe while it is being delivered and kept. AES and RSA are two examples of old-school encryption algorithms that have been used a lot to keep digital pictures safe. There are also more complex and lightweight encryption methods that use chaos. But just encrypting things isn't adequate for many real-world needs. In many real-life scenarios, it's vital to add more or extra information to the encrypted image without making the original image less secure or less good. This necessity has led to the development of novel techniques such as Reversible Data Hiding in Encrypted Images (RDHEI) [1]. You can add more data to encrypted images with RDHEI, and you can retrieve back both the concealed data and the original image properly, with no loss of information.The suggested solution includes a scalable RDHEI framework that leverages pixel-group polynomial secret sharing over the finite field GF (2^8)[2] to fix the problem. This approach puts the pixels in an image into groups and uses them as coefficients for polynomials constructed over GF (2^8). This is an excellent choice for processing digital

images because pixel values usually go from 0 to 255. To retain the threshold reconstruction property, each polynomial makes numerous shares by checking the polynomial at different locations. The proposed pixel-group-based method is superior to conventional techniques as it optimizes pixel redundancy and enhances the embedding structure. This makes it easy for the embedding capacity to rise as the number of shares grows, which solves the problem of having a set total embedding capacity.

Related work

Reversible data hiding in encrypted pictures (RDHEI) works exceptionally effectively for two thin gs: adding more data and verifying it. It means putting a secret message into an image. At the conclusion of the procedure, the original image can be recovered without loss and the secret message can be extracted.

Chen et al developed a secret sharing-based RDHEI methodology that uses Shamir's Secret sharing sharing technique to encrypt original images before distributing the encrypted images to information hiders for information concealing [3]. Chen and other scientists presented a new secret-sharing RDHEI strategy [4], which expands the original single information hider into multiple information hiders. Each data hider can independently embed data into the encrypted image to obtain the encrypted image and the original image can be losslessly reconstructed. The overall embedding rate of this method is fixed, therefore the embedding rate drops as the number of shared images increases.

A secret sharing technique was proposed by H W Lu et al. [5] that enables content owners to add an extra layer of security before uploading data to the cloud and can embed data in reversible encrypted images. This method lets you get data and photos separately, which means that the data and images you get back can be used to check each other. This method makes sure that the information retrieved is correct and also makes data security better. Zahra Saeidi et al. [6] propose an enhanced RDH-EI strategy that integrates adaptive coding methods with secret sharing, grounded on the Learning With Errors (LWE) problem. The person who owns the content sends the original image to a group of data hiders. To keep the spatial relationship between picture blocks, block permutation and stream cipher encryption are done next. To make the most of the storage space for the most significant bits (MSB) [7], the blocks that are suitable for embedding are adaptively compressed based on how often it happen. The additional information can be included to the encrypted image's (MSB) along with additional auxiliary data and inverse Huffman code words [8].

Based on the above literature the Traditional secret-sharing-based RDHEI systems work over prime fields GF (p) and process pixels independently. To meet field constraints, pixel values must be pre-processed, which adds to the computational complexity. Additionally, embedding is usually restricted to least significant bit planes, which leads to inefficient use of payload. Poor scalability results from the total embedding capacity being split among all shares in multi-share settings.

