International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 03 | Mar -2020 ISSN: 2582-3930

A New Reversible Data Hiding in Encrypted Image Based on Multi Secret Sharing and Lightweight Cryptographic Algorithms

[1]Seyed Mohamed Reboy.A, [2]Bala Murugan. G, [3]Balasubramanian. N, [4]Mohamed Rafi.M

[1]Final year MCA, Mohamed Sathak Engineering College, Kilakarai

[2]Assistant Professor, Dept of MCA, Mohamed Sathak Engineering College, Kilakarai

[3]Associate Professor, Dept of MCA, Mohamed Sathak Engineering College, Kilakarai

[4]Professor, HOD,Dept of MCA, Mohamed Sathak Engineering College, Kilakarai

ABSTRACT:Reversible data hiding in encryptedimages (RDHEI) has been prefaced for conversing image privacy and data embedding in data security. RDHEI usually involves three parties,namely,the image sender,data embedder,and receiver.On the protection with key setting, the rear e three categories: share independent secret keys (SIK) publickey, share done key (SOK)public,and share no secretkeys (SNK) private key. In SIK, the image provider and data hider must respectively and independently share secret keys with the receiver, where a sin private key, no secrets hared.However, the creative works propose din SNK-type designs by using homomorphicencryption (with exorbitant computation cost). In this paper, we address the SOK setting, where only the sender shares a secret key with the information hider, and thus the information hider can embed a secret message with none intelligence of this key.to understand our SOK design in an simple manner,we propose dare placement method by using multi-secret sharing because the underlying encryption, which indeedinducesa puff-up issue of the key size. For preserving the adaptability of the key size, we use a compression by using light weight cryptographic algorithms. Then, we demonstrate our SOK design braced the proposed methods, and show effectiveness, efficiency, and security by experiments andanalysis.

1.INTRODUCTION: Reversible data hiding (RDH) is a notion that allows to embed the additional and secret message into cover media, such as military or medical images, and to perform are versible operation that build up the hidden secret information and perfectly redesign a 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 variation expansion technique, the similarity between two adjacent pixels are doubled to release a newl east significant bit(LSB) plane for carrying these cret 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 detailed these two ideas to better pay load and image quality.Recently,a new direction of RDH known as RDH over an encrypted image(RDHEI) has been introduced.An in feriorassistantora channel administrator is in the middle of a work flow and is authorized to insert some additional data such as the origin information, image notations or authentication data,with in the encrypted image,where the original image content is unknown to this party. Indeed, medical images are encrypted for preserving the patient privacy, and a database administrator only embeds a few data into the corresponding encrypted images. For the consistency of a medical image, it must guarantee that the original content can be perfectly reconstructed after decryption-then-extraction of the secret message by the receiver. We show our sok design based on the proposed methods, and show effectiveness, adaptability, and security by experiments and analysis. We address share done key(sok) setting, where only the send ersharesa secret key with the receiver, and the data hider canembeda secret message without any intelligence of this key. Key generation, image encryption, message embedding, decryption andextraction.

2. PROBLEMDESCRIPTION

A 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 previous work 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.

3.PLANNEDDESIGN

Key Generation

Key generation creates 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.

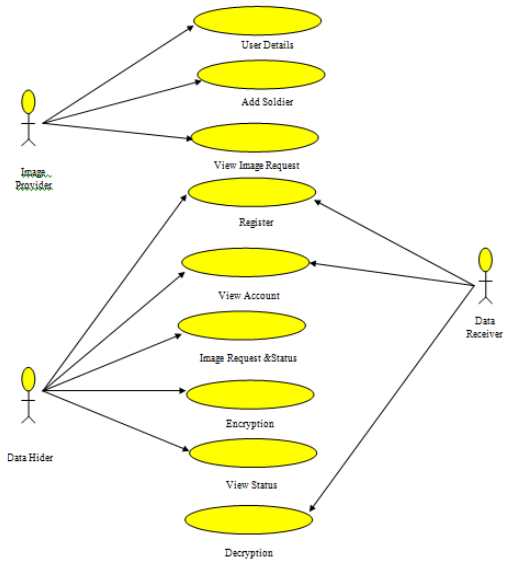
Image Decryption

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 clusters and retrives the hiddend bits from the MSB planes of each group. Important Note that because of the pseudo-random pixel selection and permutation, any attacker without the data-hiding key cannot able to obtain the parameter values and the pixel-groups, therefore cannot retrieves 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.

SYSTEM ARCHITECTURE



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.

OPERATIONAL EXPENDITURE

Our algorithm focuses on secure communication in military network.

4. CONCLUSION

A new class for 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] W. Hong and T.-S. Chen, “A local variance-controlledreversible data hiding method using prediction andhistogram-shifting,” Journal of Systems and Software,vol. 83, no. 12, pp. 2653–2663, 2010.

