Scientific Journal of Impact Factor (SJIF): 4.72

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

International Journal of Advance Engineering and Research Development

Volume 4, Issue 3, March -2017

An Information Security Technique Using Steganography

[1]Prof. A. N. Gedam, [2]Pooja Nehul, [3]Sushant Shinde, [4]Irshad Shaikh

[1,2,3,4] *Department of Computer Engineering, AISSMS's Polytechnic, Pune*

Abstract — *This technology proposes a lossless, a reversible, and a combined knowledge activity schemes for cipher text pictures encrypted by public key cryptosystems with probabilistic and holomorphic properties. Within the lossless theme, the cipher text pixels are replaced with new values to introduce the extra knowledge into many LSB-planes of cipher text pixels by multiple layer wet paper writing. Then, the embedded knowledge are often directly extracted from the encrypted domain and therefore the knowledge embedding operation doesn't have an effect on the secret writing of original plaintext image. Within the reversible theme, a preprocessing is used to shrink the image bar chart before image coding, so the modification on encrypted pictures for knowledge embedding won't cause any component oversaturation in plaintext domain. Though a small distortion is introduced, the embedded knowledge is often extracted and therefore the original image are often 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 are often at the same time performed in associate degree encrypted image. With the combined technique, a receiver could extract a neighborhood of embedded knowledge before secret writing, and extract another part of embedded knowledge and recover the first plaintext image when secret writing.*

Keywords: Image encryption, Lossless data hiding, Reversible data hiding, Public key encryption.

I. INTRODUCTION

Encryption and data hiding measure are two viable technique for information security. Whereas the encoding procedures modification over plaintext content into immersed cipher text, information concealing methods insert further information into unfold media by presenting slight alterations. In some accidental injury unsuitable things, data concealing is also performed with a lossless or reversible method. In spite of the actual fact that the expressions "lossless" and "reversible" have a same which suggests in a rendezvous of past references, we might acknowledge them during this work.
We say that data concealment technique is lossless if the display of cover signal containing installed data is same as that of distinctive cover despite the actual fact that the unfold data are adjusted for data inserting. as an example, 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 actual fact that the files of those pixels square measure changed, the real reminder the pixels square measure unbroken unaltered . Then again, we are saying Associate in Nursing data concealing system is reversible if the primary cowl substance is consummately recouped from the unfold rendition containing put in data despite the actual fact that a small bending has been conferred in data implanting strategy. Varied instruments, for instance, distinction extension, bar graph shift and lossless pressure, are used to create up the reversible data concealing systems for computerized photos. As of late, some tight forecast methodologies and ideal move probability below payload-mutilation live are familiar with enhance the execution of reversible data covering up.

II. LITERATURE SURVEY

1) High capability lossless information Embedding Technique for Palette pictures supported bar graph Analysis
AUTHORS: N. A. Saleh, H. N. Boghdad.
Recently information embedding over pictures has drawn tremendous interest, exploitation either lossy or lossless techniques. though lossy techniques will enable massive activity capability, host image can't be recovered with sound reproduction. Some applications need actual recovery of the host image, i.e. in drugs patient information is embedded while not poignant the medical image. normally lossless information activity techniques suffer from restricted capability because the host image ought to be unbroken intact. during this paper a lossless embedding technique is planned. during this technique image histograms area unit analyzed to spot the embedding capability of various image sorts. bar graph maxima and minima area unit employed in embedding capability estimation. The planned technique offers activity capability that may reach up to five hundredth of the host image size for pictures with massive monochromatic regions (cartoons-like)

2) Reversible information Embedding employing a distinction enlargement
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 address consequent distinction image for an additional layer embedding unless the present distinction image has no expandable variations left. the plain disadvantage of those techniques is that image quality might 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 number Haar rippling remodel, we have a tendency to propose a brand new American state embedding algorithmic rule, that utilizes the horizontal further as vertical distinction pictures for information activity. we have a tendency to introduce a impulsive expandable distinction search and choice mechanism. This mechanism offers even probabilities to tiny variations in 2 distinction pictures and effectively avoids matters that the most important variations within the 1st distinction image area unit burnt up whereas there's nearly no likelihood to insert in tiny variations of the second distinction image.

