International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

A Novel Data Hiding in Color Images and Videos by Lossless and Reversible Techniques in Encrypted Domain with Public Key Cryptography

Virendra Kumar & Swati Verma

(M.E.) [1], (Assistant professor) [2]

[1,2]Shri Shankaracharya Technical campus (Shri Shankaracharya Group of Institution), Junwani, Bhilai, Chhattisgarh-490020,INDIA

[1]virendrakumar165@gmail.com swreet251088@gmail.com[2]

Abstract

The data embedded and extracted must be same for better data hiding technique. There should not be any loss and the security level should be high. Probabilistic and homomorphic properties based method is proposed for cryptography in encrypted domain using an integrated technique of two techniques as reversible and lossless. In this implementation mainly focus on the adding huge amount of data in image compared to existing state of art techniques. 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. This implementation gives embedded data may be encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. As there is addition of data two times there is more data addition takes place. As well as the image contains of the embedded data image should not vary.So; finally some parameters are calculated to know the embedding capacity and robustness of the system. In the reversible scheme, a preprocessing is employed to shrink the image histogram before image encryption, so that the modification on encrypted images for data embedding will not cause any pixel oversaturation in plaintext domain. Although a slight distortion is introduced, the embedded data can be extracted and the original image cans be recovered from the directly decrypted image. Due to the compatibility between the lossless and reversible schemes, the data embedding operations in the two manners can be simultaneously performed in an encrypted image. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption. Finally; there is application of the same embedding and extraction process for video as an extension method.

Keywords: *Reversible data hiding, lossless data hiding technique, cryptography, encryption, decryption, key encryption.*

I.INTRODUCTION

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.

We say a data hiding method is lossless if the display of cover signal containing embedded data is same as that of original cover even though the cover data have been modified for data embedding. For example, in [1], the pixels with the most used color in a palette image are assigned to some unused color indices for carrying the additional data, and these indices are redirected to the most used color. This way, although the indices of these pixels are altered, the actual colors of the pixels are kept unchanged. On the other hand, we say a data hiding method is reversible if the original cover content can be perfectly recovered from the cover version containing embedded data even though a slight distortion has been

introduced in data embedding procedure. A number of mechanisms, such as difference expansion [2], histogram shift [3] and lossless compression [4], have been employed to develop the reversible data hiding techniques for digital images. Recently, several good prediction approaches [5] and optimal transition probability under payload-distortion criterion [6, 7] have been introduced to improve the performance of reversible data hiding. Combination of data hiding and encryption has been studied in recent years. In some works, data hiding and encryption are jointed with a simple manner.

For example, a part of cover data is used for carrying additional data and the rest data are encrypted for privacy protection [8]. Alternatively, the additional data are embedded into a data space that is invariable to encryption operations. In another type of the works, data embedding is performed in encrypted domain, and an authorized receiver can recover the original plaintext cover image and extract the embedded data.

This technique is termed as reversible data hiding in encrypted images (RDHEI). In some scenarios, for securely sharing secret images, a content owner may encrypt the images before transmission, and an inferior assistant or a channel administrator hopes to append some additional messages, such as the origin information, image notations or authentication data, within the encrypted images though he does not know the image content. For example, when medical images have been encrypted for protecting the patient privacy, a database administrator may aim to embed the personal information into the corresponding encrypted images. Here, it may be hopeful that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side.

II. LITERATURE SURVEY

[1] Noura A. Saleh, Hoda N. Boghdady Recently data embedding over images has drawn tremendous interest, using either lossy or lossless techniques. Although lossy 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.

[2] Jun Tian , In this study a lossless data embedding technique for 256-color palletized images has been proposed. The embedding capacity is based on the image histogram and the number of unused colors. The stego image quality is not affected as the color values are the same, only used indices are changed. Histogram analysis is performed in order to understand the capacity potential of different image types. The unused colors in the palette have been used to optimize the embedding capacity. Capacity more than 30 and 50% of the host image size has been obtained for type-3 and type-1 images respectively.

[3] Mehmet UtkuCelik In this paper, we have presented a simple and efficient reversible date-embedding method for digital images. We explored the redundancy in the digital content to achieve reversibility. Both the payload capacity limit and the visual quality of embedded images are among the best in the literature.In implement prediction-based reversible steganographic scheme based on image in painting. In this scheme the reference pixels are adaptively selected according to the distribution characteristics of the content of the image. Image in painting based on partial differential equations is used to complete the prediction process by the reference pixels. The histogram prediction error is shifted to embed the secret bits reversibly. During the extraction procedure, the same reference pixel can be exploited to conduct the prediction, which guarantees the lossless recovery of the cover image.

[4] Xiaocheng Hu, WeimingZhang ,We present a novel lossless (reversible) data-embedding technique, which enables the exact recovery of the original host signal upon extraction of the embedded information. A generalization of the well-known least significant bit (LSB) modification is proposed as the data-embedding method, which introduces additional operating points on the capacity-distortion curve. Lossless recovery of the original is achieved by compressing portions of the signal that are susceptible to embedding distortion and transmitting these compressed descriptions as a part of the embedded payload.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

[5] Xinpeng Zhang,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 introduces only a small distortion between the host and image bearing the embedded data. The capacity of the scheme depends on the statistics of the host image.

According to the optimal value transfer matrix, the auxiliary information is generated and the estimation errors are modified. Also, the host image is divided into a number of subsets and the auxiliary information of a subset is always embedded into the estimation errors in the next subset.

private key of the cryptosystem may perform decryption to retrieve the original 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 1.

