OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

Reversible Data Hiding in Encrypted Images: A Progressive Recovery Framework for Confidentiality and Integrity

Rashmi J C[1], Dr. S. Srividhya[2]

PG Scholar, B N M Institute of Technology , Bangalore, affiliated to VTU, Belagavi, Karnataka, India1 8970440548[1]
Professor & Head , Department of Information Science & Engineering, B N M Institute of Technology, Bangalore, Karnataka, India[2], rashmigowda2610@gmail.com[1] ,ssrividhya@bnmit.in[2]

Abstract: ***The rapid expansion of cloud-based platforms to store and transmit sensitive data has raised an imperative to develop reliable and fully reversible strategies that maintain data privacy protection of images and allow embedding additional data. Traditional reversible approaches to data hiding (RDH) are not effective with encrypted images, where encryption breaks spatial redundancy and capacity. To ensure this, we would suggest a stepwise restoration-based RDH scheme of encrypted images (RDH-EI). The system operates on two-key management strategy meaning the encryption and data-hiding keys are non-dependent, thus each can be performed independently to extract data and decoding of the image. The data is coded on a series of least significant bit (LSB) layers with improved capacity and low distortion. The experimental findings indicate that safe, loss-free restoration of both secreted information and original photographs is achievable, and as a consequence, the method is highly suitable in cloud storage, medical imaging, rights administration, and safe communications.***

Keywords—Reversible Data Hiding (RDH), Encrypted Images, stepwise restoration

---

I. INTRODUCTION

As cloud computing and online communication rapidly expand, the secure communication and storage of sensitive information has turned into one of the most significant research problems. The cloud-based systems are also being increasingly invoked to work with various types of data, multimedia data, i.e. images, videos and medical records. Although encryption methods offer a high level of protection against unauthorized access, they also limit usability especially when we want to add some other information like authentication codes, water marks or metadata without jeopardizing the privacy protection or quality of the original data. It has prompted increased attention to Reversible Data Hiding (RDH) methods, where concealed data are added to a digital media without leaving any trace of the hidden information or altering the original host information [1,2].

Unlike the conventional watermarking or inadvertent data hiding, Reversible Data Hiding (RDH) maintains the integrity of the cover image which is essential in the areas where accuracy is paramount. Misdiagnosis of even small distortions can happen in medical imaging, whereas security and legal evidence require data authenticity in the military and forensic context. Similarly, digital rights management and secure communication industries also need loss-free restoration. Therefore, there is a balance between privacy protection, data-carrying capacity and reversibility in RDH. Even though there is an advancement in RDH with plain images, there are issues with encrypted images. Traditional RDH utilises both space redundancy and statistical characteristics of unencrypted information to obtain high capacity. Traditional methods are ineffective because encryption alters the pixel value in an unpredictable manner and these redundancies are broken. The restriction prompts use of Reversible Data Hiding in Encrypted Images (RDH-EI) that ensures safety by encryption but allows reversible hiding of auxiliary information [1].

The current RDH-EI schemes are limited by the fact that the recovery process is strict and there is a tradeoff between data-carrying capacity and image quality, as well as recovery accuracy. Block smoothness methods or histogram shifting methods tend to add distortion at large payloads or to fail in texted areas. Others squeeze least significant bits (LSBs) to make space and tolerate poor capacity or cannot separate data extraction and decoding of the image. Most of

them also use the single-step recovery, which makes them less flexible and introduces more reconstruction errors. To address those problems, the given research examines the stepwise restoration in RDH-EI that involves the reconstruction of the encrypted picture and the hidden information in several phases rather than in a single. This approach minimizes distortion by altering the specific LSB layers, enhances the data-carrying capacity by spreading the data within recovery cycles and allows independent decoding of the image and data recovery by managing the two keys [2]. The mentioned benefits of the approach enable its application in sensitive areas like healthcare, secure cloud storage, copyright protection, and digital forensics.

Given this context, the research is guided by the following research question:

How can reversible data hiding techniques be effectively applied to encrypted images using stepwise restoration to ensure secure data embedding, accurate recovery of hidden information, and faithful reconstruction of the original image with minimal distortion in cloud-based environments?

