SECURE HIDING OF DATA IN ENCRYPTED IMAGES WITH ASYMMETRIC KEY CRYPTOGRAPHY

[1] M. CHAITANYA, [2] Dr. O. SRINIVASA RAO
[1] M.TECH SCHOLAR, [2] PROFESSOR
Department of Computer Science & Engineering,
University College of Engineering (A), JNTUK-Kakinada, Andhra Pradesh, India.

Abstract: Information stowing away and encryption are two important methods in information concealing. In the encryption strategies plaintext is converted content into garbled figure message, the information stowing procedures implant more information into the source or picture by making slight changes. This paper presents lossless, reversible & joined information plans of hiding in image content figure scrambled in cryptosystems of open key cryptography with homomorphic and the probabilistic properties in system. In the lossless phase, figure content pixels were supplanted with recent qualities for inserting data within a few least critical piece planes in figure content pixels with coding of wet paper in multi layers. It utilizes a novel reversed information hiding calculation, which can recover first picture from no twisting from stamped picture, after extraction of shrouded data. Reversible Data Hiding (RDH) in pictures was a method, by which the initial information can be recouped precisely after extraction of inserting message. JPEG RDH-EI work process incorporates three gatherings: content proprietor, data hider and beneficiary. In reversible phase, a pre-processing is utilized for shriveling picture histogram before picture encryption. By using similarity in reversible and lossless phases, the data hiding tasks in the two habitats will be same as performed with in an encoded image.

Index Terms - Image Encryption, Image Decryption, Lossless Data Hiding, Reversible Data Hiding & Histogram Shrinking.

I. INTRODUCTION

Cryptography is essentially studying of ensuring information by the goal that no one understands it that isn't approved to make as such. It enables a person to encrypt information so that the beneficiary will be main individual ready to unravel the information. Steganography was from several points in view of a dark side of cryptography. It enables an individual to conceal information within other information by the plan of not attracting doubt for the setting from where the message was moved. Steganography will be utilized for taking a record and conceal that report's information within a picture. This technique for cryptography has an assortment of utilizations that all outcome by the blend of both unique reports into one harmless archive. This subsequent information shrouds delicate data inside different information such that it shouldn't be detectable.

Steganography was more prevalently called as "Computerized Watermarking". With respect to the parent cryptography, advanced watermarking doesn't rely upon a symmetric or unbalanced encryption conspire. For example, with in the deviated encryption plot the calculation depends with an open/private key pair for encoding and decoding different messages. In a symmetric calculation messages were scrambled and unscrambled by using a similar key. Steganography utilizes neither of above strategies and depends on information stowing away to getting its assignment. Its point was to cloud the use full information so much that nobody could ever think to separate information from making the objective. It got the name computerized watermarking by the truth that the strategy can be used to store copyrights and trademarks inside information to ensure proprietor of archive. Such associations similar to the RIAA and MPAA are investigating the strategy for data hiding up to imbed uncommon labels for making it simpler to get and indict music and motion in the picture privateers.

II. RELATED WORK

Kede Ma, Nenhgai Yu, Weiming Zhang, Fengua Li and Xianfeng Zhao, [1] have made a framework, for example, before the encryption turning around a room by this easy data concealing procedure will be finished. In the previous stage the extra room was stays vacant. This strategy exploited all conventional RDH strategies for normal plain pictures and prevailing with low to no loss in the data. [2]Contrasted with past frameworks in the novel can see the enhancements from the nature of unscrambled pictures, separate data extraction & genuine reversibility. Reversible information Hiding (RDH) in pictures was a system, by using this strategy installed message was separated from the initial spread without loss. [3] For better execution of lossless data covering in pictures Author Xinpeng Zhang purposed the lossless and reversible data stowing away with ideal base technique. In the above technique originally acquired the critical ideal worth exchange. [4] As this worth evaluated mistakes are adjusted. In mystery data just by the significant data utilized for substance recuperation. It conveyed with the contrasts among the pixel esteems of initial one. The closest pixel esteems assessed by the neighbor's. Estimation blunders are changed with ideal worth exchange rule. Distinct Reversible Information Hiding in Encoded picture can be utilized. A substance of the proprietor encodes initial uncompressed image utilizing a key of encryption. A data hider may pack the bottom huge bits of the encrypted picture. It utilizes a key of data concealing for making the pixel distinction to match some additional information [5].

