IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 5, March 2025

Lossless Image Compression with Embedded Encryption

Nimse Madhuri S, Nikita Aher, Utkarsha Holkar, Harsha Bhamare
Assistant Professor, Matoshri College of Engineering and Research Centre, Nashik, India

Abstract: *In today's digital landscape, image compression plays a vital role in protecting visual data throughout its processing journey. Over the years, numerous techniques have been developed to optimize image compression, with a focus on efficient data representation and application development. A common approach involves the content owner encrypting the original image using a secure key, rendering it inaccessible to unauthorized parties. Subsequently, a data hider may employ a separate key to compress specific bits of the encrypted image, creating a sparse space that can accommodate additional data. This encrypted image, now containing extra information, can be transmitted to a receiver. If the receiver possesses the data hiding key, they can extract the additional data without needing to know the image's content. Conversely, if the receiver has the encryption key, they can decrypt the received data to obtain an image similar to the original. Moreover, if the receiver has access to both keys, they can extract the additional data and recover the original image content, ensuring a secure and efficient data transmission process.*

Keywords: Reversible data hiding operations, data hiding, Cryptography, Steganography, Reversible data hiding

I. INTRODUCTION

The proliferation of digital images on the internet has led to a growing concern for image security, particularly in sensitive applications such as confidential transmission, video surveillance, and medical imaging. The need for rapid and secure diagnosis in medical settings, for instance, underscores the importance of protecting image data. As image transmission becomes an increasingly routine practice, finding efficient ways to transmit them over networks has become a pressing issue. To reduce transmission times, data compression is essential. However, protecting this multimedia data requires additional measures, such as encryption or data hiding algorithms. In recent years, researchers have sought to integrate compression, encryption, and data hiding into a single step, with some solutions proposing the combination of image encryption and compression. Two primary approaches have emerged to address this challenge: content protection through encryption and data hiding. The former involves encrypting binary or gray-level images, while the latter aims to secretly embed messages into the data. A new challenge has arisen in embedding data in encrypted images, with previous work exploring irreversible data hiding approaches or reversible data hiding methods. By developing innovative solutions that balance compression, encryption, and data hiding, researchers can help ensure the secure transmission and storage of sensitive image data.

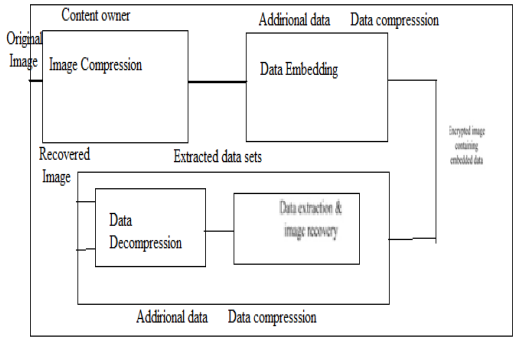

Figure1: Image compression process with architecture.

DOI: 10.48175/IJARSCT-24167

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 5, March 2025

The protection of data from unauthorized access or tampering is a critical concern in today's digital landscape, where vast amounts of information are transmitted over the internet. As the volume of data transfer continues to grow, the importance of ensuring data security has become increasingly paramount. To address this need, various techniques have been developed to safeguard data during transmission, including cryptography and steganography. Cryptography involves encrypting data into an unintelligible format, using a secret key to conceal the information, while steganography takes an additional step by hiding the encrypted data within an innocuous-looking image or other format. Encryption is a widely used method for protecting privacy, as it converts ordinary data into an unreadable format, making it inaccessible to unauthorized parties. However, there are scenarios where the content owner may not trust the service provider handling their data, and therefore, requires the ability to manipulate the encrypted data without revealing the underlying content. For instance, when sensitive data is encrypted an transmitted through a channel with limited resources, the service provider may need to compress the encrypted data without having access to the decryption key. This highlights the need for innovative solutions that can balance data security with the requirements of efficient data processing and transmission.

