Scientific Journal of Impact Factor (SJIF): 5.71

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

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

Digital Water Marking

Shivani Patil[1], Yashashree Nimonkar[2],Sneha Madane[3], Archana Mahajan[4]

[1,2,3,4]*Department of Comp engineering, College of engineering*

ABSTRACT :- *Nowadays with the ease of transmission and distribution of multimedia objects the chances of applying attacks on it has also increased. There is large number of techniques used for the secure communication of data. This paper introduces a new reversible data hiding algorithm in the encryption domain, but the main problem is that distortion at the time of data extraction. Reversible data hiding (rdh) 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, where the original content cannot be damaged. System integrates data hiding into the image encryption process to achieve different levels of access right and security. Nowadays, people show interests in hiding the secrete data in encrypted images such that both the cover images and secrete data can be protected. Both data extraction and image recovery will be formed without any error. The system is based on a hybrid algorithm that applies the techniques of encryption and data hiding to offer different security features to medical images. Results of computer comparisons demonstrate that the proposed algorithm can withstand the differential attack and outperforms other existing methods in terms of security and the message embedding capacity. The marked decrypted images of our proposed method show the best visual quality according to the psnr results.*

Keywords : *Reversible Data Hiding, Encryption, AES, LSB, PSNR, Ciphertext.*

I. INTRODUCTION

Information security consists of encryption and data hiding. Where in encryption plain text is converted into cipher text and in data hiding by doing some minor alteration the extra data is added in the original data or image. Data hiding is used in damaged situation with reversible manner and also doing without loss in data. In this paper we discuss the design, implementation and evaluation of data hiding and characteristics. Where Advanced encryption standard (AES) is used for encryption and for data hiding we are using Least significant bit algorithm (LSB). Where we can compress the data and large amount of data is hidden at the background of the image.

Here we say that data hiding is lossless because ,For example in an image the pixels with most shading part represent the image and the unused shading part are diverted to add the extra data in the respective image. Hence pixel files of that image are modified and the pixels representing the image are kept as it is no change is done within it. Hence the data hiding is lossless. Know again we also say that the data hiding is reversible because to build the reversible histogram shift lossless pressure , distinction extension has been used so the data hiding is the reversible.

This paper is as follows a brief overview of the related work and literature review is presented in section 2. Existing system are defined in section 3. LSB and AES techniques are describe in section 4. Proposed system is defined in section 5.and the last part of paper will present conclusion and future work in section 6.

II. LITRATURE SURVEY

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

Recently data embedding over images has drawn tremendous interest, using either loss-y or lossless techniques. Although loss-y 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] 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 a very difference image, they do not communicate subsequent distinction image for an additional layer embedding unless this distinction image has no expandable variations left. The apparent disadvantage of those techniques is that image quality are severely degraded even before the later layer embedding begins as a result of the previous layer embedding has dried-up all expandable

variations, together with those with massive magnitude. Supported whole number Haar rippling rework, we tend to propose a brand new DE embedding algorithmic rule, that utilizes the horizontal furthermore as vertical distinction pictures for knowledge activity. We tend to introduce a projectile expandable distinction search and choice mechanism. This mechanism offers even possibilities to tiny variations in 2 distinction pictures and effectively avoids the case that the biggest variations within the 1st distinction image are dried-up whereas there's virtually no likelihood to introduce in tiny variations of the second distinction image.

3] Title: Reversible Data Hiding
Authors: Ni, Y.-Q. Shi
The objective of this work is to mechanically generate a large variety of pictures for a specific object category (for ex-ample, penguin). A multi-modal approach using both text, meta information and visual options is employed to assemble several high-quality pictures from the online Candidate pictures area unit obtained by a text primarily based web-search querying on the article symbol (the word penguin).The web pages and therefore the pictures they contain area unit downloaded. The task is then to get rid of immaterial pictures and re-rank the rest. First, the photographs area unit re-ranked using a mathematician posterior figurer trained on the text close the image and data options (such because the image different tag, image title tag, and image filename). No visualizing formation is employed at this stage. Second, the top-rank damages area unit used as (noisy) coaching information and a SVM visual classifier is learnt to enhance the ranking more. The principal novelty is in combining text/meta-data and visual options so as to realize a very automatic ranking of the pictures.