[2] S.-W. Jung, S.-J.Ko et al., “A new histogram modification based reversible data hiding algorithm consideringthe human visual system,” IEEE Signal Processing Letters, vol. 18, no. 2, pp. 95–98, 2011.

[3] Y.-Y. Tsai, D.-S.Tsai, and C.-L. Liu, “Reversible datahiding scheme based on

neighboring pixel differences,"Digital Signal Processing, vol. 23, no. 3, pp. 919–927,2013.

[4] P. Tsai, Y.-C.Hu, and H.-L. Yeh, "Reversible imagehiding scheme using predictive coding and histogramshifting," Signal Processing, vol. 89, no. 6, pp. 1129–1143, 2009.

[5] D. M. Thodi and J. J. Rodr´ ıguez, "Expansion embeddingtechniques for reversible watermarking," IEEE transactions on image processing, vol. 16, no. 3, pp. 721–730,2007.

[6] W.-L. Tai, C.-M.Yeh, and C.-C. Chang, "Reversibledata hiding based on histogram modification of pixeldifferences," IEEE transactions on circuits and systemsfor video technology, vol. 19, no. 6, pp. 906–910, 2009.

[7] X. Zhang, "Reversible data hiding in encrypted image,"IEEE signal processing letters, vol. 18, no. 4, pp. 255–258, 2011.

[8] Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, and B. Ma, "Reversible data hiding: advances in the past two decades,"IEEE Access, vol. 4, pp. 3210–3237, 2016.

[9] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication watermark for jpeg images," in InformationTechnology: Coding and Computing, 2001. Proceedings.International Conference on. IEEE, 2001, pp. 223–227.

[10] H. Sakai, M. Kuribayashi, and M. Morii, "Adaptivereversible data hiding for jpeg images," in InformationTheory and Its Applications, 2008.ISITA 2008.International Symposium on. IEEE, 2008, pp. 1–6.

[11] A. Nikolaidis, "Reversible data hiding in jpeg imagesutilising zero quantised coefficients," IET Image Processing, vol. 9, no. 7, pp. 560–568, 2015.

[12] D. Zou, Y. Q. Shi, Z. Ni, and W. Su, "A semi-fragilelossless digital watermarking scheme based on integerwavelet transform," IEEE Transactions on Circuits andSystems for Video Technology, vol. 16, no. 10, pp. 1294–1300, 2006.

[13] M. S. A. Karim and K. Wong, "Universal data embeddingin encrypted domain," Signal Processing, vol. 94, pp.174–182, 2014.

[14] W. Hong, T.-S.Chen, and H.-Y. Wu, "An improvedreversible data hiding in encrypted images using sidematch," IEEE Signal Processing Letters, vol. 19, no. 4,pp. 199–202, 2012.

[15] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversibledata hiding in encrypted images by reserving room beforeencryption," IEEE Transactions on information forensicsand security, vol. 8, no. 3, pp. 553–562, 2013.

[16] X. Zhang, "Separable reversible data hiding in encryptedimage," IEEE transactions on

information forensics andsecurity, vol. 7, no. 2, pp. 826–832, 2012.

[17] W. Zhang, K. Ma, and N. Yu, "Reversibility improveddata hiding in encrypted images," Signal Processing,vol. 94, pp. 118–127, 2014.

[18] Y.-C. Chen, C.-W.Shiu, and G. Horng, "Encryptedsignal-based reversible data hiding with public key cryptosystem," Journal of Visual Communication and ImageRepresentation, vol. 25, no. 5, pp. 1164–1170, 2014.

[19] P. Paillier, "Public-key cryptosystems based on compositedegreeresiduosity classes," in International Conferenceon the Theory and Applications of Cryptographic Techniques. Springer, 1999, pp. 223–238.

[20] X. Zhang, J. Long, Z. Wang, and H. Cheng, "Losslessand reversible data hiding in encrypted images withpublic-key cryptography," IEEE Transactions on Circuitsand Systems for Video Technology, vol. 26, no. 9, pp.1622–1631, 2016.

[21] M. Li and Y. Li, "Histogram shifting in encrypted imageswith public key cryptosystem for reversible data hiding,"Signal Processing, vol. 130, pp. 190–196, 2017.

[22] C.-W. Shiu, Y.-C. Chen, and W. Hong, "Encryptedimage-based reversible data hiding with public key cryptography from difference expansion," Signal Processing:Image Communication, vol. 39, pp. 226–233, 2015.

[23] X. Wu, J. Weng, and W. Yan, "Adopting secret sharingfor reversible data hiding in encrypted images," SignalProcessing, vol. 143, pp. 269 – 281, 2018.

[24] A. Shamir, "How to share a secret," Communications ofthe ACM, vol. 22, no. 11, pp. 612–613, 1979.