International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 7 4437 - 4441

Novel Frame work for Improving Embedding Capacity of the System using Reversible Data Hiding Technique

Arti Yadav[1],
[1]PG Fellow, Department of Computer Engg.,G.H.R.C.E.M, Pune, India
Email:artydelhi07@gmail.com

Prof. Mrs. Minaxi Doorwar[2]
[2]Assistant Professor, Department of Computer of Engg., G.H.R.C.E.M, Pune, India
Email:minaxi.rawat@gmail.com

Abstract-Internet communication has become an essential part of infrastructure of today's world. The secret information communicated in various forms. Security of the secret information has been a challenge when the heavy amount of data is exchanged on the internet. A secure data transfer can be achieved by steganography and Cryptography. Steganography is a process of hiding the information into cover media while cryptography is the technique that encodes the message using encryption key. In this paper described the reversible data hiding concept. This maintains the property that recovered the original cover without loss of data while extracting the embedded message.

Keywords *– Steganography, Cryptography, Encryption, Data-Hiding*

*****

I. INTRODUCTION

Data protection is a major issue of concern while exchanging a data in an untrusted network, as internet is not only a single network but also it is worldwide collection of loosely connected network.Intruder can tackle information and make misuse of that or corrupt it or can say that unauthorised user can destroy the information if it is not fully secured.Steganography and Cryptography both plays a vitalrole in the area of data protection.

Steganography is data security tool which stores the secret information in cover media filein such a way that no one else except the sender of the information and the intended receiver can onlysuspect the existence of any sort of information.Cryptography is also an information security tool,
which provides encryption techniques to concel the
secret information.
A good data hiding technique shall include the following prerequisties:

[1] **Imperceptibility:** The difference between the stego medium and the original one must be very slight suchthat the unauthorized party cannot detect the embeddedinformation.
[2] **Security:** the unauthorized user cannot extract out thehidden information even if he has detected that thereare some information concealed in the stego medium.
[3] **Capacity:**How much of secret messagewhich can be embedded in the cover medium.?
[4] **Robustness:**The stego-cover medium shall be able toresist general image processing.
[5] The Advantages of BPCS-Steganography found by the experiments are as follows.
[6] The data-hiding capacity of a true color image is around 50% or else more than.
[7] A sharpening operation on the image increases thepayload capacity quite a bit.

1) Customization of a BPCS- It is most securedtechnique and provides high protection.
2) Randomization of the secret data performed by a compression operation that makes the embedded datamore intangible.

A. ***Reversible Data hiding:*** Reversible data hiding is the process of hiding the information in the cover image and extracted the embedded information exactly without loss of information. RDH method paid attention towards to the researcher because of no-degradation of the information while extracting embedded information. The effective use of reversible data hiding (RDH) with AES and BPCS. RDH method defined by different strategies such as lossless compression, Difference Expansion, Histogram shifting, Interger transform etc. Aim of all scheme to achieve high payload and low degradation when extracts the original cover medium.

Advatages of RDH:
1.) To accomplish real –reversiblity.
2.) Increase the payload capacity.
3.) Better protection.
4.) Better visual quality of image.

Problem Statement :
The reversible data hiding (RDH) in encrypted images, all previous methods embed data by reversibly vacating the room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration.All drawbacks overcome by the proposed system.The proposed system performed by reserving space for the encrypted data to hidein the cover image after that apply image encryption with the use of AES.The data hiding uses BPCS algorithm. It improves the hiding capacity with low distortion. It is easy

for the data hider to attain real-reversibility for extracting the embed datain the image.
This paper mainly focusedon datasecurity when takes place in communication.The following are the primary concern:

- Prevent form hacking.
- Achieve real reversibility.
- To provide the better security.
- Improve data embedding capacity and maintain quality.