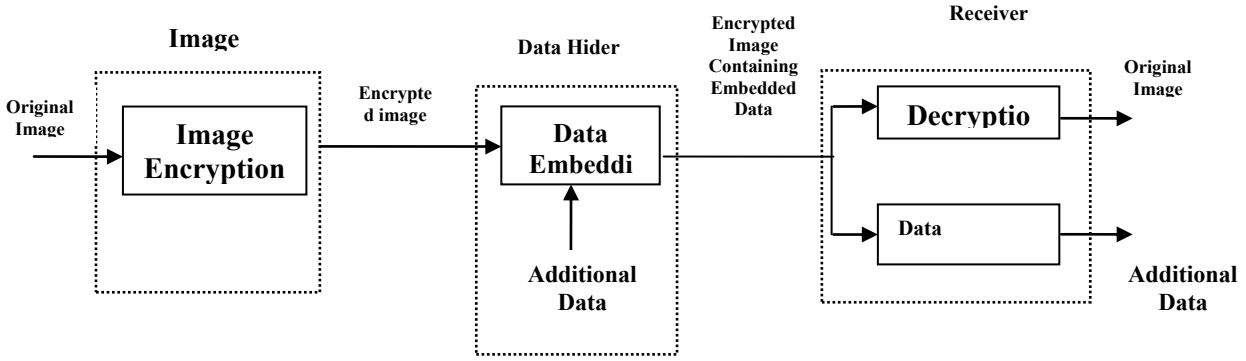

Fig1: Sketches of lossless data hiding scheme for public key encrypted image

III. LOSSLESS DATA HIDING SCHEME

In this section, 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. 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 cipher text 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

A. Image Encryption

In this phase, the image provider encrypts a plaintext image using the public key of probabilistic cryptosystem *pk*. For each pixel value $m(i, j)$ where (i, j) indicates the pixel position, the image provider calculates its ciphertext value,

$$c(i,j) = E[p_k, m(i,j), r(i,j)] \qquad (1)$$

Where, E is the encryption operation and $r(i, j)$ is a random value. Then, the image provider collects the cipher text values of all pixels to form an encrypted image.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

The public key is composed of n and a randomly selected integer g in Z^*n2 , while the private key is composed of λ and

$$\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n \qquad (2)$$

Where,

$$L(x) = \frac{(x-1)}{n} \qquad (3)$$

In this case,(1) implies

$$c(i,j) = g^{m(i,j)} \cdot (r(i,j))^{n} \bmod n^2 \qquad (4)$$

Where r(i,j) is a random integer in Z_n^*. The plaintext pixel value can be obtained using the private key,

$$m(i,l) = L\left((c(i,j))^{\lambda} \bmod n^2\right) \cdot \mu \bmod n \qquad (5)$$

Then, the encryption in (1) can be rewritten as

$$c(i,j) = g^{m(i,j)} \cdot (r(i,j))^{n^s} \bmod n^{s+1} \qquad (6)$$

where, $r(i, j)$ is a random integer in Z^*ns+1 . By applying a recursive version of Paillier decryption, the plaintext value can be obtained from the ciphertext value using the private key.

B. Data Embedding

When having the encrypted image, the data-hider may embed some additional data into it in a lossless manner. The pixels in the encrypted image are reorganized as a sequence according to the data hiding key. For each encrypted pixel, the data-hider selects a random integer $r'(i, j)$ in Z^*n and calculates

$$c'(i,j) = c(i,j) \cdot (r'^{(i,j)})^{n} \bmod n^2 \qquad (7)$$

If,Paillier cryptosystem is used for image encryption, while the data-hider selects a random integer $r'(i, j)$ in Z^*ns+1 and calculates

$$c'(i,j) = c(i,j) \cdot (r'^{(i,j)})^{n^s} \bmod n^{s+1} \qquad (8)$$

if Damgard-Jurik cryptosystem is used for image encryption.

We denote the binary representations of $c(i, j)$ and $c'(i, j)$ as $bk(i,j)$ and $b'k(i, j)$, respectively,

$$b_k(i,j) = \left\lfloor \frac{c(i,j)}{2^{k-1}} \right\rfloor \bmod 2, \qquad k = 1,2,3 \ldots \qquad (9)$$

$$b'_k(i,j) = \left\lfloor \frac{c'(i,j)}{2^{k-1}} \right\rfloor \bmod 2, \qquad k = 1,2,3 \ldots \qquad (10)$$

Clearly, the probability of $b_k(i,j)=b'_k(i,j)$(k=1,2,3…) is ½.

