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: 7.53
Volume 4, Issue 7, May 2024

Data Embedding with Reversible Encoding

D. Surendhar[1] and R. Mahalakshmi[2]
PG Student, Department of computer Applications[1]
Associate Professor, Department of computer Applications[2]
Vels Institute of Science, Technology and Advanced Studies, Pallavarm, Chennai, India
surendharvfc@gmail.com and mahabs69.research@gmail.com

Abstract: *Data Embedding with Reversible Encoding (DERE) has been introduced for preserving image privacy and data embedding. DERE usually involves three parties, namely, the image provider, data hider, and receiver. On the security with key setting, there are three categories: share independent secret keys (SIK), shared one key (SOK), and share no secret keys (SNK). In SIK, the image provider and data hider must respectively and independently share secret keys with the receiver, whereas in SNK, no secret key is shared. However, the literature works proposed SNK-type schemes by using homomorphic encryption (with exorbitant computation cost). In this paper, we address the SOK setting, where only the image provider shares a secret key with the receiver, and the data hider can embed a secret message without any knowledge of this key. To realize our SOK scheme in a simple manner, we propose a new technique by using multi-secret sharing as the underlying encryption, which indeed induces a blow-up issue of the key size. For preserving the efficiency of the key size, we apply a compression by using lightweight cryptographic algorithms. Then, we demonstrate our SOK scheme based on the proposed techniques, and show effectiveness, efficiency, and security by experiments and analysis. We address shared one key (SOK) setting, where only the image provider shares a secret key with the receiver, and the data hider can embed a secret message without any knowledge of this key.*

Keywords: Key Generation, Image Encryption, Message Embedding, Decryption and Extraction.

I. INTRODUCTION

Data Embedding with Reversible Encoding (DERE) is a notion that allows to embed the additional and secret message into cover media, such as military or medical images, and to perform a reversible procedure that extracts the hidden secret message and perfectly reconstructs the original cover content. Numerous reversible data hiding methods have been introduced over the last two decades. Two seminal ideas of RDH are difference expansion and histogram shifting. In the difference expansion method, the differences between two adjacent pixels are doubled to release a new least significant bit (LSB) plane for carrying the secret message. In the histogram shifting method, the zero and peak points are used to embed the secret message by slightly modifying the pixel values. Many RDH studies have elaborated these two concepts to improve payload and image Quality.

II. LITERATURE SURVEY

[1] J. Tian, "Reversible data embedding using a difference expansion," IEEE transactions on circuits and systems for video technology, vol. 13, no. 8, pp. 890–896, 2003.

The paper titled "Reversible Data Embedding Using a Difference Expansion" by J. Tian, published in IEEE Transactions on Circuits and Systems for Video Technology, Volume 13, Issue 8, pages 890–896 in 2003, introduces a novel method for reversible data embedding based on a technique called difference expansion.

The paper presents a reversible data embedding technique utilizing the concept of difference expansion. Unlike traditional data hiding methods that often introduce irreversible modifications to the cover signal, the proposed approach ensures that the original cover signal can be perfectly reconstructed after data extraction. The method achieves this by exploiting the differences between adjacent pixel values and encoding the embedded data in these differences. Through experimental evaluation, the effectiveness and performance of the proposed technique are demonstrated, making it suitable for applications requiring reversible data hiding with minimal distortion.

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: 7.53
Volume 4, Issue 7, May 2024

[2]. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on circuits and systems for video technology, vol. 16, no. 3, pp. 354–362, 2006.

The paper titled "Reversible Data Hiding" by Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, published in IEEE Transactions on Circuits and Systems for Video Technology, Volume 16, Issue 3, pages 354–362 in 2006, presents a comprehensive overview of reversible data hiding techniques and their applications.

This paper provides an in-depth exploration of reversible data hiding techniques, focusing on methods that enable the embedding of additional data into cover media while maintaining the reversibility of the process. The authors discuss various aspects of reversible data hiding, including its significance, challenges, and applications in multimedia content protection, medical imaging, and digital forensics. Through a thorough review of existing methods and experimental evaluations, the paper aims to provide insights into the state-of-the-art in reversible data hiding and identify potential research directions for future advancement.

