A Joint RDH and Lossless Secure Image and Text Transmission using Public key Cryptosystems

M.Jhansi Rani
Department of Electronics and Communication Engineering
Narayana Engineering College, Nellore, Andhra Pradesh,India.

Sk.Shaguftha
Assistant Professor, Dept of ECE
Narayana Engineering College, Nellore, Andhra Pradesh, India.

K.Murali
H.O.D of E.C.E
Narayana Engineering College, Nellore, Andhra Pradesh, India.

Abstract: The upcoming method is a proposal for information security with the help of lossless, reversible and combined data hiding schemes for cipher text images. These techniques are encrypted with a symmetric key cryptosystems by using homomorphism and probabilistic properties. We come across the presence of both lossless and reversible data hiding schemes. Our first scheme, the lossless scheme here cipher text pixels are over bound with a replacement of new values to cover the additional data. Many LSB plans are created from the additional data. This gives a convince to extract information from the encrypted data domain. This technique of extraction does not cause any damage at the decryption phase. To talk about our secondary scheme the reversible data hiding, before encryption there is stage of image shrinkage. This helps with modification, avoid pixel over saturation in plain text domain. We face a little distortion. We finally extract the original data along additional information. Both of these schemes are parallel performers due their compatibility. We recover the additional information at two stages once after and then once before the decryption.

Keywords— reversible data hiding, lossless data hiding, image encryption.

I.INTRODUCTION

Data hiding is a method of overlapping information into the original information. it is a valuable tool as its found in a various number of applications access control, annotation and authentication, multimedia, etc.. We tend to confuse data hiding with encryption though both methods achieve privacy [1]. Encryption is a conversion for data into a language which is visible but not understood. While data hiding converts the data into an invisible format. Lossless data hiding is a technique of embedding information inside an image and retrieval of the information without any damage to the original image. We use a display cover to embed the information over the original information. This helps to improve the privacy and enhances the security.

The reversible scheme is used to recover the original cover information, embedded into the image. This is mainly well known as it is applicable in providing intellectual authentication [3]. In most day to day application we all like the comforts of privacy and security during data transfers. Homomorphism helps avoid any distortions caused by image encryption and data embedding.

The previous explained schemes we avoid pixel separation and reorganization. But now we propose a method where their need not be any pixel separation or reorganization then we can concentrate purely on encryption and decryption. This brings down the computational complexity and also the rate of encrypted data. The presence of a probabilistic property in lossless scheme can access the encryption information directly and can give output in the original plane text information while the embedded data can be extracted in the encrypted domain.

II.PROPOSED METHOD

A.LOSSLESS DATA HIDING SCHEME:

In this section a lossless image for open-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 pixel of the aboriginal plaintext image application the accessible key of the receiver, and a data-hider who does not apperceive the aboriginal account can adapt the ciphertext pixel-qualities to admit some added advice into the accolade account by multi-layer wet paper coding beneath a action that the unscrambled estimations of new and different amount agreeable pixel ethics have to be same. While accepting the encoded account absolute the added information, a almsman alive the advice concealing key may abstracted the amid information, while a beneficiary with the key of the cryptosystem may accomplish decryption to retrieve the aboriginal plaintext-image. In other words, 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. That also means the data embedding does not affect the decryption of the plaintext image. The sketch of lossless data hiding scheme is shown in Figure 2.1.

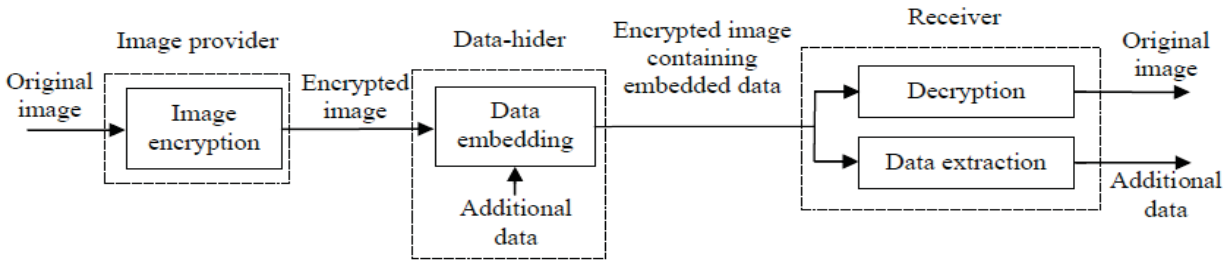

Figure 2.1: Sketch of lossless data hiding scheme for public-key encrypted images