We also define the sets $S_1 = \{(i,j|b_1(i,j)) \neq b'_1(i,j)\}$

$$S_2 = \{(i,j|b_2(i,j)) \neq b'_2(i,j), b_1(i,j) \neq b'_1(i,j)\}$$

…

$$S_k = \{(i,j|b_k(i,j)) \neq b'_k(i,j), b_k(i,j) \neq b'_k(i,j), k = 1,2,3,\cdots,k-1\} \qquad (11)$$

C. Data Extraction and Image Decryption

After receiving an encrypted image containing the additional data, if the receiver knows the data-hiding key, he may calculate the k-th LSB of encrypted pixels, and then extract the embedded data from the K LSB-layers using wet paper coding. On the other hand, if the receiver knows the private key of the used cryptosystem, he may perform decryption to obtain the original plaintext image. When Paillier cryptosystem is used, Equation (4) implies

$$c(i,j) = g^{m(i,j)} \cdot (r(i,j))^{n} + \alpha \cdot n^2 \qquad (12)$$

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

where α is an integer. By substituting (12) into (7), there is

$$c'(i,j) = g^{m(i,j)} \cdot (r(i,j) \cdot r'(i,j))^{n} + mod\ n^2 \quad (13)$$

Since $r(i, j)\cdot r'(i, j)$ can be viewed as another random integer in Z^*n, the decryption on $c'(i, j)$ will result in the plaintext value,

$$m(i,j) = L\left(\left(c'(i,j)\right)^{\lambda} mod\ n^2\right).\mu\ mod\ n \quad (14)$$

Similarly, when Damgard-Jurik cryptosystem is used

$$c'(i,j) = g^{m(i,j)} \cdot (r(i,j) \cdot r'(i,j))^{n^s} + mod\ n^{s+1} \quad (15)$$

The decryption on $c'(i, j)$ will also result in the plaintext value.

IV.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 cipher text pixel values to embed a bit-sequence generated from the additional data and error-correction 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

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

A. Histogram shrinks and image encryption:

In the reversible scheme, a small integer δ shared by the image provider, the data-hider and the receiver will be used, and its value will be discussed later. Denote the number of pixels in the original plaintext image with gray value v as hv, implying

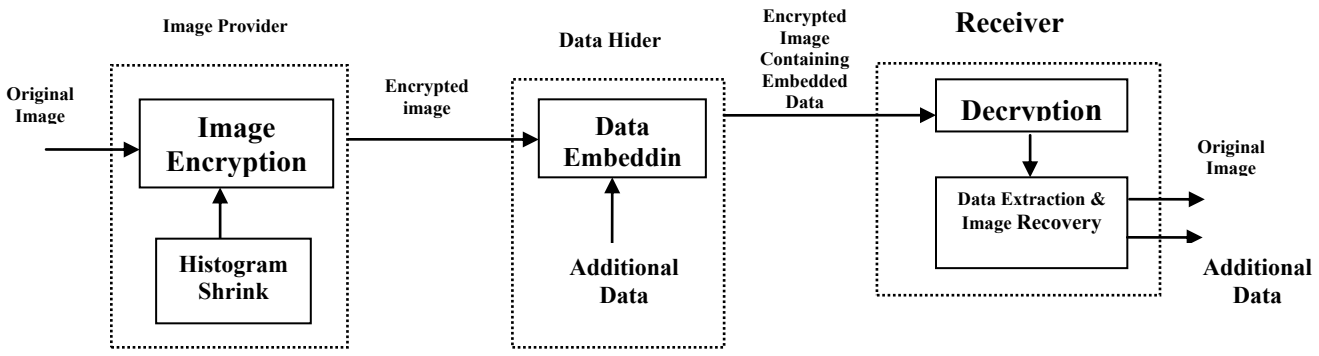

Figure 2. Sketch of Reversible Data Hiding Scheme for Public-Key-Encrypted Images

$$\sum_{v=0}^{255} h_v = N \quad (16)$$

Where, N is the number of all pixels in the image. The image provider collects the pixels with gray values in [0, δ+1], and represent their values as a binary stream BS1.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

When an efficient lossless source coding is used, the length of BS1.

$$l_1 \approx \sum_{v=0}^{\delta+1} h_v \cdot H\left[\frac{h_0}{\sum_{v=0}^{\delta+1} h_v}, \frac{h_1}{\sum_{v=0}^{\delta+1} h_v}, \cdots, \frac{h_{\delta+1}}{\sum_{v=0}^{\delta+1} h_v}\right] \quad (17)$$

Where, $H(\cdot)$ is the entropy function. The image provider also collects the pixels with gray values in [255−δ, 255], and represent their values as a binary stream BS2 with a length $l2$. Similarly,

$$l_2 \approx \sum_{v=255-\delta}^{255} h_v \cdot H\left[\frac{h_{255-\delta}}{\sum_{v=255-\delta}^{\delta+1} h_v}, \frac{h_{255-\delta+1}}{\sum_{v=255-\delta}^{\delta+1} h_v}, \cdots, \frac{h_{255}}{\sum_{v=255-\delta}^{\delta+1} h_v}\right] \quad (18)$$

Then, the gray values of all pixels are enforced into [δ+1,255−δ],

$$m_s(i,j) = \begin{cases} 255-\delta, if m(i,j) \geq 255-\delta \\ m(i,j), if\ \delta+1 < m(i,j) < 255-\delta \\ \delta+1 < m(i,j) \leq \delta+1 \end{cases} \quad (19)$$

Denoting the new histogram as $h'v$, there must be

$$h'_v = \begin{cases} 0 & ,v \leq \delta \\ \sum_{v=0}^{\delta+1} h_v & ,v = \delta+1 \\ h_v & ,\delta+1 < v < 255-\delta \\ \sum_{v=255-\delta}^{255} h_v & ,v = 255-\delta \\ 0 & ,v > 255-\delta \end{cases} \quad (20)$$

The image provider finds the peak of the new histogram,

$$V = \arg\max_{\delta+1 \leq v \leq 255-\delta} h'_v \quad (21)$$

The image provider also divides all pixels into two sets: the first set including (N−8) pixels and the second set including the rest 8 pixels, and maps each bit of BS1, BS2 and the LSB of pixels in the second set to a pixel in the first set with gray value V.