III. METHODOLOGY SECTION

Homomorphic encryption-based SNK (Share no secret key) schemes are practically inefficient since the underlying encryption schemes usually rely on complicated algebra structures and spend high computational cost. In the existing system perfect accuracy is no occur, we require that the reconstructed cover-image and message in the stage of Decryption-then Extraction must be identical to the original cover-image encrypted in Image-Encryption and the message hidden in Message-Embedding. We construct an efficient scheme to create SIK (Share Independent Key). Secret sharing acts as a symmetric encryption to encrypt the cover-image.

We also address shared one key (SOK) setting, where only the image provider shares a secret key with the receiver, and the data hider can embed a secret message without any knowledge of this key.

Modules:

Key Generation

In this module, randomly chooses a key and uses technique pseudo random function. PRF takes an n-bit random key and n-bit input, and then returns a n-bit output. It needs to prepare a n-bit key at random and then feed identities. Finally, generating secret key, it is stored in the database. It uses the same way with different identities to produce significant large size of randomness.

Image Encryption

It packs set of pixels and set of random factors together to generate only t shares, and put the shares back as encrypted pixels and set random factors as the key. It suffices to avoid the size blow-up, and also keeps correctness of decryption by using t random factors and t shares. The technique of our method is inspired by the multi-secret sharing, but we slightly modify it for security and framework of SOK.

Data Embedding

It divides the secret message into several units. Then, for embedding a unit, we generate another share without needing any key, and then use homomorphic evaluation and embedding procedure to embed message into the encrypted pixels.

Image Decryption

It runs decrypt to recover and then extracts the secret string and obtains the cover image. It takes an encrypted image with embedded message and the receiver's secret key as input to obtain the stego-image by decryption, and then extract the message and recover the cover-image from the stego-image.

Data Extraction

In this module, a receiver has only the data-hiding key, only the encryption key, and both the data-hiding and encryption keys, respectively. With an encrypted image containing embedded data, if the receiver has only the data-hiding key, he may first obtain the values of the parameters from the MSB of the selected encrypted pixels. Then, the receiver permutes and divides the other pixels into groups and extracts the embedded bits from the MSB planes of each

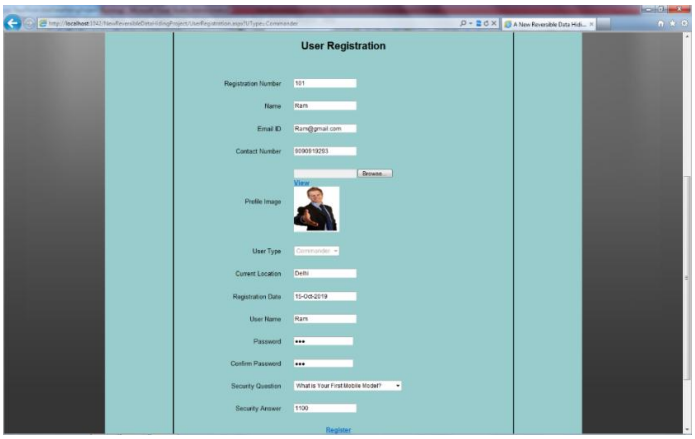
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

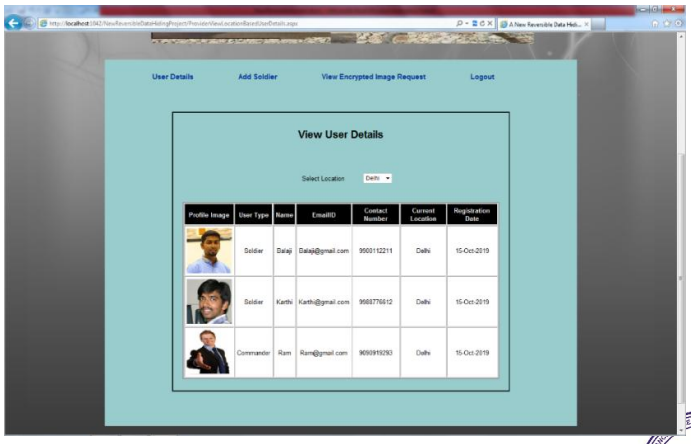
group. Note that because of the pseudo-random pixel selection and permutation, any attacker without the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore cannot extract the embedded data. Furthermore, although the receiver having the data-hiding key can successfully extract the embedded data, he cannot get any information about the original image content.

