IJMTARC – VOLUME – V – ISSUE - 19 – SEPT 2017 ISSN: 2320-1363

CRYPTOGRAPHY BASED LOSSLESS AND REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES

1.C H S KARTHI,2.Mrs A MAMATHA

[1]Pg Scholar,Department of ECE, DVR College of Engineering and Technology, Near IIT – HYD Permanent Campus, Ahead Of Patancheru, Kandi, Kashipur Village, Hyderabad, Telangana 502285

[2]Asst.Prof, Department of ECE, DVR College of Engineering and Technology, Near IIT – HYD Permanent Campus, Ahead Of Patancheru, Kandi, Kashipur Village, Hyderabad, Telangana 502285

ABSTRACT: For hiding secret data in digital images, large varieties of techniques are available, some are more complex than others. Public key cryptography has various useful applications and the technique employed depends on the requirements of the application to be designed for. Reversible data hiding is a type of data hiding techniques whereby the host image can be recovered exactly. Being lossless makes this technique suitable for medical and military applications. The ciphertext pixels are replaced with the additional data into new values to embed several ciphertext pixels by wet paper coding at multiple layer. From original image the embedded data can be extracted and the original image can be recovered from the decrypted image directly. The embedded data can directly be extracted from the encrypted domain. The decryption of original plaintext image doesn't affects data embedding operation. With the combined technique, before decryption a receiver may extract a part of embedded data, and recover the original plaintext image after decryption. A slight distortion is introduced due to the compatibility between the lossless and reversible schemes. The data embedding operations can be performed in the two manners simultaneously performed in an encrypted image and decrypted image

I. INTRODUCTION

1.1 PROJECT IDEA

Encryption and information hiding are two viable methods for information security. The ciphertext pixels are replaced with additional data as new values are embed into various LSB-planes at multi-layer wet paper coding. Then, embedded data is extracted directly from the encrypted domain, and the decryption of original plaintext image is not affected by the data embedding operation.

IJMTARC – VOLUME – V – ISSUE - 19 – SEPT 2017 ISSN: 2320-1363

While the encryption procedures change over plaintext content into mixed up ciphertext, the information concealing strategies insert extra information into spread media by presenting slight alterations. In some mutilation unsuitable situations, information concealing can be performed with a lossless or reversible way. In spite of the fact that the expressions "lossless" and "reversible" have same which means in an arrangement of past references, we would recognize them in this work. 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. 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 lossless pressure, 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.

1.2 MOTIVATION OF THE PROJECT

In Existing system there was problem of loss of data from the drawback of the existing system we got motivation.

1.3 LITERATURE SURVEY

High Capacity Lossless Data Embedding Technique for Palette Images Based on

Histogram Analysis: A lossless embedding technique is proposed as image histograms are analysed to identify the image types for different capacity. In embedding capacity estimation histogram maxima and minima techniques are used. Nowadays either lossy or lossless techniques are used for data embedding over images. Lossy techniques can allow large hiding capacity but host image cannot be recovered with high performance. In Some applications exact recovery of the host image is required, as in medical image patient data can be embedded without affecting actual image. The lossless data hiding techniques has to face from limited capacity as host image should kept personal. The proposed technique enables hiding capacity reaching up to 50% of host image. Reversible Data Embedding Using a Difference Expansion: Current difference-expansion (DE) embedding functions performs one layer embedding in difference image. Unless current difference image has no expandable differences left the expansion for another layer embedding do not turn to the next difference image. This technique has some disadvantages as image quality may have been severely degraded even before the later layer embedding begins. As the large magnitude of previous layer embedding has used up all expandable differences. We propose a new DE embedding algorithm based on integer Haar wavelet transform, which utilizes the vertical as well as horizontal difference images for data hiding. Here we have introduced a selection mechanism and dynamic expandable difference search. When there is almost no chance to embed in small differences of the second difference image this mechanism provides even chances to small differences in two difference images by which embedding effectively overcomes the situation where the largest differences in the first difference image are accepted. **REVERSIBLE DATA HIDING:**

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 spreadspectrum 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.