III.EXISTING SYSTEM

- Encryption and data hiding are two effective means of data protection. While the encryption techniques convert plaintext content into unreadable cipher text, the data hiding techniques embed additional data into cover media by introducing slight modifications.
- In some distortion-unacceptable scenarios, data hiding may be performed with a lossless or reversible manner.
- Although the terms " lossless" and " reversible" have a same meaning in a set of previous references, we would distinguish them in this work

Disadvantages of Existing System:

- Third user can easily identify the data where is encrypted.
- Once we perform encryption on image the size of image also increases.

IV. LSB TECHNIQUE

The LSB of a computer memory unit is replaced with associate degree M' s bit. this system works smart for image steganography.The Least vital Bit (LSB) is one among the most techniques in spatial domain image steganography. during this work, a replacement technique of LSB steganography has been projected that is associate degree temporary version of 1 bit LSB technique.
The LSB is that the lowest vital bit within the computer memory unit price of the image element.
The LSB based mostly image steganography embeds the key within the least vital bits of element values of the quilt image (CVR).

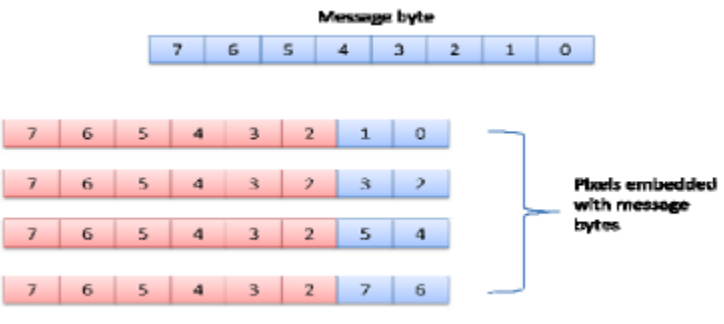


Figure 1: Proposed 4LSB Algorithm

In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB technique, just four bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same.

LSB algorithm hide information in the least significant bit of each color i.e. RGB of the carrier image. The problem states from the fact that modifying the three colors of a pixel produces a major distortion in the resulting color. So the one method that would introduce more efficiency and less distortion is Enhanced Least Significant Bit.Enhanced

LSB algorithm works in the spatial domain. It improves performance of LSB by hiding information in only one of the three colors that is blue color of the carrier image.

ALGORITHM

1. Select a cover image of size M*N as an input.
2. The message to be hidden is embedded in Blue component only of an image.
3. Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Enhanced Least Significant Bit (ELSB) of every pixel to hide information, leaving most significant bits(MSB).
4. After that Message is hidden using Bit Replacement method.

