International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Lossless and Reversible Data Hiding in Asymmetric Cryptography

Prashant Gholve[1], H. A. Hingoliwala[2]

[1]M.E (Computer) Department of Computer Engineering, JayawantraoSawant College of Engineering, Pune, India.SavitribaiPhule Pune University, Pune, Maharashtra, India -411007

[2]M.E Prof.HOD, (Computer) Department of Computer Engineering, JayawantraoSawant College of Engineering, Pune, India. SavitribaiPhule Pune University, Pune, Maharashtra, India -411007

Abstract: ***This technology proposes a lossless, a reversible, and a combined data hiding schemes for cipher text images encrypted by public key cryptosystems with probabilistic and holomorphic properties. In the lossless scheme, the cipher text pixels are replaced with new values to embed the additional data into several LSB-planes of cipher text pixels by multiple layer wet paper coding. Then, the embedded data can be directly extracted from the encrypted domain and the data embedding operation does not affect the decryption of original plaintext image. In the reversible scheme, a pre-processing is employed to shrink the image histogram before image encryption, so that the modification on encrypted images for data embedding will not cause any pixel oversaturation in plaintext domain. Although a slight distortion is introduced, the embedded data can be extracted and the original image can be recovered from the directly decrypted image. Due to the compatibility between the lossless and reversible schemes, the data embedding operations in the two manners can be simultaneously performed in an encrypted image. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption.***

Keywords: reversible data hiding, lossless data hiding, image encryption

1. Introduction

Encryption and information hiding are two viable methods for information security. While the encryption procedures change over plaintext content into mixed up cipher text, the information concealing strategies insert extra information into spread media by presenting slight alterations. In some mutilation unsuitable situations, information concealing may be performed with a lossless or reversible way. In spite of the fact that the expressions "lossless" and "reversible" have a same which means in an arrangement of past references, we would recognize them in this work[3][4].

We say that information hiding technique is lossless if the display of cover signal containing installed information is same as that of unique cover despite the fact that the spread information have been adjusted for information inserting. For instance, the pixels with the most utilized shading as a part of a palette picture are doled out to some unused shading lists for conveying the extra information, and these files are diverted to the most utilized shading[12]. Thusly, despite the fact that the files of these pixels are modified, the genuine shades of the pixels are kept unaltered. Then again, we say an information concealing system is reversible if the first cover substance can be consummately recouped from the spread rendition containing installed information despite the fact that a slight bending has been presented in information implanting strategy. Various instruments, for example, distinction extension, histogram shift and losslesspressure, have been utilized to build up the reversible information concealing systems for computerized pictures. As of late, a few decent forecast methodologies and ideal move likelihood under payload-mutilation measure have been acquainted with enhance the execution of reversible information covering up.

2. Literature Survey

1) High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis
AUTHORS: N. A. Saleh, H. N. Boghdad.
As of late information inserting over pictures has drawn huge enthusiasm, utilizing either lossy or lossless strategies. Albeit lossy procedures can permit extensive concealing limit, host picture can't be recouped with high constancy. A few applications require careful recuperation of the host picture, i.e. in drug understanding information can be implanted without influencing the restorative picture. By and large lossless information concealing procedures experience the ill effects of restricted limit as the host picture ought to be kept in place. In this paper a lossless implanting strategy is proposed. In this method picture histograms are investigated to recognize the installing limit of diverse picture sorts. Histogram maxima and minima are utilized as a part of inserting limit estimation. The proposed method gives concealing limit that can reach up to half ofthe host picture size for pictures with expansive homochromatic districts (toons like).

2) Reversible Data Embedding Using a Difference Expansion
AUTHORS:M. Bellare, S. Keelveedhi, and T. Ristenpart
Current distinction extension (DE) installing systems perform one layer implanting in a distinction picture. They don't swing to the following contrast picture for another layer inserting unless the present distinction picture has no expandable contrasts cleared out. The conspicuous burden of these procedures is that picture quality may have been extremely debased even before the later layer implanting starts on the grounds that the past layer installing has spent every single expandable contrast, incorporating those with extensive extent. In light of whole number Haar wavelet

change, we propose another DE inserting calculation, which uses the flat and additionally vertical distinction pictures for information stowing away. We present a dynamical expandable distinction look and choice instrument. This system gives even opportunities to little contrasts in two distinction pictures and viably evades the circumstance that the biggest contrasts in the first contrast picture are spent while there is no opportunity to insert in little contrasts of the second distinction picture.

