Single Key Based Encryption & Embedding Algorithm for Reversible Data Hiding

Rupali Chandraka, Rashmi Shrivas
M. Tech Student (CSE), Department of Computer Science
Mats University, Aarang, C.G. India

***Abstract* – A novel reversible data hiding algorithmic rule with improved security, which might recover the first image in severable manner with none distortion from the marked image once the hidden knowledge are extracted, is conferred during this paper. Within the content owner aspect image is encrypted by key derived random permutation algorithmic rule. {the knowledge| the info |the information} hider then hides some knowledge into the encrypted image by histogram modification primarily based data hiding, creating use of secrete key. At the receiver aspect, if the receiver has solely secrete key, then the decrypted image with high similarity with cover image will be obtained, however cannot scan the hidden knowledge. Lower bound of Peak Signal to Noise ratio (PSNR) of this technique is way more than the previous method (75.78108dB). If the receiver has only secreted key, then the hidden data will be extracted out, however cannot scan the content of the image. If the receiver has secrete key, he might initial extract the info exploitation secrete key so decode the image exploitation same secrete key. the tactic additionally contains a higher data hiding capability than the prevailing reversible data hiding techniques in encrypted image.**

***IndexTerms* – Reversible data hiding; image encryption; PSNR; key generation.**

I. INTRODUCTION

Reversible data hiding (RDH) has been intensively studied within the community of signal process. Conjointly referred as invertible or lossless data hiding, RDH is to engraft a bit of data into a bunch signal to get the marked one, from that the initial signal may be precisely recovered when extracting the embedded data. The technique of RDH is helpful in some sensitive applications wherever no permanent modification is allowed on the host signal. within the literature, most of the planned algorithms square measure for digital pictures to engraft invisible knowledge.

The speedy development of communication technology attributable to the worldwide unfold of the web and therefore the digital info revolution has given rise to an enormous increase within the use and transmission of multimedia system info, it broadens the scope of right and wrong, as there square measure privacy violations, info larceny and then on. Digital pictures square measure wide used currently each day therefore its security is incredibly very important. to forestall the info from unauthorized access, cryptography technique is wide used. Recently, additional and additional attention is paid to reversible knowledge concealing (RDH) in encrypted pictures, Reversible knowledge concealing could be a technique to engraft extra message into some distortion unacceptable cowl media, like military or medical pictures, in such some way that the initial cowl content may be utterly remodeled when extraction of the hidden message. so as to firmly share a secret image, the content owner can encrypt the image before transmitting it to the receiver. Now a day's RDH is preferred more over the other existing, since the original cover can be recovered without any loss after the embedded data is extracted while protecting the image content's confidentiality.

Data concealing is typically performed by associate degree assistant or a channel administrator. The owner of the image cannot trust the assistant or channel administrator utterly. In such cases, once the owner has to keep the secrecy of the image, by initial code the image victimization associate degree secrete key. Then channel Administrator, with none information regarding the initial image content, must hide knowledge into the encrypted image employing a secrete key.

It is conjointly desired that the receiver will extract the hidden knowledge and recover the initial image in a very divisible manner. divisible suggests that, if the receiver has the secrete key solely, he will extract the info, however cannot decipher the image. If he's having secreted key solely, it's doable to decipher the image, but cannot extract the hidden data. If the receiver is having same key, he will extract the hidden knowledge and recover the initial image.

A lots of image wonderful cryptography techniques square measure offered in literatures by considering completely different aspects of image security. cryptography algorithms falls underneath 2 general categories: substitution and transposition. Some developers like each to boost security. Substitution based mostly cryptography alters the gray level of the pixels to form the content undisclosed. A substitution based mostly image cryptography won't alter the picture element gray level, instead shuffles the pixels in random in step with some criteria. Permutation based mostly cryptography algorithms square measure lined in [1].