Since the gray values close to extreme black/white are rare, there is

$$h'_v \geq l_1 + l_2 + 16 \quad (22)$$

when δ is not too large. In this case, the mapping operation is feasible. Here, 8 pixels in the second set cannot be used to carry BS1/BS2 since their LSB should be used to carry the value of V, while 8 pixels in the first set cannot be used to carry BS1/BS2 since their LSB should be used to carry the original LSB of the second set. So, a total of 16 pixels cannot be used for carrying BS1/BS2. That is the reason that there is a value 16 in (22). The experimental result on 1000 natural images shows (22) is always right when δ is less than 15. So, we recommend the parameter δ < 15. Then, a histogram shift operation is made.

$$m_T(i,j) = \begin{cases} m_S(i,j) & ,if\ m_S(i,j) > V \\ V & ,if\ m_S(i,j) = V\ and\ the\ corresponding\ bit\ is\ 0 \\ V-1 & ,if\ m_S(i,j) = V\ and\ the\ corresponding\ bit\ is\ 0 \\ m_S(i,j) & ,if\ m_S(i,j) < V \end{cases} \quad (23)$$

In other word, BS1, BS2 and the LSB of pixels in the second set are carried by the pixels in the first set. After this, the image provider represents the value of V as 8 bits and maps them to the pixels in the second set in a one-to-one manner. Then, the values of pixels in the second set are modified as follows,

$$m_T(i,j) = \begin{cases} m_s(i,j) & ,\text{if LSB of } m_s(i,j) \text{ is same as the corresponding bit} \\ m_s(i,j)-1 & ,\text{if LSB of } m_s(i,j) \text{ is differs from the corresponding bit} \end{cases} \quad (24)$$

That means the value of V is embedded into the LSB of the second set. This way, all pixel values must fall into [δ, 255−δ]. At last, the image provider encrypts all pixels using a public key cryptosystem with additive homomorphic property, such as Paillier and Damgard-Jurik cryptosystems.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

When Paillier cryptosystem is used, the ciphertext pixel is

$$c(i,j) = g^{m_T(i,j)} \cdot \left(r(i,j)\right)^n mod\ n^2 \qquad (25)$$

And, when Damgard-Jurik cryptosystem is used, the cipher text pixel is

$$c(i,j) = g^{m_T(i,j)} . (r(i,j))^{n^s} mod\ n^{s+1} \qquad (26)$$

Then, the cipher text values of all pixels are collected to form an encrypted image.

B. Data embedding:

With the encrypted image, the data-hider divides the ciphertext pixels into two set: Set A including $c(i, j)$ with odd value of $(i+j)$, and Set B including $c(i, j)$ with even value of $(i+j)$. Without loss of generality, we suppose the pixel number in Set A is $N/2$. Then, the data-hider employs error-correction codes expand the additional data as a bit-sequence with length $N/2$, and maps the bits in the coded bit-sequence to the ciphertext pixels in Set A in a one-to-one manner, which is determined by the data-hiding key. When Paillier cryptosystem is used, if the bit is 0, the corresponding ciphertext pixel is modified as

$$c'(i,j) = c(i,j) \cdot g^{n-\delta} \cdot \left(r'(i,j)\right)^n mod\ n^2 \qquad (27)$$

where $r'(i, j)$ is a integer randomly selected in Z^*n. If the bit is 1, the corresponding ciphertext pixel is modified as

$$c'(i,j) = c(i,j) \cdot g^{\delta} \cdot \left(r'(i,j)\right)^n mod\ n^2 \qquad (28)$$

When Damgard-Jurik cryptosystem is used, if the bit is 0, the corresponding ciphertext pixel is modified as

$$c'(i,j) = c(i,j) \cdot g^{n^{S+1}-\delta} \cdot \left(r'(i,j)\right)^{n^s} mod\ n^{s+1} \qquad (29)$$

where $r'(i, j)$ is a integer randomly selected in Z^*ns+1 . If the bit is 1, the corresponding ciphertext pixel is modified as

$$c'(i,j) = c(i,j) \cdot g^{\delta} \cdot \left(r'(i,j)\right)^{n^s} mod\ n^{s+1} \qquad (30)$$

This way, an encrypted image containing additional data is produced. Note that the additional data are embedded into Set A. Although the pixels in Set B may provide side information of the pixel-values in Set A, which will be used for data extraction, the pixel-values in Set A are difficult to be precisely obtained on receiver side, leading to possible errors in directly extracted data. So, the error-correction coding mechanism is employed here to ensure successful data extraction and perfect image recovery.

C. Image decryption, data extraction and content recovery

After receiving an encrypted image containing additional data, the receiver firstly performs decryption using his private key. We denote the decrypted pixels as $m'(i, j)$. Due to the homomorphic property, the decrypted pixel values in Set A meet

$$m'^{(i,j)} = \begin{cases} m_T(i,j) + \delta & \text{, if the corresponding bit is 1} \\ m_T(i,j) - \delta & \text{, if the corresponding bit is 0} \end{cases} \qquad (31)$$

On the other hand, the decrypted pixel values in Set B are just $mT(i, j)$ since their ciphertext values are unchanged in data embedding phase. When δ is small, the decrypted image is perceptually similar to the original plaintext image.