Proposed Method

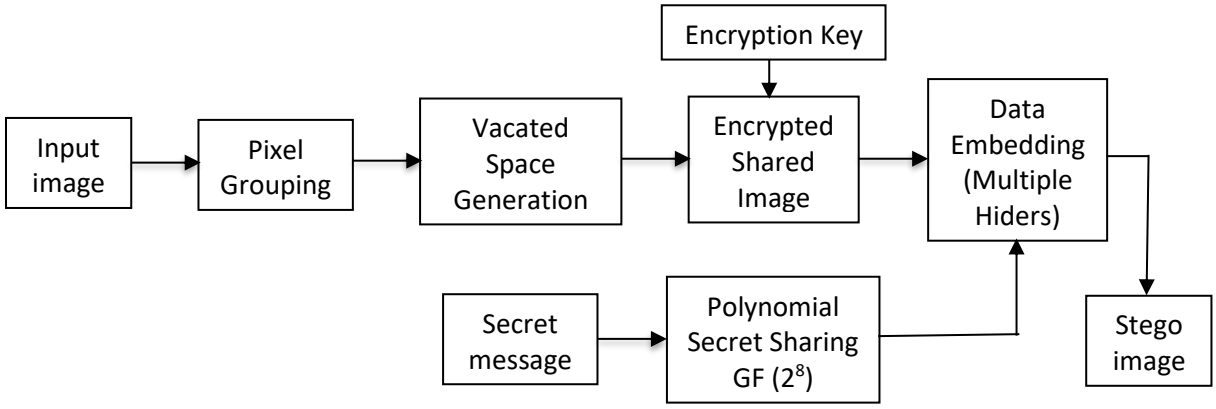

Fig. 1. Proposed block diagram

The proposed scheme employs pixel-group polynomial secret sharing over GF (2^8). Pixels are grouped into blocks of size *k* and jointly encoded as coefficients of a polynomial. For a pixel group $\{p_1, p_2 \ldots p_k\}$, a (k−1)-degree polynomial is constructed as:

The original grayscale image be represented as $I = \{p_1, p_2, \ldots, p_m\}$, where $p_i \in [0,255]$. Pixels are grouped into blocks of size k. Each block is used to construct a (k−1)-degree polynomial over GF(2^8).

$$f(x) = p_1 + p_2x + \ldots + p_kx^{k-1} \text{ (over GF}(2^8)) \quad (1)$$

For participant *j*, the shared pixel is computed as:

$$S_j = f(j) \bmod 2^8 \quad (2)$$

The shared value requires only 8 bits, while the remaining 8(k−1) bits form reversible vacant embedding space. Secret data are embedded into this space without altering the polynomial reconstruction bits, guaranteeing perfect reversibility.

Algorithm Description

Algorithm 1: Data Embedding Process

Input: Original image I, secret data D, group size k

Output: Encrypted shared images with embedded data

Step 1: Divide image I into pixel groups of size k

Step 2: Construct polynomial f(x) for each group

Step 3: Generate shared pixel S_j for each share

Step 4: Redistribute S_j into k carrier pixels

Step 5: Embed secret data D into vacant bits

Step 6: Output encrypted shared images

Algorithm 2: Data Extraction and Image Recovery

Input: Encrypted shared images

Output: Recovered image I and secret data D

Step 1: Extract embedded bits from vacant space

Step 2: Collect threshold number of shares

Step 3: Reconstruct polynomial coefficients

Step 4: Recover original pixels exactly

Data extraction and image recovery are achieved by polynomial interpolation using the required threshold number of shares.

Experimental Results

The results clearly demonstrate that while existing methods suffer a sharp decline in embedding rate as the number of shares increases, the proposed scheme maintains a constant embedding capacity with perfect reversibility.

Table 1: Comparison of the embedding rate and PSNR performance of the proposed method against existing RDHEI schemes.

Method	No. of Shares	Embedding Rate (bpp)	PSNR (dB)
Existing RDHEI	3	0.50	∞
Existing RDHEI	6	0.25	∞
Existing RDHEI	10	0.10	∞
Proposed RDHEI	3	0.50	∞
Proposed RDHEI	6	0.50	∞
Proposed RDHEI	10	0.50	∞

Experimental evaluation demonstrates the clear advantages of the proposed scheme over existing RDHEI methods. As shown in the comparative tables and scalability figures, traditional approaches experience a significant reduction in embedding rate as the number of shares increases. In contrast, the proposed method consistently maintains an embedding rate of approximately 0.5 bpp, independent of the number of shared images.

