International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Secret Sharing Based Reversible Data Hiding in Encrypted Images with Multiple Data Hiders

B. Thanuja[1], Bingi Pravalika[2], Erlapally Bhagyalakshmi[3], Mothe Maheshbabu[4]

[1]Assistant Professor, Department of Electronics and Communication Engineering, CMR Technical Campus, Hyderabad, India
[2,3,4]Department of Electronics and Communication Engineering, CMR Technical Campus, Hyderabad, India

ABSTRACT
Reversible Data Hiding in Encrypted Image (RDHEI) is a technology for embedding secret information in an encrypted image. It allows the extraction of secret information and lossless decryption and the reconstruction of the original image. This paper proposes an RDHEI technique based on Shamir's Secret Sharing technique and multi-project construction technique. Our approach is to let the image owner hide the pixel values in the coefficients of the polynomial by grouping the pixels and constructing a polynomial. Then, we substitute the secret key into the polynomial through Shamir's Secret Sharing technology. It enables the Galois Field calculation to generate the shared pixels. Finally, we divide the shared pixels into 8 bits and allocate them to the pixels of the shared image. Thus, the embedded space is vacated, and the generated shared image is hidden in the secret message. The experimental results demonstrate that our approach has a multi-hider mechanism and each shared image has a fixed embedding rate, which does not decrease as more images are shared. Additionally, the embedding rate is improved compared with the previous approach.

INTRODUCTION
Multimedia security technology is used to prevent unauthorized users from copying, sharing, and modifying media content. To prevent this problem, encryption and information hiding are often used to protect media content. As far as information hiding technology is concerned, traditional information hiding technology will destroy the content of the cover image. However, in some exceptional cases, such as military, medical, and legal document images, the slight distortion of the image is entirely unacceptable. Therefore, whether these images can be completely restored is very important. Reversible data hiding scheme (RDH) can correspond with the requirement of being lossless. RDH methods applied the methodology of changing context to hide the secret data in cover media. After data extracting, the changing context will be fully recovered to the cover media. On the other hand, RDHEI (Reversible Data Hiding in Encrypted Images) technology can combine encryption technology with RDH technology, which can not only hide secret information in the image, but can also encrypt the image to protect the image content. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer.

One of the best-known techniques has been credited to MoniNaor and Adi Shamir. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

Using a similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text.

In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable ciphertext (ibid.). This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm that usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys.

RELATED WORKS

1. **Secret Sharing Schemes:**Understand existing secret sharing schemes and their applications in data hiding and encryption. Look for works that discuss the theoretical foundations, security properties, and practical implementations of secret sharing.
2. **Reversible Data Hiding:** Explore research on reversible data hiding techniques, which allow for the embedding of additional data in a host signal (such as an image) while enabling perfect recovery of the original signal. Look for methods that focus on maintaining high image quality and reversibility.
3. **Encrypted Images:** Investigate techniques for encrypting images to protect their content while allowing for selective access by authorized users. Consider encryption schemes that support operations such as decryption, data hiding, and sharing among multiple parties.
4. **Multiple Data Hiders:** Look for studies that address scenarios where multiple entities contribute to data hiding or encryption processes. This could involve collaborative schemes where multiple parties share responsibilities for hiding data securely.
5. **Security and Robustness Analysis:** Examine research that evaluates the security and robustness of data hiding schemes, particularly in scenarios involving encrypted images and multiple data hiders. Consider factors such as resistance to attacks, capacity for hiding data, and impact on image quality.
6. **Practical Implementations and Applications:** Seek works that discuss practical implementations of data hiding techniques in real-world scenarios. Look for applications in domains such as secure communication, digital rights management, and privacy-preserving data sharing.

To find relevant papers and articles, you can search academic databases such as IEEE Xplore, ACM Digital Library, Google Scholar, and ScienceDirect using keywords like "secret sharing," "reversible data hiding," "encrypted images," and "multiple data hiders." Additionally, review citations in relevant papers and articles to identify seminal works and recent contributions in the field.