To achieve this goal, the following objectives were formulated:

1. To design and implement a reversible data hiding (RDH) scheme that embeds confidential data into encrypted images while ensuring both the hidden message and the original image can be recovered without loss.
2. To integrate stepwise restoration mechanisms that allow step-by-step reconstruction of encrypted images and concealed payload, thereby improving accuracy and reducing distortion compared to traditional RDH methods.
3. To enhance security through two-key management strategy (separate encryption and data-hiding keys), enabling independent operations of decoding of the image and concealed payload extraction.
4. To evaluate system performance in terms of data-carrying capacity, image quality, distortion level, and recovery accuracy, ensuring the method is efficient, scalable, and suitable for applications in cloud computing, healthcare, military, and copyright protection.

The suggested work fills the gap between encryption-based privacy protection and reversible data hiding in clouds. It is an effective way to secure communication though the use of a stepwise restoration framework with guaranteed high image quality, improved data-carrying capacity, and adjustable recovery.

II.LITERATURE SURVEY

The Reversible Data Hiding (RDH) and its variant (Reversible Data Hiding in Encrypted Images) RDH-eI, have received considerable interest due to their capability to hide confidential payload without preventing the restoration of the original image. Different approaches have been designed over the last ten years, starting with spatial-domain LSB substitution and histogram shifting, and moving to more advanced cryptography-hybrid techniques. In this section, the works that have been considered include their contributions, strengths, and limitations as far as secure embedding, image quality preservation and error free recovery are concerned.

The initial development of at least stepwise restoration RDH was presented by [1], who suggested a three-party model of the content holder, data hider and receiver. This method was based on a multi-stage progressive process and utilised three cycles rather than the traditional methods that used only one recovery parameter. The scheme minimised modifications to three least significant bit (LSB) layers, thus maintaining image quality and also enhancing the rate of embedding. stepwise restoration design also allowed heavier payloads, and provided a scalable and efficient solution over previous one-step schemes. Notably, this paper has shown that it is possible to resolve the inflexible trade-off of distortion versus capacity with progressive strategies though wider applications in non-controlled settings were not explored extensively.

Some of the researchers examined steganography-hybrid models. [2] suggested an improved LSB replacement technique along with cryptographic and permutation layers. It was innovative in that it used a Multi-Level Encryption Algorithm (MLEA) to do XOR on a secret key before embedding, to provide the security of pre-encryption. Besides, the scheme facilitated multi-channel embedding through breaking down of the blue channel into four sub-blocks in which messages could be distributed. The analysis of the performance of the algorithm revealed high PSNR scores of more than 80 dB, which implies excellent imperceptibility and strength of error-free recovery. The addition of several transpositions and Magic Matrix-based shuffling stage complicated computations in comparison to simpler LSB models, but this again pits the timeless balancing act of layered security versus efficiency.

Based on the background research, [3] designed a better encrypted image reversible data concealing. Their system divided encrypted images into blocks and each block would have bits embedded by flipping 3 LSBs in specific pixels of the block, with block smoothness used to recover the bit. But the first technique did not consider the correlations among neighboring blocks, which diminished the reconstruction accuracy. This was resolved by Hong et al. who added refined smoothness measures and a one side match scheme that minimized the error rates. Error rates were also experimentally tested and were found to be as low as 0.34% versus 1.21% in the original method, and this is more reliable in data recovery. This contribution emphasized the significance of capitalizing on the inter-block correlations though the block-based nature still posed

a payload limit and source artifacts in images being textured.

Unlike the spatial-domain techniques, [4] focused on compressed domains by suggesting a reversible algorithm of encrypted JPEG bitstreams. They worked around the bits with the bitstream encrypted, with the information stored in minor adjustments of individual bits. To ensure that it is reversible, error-correcting codes were incorporated so that both the concealed payload and the original bitstream may be retrieved with reliability. Flexibility was also provided in the scheme by allowing the use of two keys, i.e., those that received a dual key had the ability to obtain both the data and the cover image, whereas those that received only the encryption key could still reconstruct the image but included no concealed payload. This design was compromised between usability and privacy protection but the use of error correcting codes would inevitably add cost to the computations.

Likewise, [5] came up with Multi-Level Steganography (MLS) algorithm which combined AES and Blowfish encryption to give secure message. Their approach, uniquely, entrenched the keys themselves as key images into the stego image, and created an independent multi-key management system. This method optimised tamper resistance, and it facilitated various embedded secrets. The scheme attained large values of PSNR and resilience but the fact that chained AES-Blowfish encryption and pixel randomization were used increased the computational load and hence was less efficient when used in real time compared to single-cypher solutions.