3.Reversible information activity

AUTHORS: metal, Y.-Q. Shi

Digital watermarking, usually named as information activity, has recently been planned as a promising technique for info assurance. due to information activity, however, some permanent distortion might occur and thus the first cowl medium might not be able to be reversed precisely even when the hidden information are extracted out. Following the classification of information compression algorithms, this sort of information activity algorithms is named as lossy data activity. It is shown that almost all of the info activity algorithms rumored within the literature area unit lossy. Here, allow us to examine 3 major categories of information activity algorithmic rule. With the foremost popularly utilised spread-spectrum water- marking techniques, either in DCT domain [1] or block 8x8 DCT domain [2], round- off error and/or misestimation might happen throughout information embedding. As a result, there's no thanks to reverse the stago-media back to the first while not distortion.

4.Lossless Generalized-LSB information Embedding

AUTHORS: M. U. Celik, G. Sharma

We gift a unique lossless (reversible) data-embedding technique, that allows the precise recovery of the first host signal upon extraction of the embedded info. A generalization of the well-known least important bit (LSB) modification is planned because the data-embedding methodology, that introduces extra in operation points on the capacity-distortion curve. lossless recovery of the first is achieved by pressure parts of the signal that area unit vulnerable to embedding distortion and sending these compressed descriptions as a vicinity of the embedded payload. A prediction-based conditional entropy software engineer that utilizes unedited parts of the host signal as side-information improves the compression potency and, thus, the lossless data-embedding capability.

5.Minimum Rate Prediction and Optimized Histograms Modification for Reversible information activity

AUTHORS: X. Hu, W. Zhang, X. Li.

Prediction-error enlargement (PEE)-based reversible information activity schemes accommodates 2 steps. First, a pointy prediction-error (PE) bar graph is generated by utilizing component prediction methods. Second, secret messages area unit reversibly embedded into the prediction-errors through increasing and shifting the alphabetic character bar graph. Previous alphabetic character E ways treat the two steps severally whereas they either specialize in component prediction to get a pointy PE bar graph, or aim at bar graph modification to reinforce the embedding performance for a given alphabetic character bar graph. This paper propose a component prediction methodology supported the minimum rate criterion for reversible information activity, 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 alphabetic character sequence. Experiments demonstrate that the planned methodology outperforms the previous state-of-art counterparts considerably in terms of each the prediction accuracy and therefore the final embedding performance.

III. EXISTING SYSTEM

Encryption and information concealment square measure two effective means that of knowledge protection. whereas the cryptography techniques convert plaintext content into unclear cipher text, the data hiding techniques enter extra data into cowl media by introducing slight modifications. In some distortion-unacceptable eventualities, information concealment is also performed with a lossless or reversible manner. Though the terms “lossless” and “reversible” have a Same which means in an exceedingly set of previous references, we might distinguish them during this work.

