ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

An Approach for Data Hiding In Encrypted Image Using Public Key Cryptography

Sonam S. Gavhande[1], Prof. Mr. B. K. Chaudhari

Department of Computer Engineering, Dr. V. B. Kolte College of Engineering, Maharashtra, India [1]

Asst. Professor, Dr. V. B. Kolte College of Engineering, Maharashtra, India [2]

ABSTRACT: This technology proposes a lossless, a reversible, and a combined information activity schemes for cipher text pictures encrypted by public key cryptosystems with probabilistic and polymorphic properties. within the lossless theme, the cipher text pixels square measure replaced with new values to implant the extra information into many LSB-planes of cipher text pixels by multiple layer wet paper committal to writing. Then, the embedded information may be directly extracted from the encrypted domain and also the information embedding operation doesn't have an effect on the secret writing of original plaintext image. within the reversible theme, a preprocessing is utilized to shrink the image bar graph before image coding, in order that the modification on encrypted pictures for information embedding won't cause any constituent oversaturation in plaintext domain. though a small distortion is introduced, the embedded information may be extracted and also the original image may be recovered from the directly decrypted image. as a result of the compatibility between the lossless and reversible schemes, the info embedding operations within the 2 manners may be at the same time performed in associate degree encrypted image. With the combined technique, a receiver could extract a region of embedded information before secret writing, and extract another a part of embedded information and recover the initial plaintext image when secret writing.

KEYWORDS: Reversible data hiding, lossless data hiding, Image encryption.

I. INTRODUCTION

Encryption data and knowledge and data concealment square measure 2 variable methodology for information security. Where as the coding procedures modification over plaintext content into required cipher text, info the knowledge the data concealing ways insert additional information into unfold media by presenting slight alterations. In some injury unsuitable things, data concealing could also be performed with a lossless or reversible means. In spite of the very fact that the expressions "lossless" and "reversible" have a same which suggests in an appointment of past references, we might acknowledge them during this work.

We say that data concealment technique is lossless if the show cowl of canopy signal containing put in data is same as that of distinctive cover despite the very fact that the unfold data are adjusted for data inserting. as an example, the pixels with the foremost utilised shading as a partial neighbourhood |an square measure district region locality vicinity section of a palette image are apportioned to some unused shading lists for convincing the additional data, and these files square measure entertained to the foremost utilised shading. Thusly, despite the very fact that the files of those pixels square measure changed, the real reminder the pixels square measure unbroken unreduced. Then again, we are saying associate degree data concealing system is reversible if the primary cowl substance may be consummately recouped from the unfold rendition containing put in data despite the very fact that a small bending has been given in data implanting strategy. varied instruments, for instance, distinction extension, bar chart shift and lossless pressure, are utilised to create up the reversible data concealing systems for computerised photos. As of late, many tight forecast methodologies and ideal move chance underneath payload-mutilation live are aware of enhance the execution of reversible data covering up.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

II. LITRATURE SURVEY

1]Title : High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis
Authors: N.A. Saleh. H. N. Bohdad.

Recently information embedding over pictures has drawn tremendous interest, exploitation either lossy or losslesstechniques. though lossy techniques will permit giant concealment capabili ty, host image can't be recovered with sound reproduction. Some applications need precise recovery of the host image, i.e. in drugs patient information is embedded while not poignant the medical image. generally lossless information concealment techniques suffer from restricted capability because the host image ought to be unbroken intact. during this paper a lossless embedding technique is projected. during this technique image histograms area unit analyzed to spot the embedding capability of various image sorts. bar graph maxima and minima area unit utilized in embedding capability estimation. The projected technique offers concealment capability which will reach up to five hundredth of the host image size for pictures with giant monochromatic regions (cartoons-like)

2]Title: Reversible Data Embedding Using a Difference Expansion
Authors: M. Bellare. S. Keelveedhi. And T. Ristenpart

Current distinction-expansion (DE) embedding techniques perform one layer embedding in an exceedingly difference image. they are doing not intercommunicate successive distinction image for an additional layer embedding unless the present distinction image has no expandable variations left. the apparent disadvantage of those techniques is that image quality could are severely degraded even before the later layer embedding begins as a result of the previous layer embedding has burnt up all expandable variations, as well as those with massive magnitude. supported whole number Hare moving ridge rework, we have a tendency to propose a replacement First Stated bedding formula, that utilizes the horizontal in addition as vertical distinction pictures for knowledge activity. we have a tendency to introduce a projectile expandable distinction search and choice mechanism. This mechanism provides even possibilities to little variations in 2 distinction pictures and effectively avoids the case that the biggest variations within the 1st distinction image are burnt up whereas there's nearly no probability to enter in little variations of the second distinction image.

3]Title: From Reversible Data Hiding
Authors: Ni, Y. –Q. Shi

Digital watermarking, typically noted as knowledge activity, has recently been planned as a promising technique for data assurance. attributable to knowledge activity, however, some permanent distortion might occur and thus the initial cowl medium might not be able to be reversed specifically even once the hidden knowledge are extracted out. Following the classification of information compression algorithms, this kind {of knowledge of knowledge of information} activity algorithms is noted as lossy data activity. It is shown that the majority of the information activity algorithms according within the literature area unit loss. Here, allow us to examine 3 major categories of information activity algorithmic program. With the foremost popularly utilized spread-spectrum water- marking techniques, either in DCT domain [1] or block 8x8 DCT domain [2], round- off error and or misestimating might happen throughout knowledge embedding. As a result, there's no thanks to reverse the stage-media back to the initial while not distortion.