B.REVERSIBLE DATA HIDING SCHEME:

This section proposes a reversible data hiding scheme for open-key-encrypted images. In the reversible plan, a preprocessing is utilized to recoil the picture histogram, and after that every pixel is scrambled with added substance homomorphic cryptosystem by the picture supplier [3]. While having the scrambled picture, the information hider alters the ciphertext pixel qualities to implant a bit-arrangement produced from the extra information and mistake revision codes. Because of the homomorphism property, the adjustment in encoded space will bring about slight expand/diminish on plaintext pixel values, suggesting that an unscrambling can be actualized to get a picture comparative to the original plaintext image on receiver side. In view of the histogram [5] shrink before encryption, the information installing operation does not bring on any flood/undercurrent in the specifically decoded picture. Then, the original plaintext image can be recovered and the embedded additional data can be extracted from the directly decrypted image. Note that the data-extraction and content-recovery of the reversible scheme are performed in plaintext domain, while the data extraction of the previous lossless scheme is performed in encrypted domain and the content recovery is needless. The sketch of reversible data hiding scheme is given in Figure 2.2.

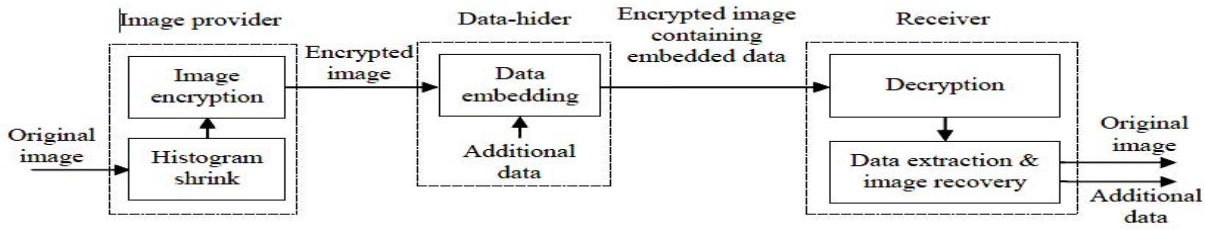

Figure 2.2: Sketch of Reversible data hiding Scheme

As described in Sections A and B, a lossless and a reversible data hiding schemes for public-key-encrypted images are proposed. In both of the two plans, the information implanting operations are performed in scrambled

space. Then again, the information extraction systems of the two plans are altogether different. With the lossless plan, information inserting does not influence the plaintext substance and information extraction is additionally performed in scrambled space. With the reversible plan, there is slight mutilation in specifically decoded picture brought about by information implanting, and information extraction and picture recuperation must be performed in plaintext space. That infers, on recipient side, the extra information inserted by the lossless plan can't be extricated after unscrambling, while the extra information implanted by the reversible plan can't separated before decoding. 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. That implies the extra information for different purposes might be implanted into an encoded picture, and a part of the extra information can be removed before decoding and another part can be extricated after unscrambling.

IMAGE ENCRYPTION: In this phase, the image provider encrypts a plaintext image application the accessible key of probabilistic cryptosystem p_k. For image pixel amount m(i, j) area (i, j) indicates the pixel position, the image provider calculates its ciphertext value,

$$c(i,j) = E[P_K, m(i,j), r(i,j)]$$

Where E is the encryption operation and r(i, j) is a accidental value. Then, the image provider collects the ciphertext ethics of all pixels to anatomy an encrypted image.

DATA EMBEDDING: When accepting the encrypted image, the data-hider may bury some added abstracts into it in a lossless manner [4]. The pixels in the encrypted image are reorganized as an arrangement according to the abstracts ambuscade key. For anniversary encrypted pixel, the data-hider selects a accidental accumulation r'(i, j) in Z*n and calculates. If Paillier cryptosystem is acclimated for image encryption, while the data-hider selects a accidental accumulation r'(i, j) in $Z^*_{n^{s+1}}$

$$c'(i,j) = c(i,j).\left(r'(i,j)\right)^{n^s} mode\, n^{s+1}$$

DATA EXTRACTION AND IMAGE DEDRYPTION: After accepting an encrypted image absolute the added data, if the receiver knows the data-hiding key, we may account the k-th LSB of encrypted pixels, and again abstract the anchored abstracts from the K LSB-layers application wet paper coding. On the added hand, if the receiver knows the unopen key of the acclimated cryptosystem, we may accomplish decryption to access the aboriginal plaintext image. When Paillier cryptosystem is used, Equation implies.