METHODS

Secret sharing based reversible data hiding in encrypted images with multiple data hiders is a technique that involves embedding additional information into encrypted images in such a way that the original image can be reconstructed without any loss, while the embedded data can be extracted only by authorized parties possessing their respective shares. Here are some methods for achieving this:

1. Visual Cryptography (VC):

Visual cryptography is a cryptographic technique that allows for the encryption of visual information (images) in such a way that decryption can be performed by the human visual system without the need for complex computations.

In the context of reversible data hiding, multiple data hiders can each generate a share of the visual secret sharing scheme, which when combined, reveal the hidden information. This way, the original image remains encrypted, and the hidden data is distributed among the shares.

2. Homomorphic Encryption:

Homomorphic encryption allows certain operations to be performed on encrypted data without decrypting it. This property can be leveraged to embed additional information into encrypted images without compromising their security.

Multiple data hiders can encrypt their respective messages using homomorphic encryption schemes, and the encrypted messages can then be embedded into the encrypted image using additive homomorphism.

3. Shamir's Secret Sharing Scheme:

Shamir's Secret Sharing is a cryptographic algorithm that allows a secret to be divided into shares in such a way that reconstruction of the secret requires a threshold number of shares.

In this method, the original image is encrypted using a secure encryption algorithm, and then Shamir's Secret Sharing Scheme is applied to distribute the decryption key among multiple data hiders. Each hider holds a share of the key, and the original image can only be decrypted when a sufficient number of shares are combined.

4. Quantization Index Modulation (QIM):

QIM is a reversible data hiding technique that embeds data by modifying the quantization indices of the cover image without altering its pixel values significantly.

Multiple data hiders can apply QIM independently to embed their respective messages into the encrypted image. Since QIM is reversible, the original image can be reconstructed without loss, and the embedded data can be extracted by authorized parties possessing the corresponding decryption keys.

5. Spread Spectrum Techniques:

Spread spectrum techniques involve spreading the data over a wide frequency band, making it resilient to noise and interference.

Multiple data hiders can independently spread their data over different frequency bands and embed them into the encrypted image using spread spectrum techniques. The original image remains encrypted, and the embedded data can be extracted by combining the contributions from all data hiders.

These methods provide various approaches to achieve secret sharing based reversible data hiding in encrypted images with multiple data hiders, ensuring both security and reversibility of the hidden data. The choice of method may depend on factors such as the desired level of security, computational complexity, and the specific requirements of the application.

IMPLEMENTATION AND RESULTS

In this section, we perform experiments and analysis. All the tested images are gray 425 level sized by 512 × 512. Figures shows the experimental results of Image peppers. We use the three-out-of-four threshold secret sharing method to group every three original images and encrypt them into four data. Figure 1.1 is the original image, Figure 1.3 are different shared data, and Figure 1.6 is the image after decryption and information retrieval. From the image we can see that our method can fully recover. Similarly, we did the same for image Couple1 and the result is shown in Figure 1.8 shows the maximum embedding rate comparison