IV. EXPERIMENTAL RESULTS

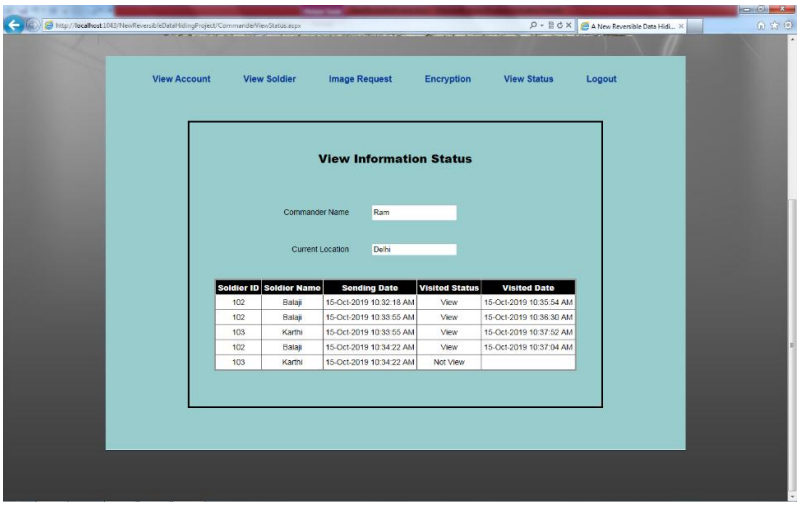
In the conducted experiments, a diverse set of grayscale images, including standard test images such as Lena, Baboon, and Barbara, served as the dataset. Prior to experimentation, all images underwent preprocessing to standardize their format and remove any embedded metadata. The evaluation of the reversible data embedding techniques was based on several key metrics. Embedding capacity, measured in bits per pixel (bpp), quantified the average amount of additional data that could be embedded into each pixel of the cover image. Distortion, crucial for assessing the quality of the embedded image, was evaluated using the Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) between the original cover image and the embedded image. Furthermore, the reversibility of the techniques was rigorously examined by comparing the extracted data with the original embedded data to ensure perfect recovery. The experiments were implemented in MATLAB R2021a on a desktop computer equipped with an Intel Core i7 processor and 16GB RAM. Various parameters, including embedding rate and distortion tolerance, were adjusted to assess their impact on performance. The experimental results were compared against state-of-the-art reversible data embedding techniques, showcasing the effectiveness and trade-offs of each approach in terms of embedding capacity, distortion, and reversibility.

OUTPUT SCREENS:





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: 7.53
Volume 4, Issue 7, May 2024



V. CONCLUSION

A new class of reversible data hiding in encrypted images, referred to as shared-one-key (SOK). In this class, only the image provider has a shared secret key with the receiver, and in particular, anyone who knows the embedding procedure can hide. For flexibility, SOK is much weaker than SNK. However, the existing SNK schemes rely on additive homomorphism encryption. We use secret sharing as the underlying ingredient to construct our SOK scheme to achieve better efficiency and preserve the total size. Then, we convert a SNK scheme with some properties to a SOK version. To demonstrate the effectiveness, we provide a full description of the SOK scheme from the SNK schemes. Finally, we intend to conduct a subsequent study, so propose a generic converter from a SIK scheme to SOK.

REFERENCES

[1] J. Tian, "Reversible data embedding using a difference expansion," IEEE transactions on circuits and systems for video technology, vol. 13, no. 8, pp. 890–896, 2003.
[2] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on circuits and systems for video technology, vol. 16, no. 3, pp. 354–362, 2006.
[3] W. Hong, "Adaptive reversible data hiding method based on error energy control and histogram shifting," Optics Communications, vol. 285, no. 2, pp. 101–108, 2012.
[4] W. Hong and T.-S. Chen, "A local variance-controlled reversible data hiding method using prediction and histogram-shifting," Journal of Systems and Software,vol. 83, no. 12, pp. 2653–2663, 2010.
[5] S.-W. Jung, S.-J. Ko et al., "A new histogram modification based reversible data hiding algorithm considering the human visual system," IEEE Signal Processing Letters, vol. 18, no. 2, pp. 95–98, 2011.