III DATA HIDING LOSSLESS SCHEME

In lossless type, lossless information concealing method to an open key scrambled pictures is suggested. In the method there were three different stages: a picture provider, a data hider and a collector. From the cryptosystem containing the probabilistic properties, the image provider encodes each and every pixels in the initial plaintext image using the open data key for beneficiary and a data hider from whom doesn't realize the initial image can adjust figure content pixel coordinates to implant some more additional data into distorted image by using coding of wet paper in multilayers with in the condition in which the unscrambled

estimations for latest and unique image content pixel's coordinates must and should be the same. When taking the distorted picture having the additional data, the recipient knowing the key of data hiding may extricate implanted information while the beneficiary of cryptosystem with private key may be performed decoding to retrieve the initial plaintext picture. By the finishing of day, installed data can be removed in the encoded space, and that can't be extricated after the unscrambling, since decoded image would be similar as the initial plaintext normal picture by the property of probabilistic. That likewise implies that the data inserting doesn't influence decoding of the normal plaintext picture.

A. Encryption of Image:

The picture provider scrambles a plaintext picture using open key in probabilistic cryptosystem pk at the point. For each pixel estimate m (g, h), where (g, h) shows pixel position, picture provider determines its figure content value where F is encryption task & r (g, h) is the arbitrary value. The picture provider collects estimates of figure containing all the pixels at that stage to frame a distorted image.

$$C(g, h) = F[pk, m(g, h), r(g, h)]$$

Damgård Jurik proposed cryptosystem [12] was also being used for encrypting plaintext picture as the generalization for Paillier cryptosystem. Here public key consists of m and element g with in $Z*ns+1$ so that the $g = (1 + m)\, j \cdot x \bmod ns+1$ for the known value of j and relatively of prime to m and x belong to the group of isomorphic for the $Z*m$, and we may take d as the private decryption key when meeting $d \bmod m \in Z*m$ and $d = 0 \bmod \lambda$. Then, the encryption in step (1) will be rewritten as

$$C(g, h) = gm(g, h) \cdot (r(g, h))ns \bmod ns+1$$

Where the r (g, h) is the randomly taken integer in $Z*$ ns+1. By the use of personal key, plaintext value can also be acquired from cipher encoded text value by the applying of a recursive variant of Paillier decryption. Note that, a same grey value at separate locations can correspond to distinct cipher encoded text values due to probabilistic properties of two cryptosystems.

B. Information Embedding:

The data concealer may install some of the additional information in image in the lossless way when having the encrypted picture. Then the image pixels in distorted image were rearranged as the configuration according to main concealing data.

$$C'(g, h) = c(g, h) \cdot (r\_(g, h))m \bmod m2$$

C. Extraction of Data and Picture Decryption:

Subsequent to accepting a distorted image having the additional data, if a collector will came to know the data hiding key, then he may ascertain the kth Least Significant Bit of the encoded data pixels and afterwards delete the implanted data from the K LSB layers by utilizing coding of wet paper. Then if again a recipient knows private decryption key of the used cryptosystem, then he can perform decoding operation to get the initial plaintext image.