There square measure completely different schemes to perform knowledge concealing techniques in encrypted image, [2] has adopted distinction enlargement technique. In his technique, one bit may be embedded into 2 consecutive pixels; thus, the utmost embedding capability is zero.5 bpp (bits per pixel). Later this technique was generalized by a latter with improved embedding capability of (n-1)/n bpp. completely different theme of reversible knowledge concealing, referred to as reserving space before cryptography is mentioned in [5]-[6]. alternative domain of RDH is bar chart based mostly technique. [7]- [8]covers completely different ways underneath this domain. a brand new technique for RDH is enforced in [9] by estimating the errors. Methods in [5], [6], [7], [10] deals with RDH in dissociable Manner.

The projected methodology may be a dissociable reversible information concealing in encrypted image with improved performance. The owner of image initial encrypts the image by permutation, creating use of associate degree secrete key. Following step utilizes the property of transposition algorithms, ie, permutation solely shuffles the pixels, the bar chart of the image remains unreduced. The data hider, with none data regarding the initial image content, hides information into the encrypted image by introducing modification in bar chart. Before concealing the information, the data hider shuffles the image once more mistreatment the random sequence calculated from secrete key and when information concealing he performs inverse permutation. At the receiver facet, if the receiver has solely secrete key, hidden information alone will be extracted, however not the image content. If receiver has solely secrete key, image the same as cowl will be decrypted. If has same key, initial hidden information will be extracted mistreatment secrete key so decode the image mistreatment same secrete key. This decrypted image is precisely same because the original image.

II. PROPOSED SYSTEM

We propose an efficient separable reversible data hiding in encrypted image with enhancement in security by indirect calculation of random sequence. A sketch of the proposed scheme is given in Fig.1.

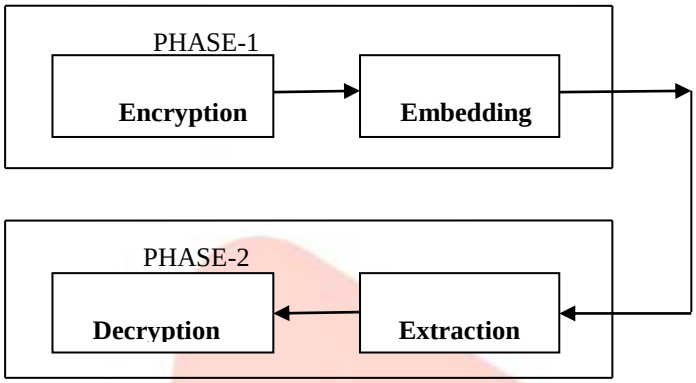

Fig.1.Overall Block Diagram of Proposed System.

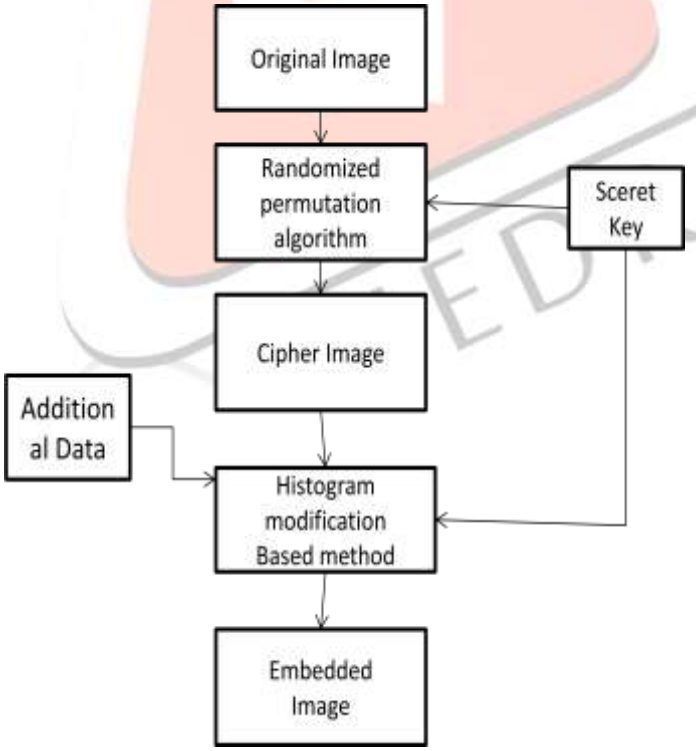

Fig.2 Flowchart of proposed system (PHASE-1)