Then, the receiver with the data-hiding key can extract the embedded data from the directly decrypted image. He estimates the pixel values in Set A using their neighbors,

$$\bar{m}_T(i,j) = \frac{m_T(i-1,j) + m_T(i,j-1) + m_T(i+1,j) + m_T(i,j+1)}{4} \qquad (32)$$

and obtain an estimated version of the coded bit-sequence by comparing the decrypted and estimated pixel values in Set A. That means the coded bit is estimated as 0 if $mT(i, j) > m'(i, j)$ or as 1 if $mT(i, j) \le m'(i, j)$. With the estimate of codedbit-sequence, the receiver may employ the error-correction method to retrieve the original coded bit-sequence and the embedded additional data. Note that, with a larger δ, the error rate in the estimate of coded bits would be lower, so that more additional data can be embedded when ensuring successful error correction and data extraction. In other words, a smaller δ would result in a higher error rate in the estimate of coded bits, so that the error correction may be unsuccessful when excessive

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

payload is embedded. That means the embedding capacity of the reversible data hiding scheme is depended on the value of δ.

After retrieving the original coded bit-sequence and the embedded additional data, the original plaintext image may be further recovered. For the pixels in Set A, $m\mathrm{T}(i, j)$ are retrieved according to the coded bit-sequence,

$$m_S(i,j) = \begin{cases} m_T(i,j) & , if\ m_T(i,j) > V \\ V & , if\ m_T(i,j) = V\ or\ V-1 \\ m_T(i,j)+1 & , if\ m_T(i,j) < V-1 \end{cases} \quad (34)$$

Collect all pixels with $m\mathrm{S}(i, j) = \delta+1$, and, according to BS1, recover their original values within [0, δ+1]. Similarly, the original values of pixels with $m\mathrm{S}(i, j) = 255-\delta$ are recovered within [255−δ, 255] according to BS2. This way, the original plaintext image is recovered.

4.2 COMBINED DATA HIDING SCHEME

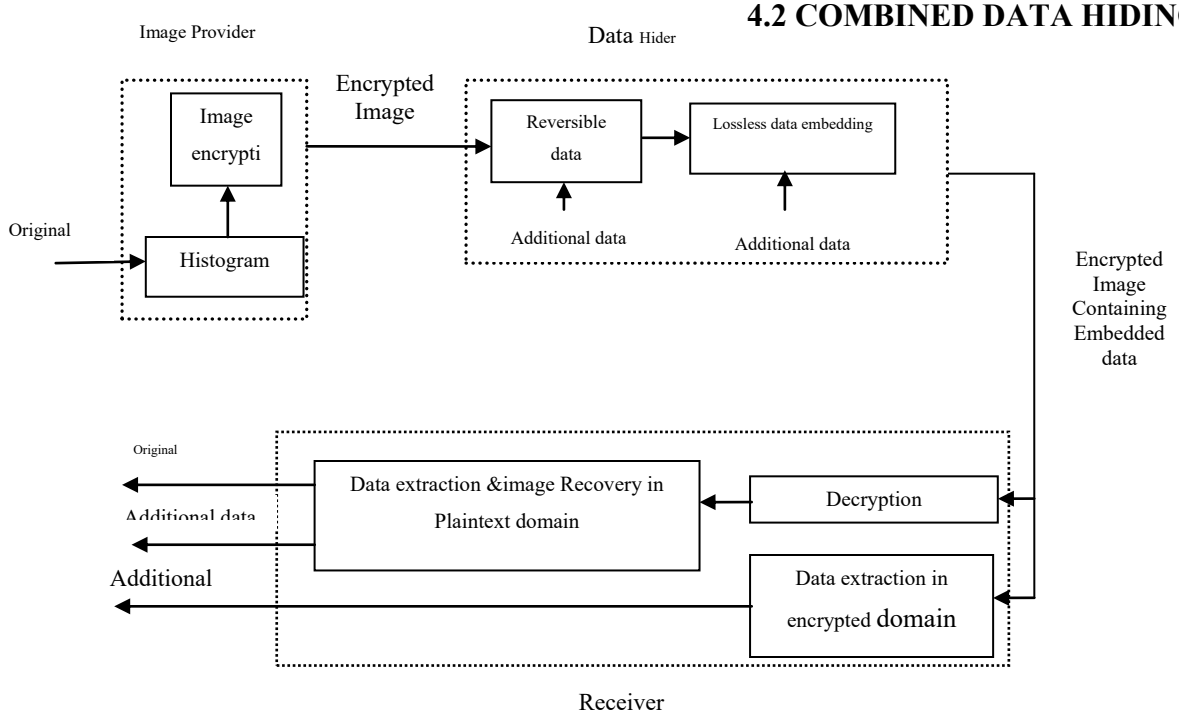

Fig. 3.Proposed Work Block Diagram

$$m_T(i,j) = \begin{cases} m'(i,j) - \delta & , \text{if the corresponding bit is 1} \\ m'(i,j) + \delta & , \text{if the corresponding bit is 0} \end{cases} \quad (33)$$

For the pixels in Set B, as mentioned above, $m\mathrm{T}(i, j)$ are just $m'(i, j)$. Then, divides all $m\mathrm{T}(i, j)$ into two sets: the first one including $(N-8)$ pixels and the second one including the rest 8 pixels. The receiver may obtain the value of V from the LSB in the second set, and retrieve $m\mathrm{S}(i, j)$ of the first set