$$C(g, h) = gm(g, h) \cdot (r(g, h))n + \alpha \cdot n2 \quad (12)$$

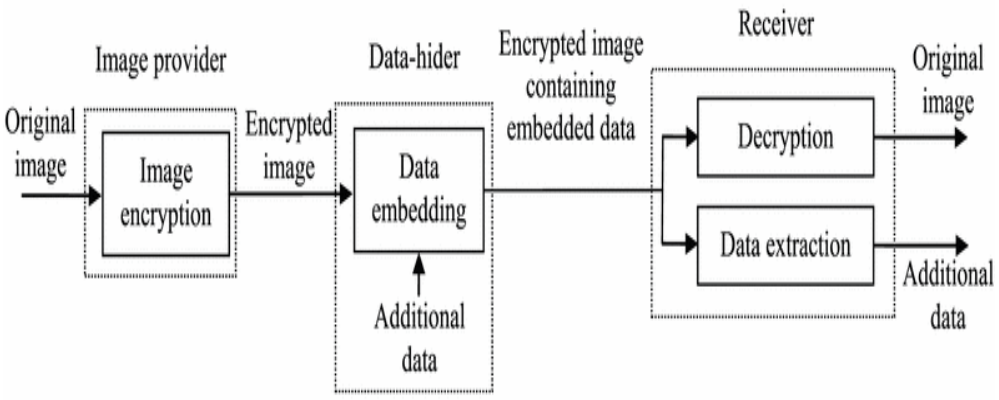


Fig 1: Architecture of the Data Hiding Scheme in Lossless way

III. DATA HIDING REVERSIBLE SCHEME

A preprocessing technique is utilized in reversible method to shrink picture histogram and each and every pixel was then encrypted by image provider with a homomorphic cryptosystem in an additive manner. The data hider modifies cipher encoded text pixels value when allowing the encoded image to incorporate in a bit sequence produced from the extra information and codes of error correction. The alteration in encoded domain will lead to a slight decrease or increase in normal plaintext pixels value due to property of the homomorphism, which implies that the decryption can also be introduced to get a picture on receiver's side comparable to initial plaintext picture. The data-embedding procedure doesn't trigger any underflow or overflow in directly decrypted picture due to the shrinking of histogram before encryption. Then it will be possible to retrieve the initial plaintext picture and to extract additional information from directly decoded picture. In plaintext domain reversible scheme's information extraction and the content recovery will be performed, while the last lossless scheme's information extraction was performed with in the domain of encryption and the content retrieval is unnecessary.

A. Shrinking of the Histogram and Encryption of Images:

A tiny integer δ shared by picture supplier, the hider data and receiver data will be utilized in reversible system and their value will be changed. Pixels number must have to be denoted in the plaintext original image with the grey values having k as h_v, implying

$$\sum_{k=0}^{255} hv = N$$

B. Embedding of Data within the Picture:

Data concealer splits text pixels in the cipher text into two sets by using the encrypted picture: Set U including the c (g, h) with the odd number values of (g + h) and the Set V includes c (g, h) with the even values of (g + h). Without the lossless in principle of the generality the pixels number in the Set U will take as M/2. Then data concealer uses an error correction of codes to expand additional information as the bit sequence length with M/2 length and then maps the M/2 bits with in the encoded bit sequence of encoded cipher text pixel in Set U from 1-to-1 manner, where key of data hiding determines the mapping method. If Paillier cryptosystem was used, the corresponded text pixels of cipher will be modified as 0.

$$c'(g, h) = c(g, h) \cdot gn-\delta \cdot (r' (g, h))m \bmod m2$$

C. Decryption of Image, Extraction of data, and the Information Recovery

Using this personal key, initially receiver conducts decryption after obtaining an encrypted image containing additional information. We will denote values of encoded pixels as the m _ (g, h). Because of the homomorphic properties the encoded pixels value in Set U will be

$$m'(g, h) = mT (g, h) + \delta, \text{ if the reference bit is 1}$$
$$mT (g, h) - \delta, \text{ if the reference bit is 0.}$$