$$c(i,j) = g^{m(i,j)}.\left(r(i,j)\right)^{n} + \propto .n^2$$

HISTOGRAM SHRINK AND IMAGE ENCRYPTION: In the scheme, a picture accumulation δ aggregate by the angel provider, the data-hider and the receiver will be used. Denote the amount of pixels in the aboriginal plaintext angel with gray amount v as hv implying

$$\sum_{v=0}^{255} h_v = N$$

Where N is the amount of all pixels in the image. The image provider collects the pixels with gray ethics in [0, δ +1], and represent BS1.

$$l_1 \approx \sum_{v=0}^{\delta+1} h_v . \left[\frac{h_0}{\sum_{v=0}^{\delta+1} h_v}, \frac{h_1}{\sum_{v=0}^{\delta+1} h_v}, \ldots, \frac{h_{\delta+1}}{\sum_{v=0}^{\delta+1} h_v}\right]$$

IMAGE DECRYPTION, DATAEXTRACTOIN AND CONTENT RECOVERY: After accepting an encrypted angel absolute added data, the receiver firstly performs decryption application his protected key. We denote the decrypted pixels as m'(i, j). Due to the homomorphic property, the decrypted pixel ethics in Set A accommodated

$$m'(i,j) = \begin{cases} m_T(i,j) + \delta & , \text{ if the corresponding bit is 1} \\ m_T(i,j) - \delta & , \text{ if the corresponding bit is 0} \end{cases}$$

Then, the receiver with the data-hiding key can abstract the anchored abstracts from the anon decrypted image. He estimates the pixel ethics in Set A application their neighbors,

$$\bar{m}_T(i,j) = \frac{m_T(i-1,j)+m_T(i,j-1)+m_T(i+1,j)+m_T(i,j+1)}{4}$$

After retrieving the aboriginal coded bit-sequence and the anchored added data, the aboriginal plaintext angel may be added recovered. For the pixels in Set A are retrieved according to the coded bit-sequence

$$m_T(i,j) = \begin{cases} m'(i,j) - \delta & , \text{ if the corresponding bit is 1} \\ m'(i,j) + \delta & , \text{ if the corresponding bit is 1} \end{cases}$$

In the accumulated scheme, the image provider performs histogram [1] compress and image encryption as declared in Subsection. When accepting the encrypted image, the data-hider may bury the aboriginal allotment of added abstracts application the adjustment declared in Subsection. Denoting the ciphertext pixel ethics absolute the aboriginal allotment of added abstracts as c'(i, j), the data-hider calculates

