International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 09 | Sep 2021 www.irjet.net p-ISSN: 2395-0072

# ADVANCED IMAGE ENCRYPTION AND DECRYPTION SYSTEM FOR INVESTIGATION APPLICATIONS USING RLDH TECHNIQUE

**B. LalithaPhaniPriya[1], D.V.R. Mohan[2]**

[1]*Student, M.Tech, Communication systems @S R K R Engineering College, Bhimavaram, A. P, India*

[2]*Professor@S R K R Engineering College, Bhimavaram, A.P, India*

---

*Abstract: This paper proposes a novel reversible and lossless image data hiding scheme over encryption and decryption domain. Nowadays, data security is essential for crime investigation applications. For this purpose, a new technique was identified i.e., reversible and lossless image data hiding encryption and decryption schemes to store the evidences and details of a crime. Such image evidences are needed to be secured for a long period. Here it proposes new methodologies like Zig-Zag scanning, LSB substitution and mixing of rows and columns for implementation of the high secured encryption and decryption system. In this process, reversible data hiding by key based and lossless data hiding by cover image techniques are used to improve the data security and cannot retrieve the original data by anyone. This process also improves the SSIM and PSNR values of the image.*

**Keywords**: **reversible, lossless, encryption, zig-zag scanning.**

## 1. INTRODUCTION:

A picture involves assurance from different security assaults. The significant rationale to protect pictures is to guarantee secrecy, respectability and credibility. Different strategies are at removal for keeping pictures secure and encryption is one of them. Encryption transforms pictures into a figure picture for the most part by help of a key [1,2]. Afterward, an approved client can recuperate the first picture by decoding, the turnaround procedure of encryption. This procedure is a piece of the examination called cryptology [3,4]. Cryptology is the expansion of cryptography; study of making figures, and cryptanalysis; study of breaking figures. Cryptography is the study of changing a coherent message into an incoherent one, and afterward to recoup it appropriately [5,6]. Plaintext: A unique message Cipher message: The coded message that can't be comprehended by anybody. Encryption: Encryption is the procedure (calculation) for changing a plaintext into a figure content [7,8,9]. Unscrambling: Decryption is the invert procedure of encryption, for example changing the figure message back to plaintext. Key: Key is the most significant information utilized by encryption calculations, known to the both approved gatherings. An encryption system depends on the key. Encryption calculations are accessible for all, thus, aggressor's goal is to accomplish the key.

## 2. LITERATURE SURVEY:

Rather than considering committed encryption calculations custom-made to the situation of encoded space information covering up, we here adhere to the traditional stream figure applied in the standard arrangement. That is, the figure content is created by bitwise Ex-ORing the plaintext with the key stream [1,2]. If not in any case indicated, the generally utilized stream figure AES in the CTR mode (AES-CTR) is accepted. The subsequent information concealing worldview over encoded space could be all the more for all intents and purposes valuable due to two reasons.

1) Stream figure utilized in the standard configuration (e.g., AES-CTR) is as yet one of the most famous and dependable encryption instruments, because of its provable security and high programming/equipment usage effectiveness.

2) Large measures of information have just been scrambled utilizing stream figure in a standard manner. At the point when stream figure is utilized, the encoded picture is created by

$$[[f]] = Enc(f,K) = f \oplus K \quad (1)$$

Where k and [[f]] mean the first and the encoded pictures, individually. Here, signifies the key stream produced utilizing the mystery encryption key K. [3,4]. The schematic outline of the expert presented message installing calculation over encoded area is appeared in Fig. 1

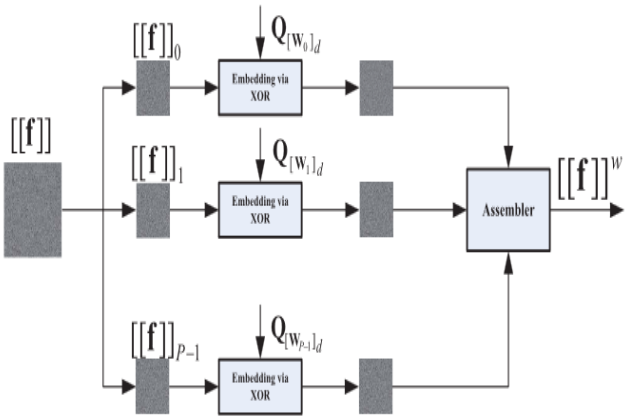


Fig-1: Schematic of data hiding over encrypted domain

Right now, loss of sweeping statement, all the pictures are thought to be 8 bits. All through this paper, we use[[x]]to speak to the encoded adaptation of x. Plainly, the first picture can be gotten by playing out the accompanying decoding capacity

Dec=([[f]],K)=[[f]] ⊕K. (2)

Right now, don't think about the instance of installing different watermarks for one single block, implying that each block is processed once at most [5,6]. For straightforwardness, we expect that the quantity of message bits to be inserted is n• A, Where A≤B and B is the quantity of blocks inside the picture. The means for playing out the message inserting are condensed as follows.