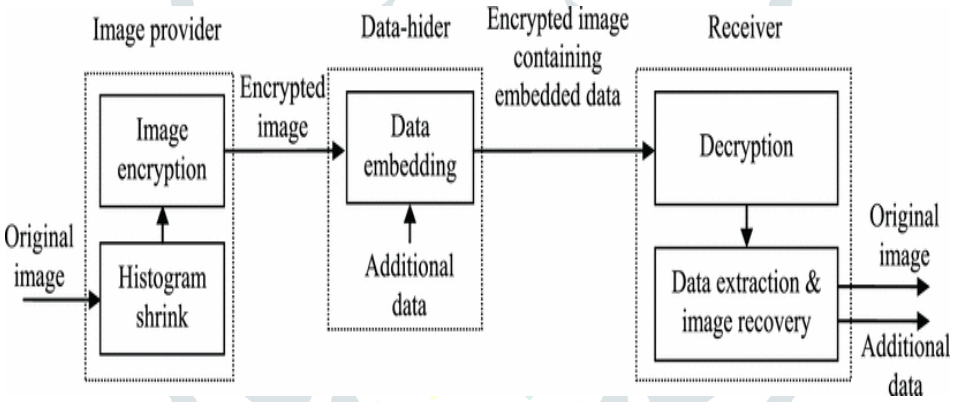


Fig 2: Architecture of the Data hiding Scheme in reversible way

IV PROPOSED SYSTEM

In some twisting situations which are unsuitable, information hiding away can also be performed by the reversible or lossless data way. Despite the truth that terms reversible and lossless have an equivalent significance in the lot of past references, this paper would recognizes them. We state that data concealing technique was lossless scheme, if the showcase of spread sign containing implanted data was same such that of the uniquely spread despite of the truth that hided information has been altered for data embedding. We propose the strategy for data inserting which is performed in the encoded space, and approved collector can recuperate to the initial plaintext spread picture and to concentrate the installed information. The above strategy is named as reversible data concealing in encrypted pictures (RDHEI).

Here, it may be confident that initial substance will be recouped with minimum blunder after the unscrambling and recover of extra message at beneficiary side. The initial picture was encoded with a XOR task with the pseudo random bits of data and will be after additional information was implanted by the flipping some of the least important bits (LSB's) of distorted picture.

Paillier Key Cryptography:

Pascal Paillier developed Paillier Cryptosystem. It was a modular, public key scheme of encryption with several interesting characteristics. To encrypt the data using Paillier system consider a public key which is established first. To initialize public key, choose 2 big primes, d and e and calculate their product, r = d·e.

Paillier Key Generation:

Consider d and e, where d and e are big prime numbers such that $d \neq e$

$r = d * e$

Calculate $\mu = \text{lcm}(d-1, e-1)$

Take $h \in Z_r^{2*}$, such that order of g will be divided by m

Public Key ⟵ (h, r)

Private Key ⟵ (d, e)

Encryption:

$o \in Z_r$

$t = h^o \cdot s^r \pmod{r^2}$, where $s \in Z_s^*$ is randomly choosen

Decryption:

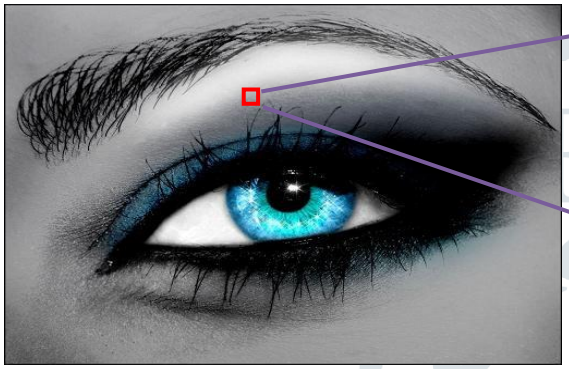
$o = (L(t^\mu \pmod{r^2}))\,(L(h^\mu \pmod{r^2}))^{-1} \pmod{r}$,

Where $L(u) = (u-1)/r$

Paillier Crypto System Keys

Encryption $t = h^o \cdot s^r \bmod r^2$

Decryption $o = \frac{(t^\mu \bmod r^2)-1}{r} \cdot \lambda \bmod r$



140	140	139	139
140	139	138	139
139	140	139	139
143	141	141	141

Paillier Encryption

3	159	186	62
45	147	83	188
170	120	62	128
127	170	181	10

Fig 3: Encryption of individual pixel in the image

BIT-FLIPPING ALGORITHM

Initialize set i=0 and λ = x.

1: ∀ n ϵ k_n = {0,1,2,3,…..,N-1}, calculate

$$Sn = \sum_{m \epsilon M(n)} \lambda n Hnm \pmod 2$$

If r=0 or i=i_{max}, stop process & give λ; else, i ⟵ i+1

2: ∀ m ϵ k_n = {0,1,2,3,……., M-1}, calculate FF E_m

3: By using FFs got in 2 to update bit flipped set β

4: Flip λ_m for all m ϵ β & go to 1.