In order to maximise robustness, [6] proposed a hybrid scheme of AES and an 8-bit XOR algorithm changed dynamically. Encryption of messages using AES was used to provide strong cryptographic security and then embedded messages using dynamic XOR within colour elements of the host image. This two-way keying (AES key and dynamic XOR-pattern) provided two security channels. It was shown that experimental results were of excellent image quality, at moderate payloads, PSNR values were above 80 dB on average. Scalability was also a concern though, with a minimum payload size of 500B, and a maximum size of 2KB, which showed a considerable drop in quality (reduced PSNR, increased MSE), it was found to be difficult to scale to larger or larger numbers of messages at once.

In addition to single-message embedding, [7] also presented multi-secret embedding, which is an act of hiding real and fake messages in the same picture. Two methods were suggested: False LSB Steganography and False JPEG Steganography. This fake message was used as a decoy, confusing the opponents as the actual message was safely embedded with second lowest significant bits or with frequency domain F5 algorithm. Rijndael-256 encryption enhanced security by balancing out the bits. Despite its usefulness in the field of deceptive communication, its shortcomings were that it became vulnerable when it became apparent that there was some concealed payload, and this is a general weakness of steganography. However, the idea of multi-secret embedding and permutation based on keys as introduced by Sidqi can still be applied to multi-channel reversible hiding systems.

[8] has dealt with capacity enhancement by using a Multi-Pixel-Pair (MPP) strategy with Hybrid Near Maximum Histogram (HNMH) techniques. Rather than accepting a single peak in the histogram, pairs of pixels were utilised to hide data, leading to a huge increase in hiding capacity- by a factor of 37.48 over classical HNMH. Additional improvements were realised with 8x8 cover image partitioning which resulted in 7.05% better embedding and security improvement with variable partitioning. Nonetheless, scaling down to very small sizes (e.g. 64x 64 and beyond) was associated with quality loss signifying diminishing returns to very segmented images.

data-carrying capacity on encrypted domains was also enhanced by [9] who came up with Two Layer Embedding Scheme (2LES) of RDH-EI. The technique employed second LSB and LSB planes, which greatly increased payload. Multi-key separation was used to improve security: one key was used to rearrange the blocks, one key was used to encrypt the image, one key was used to encrypt the message and one key was to embed control. This provided decryption and extraction operations that were independent, enhancing compromise resilience. Relying on blockchain to verify integrity and expand prediction algorithms with complexities, however, added unwanted overhead to implementation in real-world applications.

data-carrying capacity on encrypted domains was also enhanced by [9] who came up with Two Layer Embedding Scheme (2LES) of RDH-EI. The technique employed second LSB and LSB planes, which greatly increased payload. Multi-key separation was used to improve security: one key was used to rearrange the blocks, one key was used to encrypt the image, one key was used to encrypt the message and one key was to embed control. This provided independent decryption and extraction, which enhanced resiliency to compromise. Relying on blockchain to verify integrity and expand prediction algorithms with complexities, however, added unwanted overhead to implementation in real-world applications.

[11] further improved AES-128 using chaotic maps to enhance the confusion and diffusion. The variable S-boxes, dynamic ShiftRows, and XOR diffusion were used in the dual-layer encryption. As QR codes, with LSB steganography, keys and covert hint messages could be managed in multi-key format and shared safely. The algorithm was very resilient and would recover error-free but with more computational overhead than the standard AES.

[12] suggested Magic LSB Substitution Method (M-LSB-SM) which involved encrypting the confidential payload with MLEA and breaking it into four blocks, which served as sub-images of I-plane in HSI colour space. Before embedding, sub-images were rotated using unique keys, to provide four channels of independent embedding. This encryption, block division and key rotation combination enhanced imperceptibility and security. But, as with other LSB-based spatial techniques, it was still susceptible to both statistical and transform-domain attacks.

In a nutshell, the current RDH and RDH-EI techniques have registered a gradual advance in spatial, compressed, cryptography, and hybrid techniques. Although they present varying degrees of embedded capacity, security, and recovery precision, scalability, computational efficiency and robustness of cloud-based applications are still problematic.

Although these progresses have been made, modern RDH-EI solutions have major limitations, including single-step recovery, data-carrying capacity versus image quality trade-offs, independent data or image operations and computationally expensive execution. The concept of stepwise restoration is under-researched, so there is a need to focus on the dual-key RDH-EI scheme that guarantees a secure embedding, correctly recovered and faithful image reconstruction at the lowest distortion level.