AES TECHNIQUE

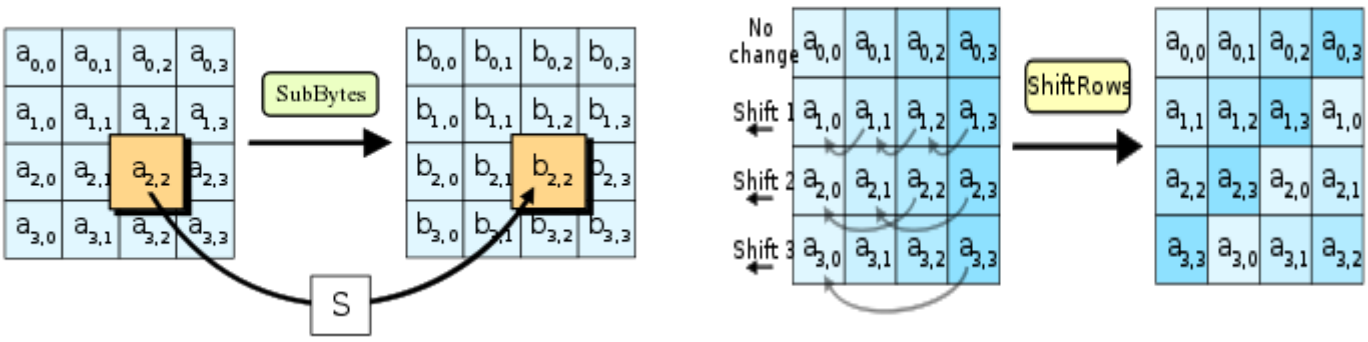
The Advanced Encryption Standard is a specification for encyption of electronic data.AES has a fixed block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.AES is a symmetric-key algorithm, it uses the same key for both encrypting and decrypting the data.AES is based on a design principle known as a substitution permutation network.AES operates on a 4 × 4 column-major order matrix of bytes termed as states. For instance,16 bytes are representated as:

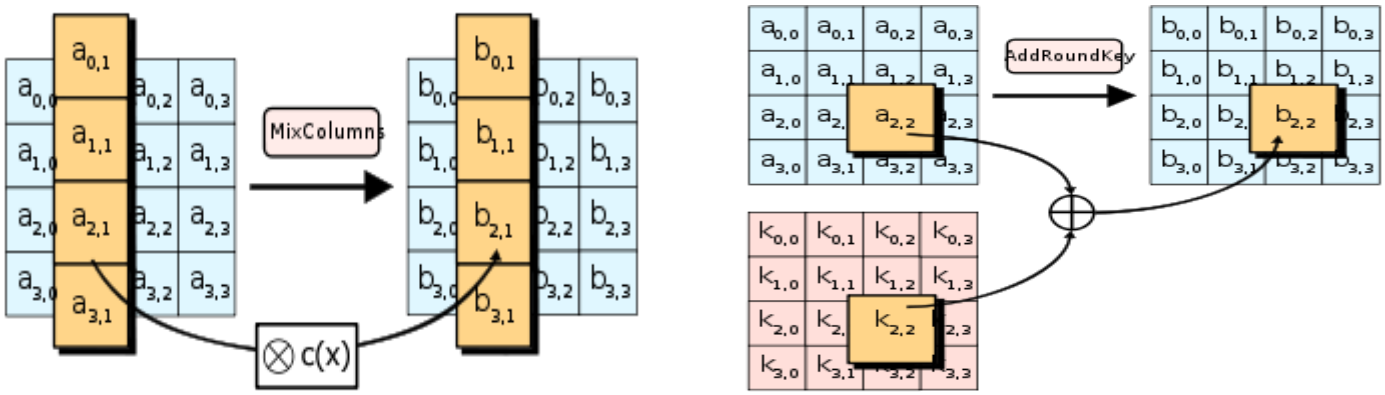
$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

ALGORITHM

1. Key Expansion: Round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial Round:
(i) Add Round Key: Each byte of the state is combined with a block of the round key using
using bitwise xor.
3. Rounds:
(i) Sub Bytes: A non-linear substitution step where each byte is replaced with another according to a lookup table.
(ii) Shift Rows: A transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
(iii) Mix Columns: A mixing operation which operates on the columns of the state, combining the four bytes in each column.
(iv) Add Round Key

4. Final Round (no Mix Columns):
(i) Sub Bytes
(ii) Shift Rows
(iii) Add Round Key.





V. PROPOSED SYSTEM

We say information knowledge concealing technique is reversible if the initial cowl content may be absolutely recovered from the quilt version containing embedded information although a small distortion has been introduced in data embedding procedure. Variety of mechanisms, like distinction enlargement, bar chart shift and lossless compression, are utilized to develop the reversible information concealing techniques for digital pictures. Recently, many smart prediction approaches and best transition likelihood below payload-distortion criterion are introduced to enhance the performance of reversible information concealing.

