Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 5, May -2016

Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography

Abstract —*This technology proposes a lossless, a reversible, and a joined information hiding plans for ciphertext pictures scrambled by open key cryptosystems with probabilistic and holomorphic properties. In the lossless plan, the ciphertext pixels are supplanted with new values to insert the extra information into a few LSB-planes of ciphertext pixels by different 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 unique plaintext picture. In the reversible plan, a preprocessing is utilized to recoil the picture histogram before picture encryption, so that the change on encoded pictures for information implanting won t bring about any pixel oversaturation in plaintext area. Despite the fact that a slight twisting is presented, the inserted information can be extricated and the first picture can be recouped from the straightforwardly decrypted image. Because of the similarity between the lossless and reversible plans, the information implanting operations in the two conduct can be at the same time performed in an encoded picture. With the joined strategy, a recipient might separate a piece of inserted information before unscrambling, and concentrate another piece of installed information and recuperate the first plaintext picture after decoding.*

Keywords- *reversible data hiding, lossless data hiding, image encryption*

I. INTRODUCTION

Encryption and data hiding are two practical strategy for data security. While the encryption systems change over plaintext content into mixed up ciphertext, the data covering methodologies embed additional data into spread media by showing slight modifications. In some mutilation unacceptable circumstances, data covering might be performed with a lossless or reversible way. Notwithstanding the way that the expressions "lossless" and "reversible" have a same which implies in a plan of past references, we would remember them in this work.

We say that data hiding procedure is lossless if the presentation of spread sign containing introduced data is same as that of special spread regardless of the way that the spread data have been balanced for data embeddings. Case in point, the pixels with the most used shading as a part of a palette picture are doled out to some unused shading records for passing on the additional data, and these documents are occupied to the most used shading. In this way, in spite of the way that the documents of these pixels are adjusted, the bona fide shades of the pixels are kept unaltered. Of course, we say a data disguising framework is reversible if the principal spread substance can be perfectly recovered from the spread interpretation containing introduced data regardless of the way that a slight twisting has been displayed in data embedding procedure. Different instruments, for instance, qualification expansion, histogram shift and lossless weight, have been used to develop the reversible data hiding frameworks for modernized pictures. Starting late, a couple of not too bad gauge philosophies and perfect move probability under payload-mutilation measure have been familiar with upgrade the execution of reversible data hiding.

II. 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 which 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 consist 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 propose 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.

III. SURVEY OF PROPOSED SYSTEM

We say an data hiding technique is reversible if the first cover substance can be flawlessly recouped from the spread adaptation containing installed information despite the fact that a slight bending has been presented in information implanting system. Various components, for example, contrast extension, histogram shift and lossless pressure, have been utilized to add to the reversible information concealing methods for computerized pictures. As of late, a few decent forecast approaches and ideal move likelihood under payload-bending rule have been acquainted with enhance the execution of reversible data hiding.

IV. MODULES

1.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

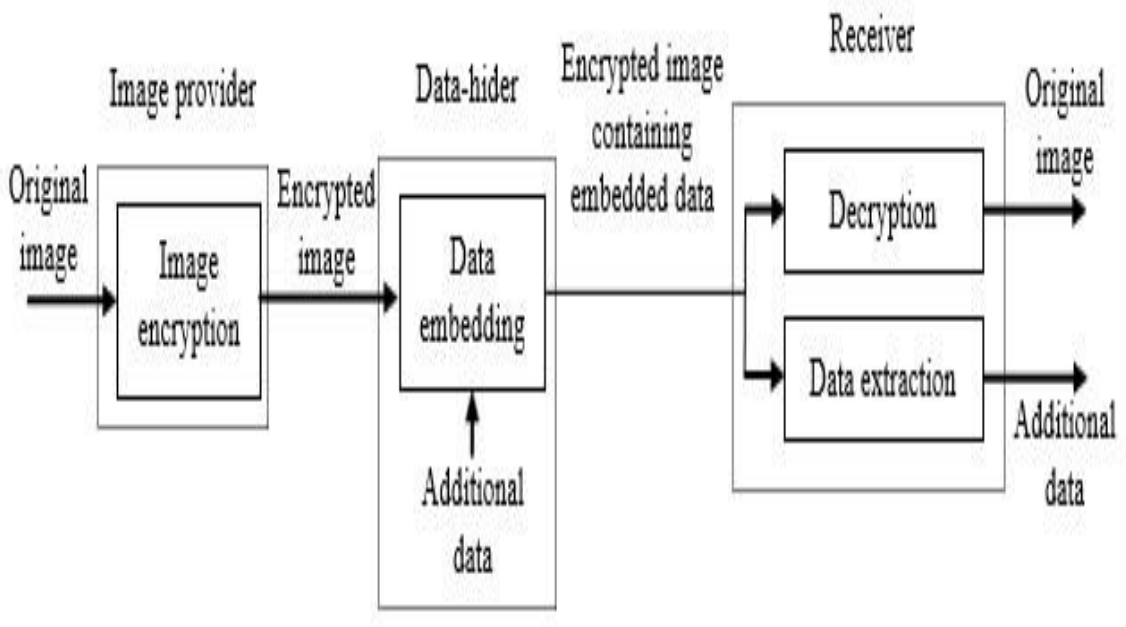
2.Reversible Data Hiding Scheme

- ✓ 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.

3. 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 data embedding, 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.