III.METHODOLOGY

In this section, the procedure of applying the reversible data hiding in encrypted images (RDH-EI) based on the stepwise restoration framework is described. The proposed scheme overcomes shortcomings of traditional RDH schemes, to provide high data-carrying capacity, low distortion and independent recovery of concealed payload and the original image. This methodology is comprised of five parts which are: (i) system model, (ii) the encryption process, (iii) the process of data embedding, (iv) the stepwise restoration mechanism and (v) the security and performance characteristics.

System Model

The general model in fig.1. has 3 main players, the content owner, the data hider and the receiver.

- Before the outsourcing of the picture, the rightful owner of the content encrypts the original message with a secure encryption algorithm to provide privacy protection before sending it to the cloud.
- The data hider puts in more information in the encrypted image including authentication codes or metadata without reading the actual content of the image.
- Depending on the keys that are available, the receiver removes the concealed payload and/or restores the original image.

The system uses two-key management strategy in order to ensure security and flexibility:

Encryption Key (EK): The content owner uses the EK to encrypt the image and to decrypt the image later.

Data-Hiding Key (DHK): Utilised by the data hider to conceal and de conceal confidential payload.

This segregation allows data extraction and decoding of the image to be separated processes, which is useful in overcoming the problem of inseparability in the previous RDH designs.

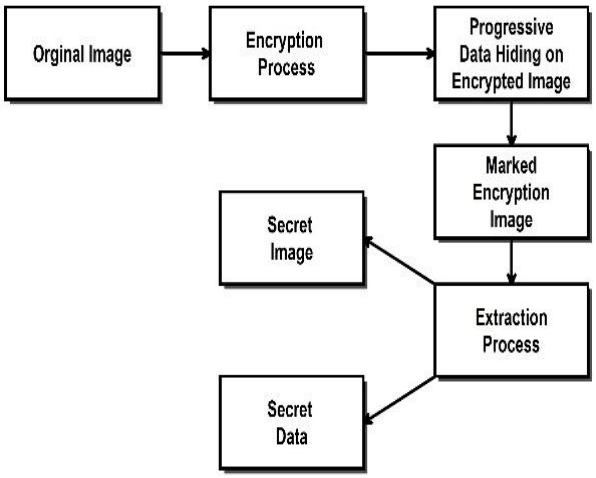

Fig 1:System Architucure

Encryption Process

The encryption procedure secures secrecy of the original image but ready it to be reversibly data hidden. The suggested structure is a combination of XOR encryption which can be used to scramble lightweight images and AES (Advanced Encryption Standard) which can be used to encrypt data.

Input: Original image and encryption key (EK).

XOR Encryption: The picture is scanned in a grid of RGB pixel data. All the bits of the pixel values are XORed with the encryption key or a pseudo-random key stream based on EK. This step offers lightweight scrambling, and eliminates statistical confusion**.**

AES Encryption: AES in counter mode (AES-CTR) is used to improve the privacy protection, and XOR has already been performed. This makes the encryption process resilient to both the brute-force and differentials attacks, and very applicable in secure cloud-based applications.

Output: This gives a completely encrypted picture, and this can be embedded in the data. It is a two-level encryption that balances both the security and the efficiency of the computation and the encrypted image will be the same as random noise.

Data Embedding Process

After encrypting the image, the data hider encrypts

confidential information with data-hiding key (DHK). It works by operating on the layers of the encrypted image that are the least significant bits (LSBs) in the sense that they are the least perceptible.

Steps:

- Turn the encrypted data-hiding key into binary and diagonally map it on the encrypted picture.
- Break up the secret message into bits and encode it in binary.
- Get the R- component (red channel) of the pixel at every mapped pixel location.
- Partially change the least significant bit (LSB) of the pixel value to the message bit.
- data-carrying capacity is reached by repeating the process in several LSB layers.

Key Features:

- Dual Embedding Strategy: It is a strategy of embedding a message and DHK, which guarantees approved recovery.
- Controlled Distortion: Only the LSBs are altered, as this reduces visual distortion.
- Multi-layer Embedding: Distribution of the payload is performed in three layers over LSB, with a compromise between capacity and quality.