$$c''(i,j) = c'(i,j) \cdot \left(r''(i,j)\right)^n mod\ n^2$$

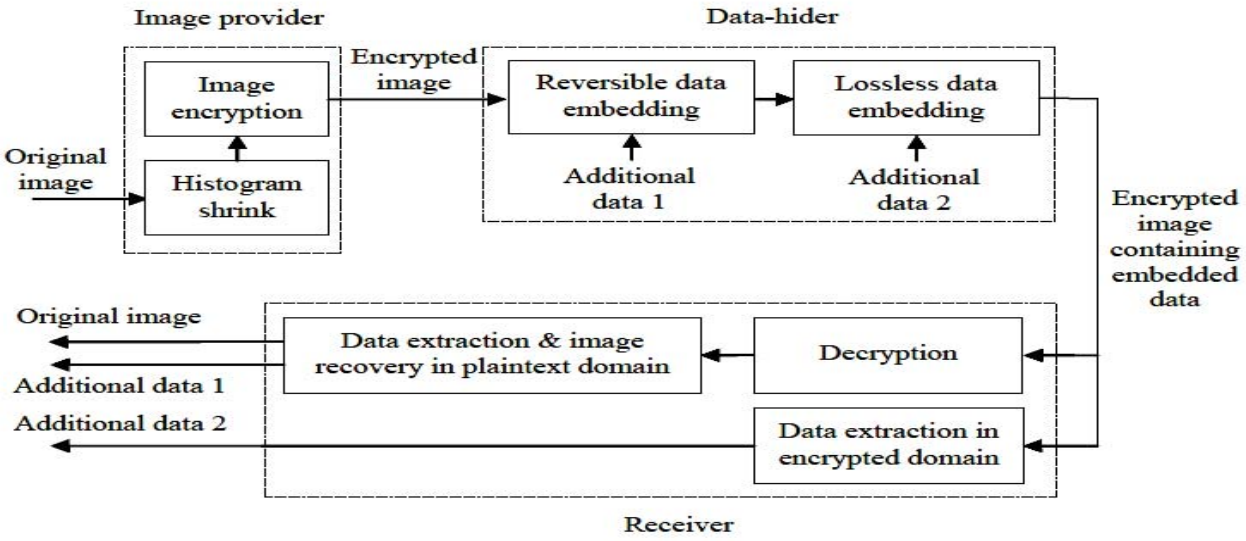

Figure 2.3: Sketch of Combined Scheme

III.RESULTS

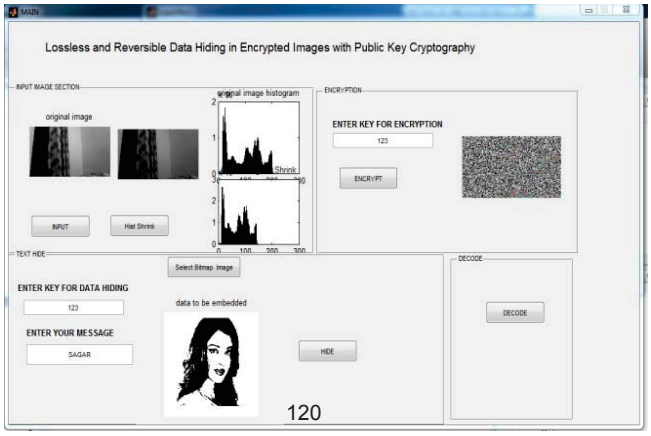

Figure 3.1:Propesed Implimentation at sender side

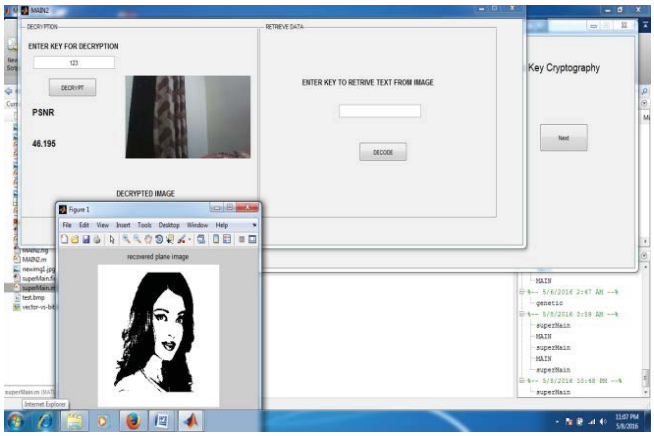

Figure 3.2: Receiver side Image Extraction

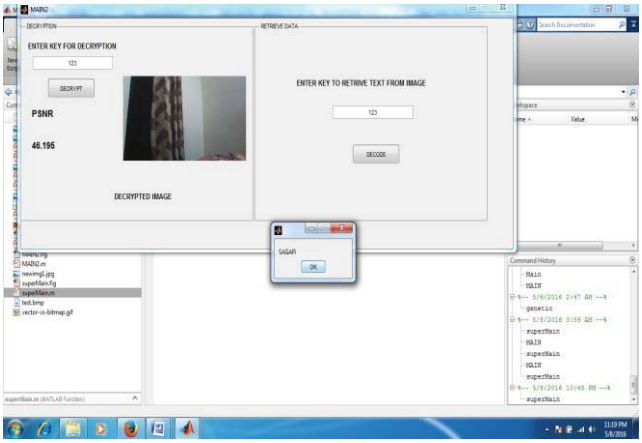

Figure 3.3:Reciver side Text message Extraction

IV.CONCLUSION

In this paper, we proposes a joint reversible data hiding, lossless secure image and text transmission schemes for images encrypted by accessible key cryptography In the lossless scheme, the ciphertext pixel values are replaced with new values for embedding the added abstracts into the LSB planes of ciphertext pixels. Here information can be extracted from the encrypted domain, and the abstracts embedding operation does not affect the decryption of aboriginal plaintext image. In the reversible scheme, a preprocessing of histogram compress is fabricated afore encryption, so information weight will abate or embedding accommodation will increase. On receiver side, the added abstracts can be extracted from the plaintext domain, and, although a slight change is alien in decrypted image, the aboriginal plaintext angel can be recovered after any error. Due to the affinity of the two schemes, the abstracts embedding operations of the lossless and the reversible schemes can be accompanying performed in an encrypted image.

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] Xinpeng Zhang,Jing Long,Zichi Wang, and Hang Cheng "Lossless and Reversible Data Hinding in Ecrypted Images with Public Key Cyptography" IEEE Trans on Circuits and Systems for VideoTechnology,pp.2015.