1) Initialize the index value of the block i=1.

2) Retrieve the n bits, which are to be embedded are denoted by Wi.

3) Locate the open key Q[Wi] connected with Wi, where the file [Wi] spoke to in decimals of Wi. For example, when n=3 and Wi=010, the relating open key is Q2.

4) Implant the size-n message bits Wi into the ith block through

[[f]]wi=[[f]]i⊕Q[Wi]d.(3)

5) Increasei=i+1 and repeat Steps 2–4 until all the message bits are inserted.

The schematic diagram of the data extraction is as shown in the fig.2.

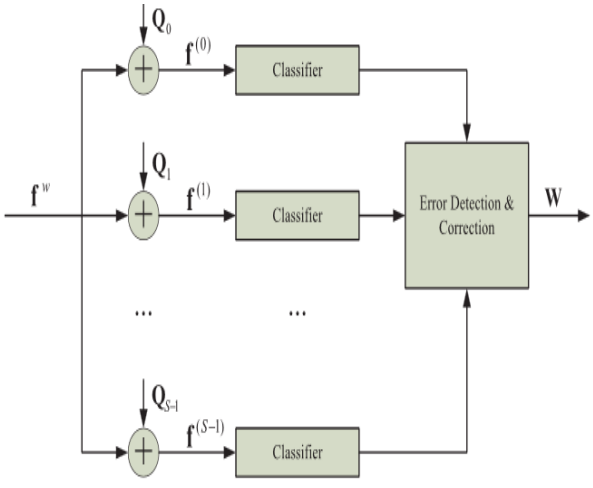



Fig-2: Schematic of the data extraction

The proposed error amendment approach depends on the accompanying key perception: on the off chance that a square is accurately decoded, at that point with high likelihood, there are some comparative fixes around it. Such a property of nonlocal picture likeness propels us to rank all the potential competitor hinders as indicated by the base separation with the patches in a nonlocal search window. By including the surface heading and scale into the above minimization system, we could additionally improve the mistake amending execution, however we find that the extra increase is somewhat restricted and the acquired intricacy is enormous. The applicant (j) that gives the littlest (j) listen chose as the decoded square, after deciding the file of the utilized open key, the implanted message bits and the first picture square can be clearly recouped by steganography [7]. The recuperation picture won't get the more precision as appeared in the fig.3.

a. Input b. Output

Fig-3: Directly encrypted and decrypted data of existing scheme.

We express a data hiding strategy is lossless if the feature of spread sign containing embedded data is same as that of one of a kind spread in spite of the way that the spread data have been adjusted for data embedding. For example, the pixels with the most used concealing in a palette picture are named to some unused concealing records for passing on the additional data, and these rundowns are redirected to the most used concealing. Along these lines, regardless of the way that the documents of these pixels are changed, the real shades of the pixels are kept unaltered.

Of course, we express a data covering procedure is re-versible if the main spread substance can be amazingly recovered from the spread structure containing embedded data regardless of the way that a slight turning has been exhibited in data im-planting technique. Different frameworks, for instance, differentiate augmentation, histogram move and lossless weight, have been used to develop the reversible data covering techniques for mechanized pictures. Starting late, a couple of not too bad conjecture approaches and perfect advancement probability under payload-bending establishment have been familiar with improve the presentation of reversible data stowing endlessly [10].

**3. PROPOSED METHOD:**

In this method, we followed the workflow of a Reversible and Lossless Data Hiding (RLDH) scheme for the encryption and decryption of the images. This process includes three

actors, the person, to whom the data belongs will encrypts the actual data and drives it to the block, which is used to hide the data; the data hider creates the marked image and sends to the receiver; and the receiver reconstruct the original image through decryption and data extraction. In fig. 4 the sketch of the complicated architecture is represented.

