International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Lossless and Reversible Combine Data Hiding using 4LSB in Encrypted Images with Asymmetric Cryptography

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

[1]M.E (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India.
Savitribai Phule Pune University, Pune, Maharashtra, India -411007

[2]Asst. Prof. HOD, Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India.
Savitribai Phule Pune University, Pune, Maharashtra, India -411007

Abstract: ***Abstract: This system proposes a lossless, a reversible, and a consolidated statistics hiding plans for determine content pix scrambled by means of open key cryptosystems with probabilistic and homomorphic houses. Inside the lossless plan, the discern content material pixels are supplanted with new values to install the greater records into some LSB-planes of parent content pixels by using making use of 4LSB. At that factor, the implanted records can be straightforwardly eliminated from the encoded place through utilizing blowfish calculation and the records putting process does not have an impact on the decoding of unique plaintext photo document. Inside the reversible method, a pre-getting ready is applied to percent the picture histogram before photo encryption, in order that the alteration on encoded pictures for statistics implanting does not bring about any pixel oversaturation in plaintext place. No matter the reality that a little bending is presented, the inserted records can be eliminated and the primary photograph report can be recuperated from the straightforwardly unscrambled image. Because of the similarity between the lossless and reversible technique, the information inserting bureaucracy inside the two behaviors may be on the identical time executed in an encoded picture. With the joined new manner, a beneficiary might separate a bit of inserted statistics earlier than interpreting, and concentrate different piece of established information of the document and recuperate the primary plaintext image after unscrambling.***

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

1. Introduction

Encryption and statistics hiding up are two appropriate strategies for records security. While the encryption techniques exchange over plaintext content into stirred up determine message, the data disguising tactics embed extra information into spread media through introducing mild adjustments. In some mutilation unsatisfactory circumstances, records disguising is probably finished with a lossless or reversible manner. No matter the manner that the expressions "lossless" and "reversible" have a same which implies in a plan of past references, we'd don't forget them in this paintings[3][4].

We say that records hiding method is lossless if the presentation of spread sign containing delivered information is equal as that of one in all a kind unfold no matter the manner that the unfold facts had been balanced for facts embedding's. As an instance, the pixels with the most used shading as part of a palette picture are doled out to a few unused shading facts for passing on the additional information, and these documents are redirected to the most used shading[12]. Subsequently, in spite of the way that the documents of these pixels are altered, the genuine sunglasses of the pixels are saved unaltered. However, we say a statistics canceling framework is reversible if the main unfold substance may be perfectly recovered from the unfold interpretation containing delivered information irrespective of the manner that a slight twisting has been exhibited in information embedding machine. Exclusive instruments, for example, refinement augmentation, histogram shift and lossless weight, were used to develop the reversible records hiding frameworks for modernized photos. Beginning overdue, multiple now not too horrific estimate techniques and best circulate possibility under payload-mutilation measure had been familiar with improve the execution of reversible records hiding [7][13].

2. Literature Review

1) High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis
AUTHORS: 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.
Descriptions: Recently data embedding over images has drawn tremendous interest, using either lossy or lossless techniques. Although lossy techniques can allow large hiding capacity, host image cannot be recovered with high fidelity. Some applications require exact recovery of the host image, i.e. in medicine patient data can be embedded without affecting the medical image. In general lossless data hiding techniques suffer from limited capacity as the host image should be kept intact. In this paper a lossless embedding technique is proposed. In this technique image histograms are analyzed to identify the embedding capacity of different image types. Histogram maxima and minima are used in embedding capacity estimation. The proposed technique gives hiding capacity that can reach up to 50% of the host image size for images with large homochromatic regions (cartoons-like)

2) Reversible Data Embedding Using a Difference Expansion

AUTHORS: J. Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Trans. on Circuits and Systems for Video Technology, 13(8), pp. 890−896, 2003.