As described in Sections 3 and 4, a lossless and a reversible data hiding schemes for public-key-encrypted images are proposed. In both of the two schemes, the data embedding,

$$m_S(i,j) = \begin{cases} m_T(i,j) & , \text{if LSB of } m_s(i,j) \text{ and } m_T(i,j) \text{ are same} \\ m_T(i,j)+1 & , \text{if LSB of } m_s(i,j) \text{ and } m_T(i,j) \text{ are differs} \end{cases} \quad (35)$$

Operations are performed in encrypted domain. When having the encrypted image, the data-hider may embed the first part of additional data using the method described

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

in Subsection 3.B. Denoting the ciphertext pixel values containing the first part of additional data as $c'(i, j)$, the data-hider calculate

$$c''(i,j) = c'(i,j) \cdot \left(r''(i,j)\right)^{n} mod\ n^2 \qquad (36)$$

$$c''(i,j) = c'(i,j) \cdot \left(r''(i,j)\right)^{n^s} mod\ n^{s+1} \qquad (37)$$

where $r''(i, j)$ are randomly selected in Z^*n or Z^*ns+1 for Paillier and Damgard-Jurik cryptosystems, respectively.

V.EXPERIMENTAL RESULTS

A. FOR IMAGES

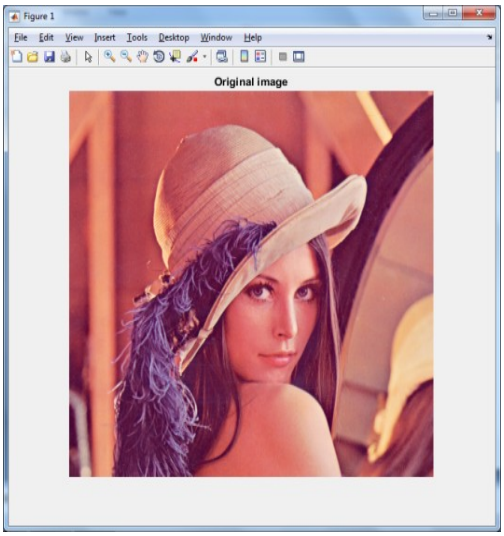

Fig1: Original Image

This is the input image for proposed work which is in color format. But the operations are difficult if we work directly on color image.

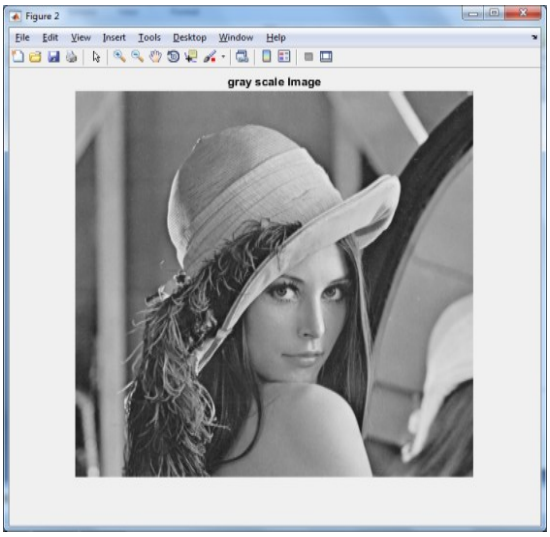

Fig2. Gray Scale Image

For reducing the computational complexity there is conversion of image to gray scale. The total processing is on converted gray scale image only.

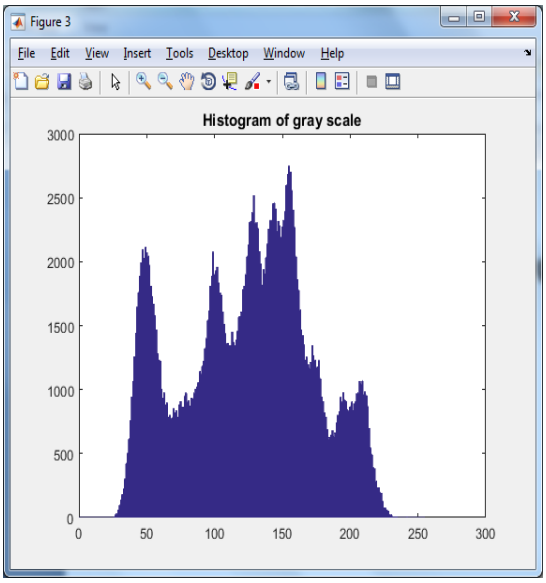

Fig 3. Histogram of Gray scale image

Graphical representation of input gray scale image as shown in fig.3.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

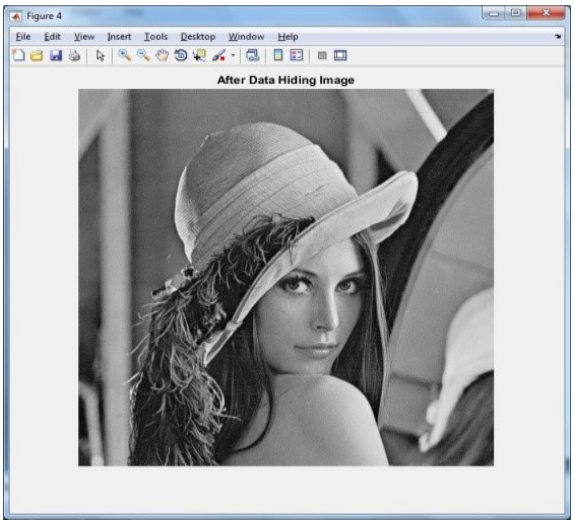

Fig 4. Data Embedded Image

The embedded image is obtained by combined technique (i.e. using both lossless and reversible data hiding technique)