The RDH process includes 4 sub processes and 4 different algorithms, namely encryption, embedding, decryption and recovery.

Encryption: Image encryption process can be defined as follows:

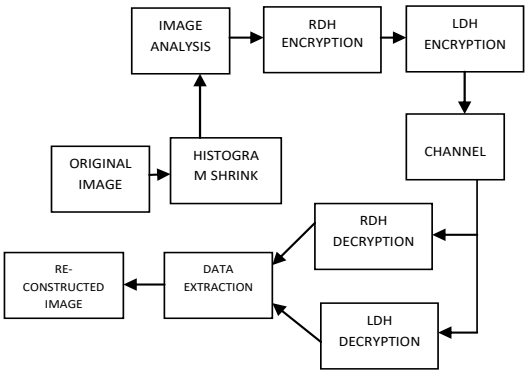



Fig-4: TWO LEVEL ENCRYPTION SYSTEM

Let the size of the actual image is M×N, at that point it tends to be changed into gray scale picture by the accompanying equation

$I(i,j) = I\,gray(i,j) \times (a + b)$ (4)

Where, I = actual image, 2a = M and 2b = N and Igray(i,j) = grayscale weight c

reated from the RGB scale. Presently the encoded picture

$IE(i,j) = I(i,j) \oplus K(i,j)$ (5)

Where K(i,j) is the key framework created utilizing any awry arbitrary capacity of request M × N.

Converting the three planes (Red, Green and Blue) of the stego image to one column of decimal pixels values using zigzag scanning (zigzag scanning for each plane). The size of the column vector will be (M×N×3) pixels, where (M) indicates to the number of rows in the original image, (N) indicates to the number of columns in the original image and (3) is the number of planes of the original image. Converting the column vector of pixels values to its representation in the binary value. After that, the size of the obtained matrix equal to (M×N×3×8) bits, where (8) indicates to the number of bits (where each pixel in the image is represented by one byte that equals to 8 bits). Then Data Embedding is performed through LSB substitution, Image marking or data embedding process can be defined as follows: The embedding operation is done only with some marked blocks of encrypted image. A series of operation are done between two consecutive pixel values to make some changes in the 3 LSB.

Thereafter a secret bit is embedded in the 4th LSB as marked embedded pixel. We have gone through a few reversible methods and used different combinations for data embedding. The adhered method is the best among them in terms of image recovery. Therefore, based on the reversibility constraint, we have chosen this proposed method. Here we isolate the encoded picture IE into non covering picture squares of request Z × Z. Leave it alone n. For all choices square Bq beginning from q=1 to n, for example for all in any event, tallying squares, presently implanting into a pixel can be made as follows:

a. Let the 1st row should not be changed.

b. The X-OR operation activity between the three LSB bits of the continuous columns x and y should be performed.

c. In the event that the X-OR output is 000, at that point the pixel will stay unaltered. Else Left pivot the 3 LSB of line x and flip the 4 th LSB. Proceed with stage 2 for every single stamped square. At last join the squares to shape the inserted picture.

After completion of these 3 steps, the image is totally encrypted with the reversible data hiding scheme over the key and the schematic diagram for this process is as shown in fig.5.

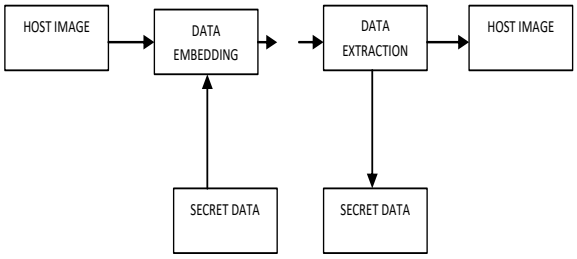



Fig-5: Reversible Data Hiding

Histogram is a statistical representation. The histogram of any digital image isa graphical portrayal of power conveyance in a picture. It speaks to the quantity of pixels for every force esteem. Conveyance of power esteems in a picture can be made a decision by taking a gander at the histogram of the picture. On the off chance that I is a computerized picture with dim level range [0, Z − 1], the histogram of picture I can be characterized as a discrete capacity H(rk) to such an extent that: H(rk) = nk where, rk is characterized as the k th dark level and nk is characterized as the quantity of pixels having rk dim level. The lossless information concealing plan is appeared in fig.6 is joined with the reversible information concealing plan to improve the security and precision for the picture.