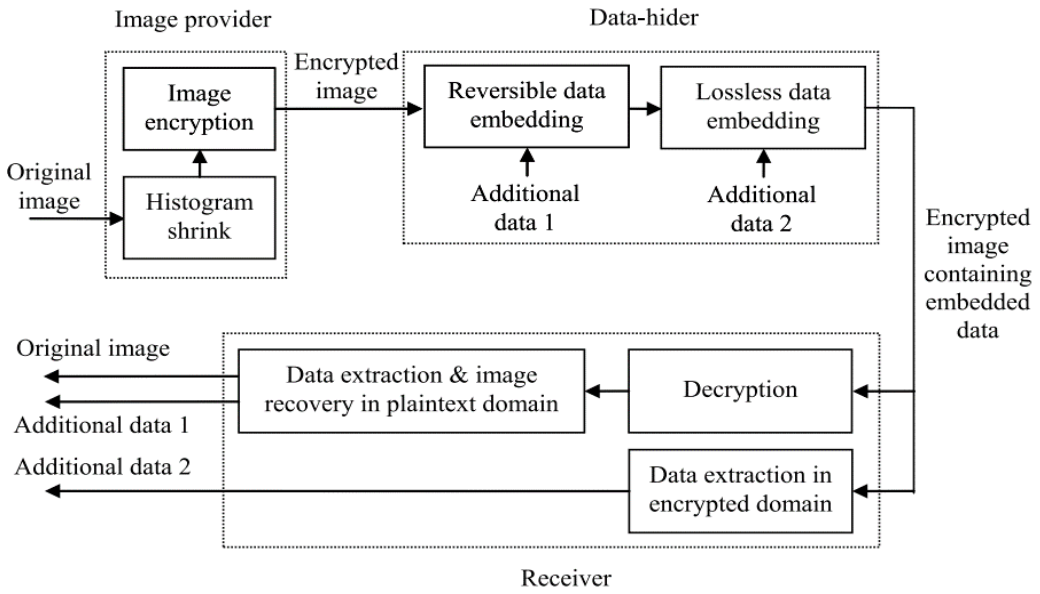


Fig 4: Sketch for combined data hiding for the public key encrypted data images

4.1 Advantages:

- This method can use the advantages of all the traditional techniques of RDH achieves the better performance for the normal plain images & without any loss of secrecy.
- This new technique can attain true reversibility, distinct extraction of information and significantly improve the quality of labelled decrypted pictures.