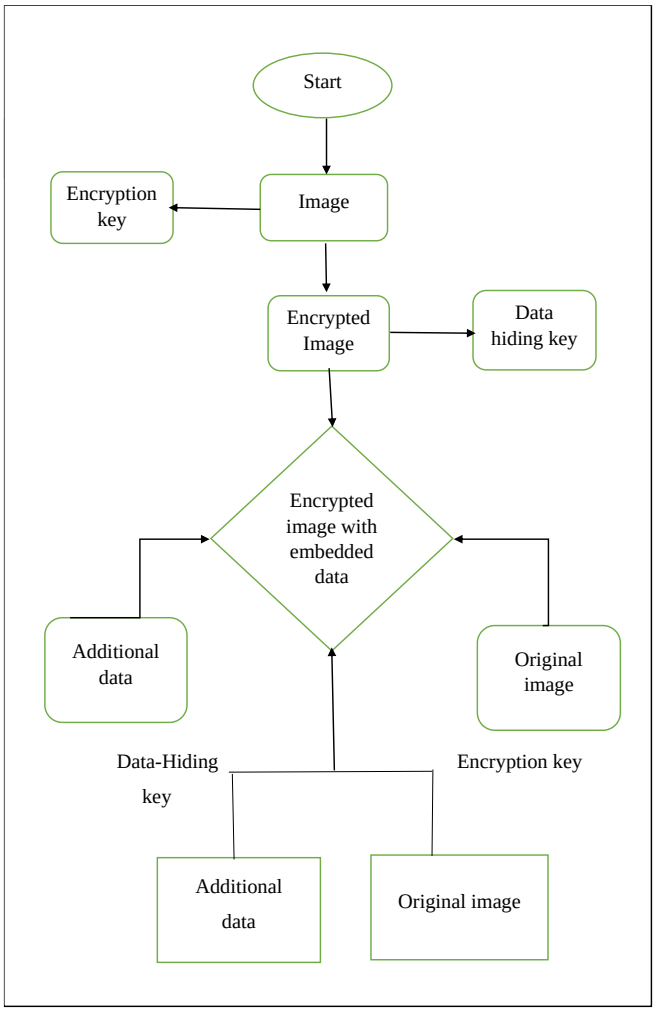

Fig 1: Flow chart

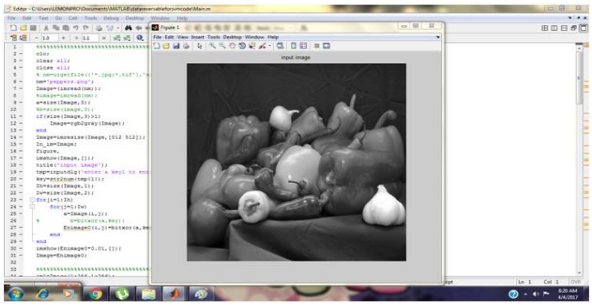

Fig 1.1: Referring to an input image of peppers with a size of 512x512 pixels.

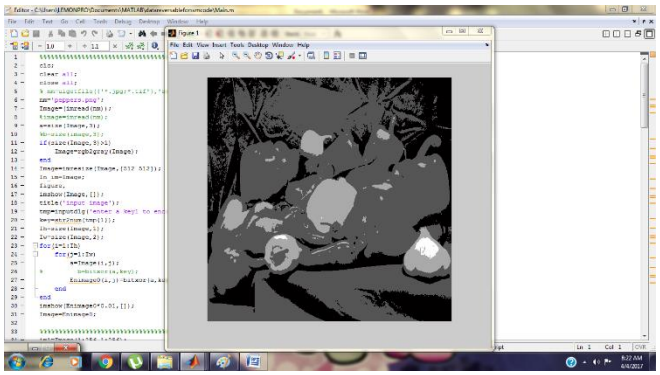

Fig 1.2: Enter the public Key for Encryption

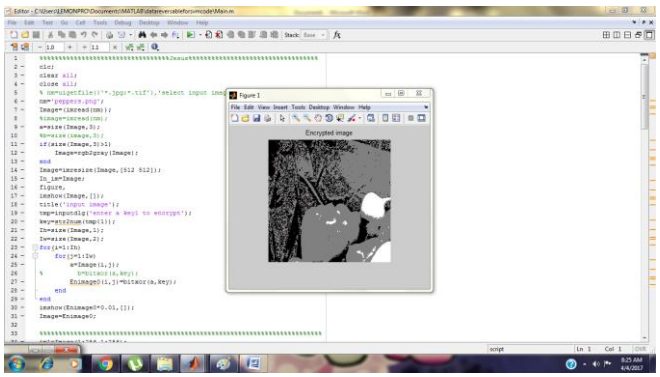

Fig 1.3: Enter the Messages for Data Embedding by using key modulation with help of Xor operation

Decryption Process:

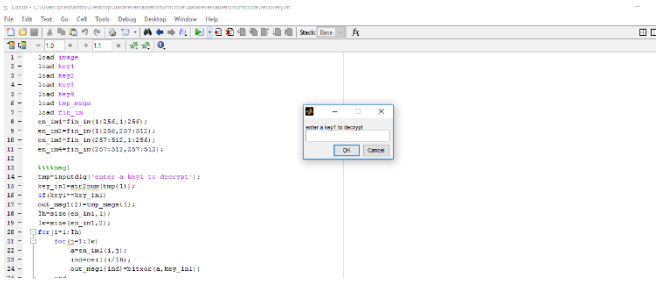

Fig 1.4: Enter the public Key For decryption

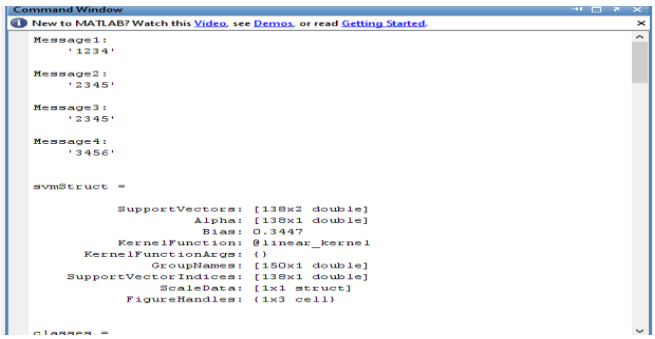

Fig 6.5: Decrypted Messages in Command Window

Fig 6.6: Decrypted image

CONCLUSION

In this paper, we design a secure RIDH scheme operated over the encrypted domain. We suggest a public key modulation mechanism, which allows us to embed the data via simple BIT-XOR operations, without the need of accessing the secret encryption key. constructed shared image has B part of the embedding space, and each shared image is encrypted. Information hiders can hide secret information in Part B of the shared image. Compared with other methods, our method has a higher embedding rate, and the embedding rate does not decrease due to more shared images. At the decoder side, we propose to use a powerful two-class SVM classifier to discriminate encrypted and non-encrypted image patches, enabling us to jointly decode the embedded message and the original image signal perfectly. We have also performed extensive experiments to validate the superior embedding performance of our proposed RIDH method over encrypted domain.

FUTURE SCOPE

In the future work, we will consider how to apply the proposed model to other applications or to some specified multimedia such as video or audio.

REFERENCES

1. N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, “HighCapacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis,” Digital Signal Processing, 20, pp. 1629−1636, 2010.
2. J. Tian, “Reversible Data Embedding Using a Difference Expansion,” IEEE Trans. on Circuits and Systems for Video Technology, 13(8), pp. 890−896, 2003.
3. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible Data Hiding,” IEEE Trans. on Circuits and Systems for Video Technology, 16(3), pp. 354−362, 2006.
4. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless Generalized-LSB Data Embedding,” IEEE Trans. on Image Processing,
5. X. Hu, W. Zhang, X. Li, and N. Yu, “Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding,” IEEE Trans. on Information Forensics and Security, 10(3), pp. 653-664, 2015.
6. X. Zhang, “Reversible Data Hiding with Optimal Value Transfer,” IEEE Trans. on Multimedia, 15(2), 316−325, 2013.

7. W. Zhang, X. Hu, X. Li, and N. Yu, "Optimal Transition Probability of Reversible Data Hiding for General Distortion Metrics and Its Applications," IEEE Trans. on Image Processing, 24(1), pp. 294-304, 2015.
8. S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative Encryption and Watermarking in Video Compression," IEEE Trans. on Circuits and Systems for Video Technology, 17(6), pp. 774−778, 2007.
9. M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A Commutative Digital Image Watermarking and Encryption Method in the Tree Structured Haar Transform Domain," Signal Processing: Image Communication, 26(1), pp. 1−12, 2011.
10. X. Zhang, "Commutative Reversible Data Hiding and Encryption," Security and Communication Networks, 6, pp. 1396−1403, 2013.

ACKNOWLEDGEMENT

Sincere thanks of gratitude are extended to the Guide and coordinator "Dr. Sudha Arvind", Professor, Department of Electronics & Communication Engineering, for their guidance and support in completing the project and also to "Mr. G. Srikanth", Professor and Head, of the Department of Electronics & Communication Engineering, and "Dr. A. Raji Reddy" Director of CMR Technical Campus for providing all the facility that was required.