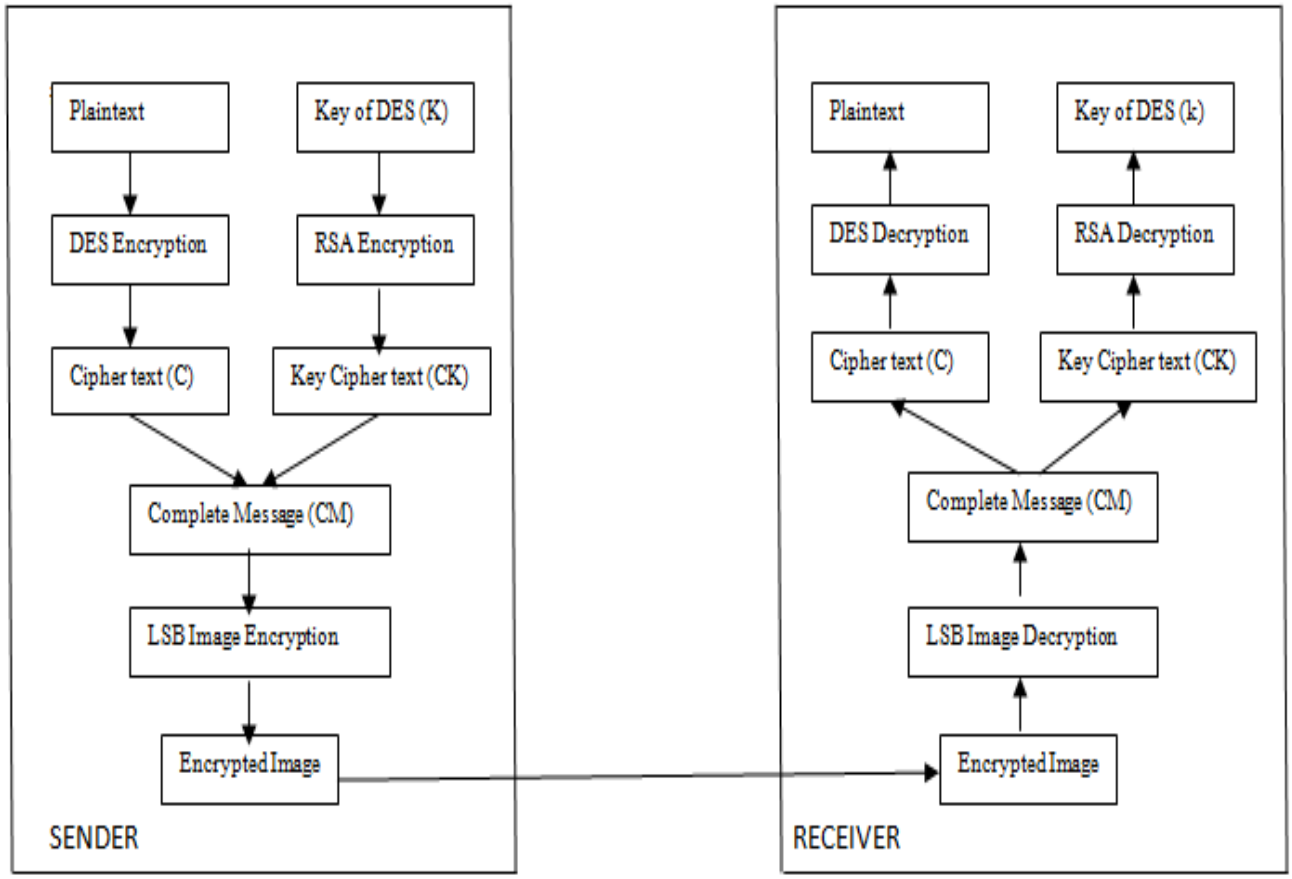

Fig:- Existing System

1) Data encryption using steganography:
Steganography was obtaining utilized in earlier days to send the information to the receiver. The regular secret's utilized by each sender and receiver to cipher and decode the information.
Disadvantage:
As same secret's utilized by each sender and receiver there were extremely possibilities to decode the information by the unauthorized person.
2) Knowledge security on the premise of cryptography
Cryptography is that the thanks to offer security to stop the spoken language between sender and receiver. it's 2 sorts as
1) Symmetric key cryptography
2) Asymmetric key cryptography

IV. PROPOSED SYSTEM

We say a data hiding methodology is reversible if the initial cowl content is absolutely recovered from the cover version containing embedded information albeit a small distortion has been introduced in data embedding procedure. Variety of mechanisms, like distinction enlargement, bar graph shift and lossless compression, are utilized to develop the reversible information concealing techniques for digital pictures. Recently, many sensible prediction approaches and optimum transition likelihood beneath payload-distortion criterion are introduced to boost the performance of reversible information concealing.