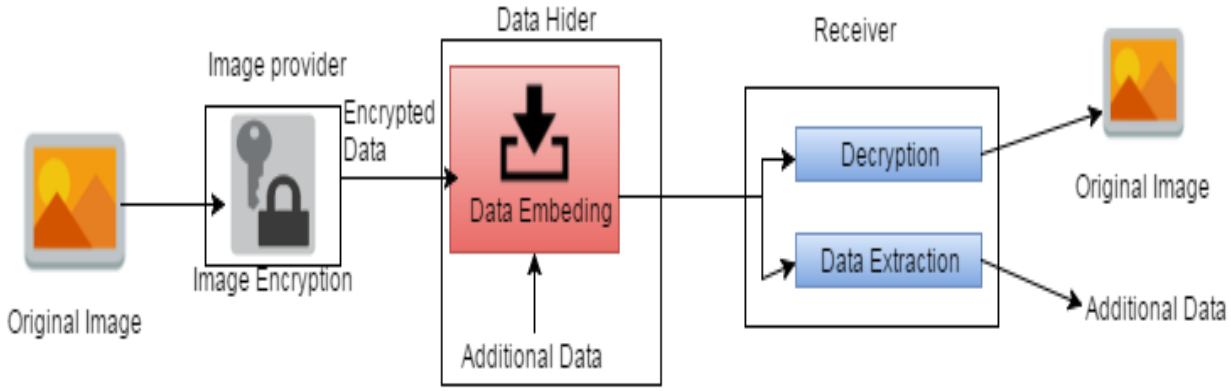


Fig.1 Architecture of proposed System

Advantages of Proposed System:

- We can perform comp ration as well as data encryption on back side of image.
- We can easily hide the large amount of data in background of image.

VI. CONCLUSION

This work proposes a lossless, a reversible, and a combined data concealment devices for figure content footage disorganized by open key cryptography with probabilistic and holomorphic merchandise. Within the lossless set up, the cipher text constituent skills area unit replaced with new values for putting in the additional data into the LSB-planes of cipher text pixels. Thusly, the put in data may be brazenly off from the disorganized space, and also the data planting operation doesn't influence the unscrambling of distinctive plaintext image. Within the reversible set up, a pre-processing of bar chart expert is formed before coding, and a half cipher text constituent skills area unit 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 given in ordered picture; the primary plaintext image may be improved with no mistake. Attributable to the two's similarity plots, the data implanting tasks of the lossless and also the reversible plans may be all the whereas performed during a disorganized image. During this approach, the collector might take away a chunk of put in data within the disorganized area, and focus another section of inserted data and retrieve the primary plaintext image within the plaintext space.

REFRENCES

[1] Aura Conci, Andre Luiz Brazil, Simone Bacellar Leal Ferreira and Trueman MacHenri , AES Cryptography in Color Image Steganography by Genetic Algorithms, IEEE 2015.

[2] Zinia Sultana , Fatima Jannat , Sadman Sakib Saumik, Niloy Roy, Nishith Kumar Datta, Muhammad Nazrul Islam , " A New Approach to Hide Data in Color Image Using LSB Steganography Technique, 2017 3rd International Conference on Electrical Information and Communication Technology (EICT), 7-9 December 2017.

[3] Sofyane Ladgham Chikouche, Noureddine Chikouche, An Improved Approach for LSB-Based Image Steganography using AES Algorithm," The 5th International Conference on Electrical Engineering Boumerdes (ICEE-B) October 29-31, 2017.

[4] Nurhayati, Syukri Sayyid Ahmad ," Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Cryptographic Algorithm " .

[5] Miss. Chaitali. D. Raut, Data Hiding Technique in Video Using a Secrete Key , 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR' 16).