LOSSLESS GENERALIZED-LSB DATA EMBEDDING: We present a lossless data-embedding technique, where the exact recovery of the original host image signals upon extraction of the embedded information. As the data-embedding method a generalization of the well-known least significant bit (LSB) modification is proposed. Here Capacity-distortion curve introduces additional operating points. Signals that are used for embedding distortion can transmit compressed descriptions as part of the embedded payload and lossless recovery of the original is achieved by compressing portions. Unaltered portions of the host signal are utilized by prediction-based conditional entropy coder. Here Sideinformation improves the compression efficiency as well as the lossless data-embedding capacity. Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding: Prediction Error Expansion (PEE) reversible data hiding schemes consist of two steps. In First, pixel prediction strategies are utilized by a sharp prediction-error (PE) histogram. In Second, secret messages are reversibly embedded into the prediction-errors through expanding and thus shifting the PE histogram. PEE methods treat the two steps independently and they aim at histogram modification to

advance the embedding performance for a PE histogram or either focuses on pixel prediction to obtain a sharp PE histogram. Proposed a new pixel prediction method based on the minimum rate criterion which is used for reversible data hiding. This establishes the consistency between the two steps and optimal embedding performance on the generated PE sequence is optimized by histograms modification scheme. Both final embedding performance and prediction accuracy is demonstrated using previous state-of-art counterparts significantly.

II EXISTING SYSTEM

1) Data encryption using steganography

Steganography was getting used in earlier days to send the data to the receiver. The symmetric key is used by both sender and receiver to encrypt and decrypt the data. Disadvantage: As same key is used by both sender and receiver there was highly chances to decrypt the data by the unauthorized person.

2) Data security on the basis of cryptography Cryptography is the way to provide security to prevent the conversation between sender and receiver. It has two types as

1) Symmetric key cryptography

2) Asymmetric key cryptography Symmetric key Cryptography also called as Public key cryptography is better but some disadvantage in that system they are as follows

PROPOSED SYSTEM The system based on the public key cryptography has advantages over the existing system as it uses two separate keys for the encryption and decryption purpose. Both sender and receiver use the different keys where sender uses the public key and receiver uses the private key. As the sender has public key which is publically visible if third person want to know about the data , person will failed to find the data as it will get opened by the private key of the receiver.

IJMTARC – VOLUME – V – ISSUE - 19 – SEPT 2017 ISSN: 2320-1363

III. GOALS AND OBJECTIVES To propose a reversible, a lossless and a combined data hiding schemes with probabilistic and homomorphic properties for ciphertext images encrypted by public key cryptosystems.

IV. SCOPE

Future scope A lossless, a reversible, and a combined information hiding plans for figure content pictures scrambled by open key cryptography with homomorphic and probabilistic 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 pre-processing 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.

4.1 Detailed System Design of NLP Encryption and information hiding are two viable method for information security. While the encryption procedures change over plaintext content into mixed up ciphertext, 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 reversible or lossless 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. 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. 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 lossless pressure, 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.

4.2 Method project progress and algorithm

MODULES:

- Lossless Data Hiding Scheme
- Reversible Data Hiding Scheme
- Combined Data Hiding Scheme

MODULES DESCRIPTON:-

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.

IJMTARC – VOLUME – V – ISSUE - 19 – SEPT 2017 ISSN: 2320-1363

- 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

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 bitsequence generated from the additional data and errorcorrection 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

IJMTARC – VOLUME – V – ISSUE - 19 – SEPT 2017 ISSN: 2320-1363

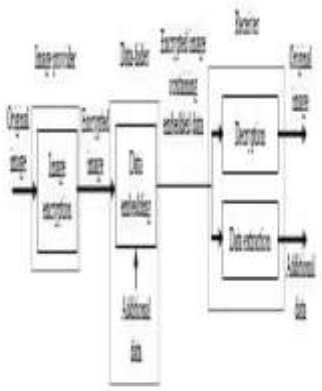
and the embedded additional data can be extracted from the directly decrypted image.

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.

V Architecture



CONCLUSION

An image retrieval system is presented by exploiting the ODBTC encoded data stream to construct the image features, namely Color Co-occurrence and Bit Pattern features. As documented in the experimental results, the proposed scheme can provide the best average precision rate compared to various former schemes in the literature. As a result, the proposed scheme can be considered as a very competitive candidate in color image retrieval application. For the further studies, the proposed image retrieval scheme can be applied to video retrieval. The video can be treated as sequence of image in which the proposed ODBTC indexing can be applied directly in this image sequence. The ODBTC indexing scheme can also be extended to another color space as opposed to the RGB triple space. Another feature can be added by extracting the ODBTC data stream, not only CCF and BPF, to enhance the retrieval performance. In the future possibilities, the system shall be able to bridge the gap between explicit knowledge semantic, image content, and also the subjective criteria in a

framework for humanoriented testing and assessment.

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

ISSN: 2320-1363

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.