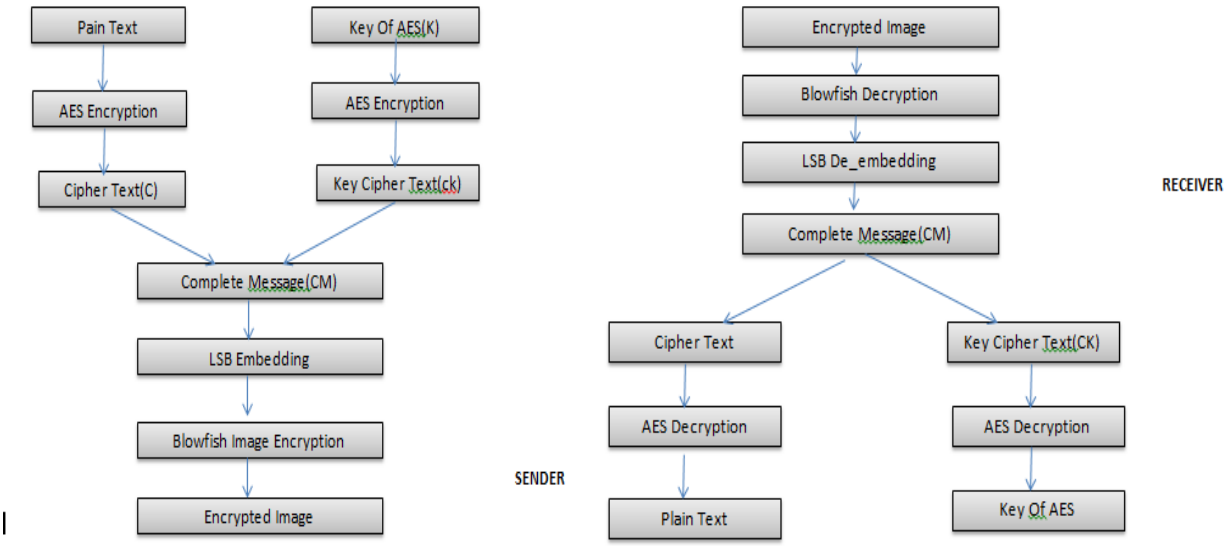

Fig:- Proposed System

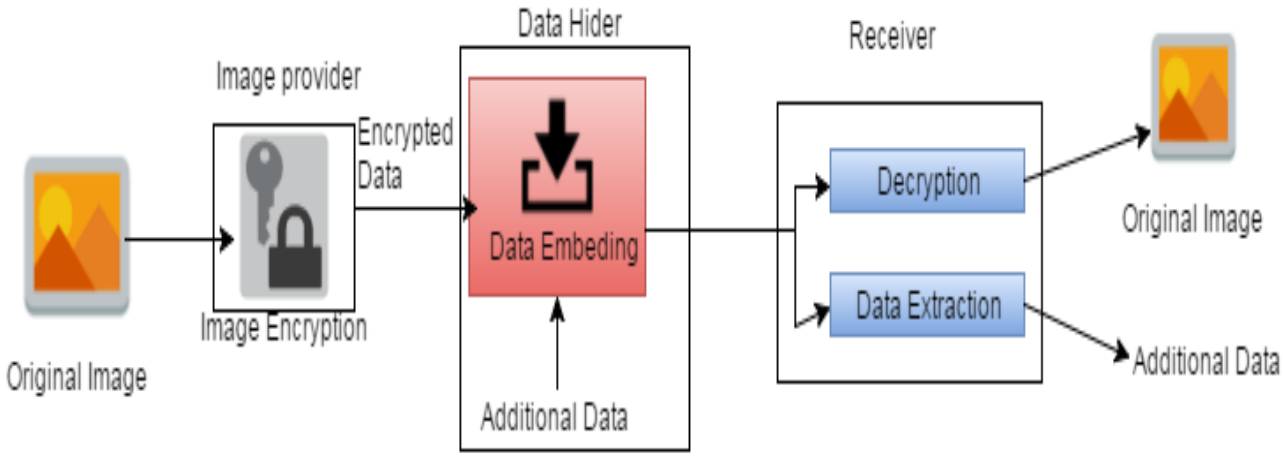

Figure1: System Architecture

V. Various Encryption Algorithm

A. Blowfish Algorithm

Blowfish has 16 rounds.
The input is a 64-bit data element, x.