V SYSTEM ARCHITECTURE & DESIGN

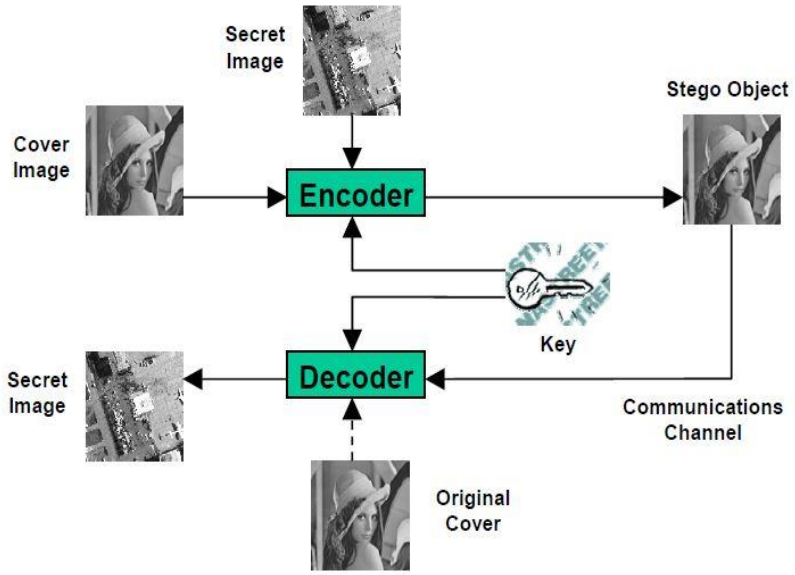


Fig 5: Generic method of encoding and decoding

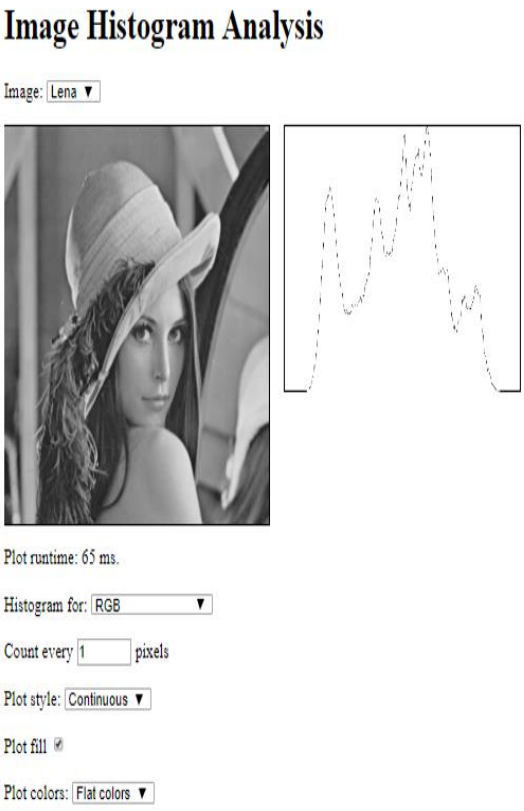


Fig 6: Histogram analysis-I

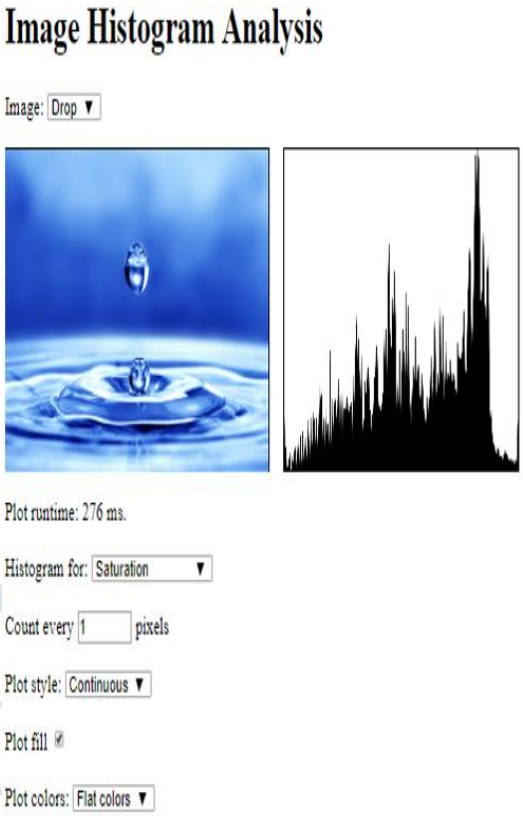


Fig 7: Histogram analysis-ii

VI EXPERIMENTAL EVALUATION:

A high dimensional color image such as the below figure 8, was taken and a data of approximately 150 words were inserted in the image by using the above combined techniques.

Fig 8: Image before inserting data

Fig 9: Image after insertion of data

After the insertion of data the picture will be as figure 9, which looks very similar to the figure e to the human naked eye. But, as we stored the data in the figure e, some distortion is present in it. With the increase of the data the distortion will also increase. The two figures variation can be found out by using the histogram analysis. The histogram analysis of the both figures are show in figure 10 and 11. The shape of the histogram will remains same but the crust of the histograms will differ. These are the places where the data is stored to minimize the picture distortion.