3) Reversible Data Hiding
AUTHORS: Ni, Y.-Q. Shi
Advanced watermarking, frequently alluded to as information covering up, has as of late been proposed as a promising procedure for data confirmation. Inferable from information stowing away, be that as it may, some changeless bending may happen and subsequently the first cover medium will most likely be unable to be turned around precisely even after the concealed information have been removed out. Taking after the arrangement of information pressure calculations, this sort of information concealing calculations can be alluded to as lossy information stowing away. It can be demonstrated that a large portion of the information concealing calculations reported in the writing are lossy. Here, let us analyze three noteworthy classes of information concealing calculation. With the most prominently used spread-range water-stamping procedures, either in DCT area [1] or piece 8x8 DCT space [2], round-off blunder and/or truncation mistake might occur amid information implanting. Subsequently, there is no real way to turn around the stago-media back to the first without twisting.

4) Lossless Generalized-LSB Data Embedding
AUTHORS: M. U. Celik, G. Sharma
We display a novel lossless (reversible) information installing method, which empowers the precise recuperation of the first host endless supply of the inserted data. A speculation of the understood slightest noteworthy piece(LSB) change is proposed as the information inserting strategy, which presents extra working focuses on the limit mutilation bend. Lossless recuperation of the first is accomplished by packing segments of the sign that are helpless to implanting mutilation and transmitting these compacted portrayals as a piece of the installed payload. A forecast based restrictive entropy coder which uses unaltered parts of the host signal as side-data enhances the pressure productivity and, in this manner, the lossless information installing limit.

5) Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding
AUTHORS: X. Hu, W. Zhang, X. Li.
Forecast mistake extension - based reversible information concealing plans comprise of two stages. Initial, a sharp expectation blunder histogram is produced by using pixel forecast methodologies. Second, mystery messages are reversibly implanted into the expectation blunders through growing and moving the PE histogram. Past PEE routines treat the two stages freely while they either concentrate on pixel expectation to get a sharp PE histogram, or go for histogram change to upgrade the implanting execution for a given PE histogram. This paper propose a pixel forecast technique taking into account the base rate measure for reversible information concealing, which builds up the consistency between the two stages basically. What's more, correspondingly, a novel improved histograms alteration plan is exhibited to surmise the ideal implanting execution on the produced PE arrangement. Analyses show that the proposed system beats the past condition of-craftsmanship partners essentially as far as both the forecast precision and the last installing execution.

3. Proposed System

- We say a data hiding method is reversible if the original cover content can be perfectly recovered from the cover version containing embedded data even though a slight distortion has been introduced in data embedding procedure. A number of mechanisms, such as difference expansion, histogram shift and lossless compression, have been employed to develop the reversible data hiding techniques for digital images.
- Recently, several good prediction approaches and optimal transition probability under payload-distortion criterion have been introduced to improve the performance of reversible data hiding.

4. Module Description

a) Lossless Data Hiding Scheme

- A lossless data hiding scheme for public-key-encrypted images is proposed. There are three parties in the scheme: an image provider, a data-hider, and a receiver.
- With a cryptosystem possessing probabilistic property, the image provider encrypts each pixel of the original plaintext image using the public key of the receiver, and a data-hider who does not know the original image can modify the ciphertext pixel-values to embed some additional data into the encrypted image by multi-layer wet paper coding under a condition that the decrypted values of new and original cipher-text pixel values must be same.
- When having the encrypted image containing the additional data, a receiver knowing the data hiding key may extract the embedded data, while a receiver with the private key of the cryptosystem may perform decryption to retrieve the original plaintext image.
- The embedded data can be extracted in the encrypted domain, and cannot be extracted after decryption since the decrypted image would be same as the original plaintext image due to the probabilistic property.

b) Reversible Data Hiding Scheme.

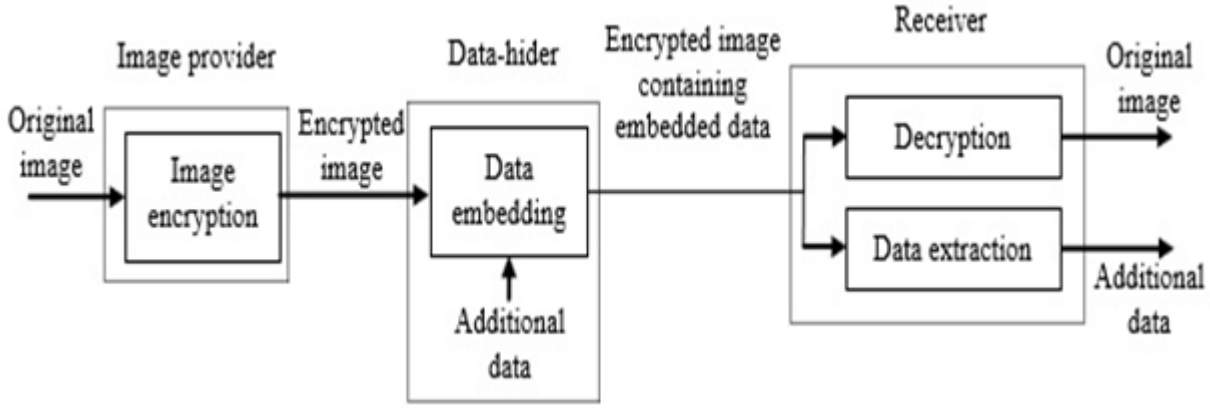
- This section proposes a reversible data hiding scheme for public-key-encrypted images. In the reversible scheme, a preprocessing is employed to shrink the image histogram, and then each pixel is encrypted with additive homomorphic cryptosystem by the image provider.
- When having the encrypted image, the data-hider modifies the ciphertext pixel values to embed a bit-sequence generated from the additional data and error-correction codes.