II. Related Work

A. ***Title:*** *"Reversible data-Hiding in Encrypted Images by reserving Room before encryption".*

Author-: Kede Ma, Wei. Zhang, Xianfeng Zhao.
Summary-
Wei Zhang and Xianfeng Zhao have proposed the system that maintains the reversibility. This paper defines the reversible data hiding in encrypted image by using spare space as reserving room before encryption. Here more attention on RDH technique which maintains the reversibility that means original cover recovered after embedding additional data. It provides the security and confidentiality to user. It is new topic for cloud data management because of privacy-preserving requirements. The Existing System implemented by the use of the concept of RDH in encrypted images by vacant room before encryption, but proposed system was opposite of it in this we use the reserving concept before encryption. The advantages of this proposed system is to maintain the extra space for embedding data in data hider module. This system achieves excellent performance without any loss of data.

B. ***Title:*** *"Reversible data embedding using a difference expansion".*

Author: "J. Tian"
Summary-
J. Tian has proposed a system which uses difference expansion method for embedding data in reversible manner for digital images. Reversible data embedding means lossless embedding. Here quality degradation was very low after embedding the data. This paper describes how to measure the performance of the system by using the concept of reversible data embedding. This can be measure through various factors such as the payload capacity limit, visual quality and complexity. This system uses the differences between two neighbouring pixels. The LSB's of the differences areall zero and this embedded to the message. The benefits of the system are no loss of data while performing compression and decompression. This system is useful for audio and video data. The
drawbacks of the system are achieving error because of division by 2 and due to bit replacement visual quality degrade.

C. ***Title:*** *"Reversible data hiding".*

Author: "Z. Ni, Y. Shi, N. Ansari, and S. Wei".
Summary:
Z. Ni, Y. Shi, N. Ansari, and S. Wei, have proposed a system thatperform the Reversible Data hiding by using the histogram shiftoperation for RDH. In this system used the spare space forembedding the data by shifting the bins of gray scale values. The
embedding capacity measured by the use of number of pixels inpeak point. This system has some benefits such as it is simple andhas constant PSNR ratio, capacity is high and distortion is very
low. This system has some disadvantages such as more timeconsuming while searching the image number of times.

D. ***Title:*** *"Efficient reversible watermarking based errorexpansion and pixel selection".*

***Author*:** "X. L. Li, B. Yang, and T. Y. Zeng"
Summary:
X. L. Li, B. Yang, and T. Y. Zeng have used a hybrid algorithm. It Is basically uses three algorithms adaptive embedding, Predictive –Error Expansion (PEE) and Pixel selection. Predictive Error expansion is important for embedding the data and used for reversible watermarking. It provides authentication and integrity to the user. It also improves the payload with low distortion. Where distortion free data required we use the concept of watermarking. PEE is an improvement of the Difference Expansion (DE). The proposed system described the threshold value for pixel of image and it divides the image pixels into two parts. Afterward select the pixel on the basis of capacity parameter and threshold. Adaptive embedding and pixel selection performed simultaneously. This system reduces the embedding impact with the use of decreasing the modification and improves the visual quality. .

E. ***Title:*** *"Reversible image watermarking using interpolation"*

***Author*:** "L. Luo et al.".
***Summary*:**
L. Luo et al. have used an interpolation technique for reversible image watermarking. Reversible image watermarking restores the original image without any distortion after performing the extraction of hidden data. In this system we can embed large amount of covert data for imperceptible modification. Digital watermarking is the form of data hiding that are used to embed the covert information into digital signal. This paper based on adaptive interpolation-error expansion, which provides very low distortion rate and lager capacity. It also improves the image quality.

III. Previous Arts

Since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient, why still so obsessed to find novel RDH methods working directly for encrypted images? If reverse the order ofencryption and vacating room, i.e., reserving room prior to image encryption content owner side, the RDH tasks inencrypted images would be more natural and much easier which leads us to the novel framework, "reserving roombefore encryption (RRBE)".

 ISSN: 2321-8169
4437 - 4441

Actually, to construct the encrypted image, the first stage can be divided into three steps: image partition, self -reversible embedding followed by image encryption. At the beginning, image partition step divides original image into two parts and ; then, the LSBs of are reversibly embedded into with a standard RDH algorithm so that LSBs of can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version .