Descriptions: Current difference-expansion (DE) embedding techniques perform one layer embedding in a difference image. They do not turn to the next difference image for another layer embedding unless the current difference image has no expandable differences left. The obvious disadvantage of these techniques is that image quality may have been severely degraded even before the later layer embedding begins because the previous layer embedding has used up all expandable differences, including those with large magnitude. Based on integer Haar wavelet transform, we propose a new DE embedding algorithm, which utilizes the horizontal as well as vertical difference images for data hiding. We introduce a dynamical expandable difference search and selection mechanism. This mechanism gives even chances to small differences in two difference images and effectively avoids the situation that the largest differences in the first difference image are used up while there is almost no chance to embed in small differences of the second difference image.

3) Reversible Data Hiding

AUTHORS: 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.

Descriptions: Digital watermarking, often referred to as data hiding, has recently been proposed as a promising technique for information assurance. Owing to data hiding, however, some permanent distortion may occur and hence the original cover medium may not be able to be reversed exactly even after the hidden data have been extracted out. Following the classification of data compression algorithms, this type of data hiding algorithms can be referred to as lossy data hiding. It can be shown that most of the data hiding algorithms reported in the literature are lossy. Here, let us examine three major classes of data hiding algorithm. With the most popularly utilized spread-spectrum water- marking techniques, either in DCT domain [1] or block 8x8 DCT domain [2], round- off error and/or truncation error may take place during data embedding. As a result, there is no way to reverse the stago-media back to the original without distortion.

4) Lossless Generalized-LSB Data Embedding

AUTHORS: 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.

Descriptions: We present a novel lossless (reversible) data-embedding technique, which enables the exact recovery of the original host signal upon extraction of the embedded information. A generalization of the well-known least significant bit (LSB) modification is proposed as the data-embedding method, which introduces additional operating points on the capacity-distortion curve. Lossless recovery of the original is achieved by compressing portions of the signal that are susceptible to embedding distortion and transmitting these compressed descriptions as a part of the embedded payload. A prediction-based conditional entropy coder who utilizes unaltered portions of the host signal as side-information improves the compression efficiency and, thus, the lossless data-embedding capacity.

5) Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding

AUTHORS: 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.

Descriptions: Prediction-error expansion (PEE)-based reversible data hiding schemes consists of two steps. First, a sharp prediction-error (PE) histogram is generated by utilizing pixel prediction strategies. Second, secret messages are reversibly embedded into the prediction-errors through expanding and shifting the PE histogram. Previous PEE methods treat the two steps independently while they either focus on pixel prediction to obtain a sharp PE histogram, or aim at histogram modification to enhance the embedding performance for a given PE histogram. This paper proposes a pixel prediction method based on the minimum rate criterion for reversible data hiding, which establishes the consistency between the two steps in essence. And correspondingly, a novel optimized histograms modification scheme is presented to approximate the optimal embedding performance on the generated PE sequence. Experiments demonstrate that the proposed method outperforms the previous state-of-art counterparts significantly in terms of both the prediction accuracy and the final embedding performance.

3. Proposed System

We say a data hiding strategy is reversible if the first cover substance can be impeccably recouped from the spread form containing implanted information despite the fact that a slight twisting has been presented in information inserting technique. Various components, for example, distinction extension, histogram shift and lossless pressure, have been utilized to build up the reversible information concealing procedures. So proposed methodology a combined data hiding schemes for cipher text images encrypted by public key cryptosystems with probabilistic and homomorphic properties. In the lossless scheme, the cipher text pixels are replaced with new values to embed the additional information into several LSB-planes of cipher text pixels by using 4LSB. Then, the embedded data can be directly extracted from the encrypted domain by using blowfish algorithm and the data embedding process does not affect the decryption of original plaintext image file. In the reversible procedure, a pre-handling is utilized to compress the image histogram before image encryption, so that the alteration on encoded image for information embedding does not create any pixel oversaturation in plaintext space. In spite of the fact that a little twisting is presented, the embedded information can be extracted and the first image record can be recover from the straightforwardly decrypted image. Because of the similarity between the lossless and reversible system, the information embedding forms in the two behaviour can be at the same time performed in a encrypted image. With the consolidated new system, a receiver might extricate a piece of embedded data before decoding, and extract other piece of

embedded data of the record and recover the first plaintext image after decryption.