V. SYSTEM ARCHITECTURE



VI. Mathematical Model:

Mathematical model of the proposed system
Consider, S = {I, IEK, D, DEK, DHK, EI, ED, EID, CEID, DI, RI}
I: Original Image,
IEK: Encryption Key,
D: Data,
DEK: Data Encryption Key,
DHK: Data Hid ing Key,
EI: Encrypted Image,
ED: Encrypted Data,
EID: Encrypted image containing embedded encrypted data,
CEID: Compressed encrypted image containing embedded data,
DI: Decrypted image,
RI: Recovered Image.
Functions:
F1-It is a function is used to encrypt an image.
F2-It is a function is used to encrypt a data.
F3-This function will embed encrypted data into encrypted image.
F4-It is a function is used for compression of encrypted image containing embedded encrypted data.
F5-It is a function is used for decompression of encrypted image containing embedded encrypted data.
F6-It is a function used todecrypt an image.
F7-It is a function used to data extraction and Image recovery.
F8-It is a function used to decrypt a data.
F9-It is a function used for data extract ion.
F10-It is a function used to directly data extraction and image recovery.
This proposed system includes functions that are given below:
1.Function F1 returns an encrypted image.
F1 (I, IEK) → {EI}
2.Function F2 returns an encrypted data.
F2 (D, DEK) → {ED}
3.Function F3 returns an encrypted image containing embedded encrypted data.
F3 (EI,ED, DHK) → {EID}
4.Function 4 returns the compressed encrypted image containing embedded encrypted data.
F4 (EID) → {CEID}
5.Function 5 will deco mpress the compressed encrypted image containing embedded encrypted data and returns encrypted image containing embedded encrypted data.
F5 (CEID) → {EID}
6.Function 6 returns decrypted image.
F6 (EID, IEK) → {DI}
7.Function 7 returns the extracted encrypted data and recovered image.
F7 (DI, DHK, IEK) → {ED, RI}
8.Function 8 returns the data which is similar to original data.
F8 (ED, DEK) → {D}
9.Function 9 returns the encrypted data.
F9 (EID, DHK) → {ED}
10.Function 10 returns the extracted encrypted data and recovered image.
F10 (EID, DHK, IEK) → {ED, RI}

VI I. ALGORITHM

Blowfish Algorithm:

This algorithm has 16 rounds.

The input is a 64-bit data element, d.

1) Divide d into two 32-bit halves: d1, d2.

2) Then, for n = 1 to 16:
   d1 = d1 XOR Xn
   d2 = F (d1) XOR d2

3) Swap d1 and d2

4) After the sixteenth round, swap d1 and d2 again to undo the last swap.

5) Then, d2 = d2 XOR X17 and d1 = d1 XOR X18.

6) Finally, recombine d1 and d2 to get the cipher text.

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 colour 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 steganographic 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

VIII. CONCLUSION AND FUTURE WORK

This work proposes a lossless, a reversible, and a joined hiding plans for figure content pictures mixed by open key cryptography with probabilistic and homomorphic properties. In the lossless plan, the ciphertext pixel qualities are supplanted with new values for introducing the additional data into the LSB-planes of ciphertext pixels. Along these lines, the introduced data can be clearly expelled from the mixed region, and the data embedding operation does not impact the unscrambling of special plaintext picture. In the reversible arrangement, a preprocessing of histogram specialist is made before encryption, and a half of ciphertext pixel qualities are adjusted for data embeddings. On recipient side, the additional data can be isolated from the plaintext space, and, regardless of the way that a slight contorting is displayed in unscrambled picture, the main plaintext picture can be recovered with no oversight. In light of the two's comparability plots, the data embedding operations of the lossless and the reversible arrangements can be at the same time performed in a mixed picture. Along these lines, the authority might evacuate a bit of introduced data in the mixed space, and focus another bit of embedded data and recover the principal plaintext picture in the plaintext area.

IX. RESULT

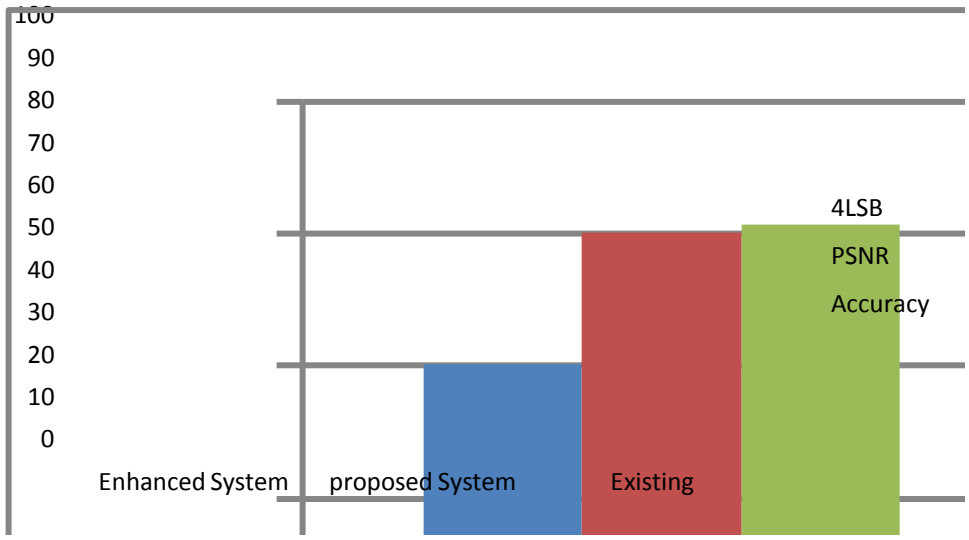
1. Compare Existing Vs Proposed w.r.t Performance

a. Tabular Representation:

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

Table 7.1 Existing Vs Proposed System

b. Graphical Representation:



X 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.