II. LITERATURE REVIEW

The concept of scalable image compression encompasses a range of techniques aimed at maintaining image quality while reducing file size. To achieve this, it is essential to analyze various data processing and compression algorithms, as well as recent advancements in formation technique development. This involves examining the different development features and processes involved in image compression, including the management of transparent images. The application of image compression is not limited to data transfer, but also extends to security events and the protection of original images. For instance, when sensitive information is encrypted and transmitted, a channel provider without access to the cryptographic key may need to compress the encrypted data due to limited channel resources. To address this challenge, researchers have developed lossless compression techniques for encrypted images, such as using low-density parity-check codes to layer the encrypted image. Additionally, lossy compression techniques can be employed to efficiently compress encrypted images by discarding the excessively rough and fine data of coefficients produced from orthogonal transformations. By applying these techniques, the recipient of the compressed image can recover the original image by reconstructing the coefficients. Furthermore, the calculation of transformations in the encrypted domain has also been explored, leveraging the homomorphic properties of the underlying cryptosystem to implement discrete Fourier transforms in the encrypted space.

Even if an individual responsible for hiding data is unaware of the original content, they can still embed additional information into the encrypted image by manipulating the least significant bits using a data hiding key. This process creates a sparse space that can accommodate the extra data, allowing for efficient and secure transmission. Upon receiving the encrypted image containing the additional information, the recipient has the option to extract the extra data using only the data hiding key, or to obtain an image similar to the original one by using only the encryption key. This approach enables flexible and secure data transmission, where the recipient can choose to access either the original image or the embedded information, depending on their authorization and the keys they possess.When the recipient possesses both the encryption key and the data hiding key, they can extract the additional information and recover the original content without any degradation, provided that the amount of embedded data is not excessively large. By leveraging the spatial correlation inherent in natural images, the recipient can successfully retrieve the original image and the embedded information, ensuring a seamless and lossless recovery process. This approach enables the recipient to access both the original content and the additional information, making it a highly efficient and secure method for data transmission and storage.The reversible data hiding technique involves a two-step process, where the image is first compressed and encrypted using an encryption key, and then the data to be hidden is embedded into the image using a data hiding key. At the receiving end, the process is reversed, where the image is first extracted using the encryption key, and then the embedded data is extracted using the data hiding key. This serial process requires the receiver to have both keys in order to access the original image and the hidden data. In scenarios where the channel provider lacks knowledge of the cryptographic key, they may compress the encrypted data to conserve channel resources. Researchers have developed methods to compress encrypted images in a lossless manner, such as using low-density parity-check codes for binary images. Additionally, techniques like progressive decomposition and rate-compatible punctured turbo codes have been developed for

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 5, March 2025

compressing encrypted gray images. These methods enable efficient compression of encrypted images by discarding unnecessary information, allowing the receiver to reconstruct the original image by retrieving the coefficients. By leveraging these techniques, reversible data hiding can be achieved, enabling secure and efficient transmission of images and hidden data

III. REVERSIBLE DATA HIDING

Reversible data hiding is a sophisticated technique used to conceal secret messages within digital images, enabling secure and private communication. This method involves embedding additional information into a cover image in a reversible manner, allowing the original image to be perfectly restored after the hidden message is extracted. Historically, data hiding has been utilized for covert communication, and in some cases, the embedded images are further encrypted to prevent analysis and detection of the hidden message. This technique is particularly useful in applications where the owner of the image wishes to maintain confidentiality, such as in military or medical imaging. In these scenarios, the content owner must encrypt the image before sharing it with the data hider, ensuring that the sensitive information remains protected. The recipient of the image can then extract the embedded message and recover the original image, maintaining the confidentiality and integrity of the data. Recently, numerous reversible data hiding methods have been developed, offering enhanced security and privacy features. As a means of protecting sensitive information, encryption is a widely used and effective technique. When sharing confidential images, content owners often encrypt the data before transmission, ensuring that only authorized parties can access the information

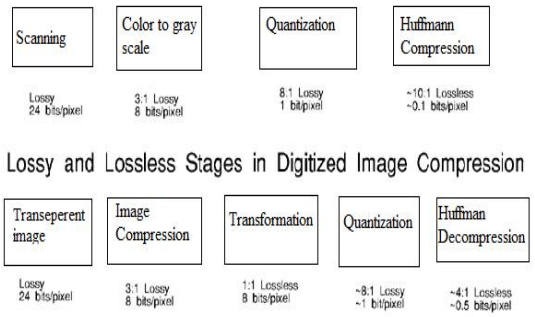

Figure 2: Procedure for image compression image extraction with suitable processing.