4. Mathematical Model

Mathematical model of the proposed system
Consider, S = {A, IE, D, DE, DH, EI, E, EID, CEI, D, R}
A: Original Image,
IE: Encryption Key,
D: Data,
DE: Data Encryption Key,
DH: Data Hiding Key,
EI: Encrypted Image,
E: Encrypted Data,
EID: Encrypted image containing embedded encrypted data,
CEI: Compressed encrypted image containing embedded data,
D: Decrypted image,
R: Recovered Image.

Functions:
F1- This function is used for an image encryption.
F2- This function is used for data encryption.
F3- This function is used to embed encrypted data into encrypted image.
F4- This function is used for encrypted image compression containing embedded encrypted data.
F5- This function is used for encrypted image decompression containing embedded encrypted data.
F6- This function is used for an image decryption.
F7- This function is used for extraction of data and for the recovery of Image.
F8- This function is used for data decryption.
F9- This function is used for extraction of data.
F10- This function is used for data extraction directly and recovery of the image.

This proposed system includes functions that are given below:

1. Function F1 returns an encrypted image.
F1 (A, IE) → {EI}
Function F2 returns an encrypted data.
F2 (D, DE) → {E}
3. Function F3 returns an encrypted image containing embedded encrypted data.
F3 (EI, E, DH) → {EID}
4. Function 4 returns the compressed encrypted image containing embedded encrypted data.
F4 (EID) → {CEI}
5. Function 5 will decompress the compressed encrypted image containing embedded encrypted data and returns encrypted image containing embedded encrypted data.
F5 (CEI) → {EID}
6. Function 6 returns decrypted image.
F6 (EID, IE) → {D}
7. Function 7 returns the extracted encrypted data and recovered image.
F7 (D, DH, IE) → {E, R}
8. Function 8 returns the data which is similar to original data.
F8 (E, DE) → {D}
9. Function 9 returns the encrypted data.
F9 (EID, DH) → {E}
10. Function 10 returns the extracted encrypted data and recovered image.
F10 (EID, DH, IE) → {E, R}

5. System Architecture

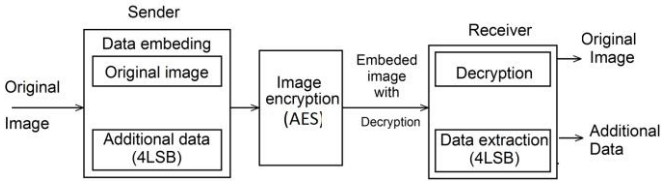


Figure 1: System Architecture

6. Algorithm

4LSB:
1) Each frame or image is made up of no of individual pixels. Each of these pixels in an image is made up of a string of bits the 4least significant bit of 8-bit true color image is used to hold 4-bit of our secret message image by simply overwriting the data that was already there.
2) In hiding process, the last 4 bits of image or frame pixel is replaced with 4 bits of our secret data.
3) For this secret data which is also sequence of bytes are broken down into set of 4 bits. To hide each character of secret message we need two pixels. So the number of characters that we can hide in (mx m) image is given by the following equation.
Total size of one frame ÷ 8 ----------(1)
4) Suppose size of a single frame is 160KB, then for 1LSB, maximum data that can be hidden is 1×20KB = 20KB. For 2LSB it is 2×20KB = 40KB. For 3LSB it is 3x20=60KB. For 4LSB it is 4×20KB =80KB. If steganographc process go beyond 4LSB, i.e. for 5LSB it is 5×20KB=100 KB, means that size of the data can be hide is more than 50%, hence it is look like visible watermarking.
5) For implementing steganography proposed method is using 4LSB algorithm. Any data change in least significant bit does not change the value of data significantly.