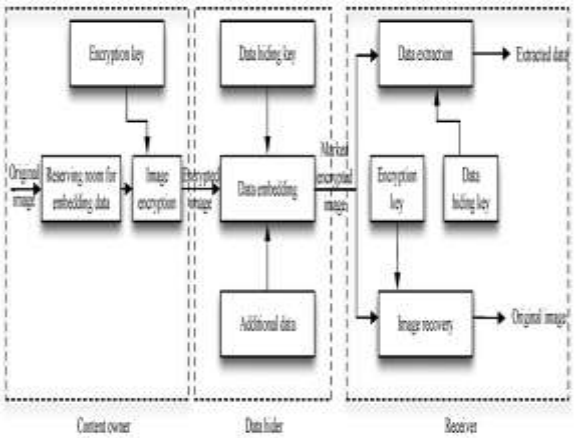

Figure 1 a) Existing system

IV. PROPOSED METHOD

In the proposed system Fig 1(b), the content owner first reserves the enough space on original image into its encryptedversion with encrypted key.

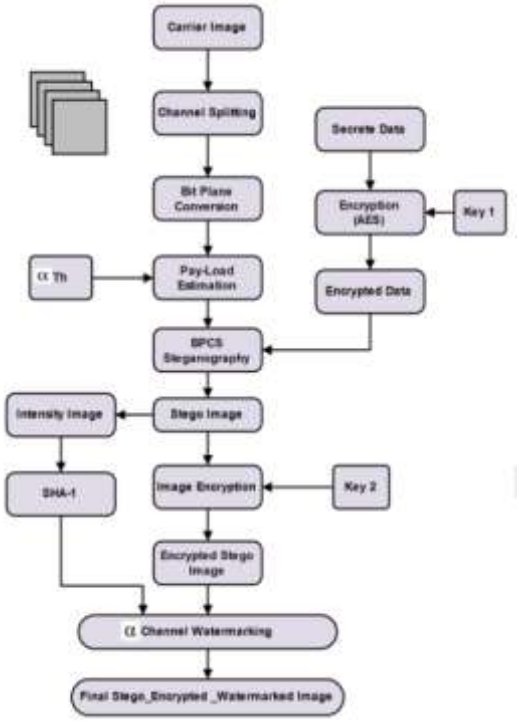

Figure 1 b) Proposed System Flow Diagram

Next the data is encrypted using AES algorithm and embedding process starts. The dataembedding process in encrypted images is inherently for the Data hider needs to accommodate into the sparse spaceprevious emptied out.On marked encrypted image apply the alpha –channel watermarking for integrity verification. The Data extraction and image recovery are identical to that of framework VRAE.

Next elaborate the practical framework which consists of following phases:

A. *Generation of Encrypted Data:*

Generate encrypted data by using the AES algorithm (128-bits key). The flowchart below explains the encryption and Decryption method of AES algorithm as shown in following figure 2:

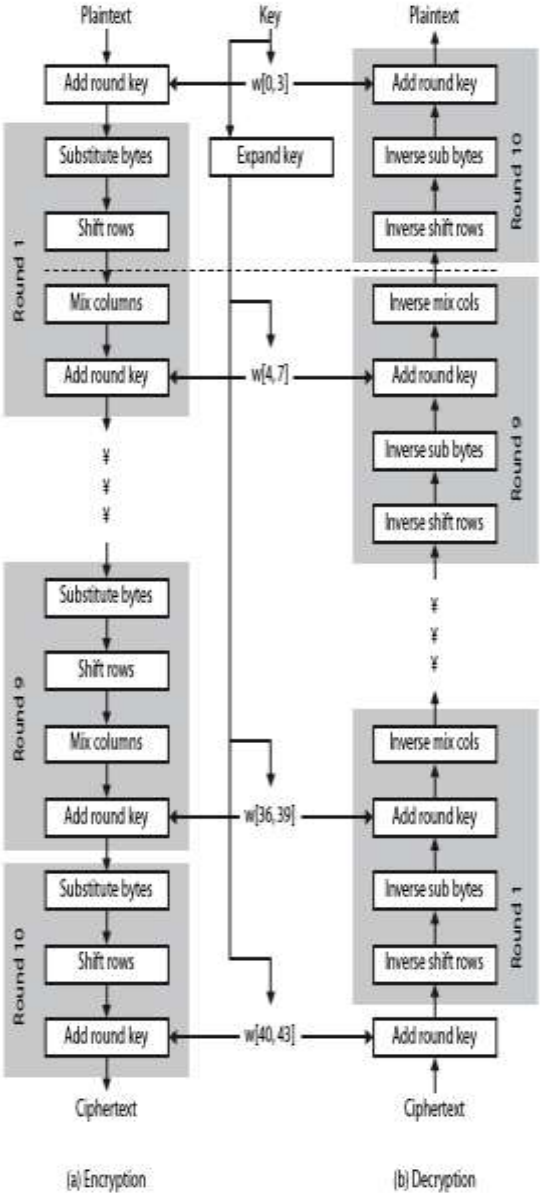

Figure2: Steps of AES algorithm

B. *Data Hiding:*

Once the data hider acquires the encrypted Data DE, embed into the cover image I by using the Bit Plan Complexity Segmentation (BPCS) algorithm.BPCS attempts to address the shortcomings of LSBinsertion by

searching an image for noise-likeregions. These regions are replaced with watermarkdata, while informative regions are undisturbed.The algorithm works as follows:

Step1. Convert a 2^m x 2^m N-bit/pixel image from natural binary into N-bit Gray Code.
Step2.Decompose the N-bit Gray code into N Single-bit planes. Each plane forms abinary image.
Step3.Divide each bit plane into 8x8 tiles.
Step4.For each tile, compute the complexity α.
Step5.If α is above a threshold, replace the tile with watermark data.
Step6.The bit-planes are recombined to form an N-bit channel in Gray code.
Step7.The Gray code is converted back to natural binary.

The complexity metric is defined as:
$\alpha = k/(2 \times 2^m \times (2^m - 1))$
where a tile has size 2^m x 2^m and k is the sum of xor-ing adjacent bits in a tile, both in the horizontal and vertical direction.
The valid range for $\boldsymbol{\alpha}$ is $0 < \boldsymbol{\alpha} < 1$.

C. Generation of Encrypted Images:

Image encrypted with the use of AES algorithm. It takes above mention steps for encryption in figure2.

D. Watermarking:

Watermarking checks the integrity of the image. If third party make changes in the original image then it prevent from this kind of modification.

E. Data Extraction /image recovery:

Data Extraction and image recovery perform by the receiver with the decryption algorithm.

V. Experimental Results

The proposed system tested on public images as seen figure 3.Consider 512 ×512×8 size of Lena, Baboon, Peppers images, while monarch image size is 768×512. Table1 and figure4 shows the available lossless data embedding capacity (in Bytes (x8 bits))obtained for various embedding strengths (levels).

TABLE1: LOSSLESS EMBEDDING CAPACITY (IN BYTES) VS. EMBEDDING LEVELS (L) AND AVERAGE PSNR(DB) AT FULL CAPACITY

Level(Bit Planes)	1	2	3	4	5	6	7	8
PSNR(dB)	55.9481	51.2295	45.0794	37.9948	34.1188	30.2271	28.0592	26.7270
Pepper	93732	187302	280603	371459	438350	465298	475354	478355
Lena	96480	180034	275369	361962	418363	445248	454942	458037
Baboon	96764	193524	290092	385225	474882	549954	597932	614340
Monarch	144423	289134	433277	506665	554876	574721	579865	580115

In Figure 4, see that the capacity of the proposed method depends largely on the characteristics of the cover image. Images with large smooth regions, e.g. peppers and Baboon accommodate higher capacities than images with irregular textures.