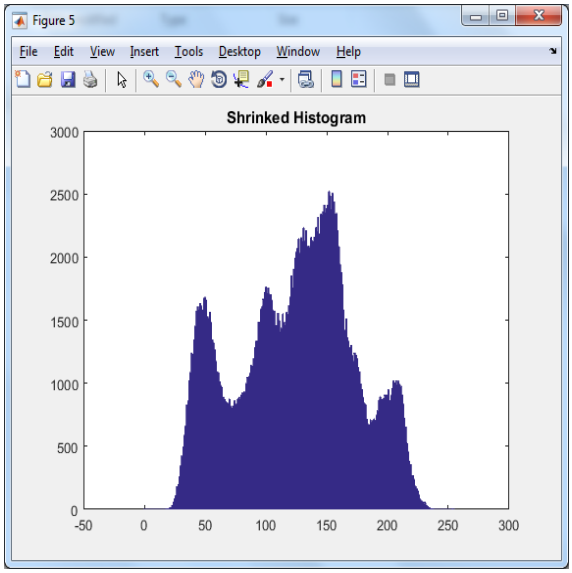

Fig 5. Shrink Histogram of Embedded Image

Data is embedded into image as per the given requirements. After that shrink histogram of embedded image calculated.

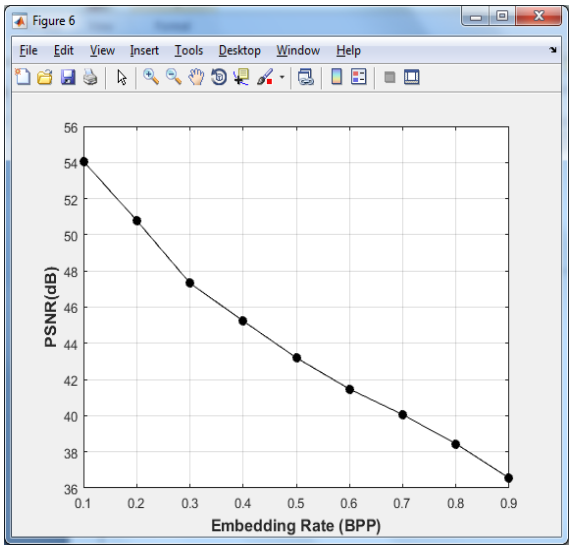

Fig6 : Plot of Embedding rate vs.PSNR

Above fig. represents the graph of embedding rate in bpp vs. PSNR in dB. In existing algorithms there is sudden decrease in PSNR as embedding rate increases. But by observation of this graph we can say that with embedding rate PSNR not decreased abbruptly.

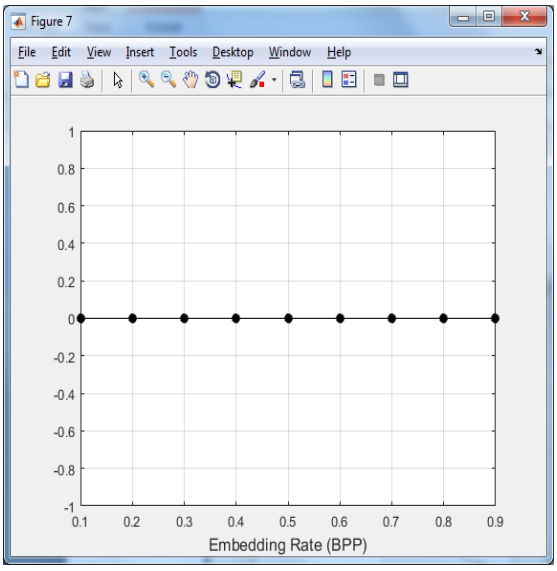

Fig7: Embedding rate performance

Embedding rate performance of the Ideal system.The embedding rate will be incraesed without causing any problem for PSNR values.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

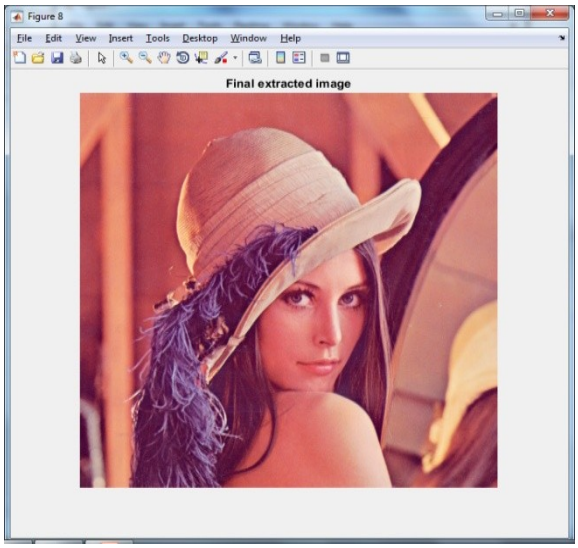

Fig8. Extracted Original image

Final extracted image for given embedded image. The extraction algorithm again contains the exactly opposite process of data embedding with lossless and reversible data hiding.