AES:
The AES-256 algorithm is composed of three main parts: Cipher, Inverse Cipher and Key Expansion. Cipher converts data to an unintelligible form called cipher text while Inverse Cipher converts data back into its original form called plaintext. Key Expansion generates a Key Schedule that is used in Cipher and Inverse Cipher procedure. Cipher and Inverse Cipher are composed of specific number of rounds for its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations:
1) Byte substitution using a substitution table (S-box)
2) Shifting rows of the State array by different offsets
3) Mixing the data within each column of the State array
4) Adding a Round Key to the State

The Cipher transformations can be inverted and then implemented in reverse order to produce a straightforward Inverse Cipher for the AES algorithm. The individual transformations used in the Inverse Cipher.

1) Inverse Shift Rows
2) Inverse Sub Bytes
3) Inverse Mix Columns
4) Add Round Key

The AES inverse cipher core consists of a key expansion module, a key reversal buffer, an initial permutation module, a round permutation module and a final permutation module. The key reversal buffer first store keys for all rounds and the presents them in reverse order to the rounds. The round permutation module will loop maternally to perform 14 iterations (for 256 bit keys).

7. Result Analysis

Here, Whole System taken many more attribute for the input purpose but here author mainly focuses on the Time and performance of system.

Expected Result:-

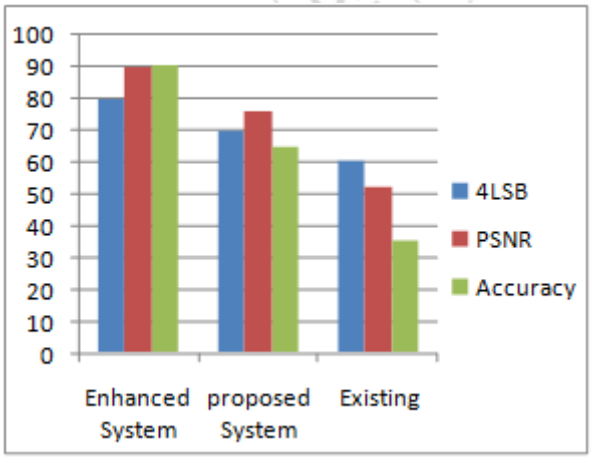
1. Compare Existing Vs. Proposed w.r.t Performance

Tabular Representation:

Table 1: Existing Vs. Proposed System

Methodology	4LSB	PSNR	Accuracy
Enhanced proposed System	80%	90%	90.6%
Proposed System	70%	76%	65%
Existing System	60.5%	52.5%	35%

2. Graphical Representation:



8. Conclusion and Future Work

This work proposes a lossless, a reversible and joined facts hiding preparations for figure content material photographs mixed via open key cryptography with probabilistic and homomorphic homes. Within the lossless association, the cipher textual content pixel characteristics are supplanted with new values for introducing the additional facts into the LSB-planes of cipher text pixels. In this way, the brought data can be in reality expelled from the blended variety, and the facts embedding operation does no longer impact the unscrambling of unique plaintext photograph. In the reversible arrangement, a preprocessing of histogram marketing consultant is made earlier than encryption, and a 1/2 of cipher textual content pixel qualities are adjusted for facts embedding's. On recipient side, the extra statistics can be remote from the plaintext space, and, disregarding the way that a slight contorting is delivered in unscrambled picture, the number one plaintext photograph can be recovered without errors. Because of the 2's comparability plots, the records embedding operations of the lossless and the reversible preparations can be at the same time carried out in a mixed picture. Along those traces, the authority may evacuate a chunk of introduced facts within the combined space, and awareness any other bit of embedded records and get better the main plaintext photograph within the plaintext region.

9. Future Scope

In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

References

[1] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography" IEEE Transactions on Circuits and Systems for Video Technology, 1051-8215 (c) 2015.
[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. 55−258, 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.

Author Profile

Mr. Prashant Gholve, M.E (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India - 411007

Mr. H.A.Hingoliwala, Asst. Prof. HOD, Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India - 411007