4]Title: Lossless Generalized-LSB Data Embedding
Authors: M . U. Celik. G. Sharma

We gift a unique lossless (reversible) data-embedding technique, that allows the precise recovery of the initial host signal upon extraction of the embedded data. A generalization of the well-known least vital bit (LSB) modification is projected because the data-embedding methodology, that introduces further operative points on the capacity-distortion curve. lossless recovery of the initial is achieved by pressure parts of the signal that square measure liable to embedding distortion and transmission these compressed descriptions as a locality of the embedded payload. A prediction-based conditional entropy applied scientist that utilizes unchanged parts of the host signal as side-information improves the compression potency and, thus, the lossless data-embedding capability.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

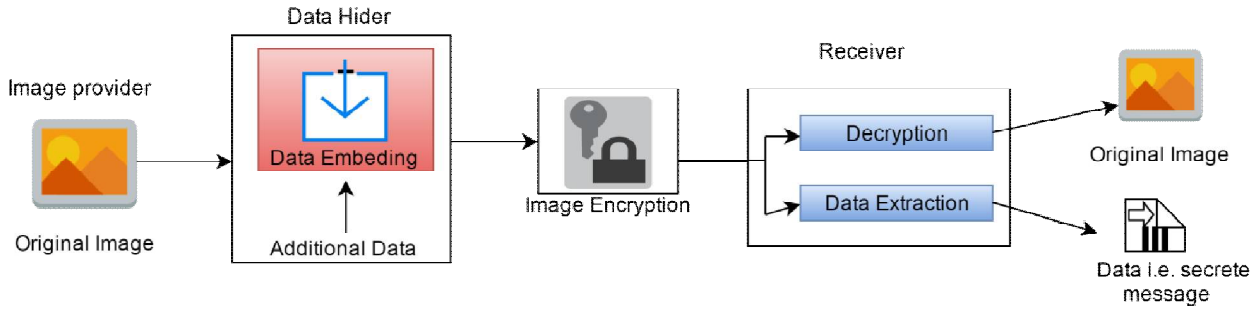
Vol. 4, Issue 10, October 2016

5]Title: Minimum Rate Prediction and optimized Histograms Modification for Reversible Data Hiding
Authors: X. Hu, W. Zhang, X.Li.

Prediction-error growth (PEE)-based reversible information concealing schemes incorporates 2 steps. First, a pointy prediction-error (PE) bar chart is generated by utilizing component prediction ways. Second, secret messages are reversibly embedded into the prediction-errors through increasing and shifting the letter bar chart. Previous letters ways treat the 2 steps severally whereas they either specialize in component prediction to get a pointy PE bar chart, or aim at bar chart modification to boost the embedding performance for a given letter bar chart. This paper propose a component prediction methodology supported the minimum rate criterion for reversible information concealing, that establishes the consistency between the 2 steps in essence. And correspondingly, a unique optimized histograms modification theme is conferred to approximate the optimum embedding performance on the generated letter sequence. Experiments demonstrate that the projected methodology outperforms the previous state-of-art counterparts considerably in terms of each the prediction accuracy and therefore the final embedding performance.

III. PROPOSED SYSTEM

We say information a knowledge| an information activity technique is reversible if the first cowl content will better recovered from the quilt version containing embedded information even supposing a small distortion has been introduced in data embedding procedure. variety of mechanisms, like distinction enlargement, bar graph shift and lossless compression, are used to develop the reversible information activity techniques for digital pictures. Recently, many smart prediction approaches and optimum transition chance beneath payload-distortion criterion are introduced to boost the performance of reversible information activity.



Advantages of Proposed System:

- We can perform comparison as well as data encryption back encryption back side of image.
- We can easily hide the large amount of data background of image.

IV. CONCLUSION

This work proposes a lossless, a reversible, and a combined data concealing plans for figure content foot age disorganized by open key cryptography with probabilistic and homomorphism properties. Within the lossless set up, the cipher text element qualities are supplanted with new values for putting in the additional data into the LSB-planes of cipher text pixels. Thus, the data put in may be squarely far from the disorganized space, and therefore the data implanting operation doesn't influence the unscrambling of distinctive plaintext image. Within the reversible set up, a preprocessing of bar graph healer is created before encoding, and a 1/2 cipher text element qualities are altered for data inserting. On beneficiary facet, the additional data may be separated from the plaintext area, and, in spite of the very fact that a small twisting is bestowed in unscrambled image, the primary plaintext image may be recuperated with no mistake. attributable to the two's similarity plots, the data implanting operations of the lossless and therefore the reversible plans may be all the whereas performed during a disorganized image. during this means, the collector could take away a bit of put in data within the disorganized area, and concentrate another piece of inserted data and recoup the primary plaintext image within the plaintext space.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

REFRENCES

[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.