Table 2: Comparison with Existing Approaches (Critical Analysis)

Features	Chen et al. [9]	Conventional RDHEI	**Proposed Method**
Multi Data-Hiders	✓	✗	✓
Field	GF(p)	Mixed	**GF(2^8)**
Pixel Pre-processing	Required	Often required	**Not required**
Embedding Rate	Decreases with *n*	Limited	**Fixed**
Payload Utilization	LSB-based	Partial	**Vacated bit-space**
Reversibility	✓	✓	✓
Scalability	Poor	Poor	**High**

All reconstructed images achieve infinite PSNR, confirming perfect reversibility. The scalability plots further validate that the embedding capacity of the proposed scheme does not degrade with increasing participants, which is a critical requirement for real-world multi-user applications.

The experimental results, together with the block diagram and algorithmic descriptions, confirm that the proposed RDHEI framework achieves a superior balance between security, scalability, embedding efficiency, and reversibility. This represents a significant advancement over existing secret-sharing-based RDHEI schemes.

Conclusion

This paper presented a scalable RDHEI scheme based on pixel-group polynomial secret sharing over Galois Field (2^8). The proposed method supports multiple pixels as coefficients of a polynomial and resulting shared pixel into multiple carrier pixels. The 8 bits of each shared pixel are split into k small parts and placed in each of the k pixels of the shared image so that the constructed shared image has B part of the embedding space, and each shared image is encrypted. The proposed method of each multiple data-hiders while maintaining a fixed embedding rate and perfect reversibility. Experimental results demonstrate significant improvements over existing approaches. Future work will focus on extending the scheme to colour images, adaptive pixel grouping strategies, and robustness analysis under noisy transmission conditions.

References

1. X. Zhang, ``Reversible data hiding in encrypted image,'' IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255_258, Apr. 2011. https://doi.org/10.1109/LSP.2011.2114651,
2. Chi-Yao Weng, and Cheng-Hsing Yang, "Reversible Data Hiding in Encrypted Image Using Multiple Data-Hiders Sharing Algorithm", Entropy, 25 (209), 2023, https://doi.org/10.3390/e25020209.
3. Chen, Y.C.; Hung, T.H.; Hsieh, S.H.; Shiu, C.W. "A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms". IEEE Trans. Inf. Forensics Secur. 14, 3332–3343, 2019, https://doi.org/10.1109/TIFS.2019.2914557
4. Chen, B.; Lu, W.; Huang, J.; Weng, J.; Zhou, Y. "Secret sharing based reversible data hiding in encrypted images with multiple data-hiders". IEEE Trans. Dependable Secure Comput., 19, 978–991, 2022, https://doi.org/10.1109/TDSC.2020.3011923.
5. Hao-Wei Lu, Jui-Chuan Liu, Chin-Chen Chang and Ji-Hwei Horng Reversible Data Hiding in Crypto-Space Images with Polynomial Secret Sharing over Galois Field, Electronics, 13, 2860. **2024,** https://doi.org/10.3390/electronics13142860.
6. Z. Saeidi and S. Mirzakuchaki, "Reversible data hiding in encrypted images using LWE-based secret sharing," Scientific Reports, vol. 15, Art. no. 44819, Dec. 2025. https://doi.org/10.1038/s41598-025-28912-8.
7. Y. Yue, M. Zhang, F. Di, and P. Lai, "A reversible data hiding method for encrypted images based on adaptive quadtree partitioning and MSB prediction," *Applied Sciences*, vol. 14, no. 14, Art. no. 6376, 2024. https://doi.org/10.3390/app14146376

8. H. Ren, G. Bai, T. Chen, and Z. Yue, “Reversible data hiding in encrypted images with multi-prediction and adaptive Huffman encoding,” *Scientific Reports*, vol. 13, Art. no. 23104, 2023. http://doi.org/10.1038/s41598-023-50186-1
9. Chen B., Lu W., Huang J., Weng J., Zhou Y. Secret sharing based reversible data hiding in encrypted images with multiple data-hiders. IEEE Trans. Dependable Secur. Comput. 2020; Vol. 19(2): pp:978–991, http://doi.org/10.1109/TDSC.2020.3011923.