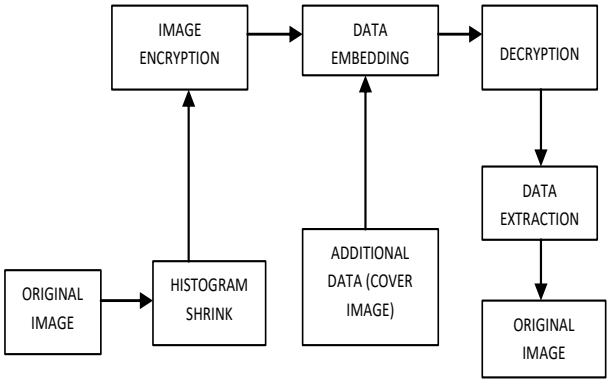



Fig-6: Lossless Data Hiding

**3.1 Data Embedding**: The fundamental histogram receptacle moving system utilizes the histogram of unique spread picture. The principle thought behind utilizing the histogram is to use the pinnacle point (the most regularly happening pixel worth) and zero point (the pixel esteem relating to which there is no dark scale an incentive in the picture) of the histogram of unique picture. The pixels between top point and zero point have been moved by 1 unit to make space by top point and watermark bits are implanted right now. In this procedure, histogram of given picture is created. Pinnacle point and zero point of the histogram are put away. It is accepted that the estimation of pinnacle point is in every case not exactly the estimation of zero point. Entire picture is checked in a succession and all pixels between highest point and zero point are moved to directly by 1 to make space for information implanting by the pinnacle point. Again, filter the picture and where pixel esteem is seen as equivalent to top point, check the to-be-implanted watermark bit grouping. On the off chance that it is "1", the grayscale pixel esteem is augmented by 1, in any case pixel esteem stays unaltered.

**3.2 Retrieval Process**: In order to retrieve the watermark and recovery of actual cover image, watermarked picture is checked and if pixel esteem is seen as 1 more noteworthy than highest point esteem, "1" is separated as watermark bit. In the event that pixel esteem is equivalent to the pinnacle point esteem, "0" is removed as watermark bit. Right now, is removed from the watermarked picture. Entire picture is filtered by and by and all pixel esteems y, with the end goal that y ∈ (top point, zero point], are subtracted by 1. Right now, picture can be recouped. In the event that a pixel is found having grayscale esteem 95 (for example 96 − 1), "1" is removed as watermark bit and if pixel esteem is discovered equivalent to 96, "0" is separated as watermark bit. Right now, is removed. For recouping the first picture, entire watermark picture is examined by and by, and if pixel esteem y is discovered to such an extent that y ∈ [25, 96], the pixel esteem y is augmented by 1. Right now, Lena picture can be recouped.

## 4. SIMULATION RESULTS:

The original image that we have taken for the simulation purpose as shown in the fig.7(A). in addition to this reference image will be considered as shown in fig.B. This image is used for the lossless image data hiding scheme. Whereas in fig.C, the encrypted reference image using LDH technique followed by Compresses image with key and reference (RLDH) technique shown in fig.D. Finally, the retrieved image is displayed in the fig.E.