Table 1 Embedding rate in bpp vs. PSNR of paper [1],paper[2] and proposed work PSNR

Parameters / S.no	Embedding Rate(bpp)	[1] PSNR	[2] PSNR	Proposed PSNR
1	0.1	50	52	55
2	0.2	45	46	49
3	0.3	42	45	47
4	0.4	39	40.5	42.5
5	0.5	35	36.5	40.5
6	0.6	30	33	38

B. FOR VIDEOS

As there is trend in video processing nowadays, the proposed implementation is extended to video processing application for reversible and lossless data hiding. Same work is extended for videos. Video is nothing but number of frames for fraction of seconds. Video processing systems require a stream processing architecture, in which video frames from a continuous stream are processed one (or more) at a time. This type of processing is critical in systems that have live video or where the video data is so large that loading the entire set into the workspace is inefficient.

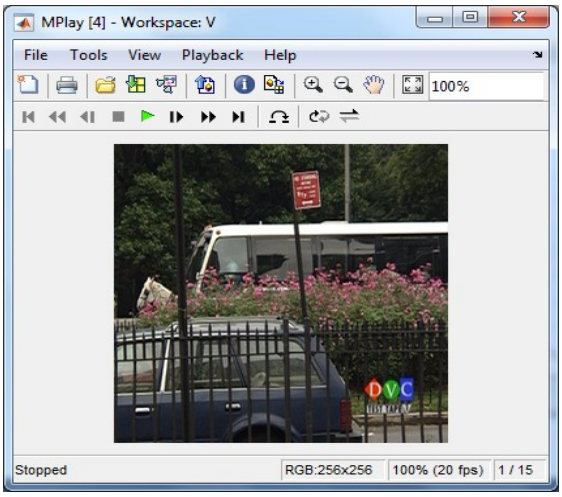

Fig 9.Original Video

Input sample video is given for proposed work which is not having any noises.

The data video is applied as input for proposed work. All processing is based on

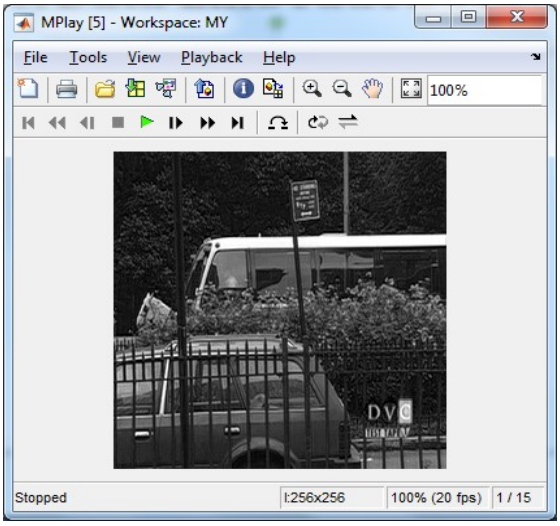

Fig 10. Data Embedded Video

Data embedded video is represented above. As per the proposed work same data is added into video.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

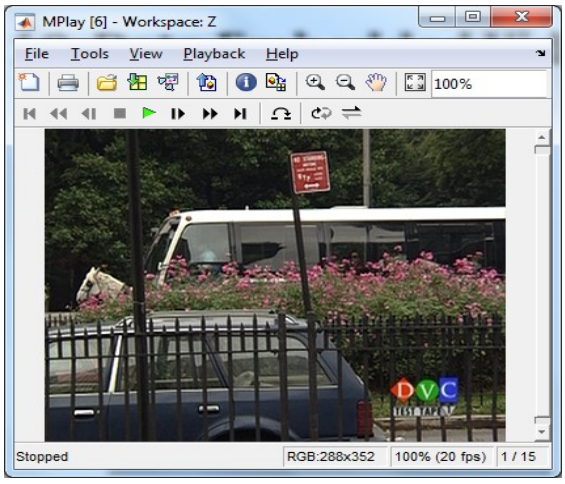

Fig **11.Extracted Video**

Final extraction algorithm for extraction of the video which is having the same data as previous.

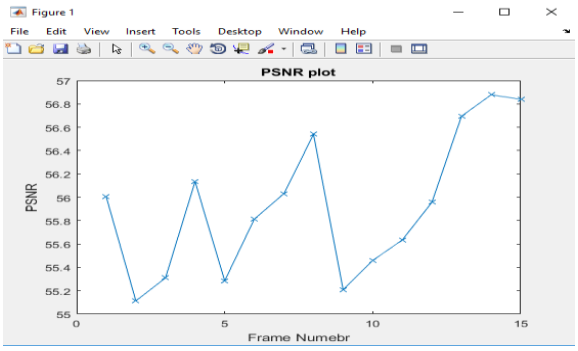

Fig.12 **Frame Number vs. PSNR Plot**

VI. CONCLUSION

This work proposes a lossless, a reversible, and a combined data hiding schemes for cipher-text images encrypted by public key cryptography with probabilistic and homomorphic properties. In the lossless scheme, the ciphertext pixel values are replaced with new values for embedding the additional data into the LSB-planes of ciphertext pixels. This way, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. In the reversible scheme, a preprocessing of histogram shrink is made before encryption, and a half of ciphertext pixel values are modified for data embedding. On receiver side, the additional data can be extracted from the plaintext domain, and, although a slight distortion is introduced in decrypted image, the original plaintext image can be recovered without any error. Due to the compatibility of the two schemes, the data embedding operations of the lossless and the reversible schemes can be simultaneously performed in an encrypted image. So, the receiver may extract a part of embedded data in the encrypted domain, and extract another part of embedded data and recover the original plaintext image in the plaintext domain. The same implementation is studied for video as there is trend in video processing nowadays.

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.