The result is a tagged encrypted image, which contains both the encrypted content and the concealed payload.

stepwise restoration Mechanism

The foundation of the suggested methodology is the step-by-step reconstruction process of the concealed payload and the original image through the use of the stepwise restoration process. stepwise restoration is more flexible, error-free, and better-quality images, as opposed to traditional RDH schemes that are trying to recover in a single step. There are two scenarios of recovery:

Case 1: Here the receiver uses data-saving key only (DHK) and not encryption key. Encoded image is scanned to find the mapped key positions and the least significant bits (LSB) are retrieved to match with the positions. These values are reconstructed again to decode the hidden message and the original image is encrypted so that it is not deciphered.

Case 2: Image Recovery : In this case, the receiver utilises the encryption key (EK) in the absence of the DHK. The result of encrypted decoding of the image by inverse XOR is then decrypted with AES and the original image can be restored back with high fidelity. But in this scenario the secret embedded data will not be extracted so that only the visual content is extracted.

Case 3: Full Recovery: In case, the receiver has EK and DHK, then full recovery can be achieved. Information mining and image restoration are carried out separately but gradually. Information stored in the tagged encrypted image is decoded and the original image is realised with information intact and no loss of information is noticed hence fully reversible.

Progressive Stages: Recovery Progressive stages are characterised by processing of one LSB layer at a time. The errors are minimised by processing small pieces of data at a time. The last step makes sure that there is an ideal reconstruction of the hidden information as well as the original picture. Such a framework is flexible and allows various receivers having various keys to gain access to the information that they should.

Security and Performance Features

The suggested methodology helps to solve the main issues of RDH-EI with the following characteristics:

- **Dual-Key Security:** EK and DHK are separated, so that unauthorized users who have partial access cannot recover data and image. This goes a long way in minimizing security risks within the cloud environment.
- **Low Distortion**: The scheme provides high-quality image reconstruction with maximum signal-to-noise ratio (PSNR) values that can be used in sensitive applications like medical imaging.
- **High data-carrying capacity:** Multi-layer embedding enables higher amounts of confidential payload to be stored without impact on quality, compared to the lower-quality conventional RDH methods that utilize only one embedding strategy.
- **Independent Operations**: It is possible to perform data extraction and decoding of the image independently and eliminate the inseparability problem inherent in most previous schemes.
- **Scalability:** The framework is capable of grayscale and color images and thus can be used in different multimedia applications in cloud storage and transmission.

Workflow Summary

The suggested methodology is a series of four stages as in fig. 2. The original image is first encrypted by combining both XOR and AES algorithm with an encryption key by the content owner to provide high security. Second, the data hider inserts the secret information in to the encrypted image using a data-hiding key resulting in a tagged

encrypted image. This labelled image is subsequently sent or saved safely in the cloud. Lastly, at the receiver end, one may be able to recover concealed payload, a copy of the original image or both by using stepwise restoration cycles, depending on the keys that are present. This combined workflow ensures privacy protection, reversibility and flexibility, thus responding to the high security standards of cloud-based applications.