Figure 3: Test set of public figure images

The capacity of the scheme increases roughly linearly with numberof levels (or exponentially with number of bit-planes). This is dueto stronger correlation among more significant levels (bit-planes)of the image. The rate of the increase, however, is not constanteither among images or throughout the levels.
Note that the embedding capacities illustrated in Figure4.

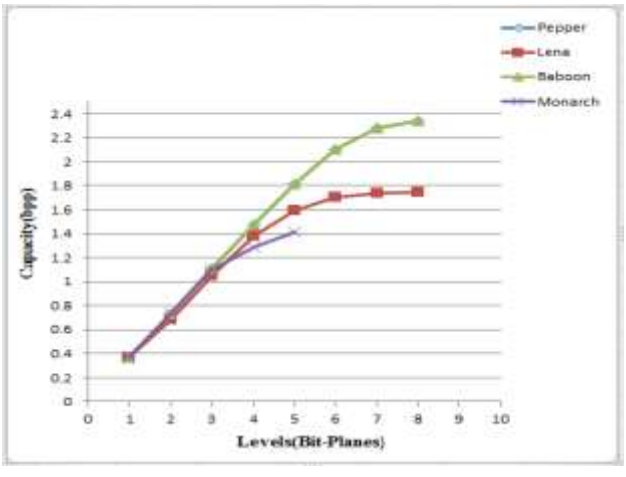

Figure 4: Capacity Vs Levels (Bit-Palnes) of allimages.

The higher embedding level implies significantly higher distortion in the stegano- image.

VI. CONCLUSION

Reversible Data hiding is new topic for providing privacy to the cloud data management. A novel lossless (reversible) data embedding (hiding) technique is presented. The technique provides high embedding capacities, allows complete recovery of the original host signal, and introducesonly a small distortion between the host and image bearingthe embedded data. The capacity of the scheme depends on thestatistics of the host image.

REFERENCES

[1] Kede Ma, Wei. Zhang, Xianfeng Zhao, "Reversible data Hiding in Encrypted Images by reserving Room before encryption", IEEE trans. On information forensics and security, vol,8 No.3 , march 2013.

[2] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding" Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354 [6] X. L. Li, B. Yang, and T. Y. Zeng, "on adaptive prediction-error expansion and pixel selection Image Process., vol. 20, no. 12, pp. 3524. Mar. 2006.

[3] Xiaolong Li, Weiming Zhang, Bo Ou and Bin Yang, "A brief review on reversible data hiding: current techniques and future prospects" IEEE Trans. ,2014

[4] 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, 2015.

[5] L. Luo et al., "Reversible image watermarking using interpolation ," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–G. Xuan, J. Chen, J. Zhu, Y.Q. Shi, Z. Ni, and W. Su, "Lossless Data hiding.

[6] Jiantao Zhou,Weiwei Sun, Li Dong, Xianming Liu, and Yuan Yan Tang,"Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation", IEEE Transactions on Circuits and Systems for Video Technology,2015.

[7] Wien Hong, Tung-Shou Chen, and Han-Yan Wu "An Improved Reversible Data Hiding in Encrypted Images Using Side Match" IEEE Signal Processing Letters , Vol. 19, NO. 4, April 2012

[8] Xinpeng Zhang,"Reversible Data Hiding in Encrypted Image", IEEE Signal Processing Leterrs, Vol. 18, No. 4, April 2011.

[9] Li,Di Xiao, Ayesha Kulsoom and Yushu Zhang "Improved reversible data hiding for encrypted images using full embedding strategy", Electronics Letters 30th April 2015 Vol. 51 No. 9 pp. 690–691.

[10] L. Luo et al., "Reversible image watermarking using interpolation ," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–G. Xuan, J. Chen, J. Zhu, Y.Q. Shi, Z. Ni, and W. Su, "Lossless Data hiding Mar2010.

[11] Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng, and Xiaojie Guo, "High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation", IEEE Trans. on cybernetics, 2