Reversible data hiding is a technique that enables the embedding of additional information into sensitive media, such as military or medical images, in a way that allows for the perfect restoration of the original content after the hidden message is extracted. This method is particularly useful in situations where the integrity of the original data must be maintained, and any distortion or alteration is unacceptable. Encryption is a widely used and effective means of protecting sensitive information, as it converts ordinary signals into incomprehensible data that can only be deciphered with the correct decryption key. However, in certain scenarios, content owners may not trust the service providers handling their encrypted data, and therefore, require the ability to manipulate the encrypted data without revealing the underlying content. For instance, when encrypted data is transmitted through a channel with limited resources, the channel provider may need to compress the data without having access to the decryption key. In such cases, a reversible data hiding scheme for encrypted images is essential, as it enables the addition of supplementary information, such as origin data or authentication codes, to the encrypted image without compromising the original content. This scheme also ensures that the original content can be recovered without any errors or distortions after decryption and extraction of the additional message at the receiver's end.

IV. METHODOLOGY

The proposed scheme is made up of image encryption, data embedding and data extraction, image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data- hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. If the receiver has only the data-hiding key, the can extract the additional data though he does not know the image content. If he has only the encryption key, he can decrypt the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 5, March 2025

received data to obtain an image similar to the original one, but cannot extract the embedded additional data. If he receiver has both the data-hiding key and the encryption key, can extract the additional data and recovertheoriginalimage without any error when theamountofadditionaldataisnottoolarge.At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affectstheLSB,a decryptionwith the encryption key can result in an image similar to the original version.

V. EXPERIMENTAL RESULTS

Image Encryption

The rapid advancements in communication technology have sparked a significant interest in the transmission of digital images. Nevertheless, the increasing processing power and storage capacity of computers have also made it easier for unauthorized individuals to access sensitive information. To mitigate this risk, encryption techniques have been developed, which involve the use of complex mathematical algorithms and keys to transform digital data into an unreadable cipher code before transmission. Conversely, decryption techniques are used to retrieve the original data from the cipher code using the corresponding keys and algorithms. Despite the growing importance of image transmission, the rise of illegal data access has become a pressing concern in both wireless and general communication networks. As a result, ensuring information privacy has become a formidable challenge, necessitating the development of robust security measures to safeguard sensitive data and prevent unauthorized access.

Data Embedding

This module facilitates the embedding of additional data into an image, which is then secured using a Data-Hiding Key. The process begins with the content owner encrypting the original image using an encryption key. Subsequently, a data-hider, who is unaware of the original content, can compress the least significant bits of the encrypted image using a data-hiding key. This compression creates a sparse space that can accommodate the additional data. Once the encrypted image contains the additional data, the receiver has the flexibility to extract the additional data using only the data-hiding key or to obtain an image that closely resembles the original one using only the encryption key. If the receiver possesses both keys, they can extract the additional data and restore the original content without any errors, provided that the amount of additional data is not excessive. This is made possible by leveraging the spatial correlation inherent in natural images, which enables the accurate recovery of the original content