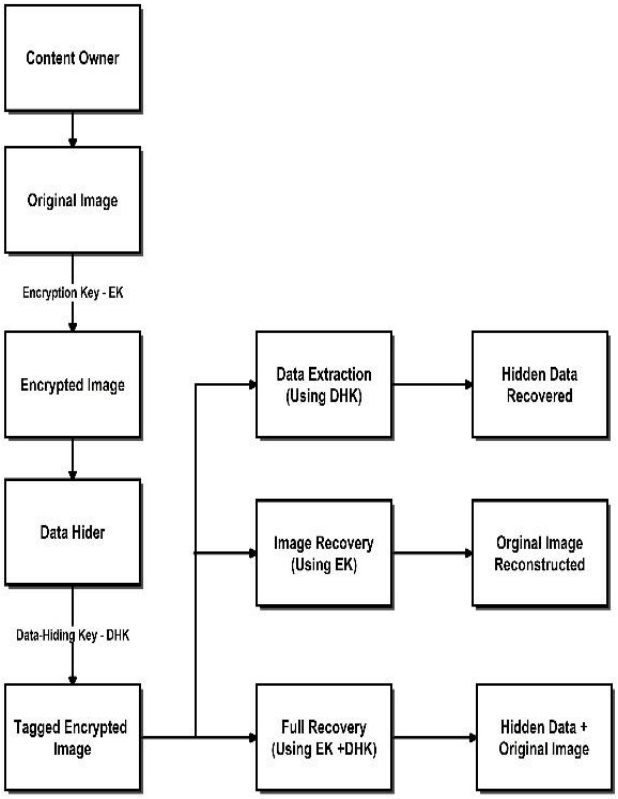

Fig. 1.Workflow for RDH in Encrypted Images with stepwise restoration

Advantages of the Proposed Method

The suggested RDH-EI scheme with stepwise restoration has several benefits relative to current methods, such as the large payload capability through multi-layer data distribution, the low distortion and the image quality is always high at high payloads, and security capability of the scheme due to the dual-key control. It is also capable of flexible recovery, and can-do independent data extraction and decoding of the image. These characteristics render the scheme highly applicable in engineering practices like medical imaging, military communications, digital rights management and forensic investigations.

Results and Performance Analysis

Experiments were performed on benchmark test images in order to test the effectiveness of proposed system with stepwise restoration. This analysis took into consideration two important points: (i) the quality of the images after recovery, so that the encryption, embedding, and recovery operations do not introduce any fidelity distortions and (ii) the accuracy of data extraction, to verify the accurate recovery of the hidden text messages. Quantitative metrics were used and functional validation was done.

Structural Similarity Index Measure (SSIM)

The decoded image scored 1.0000 on SSIM meaning it had a structural similarity with the original. Simultaneously, the PSNR value was 65.52 dB, which is much higher than the PSNR value of 40 dB used as a reference of excellent quality. These findings prove the claim that the recovery process is truly a lossless transformation, which does not cause any distortion that can be measured. Visual judgement supported this observation. the decrypted image could not be distinguished by the original in the respects of colour utilisation, continuity in texture and edge sharpness.

Data Extraction Accuracy

In order to evaluate the strength of concealed payload recovery, three distinct secret text messages were hiding with different keys of data hiding (k1, k2, k3). The three messages were all correctly retrieved during recovery as in fig. 3. and were not corrupted, resulting in 100% accuracy of extraction (3/3). This goes to show the integrity of embedding and extraction processes in the stepwise restoration framework. Moreover, Key tests yielded no significant results with wrong keys, which proves that access to the hidden information is key-dependent strictly. This discriminative retrieval justifies the principle of two-layer security: encryption provides the security of image laws, and keyed embedding controls the security of hidden payload. This controlled access will enable various stakeholders to recover either the image, concealed payload or both data independently, as per their authorized keys.

Fig. 2.Recovered hidden messages using data-hiding keys k1, k2, and k3

Visual Comparison

Besides numerical assessment, a comparison of the original and recovered images was made side by side as in fig. 4. Only no noticeable differences were detected, where both pictures had the same accuracy in color, smoothness of texture, and structural sharpness. This subjective validation helps to prove the distortion-free recovery and complements the SSIM and PSNR results.

Fig. 3.Original vs Decrypted Output

Summary of Experimental Results

The general results are summarized in Table I, which summarizes quality performance, accuracy of data recovery, and the results of unauthorized access.

TABLE I. EXPERIMENTAL RESULTS OF THE PROPOSED RDH-EI SCHEME

Metric	Result
SSIM	1
PSNR (dB)	65.52
Data Extraction Accuracy	100% (3/3)
Unauthorized Access	0%

The findings indicate that the scheme suggested ensures the loss-free restoration of images, and a complete elimination of errors during data extraction, and efficiently implements multi-key selective access. The system enables a good compromise between privacy protection, reversibility and controlled access by obtaining both high objective scores (SSIM, PSNR) and reliable functional correctness (100% data retrieval, zero leakage).

Discussion and Comparative Analysis

COMPARATIVE ANALYSIS

Method	Capacity	Quality	Security	Recovery
Block-based [3]	Moderate	~40 dB	Single key	One-step
Histogram shifting [8]	High	~43 dB	Single key	One-step
Hybrid AES+Stego [6]	Moderate	50–55 dB	Complex	One-step
Proposed Scheme	High	65.52 dB	Dual-key	Progressive

The developed recovery-based RDH-EI scheme demonstrated 100 per cent recovery with SSIM = 1.0000 and PSNR = 65.52 dB, which is evidently above acceptable quality levels. Authenticated messages were indeed extracted with 100 percent accuracy and adversarial attempts were not successful, which demonstrates both fidelity and security. Our scheme has a larger payload, supports multi-layer LSB embedding, dual-key based selective access, and stepwise restoration over reduced error and increased flexibility, in comparison to block-based, histogram-shifting and hybrid RDH-EI methods.