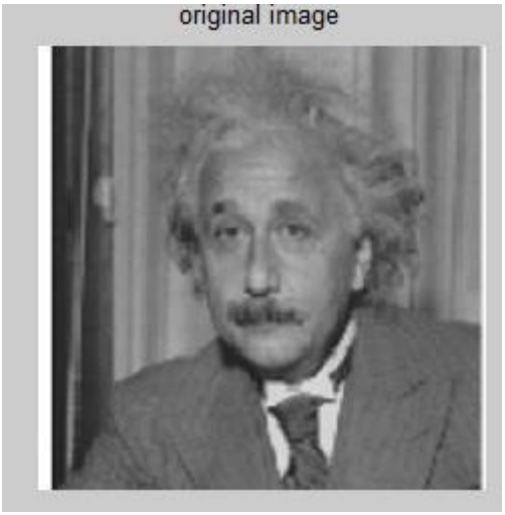
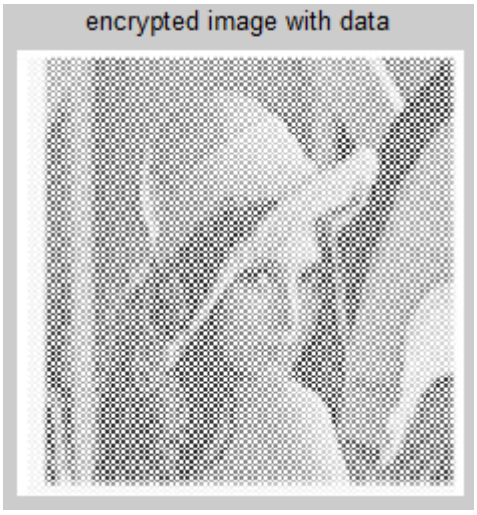
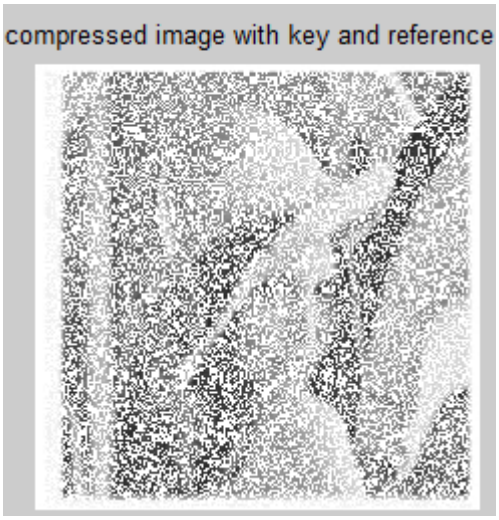



Fig-7: (A)- Actual Image

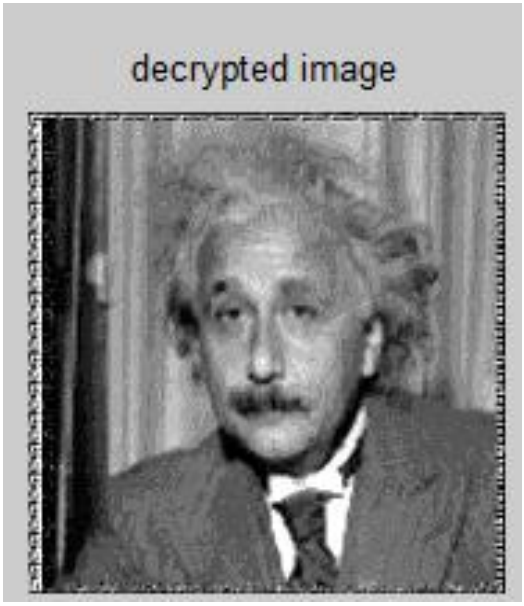

(B)- Reference Image




(C)- Encrypted reference image using LDH tehnique.




(D)- Compressed image with key and Reference(RLDH)




(E): Retrieved image.

Table-1: Parameters Summary for Existing and Proposed methods:

| PARAMETERS | EXISTING METHOD | PROPOSED METHOD |
|---|---|---|
| **PSNR (dB)** | 53.8009 | 56.6221 |
| **MSE** | 0.2502 | 0.14154 |

**Conclusion**:

The paper proposed a new technique, Reversible and Lossless Data Hiding (RLDH) method for encryption and decoding of pictures, with high PSNR and low MSE values for investigation applications with high security compared to Existing techniques.

**References:**

[1] Jianto Zhou, Li Dong, "Secure reversible image data hiding over encrypted domain via key modulation., IEEE transactions on circuits and systems for video technology, vol. 26, no.3, March 2016, pp. 3524–3533.

[2] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, Dec. 2011, pp. 316–325.

[3] X. Zhang, "Reversible data hiding with optimal value transfer," IEEE Trans. Multimedia, vol. 15, no. 2, Feb. 2013.

[4] [20] X. Zhang, Z. Qian, G. Feng, and Y. Ren, "Efficient reversible data hiding in encrypted images," J. Vis. Commun. Image Represent., vol. 25, no. 2, Feb. 2014, pp. 322–328.

[5] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, Mar. 2010, pp. 180–187.

[6] M. Barni, P. Failla, R. Lazzeretti, A. Sadeghi, and T. Schneider, "Privacy-preserving ECG classification with branching programs and neural networks," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, Jun. 2011, pp. 452–468.

[7] Z. Erkin, T. Veugen, T. Toft, and R. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, Jun. 2012, pp. 1053–1066.

[8] M. Chandramouli, R. Iorga, and S. Chokhani, "Publication citation: Cryptographic key management issues & challenges in cloud services," US Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 7956, 2013, pp. 1–31.

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

[10] 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.