Image Decryption

This module describes an Image Decryption Process, where the content owner secures the original image using an encryption key. A data-hider, without knowledge of the original content, can then compress the encrypted image's least significant bits using a data-hiding key, creating a sparse space for additional data. The receiver can extract this additional data using only the data-hiding key or obtain a similar image to the original using only the encryption key. If the receiver possesses both keys, they can extract the additional data and recover the original content without errors, leveraging the spatial correlation in natural images, provided the additional data is not excessive. Furthermore, if a lossless compression method is applied to the encrypted image with embedded data, the additional data can still be extracted, and the original content can be recovered, as the lossless compression does not alter the encrypted image's content. To evaluate the distortion in the directly decrypted image, three quality metrics are employed: Peak Signal-to-Noise Ratio (PSNR), the Watson metric, and a universal quality index. PSNR, a widely used engineering term, measures the ratio of the maximum possible signal power to the power of corrupting noise, typically expressed in decibels due to the wide dynamic range of many signals. PSNR is commonly used to assess the quality of reconstruction in lossy compression codecs, such as those used in image compression. The Watson metric is a perceptual quality metric that leverages the characteristics of the human visual system to quantify the total perceptual error in an image. This metric is based on the Discrete Cosine Transform (DCT) and considers three key factors: contrast sensitivity, luminance masking, and contrast masking. In addition to the Watson metric, a quality index is also used, which operates in the spatial domain and combines three components: correlation loss, luminance distortion, and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 5, March 2025

contrast distortion. The quality of an image is evaluated based on the values of PSNR, Watson metric, and quality index, where higher PSNR values, lower Watson metric values, or higher quality index values indicate better image quality. The figures illustrating the results use the embedding rate as the x-axis and the corresponding PSNR, Watson metric, or quality index values as the y-axis, providing a visual representation of the relationship between the embedding rate and image quality.

VI. CONCLUSION

A new approach to reversible data hiding in encrypted images is presented, comprising three distinct phases: image encryption, data embedding, and data extraction/image recovery. The process begins with the content owner encrypting the original image using an encryption key. Subsequently, a data-hider, without knowledge of the original content, can compress the least significant bits of the encrypted image using a data-hiding key, thereby creating a sparse space to accommodate additional data. The recipient of the encrypted image with embedded data can then extract the additional data using only the data-hiding key or obtain an image similar to the original one using only the encryption key. If the recipient possesses both keys, they can extract the additional data and recover the original content without errors, leveraging the spatial correlation in natural images, provided the amount of additional data is not excessive. Furthermore, if a lossless compression method is applied to the encrypted image with embedded data, the additional data can still be extracted, and the original content can be recovered, as the lossless compression does not alter the content of the encrypted image. This approach enables efficient and secure data hiding in encrypted images, ensuring that the original content can be recovered without errors.

REFERENCES

[1] "*Study on Separable Reversible Data Hiding in Encrypted Images*", International Journal of Advancements in ResearchTechnology, Volume 2, Issue 12, December-2013 223 ISSN 2278-7763

[2] W. Liu, W.Zeng, L. Dong, and Q. Yao,"*Efficient compression of encryptedgrayscale images*," *IEEE Trans. ImageProcess.*, vol. 19, no. 4, pp. 1097–1102, Apr.2010.

[3] X. Zhang, "*Lossy compression and iterativereconstruction for encrypted image*," *IEEETrans. Inform. Forensics Security*, vol. 6,no. 1,pp. 53–58, Feb. 2011.

[4] T. Bianchi, A. Piva, and M. Barni, "*On theimplementation of the discrete Fouriertransform in the encrypted domain,*" *IEEETrans. Inform.Forensics Security*, vol. 4, no.1, pp. 86–97, Feb. 2009

[5] Spread spectrum image steganography

[6] Altering based approach to adaptive steganography

[7] Chung-Li Hou,ChanChunLu,Shi-Chun Tsai and Wen- Guey Tzeng An optimal Tree Based Parity Checking

[8] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "*An efficient buyer-sellerwatermarking protocol based on composite signal representation*," inProc.11th ACM Workshop Multimedia and Security, 2009, pp. 9–18

[9] S. Lian, Z. Liu, Z. Ren, and H. Wang,"*Commutative encryption andwatermarkingin video compression*," *IEEE Trans. CircuitsSyst. VideoTechnol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007