- Due to the homomorphic property, the modification in encrypted domain will result in slight increase/decrease on plaintext pixel values, implying that a decryption can be implemented to obtain an image similar to the original plaintext image on receiver side.
- Because of the histogram shrink before encryption, the data embedding operation does not cause any overflow/underflow in the directly decrypted image. Then, the original plaintext image can be recovered and the embedded additional data can be extracted from the directly decrypted image.

c) Combined Data Hiding Scheme.

- A lossless and a reversible data hiding schemes for public-key-encrypted images are proposed. In both of the two schemes, the data embedding operations are performed in encrypted domain.
- On the other hand, the data extraction procedures of the two schemes are very different. With the lossless scheme, data embedding does not affect the plaintext content and data extraction is also performed in encrypted domain.
- With the reversible scheme, there is slight distortion in directly decrypted image caused by dataembedding, and data extraction and image recovery must be performed in plaintext domain.
- That implies, on receiver side, the additional data embedded by the lossless scheme cannot be extracted after decryption, while the additional data embedded by the reversible scheme cannot extracted before decryption.
- In this section, we combine the lossless and reversible schemes to construct a new scheme, in which data extraction in either of the two domains is feasible

5. System Architecture



6. Conclusion

This work proposes a lossless, a reversible, and a combined information hiding plans for figure content pictures scrambled by open key cryptography with probabilistic and homomorphic properties. In the lossless plan, the ciphertext pixel qualities are supplanted with new values for installing the extra information into the LSB-planes of ciphertext pixels. Thusly, the installed information can be straightforwardly removed from the scrambled area, and the information implanting operation does not influence the unscrambling of unique plaintext picture. In the reversible plan, a preprocessing of histogram therapist is made before encryption, and a half of ciphertext pixel qualities are altered for information inserting. On beneficiary side, the extra information can be separated from the plaintext space, and, in spite of the fact that a slight twisting is presented in unscrambled picture, the first plaintext picture can be recuperated with no mistake. Because of the two's similarity plots, the information implanting operations of the lossless and the reversible plans can be all the while performed in a scrambled picture. In this way, the collector may remove a piece of installed information in the scrambled space, and concentrate another piece of inserted information and recoup the first plaintext picture in the plaintext area.

References

[1] N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, “High Capacity 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, 14(2), pp. 253–266, 2005.
[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.
[11] X. Zhang, "Reversible Data Hiding in Encrypted Image," IEEE Signal Processing Letters, 18(4), pp. 255−258, 2011.
[12] W. Hong, T.-S.Chen, and H.-Y. Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match," IEEE Signal Processing Letters, 19(4), pp. 199−202, 2012.
[13] J. Yu, G. Zhu, X. Li, and J. Yang, "An Improved Algorithm for Reversible Data Hiding in Encrypted Image," Proceeding of the 11th International Workshop on Digital-Forensics Watermark (IWDW 2012), Shanghai, China, Oct. 31-Nov. 02, 2012, Lecture Notes in Computer Science, 7809, pp. 358-367, 2013.
[14] W. Puech, M. Chaumont, and O. Strauss, "A Reversible Data Hiding Method for Encrypted Images," Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, Proc. SPIE, 6819, 2008.
[15] X. Zhang, "Separable Reversible Data Hiding in Encrypted Image," IEEE Trans. Information Forensics & Security, 7(2), pp. 526−532, 2012.
[16] Z. Qian, X. Zhang, and S. Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream," IEEE Trans. on Multimedia, 16(5), pp. 1486−1491, 2014.
[17] M. S. A. Karim, and K. Wong, "Universal Data Embedding in Encrypted Domain," Signal Processing, 94, pp. 174-182, 2014.
[18] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," IEEE Trans. Information Forensics & Security, 8(3), pp. 553-562, 2013.
[19] W. Zhang, K. Ma, and N. Yu, "Reversibility Improved Data Hiding in Encrypted Images," Signal Processing, 94, pp. 118-127, 2014.
[20] Y.-C. Chen, C.-W.Shiu, and G. Horng, "Encrypted Signal-Based Reversible Data Hiding with Public Key Cryptosystem," Journal of Visual Communication and Image Representation, 25, pp. 1164-1170, 2014.