IV.CONCLUSION & FUTURE WORK

The paper introduced a novel recovery-based reversible data hiding system (RDH-EI) that is aimed at the secure, lossless, and versatile embedding of data to the cloud environment. The scheme uses two-key management strategy based on multi-layered LSB embedding, allowing the independent decoding of the image and concealed payload recovery to improve the convenient use and privacy. The experimental findings revealed 100 percent image recovery (SSIM = 1.0000, PSNR = 65.52 dB) and 100 percent correct message re-retrieval using correct keys, and illegal attempts were always unsuccessful, which proves robustness. Higher capacity, reduced distortion, and enhanced flexibility were demonstrated by comparative analysis as compared to current methods of RDH-EI. The strategy has a high potential in medical imaging, clouding store, digital rights management and military communications. Future research will focus on the adaptive embedding of image of different types and lightweight deep learning networks to be resistant to sophisticated statistical attacks.

V.REFERENCES

[1] Z. Qian, X. Zhang, and G. Feng, "Reversible Data Hiding in Encrypted Images Based on stepwise restoration," IEEE signal processing letters, vol. 23, no. 11,pp.1672–1676,Nov.2016, doi: https://doi.org/10.1109/lsp.2016.2585580.

[2] S. Rahman et al., "A novel and efficient digital image steganography technique using least significant bit substitution," Scientific Reports, vol. 15, no. 1, Jan. 2025, doi: https://doi.org/10.1038/s41598-024-83147-3.

[3] W. Hong, T.-S. Chen, and H.-Y. Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match," IEEE Signal Processing Letters, vol. 19, no. 4, pp. 199–202, Apr. 2012, doi: https://doi.org/10.1109/lsp.2012.2187334.

[4] Z. Qian, X. Zhang, and S. Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream," IEEE Transactions on Multimedia, vol. 16, no. 5, pp. 1486–1491,Apr.2014, doi: https://doi.org/10.1109/tmm.2014.2316154.

[5] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image Steganography Using LSB and Hybrid Encryption Algorithms," Applied Sciences, vol. 13, no. 21,p.11771,Jan.2023, doi: https://doi.org/10.3390/app132111771.

[6] D. Madhu, S. Vasuhi, and A. Samydurai, "Dynamic 8-bit XOR algorithm with AES crypto algorithm for image steganography," Signal, Image and Video Processing, vol. 18, no. S1, pp. 429–445, Apr. 2024, doi: https://doi.org/10.1007/s11760-024-03165-6.

[7] H. M. Sidqi, "Efficient Multi-Secret Digital Images Steganography," Journal of Computer Science, vol. 16, no.2,pp.249–256,Feb.2020, doi: https://doi.org/10.3844/jcssp.2020.249.256.

[8] Adnan Sondas and Necla Bandirmali Erturk, "Dynamic data hiding capacity enhancement for the Hybrid Near Maximum Histogram image steganography based on Multi-Pixel-Pair approach," Multimedia Tools and Applications,Apr.2024, doi: https://doi.org/10.1007/s11042-024-19059-1.

[9] A. K. Rai, H. Om, S. Chand, and C.-C. Lin, "High-Capacity Reversible Data Hiding Based on Two-Layer Embedding Scheme for Encrypted Image Using Blockchain," Computers, vol. 12, no. 6, p. 120, Jun. 2023, doi: https://doi.org/10.3390/computers12060120.

[10] Z. Hua, Y. Wang, S. Yi, Y. Zhou, and X. Jia, "Reversible Data Hiding in Encrypted Images Using Cipher-Feedback Secret Sharing," IEEE Transactions on Circuits and Systems for Video Technology, vol. 32, no.8,pp.4968–4982,Aug.2022, doi: https://doi.org/10.1109/tcsvt.2022.3140974.

[11] Bayesh, Md Rishadul, D. Das, and M. Ahadullah, "A Dual-Layer Image Encryption Framework Using Chaotic AES with Dynamic S-Boxes and Steganographic QR Codes," arXiv.org, 2025. https://arxiv.org/abs/2506.13895

[12] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," Multimedia Tools and Applications, vol. 75, no. 22, pp. 14867–14893, May 2015, .