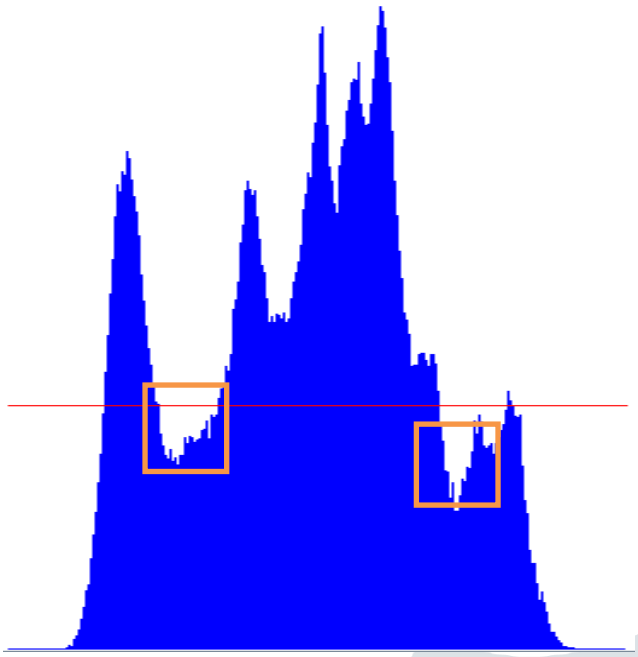


Fig 10: Histogram representation of image

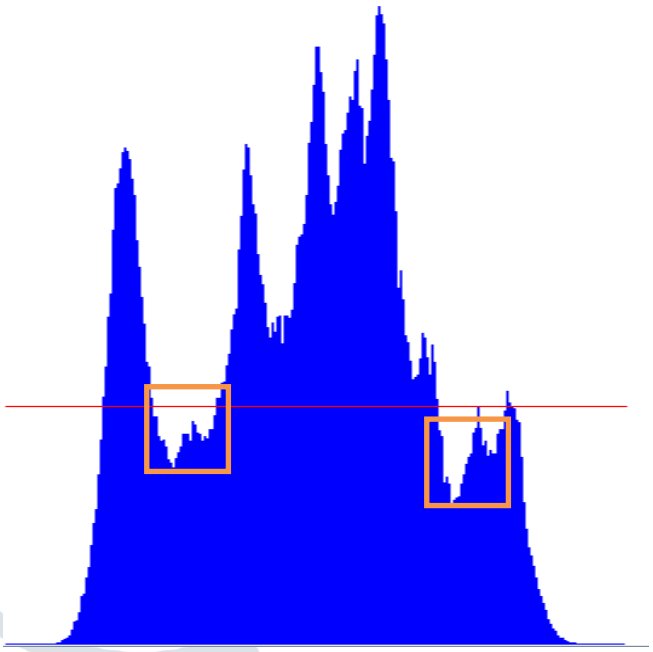


Fig 11: Same Image Histogram after Inserting Data

VII CONCLUSION & FUTURE ENHANCEMENT

Within the reversible phase, a pre-processing of the histogram psychologist was made ready before the encryption and the half of figure content pixels coordinates were adjusted for the information insertion. On the receiver's side, additional data can also be differentiate from the plaintext space and fact is that a narrow contortion is to be presented in the unscrambled image, the initial plaintext image can be recuperated with less to no mistake in it. Due to the common things of two plans, the data installing activities of reversible and lossless phases can also be performed at same time in the distorted image. By this manner, beneficiary can take a portion in implanted data in distorted space and can concentrate on the other part of the installed data and reorder first plaintext image in the plaintext area.

Promising methods like DCT, DWT and adaptive steganography, particularly when the hidden message is tiny, are not susceptible to assaults. They change the transform domain coefficients, resulting in minimal distortion of the picture. Generally, when compared with spatial domain algorithms, such methods tend to have a reduced payload. Some promising output was implemented by the experiments in discrete cosine transform (DCT) coefficients and they diverted the attention of the researcher to JPEG pictures. This method will preserve the both image quality and data quality but there are still some quality issues raises it the data is very large. New techniques has to be developed using the pixels to store large data without fading away the image.

VIII REFERENCES

[1] 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.

[2] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[3] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding,"IEEE Trans. Image Process., vol. 14,no. 2, pp. 253–266, Feb. 2005.

[4] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 653–664, Mar. 2015.

[5] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[6] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 1592. Berlin, Germany: Springer-Verlag, 1999, pp. 223–238.

[7] I. Damgård and M. Jurik, "A generalisation, a simplification and some applications of Paillier's probabilistic public-key system," in Public Key Cryptography. Berlin, Germany: Springer-Verlag, 2001,pp. 119–136.

[8] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper," IEEE Trans. Signal Process., vol. 53, no. 10, pp. 3923–3935, Oct. 2005.

[9] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562,Mar. 2013

[10] J. Yu, G. Zhu, X. Li, and J. Yang, "An improved algorithm for reversible data hiding in encrypted image," in Proc. 11th Int. Workshop Digit. Forensics Watermaking (IWDW), vol. 7809. Shanghai, China, Oct./Nov. 2012, pp. 358–367.