1) Divide x into two 32-bit halves: xL, xR.
2) Then, for i = 1 to 16:
   xL = xL XOR Pi
   xR = F(xL) XOR xR
3) Swap xL and xR
4) After the sixteenth round, swap xL and xR again to undo the last swap.
5) Then, xR = xR XOR P17 and xL = xL XOR P18.
6) Finally, recombine xL and xR to get the ciphertext.

Blowfish Encryption Algorithm

Blowfish was designed in 1993 by Bruce Scheier as a fast, alternative to existing encryption algorithms such AES, DES and 3 DES etc.

Blowfish is a symmetric block encryption algorithm designed in consideration with,

- **Fast :** It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.
- **Compact:** It can run in less than 5K of memory.
- **Simple:** It uses addition, XOR, lookup table with 32-bit operands.
- **Secure:** The key length is variable ,it can be in the range of 32~448 bits: default 128 bits key length.
- It is suitable for applications where the key does not change often, like communication link or an automatic file encryptor.

B. Advanced Encryption Standard Algorithm (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 both 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).

C. Least Siginificant Bit Algorithm (LSB)

Today, when converting an analog image to digital format, we usually choose between three different ways of representing colors:

- 24-bit color: every pixel can have one in 2^24 colors, and these are represented as different quantities of three basic colors: red (R), green (G), blue (B), given by 8 bits (256 values) each.
- 8-bit color: every pixel can have one in 256 (2^8) colors, chosen from a palette, or a table of colors.
- 8-bit gray-scale: every pixel can have one in 256 (2^8) shades of gray.

LSB insertion modifies the LSBs of each color in 24-bit images, or the LSBs of the 8-bit value for 8-bit images.

VI. RESULT ANALYSIS

This data hiding system provides secret data at receiver side. In this system the sender sends the cipher text to the receiver. The proposed system should cover the data behind the image and a combined data hiding schemes for cipher text images encrypted. 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 multi-layer wet paper coding. Then, the embedded data should be directly extracted from the encrypted domain, and the data embedding operation should not affect the decryption of original plaintext image.

VII. CONCLUSION

This work proposes a lossless, a reversible, and a combined info concealing plans for figure content footage disorganized by open key cryptography with probabilistic and homomorphic properties. within the lossless arrange, the cipher text qualities are supplanted with new values for putting in the additional info into the LSB-planes of cipher text pixels. Thusly, the put in info is foursquare off from the disorganized space, and therefore the info implanting operation doesn't influence the unscrambling of distinctive plaintext image. Within the reversible arrange, a pre-processing of bar graph expert is formed before secret writing, and a half cipher text qualities are altered for info inserting. On beneficiary aspect, the additional info is separated from the plaintext area, and, in spite of the very fact that a small twisting is given in unscrambled image, the primary plaintext image is recuperated with no mistake. Attributable to the two's similarity plots, the data implanting operations of the lossless and therefore the reversible plans is all the whereas performed in a very disorganized image. during this method, the collector might take away a chunk of put in info within the disorganized area, and concentrate another piece of inserted info and recoup the primary plaintext image within the plaintext space.

VIII. REFRENCES

[1] Sandeep Singh, Aman Singh, "An Information Security Technique Using DES-RSA Hybrid and LSB," IJETCAS.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] X. Zhang, "Reversible Data Hiding with Optimal Value Transfer," IEEE Trans. on Multimedia, 15(2), 316−325, 2013.

[8] 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.

[9] 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.

[10] 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.

[11] X. Zhang, "Commutative Reversible Data Hiding and Encryption," Security and Communication Networks, 6, pp. 1396−1403, 2013.

[12] X. Zhang, "Reversible Data Hiding in Encrypted Image," IEEE Signal Processing Letters, 18(4), pp. 255−258, 2011.

[13] 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.

[14] 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.

[15] 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.

[16] X. Zhang, "Separable Reversible Data Hiding in Encrypted Image," IEEE Trans. Information Forensics & Security, 7(2), pp. 526–532, 2012.

[17] Z. Qian, X. Zhang, and S. Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream," IEEE Trans. on Multimedia, 16(5), pp. 1486–1491, 2014.

[18] M. S. A. Karim, and K. Wong, "Universal Data Embedding in Encrypted Domain," Signal Processing, 94, pp. 174-182, 2014.