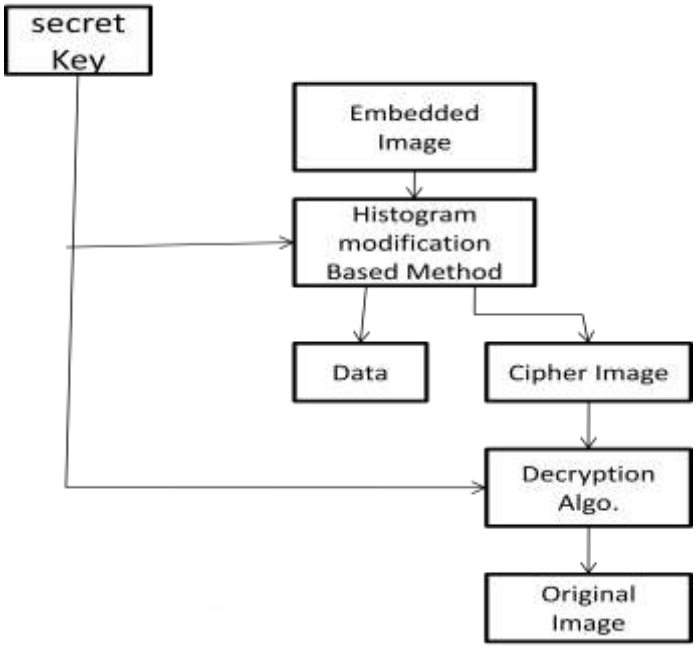

Fig.3.Flowchart of proposed work (PHASE-2) reverse process

A. Image Encryption

Assume we are considering a color image of size m × n (where m represents row & n represents column of the matrix). First scan the image into a matrix sized m × n.

We use the random permutation method in to encrypt the image. Recall that a permutation π is one-to-one and onto function

$$\pi : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$$

A permutation defines a reordering of the elements 1, . . . , n. It can be specified by the new values. e.g. (2 4 3 5 1) specifies a permutation where $\pi(1) = 2$, $\pi(2) = 4$, $\pi(3) = 3$, $\pi(4) = 5$ and $\pi(5) = 1$.

There are n! permutations of n elements. That's too many to generate them by numbering them all and choosing one at random. Random permutations are quite useful in randomized algorithms. So its helpful to have efficient algorithms for generating them. But more than this, certain algorithms give us good characterizations of random permutations for use in proofs. An algorithm breaks a calculation down into small steps. Those steps can be convenient to use in proofs of correctness for randomized algorithms. We'll see a concrete example of this shortly. Generating a random permutation is like "unsorting". A sort program can make an arbitrary permutation of elements to place them in ascending order. If the swaps in a sorting program are replaced by random swaps in a consistent way, we obtain a random permutation generator. If done carefully, we can generate random permutations with the uniform distribution. One such algorithm which gives a uniform distribution on permutations, we can use the following method. Assume an array A with n elements, initialized to the identity permutation so that A[i] = i for all i.

```
RandomPerm(A, n)
for i = 1 to n-1
choose j uniformly at random from [i,...,n]
swap A[i] and A[j]
```

B. Data Hiding

As permutation primarily based cryptography don't alter the histogram of original image, histogram modification primarily based technique in [5] are often accustomed hide information into the encrypted image. A transparent plan regarding histogram and image organization is that the requirement for the higher understanding of the conception [10]. The method follows:

- Pseudo every which way turn the encrypted image pixels exploitation information data hiding key. Adopt identical mechanism delineate for generating random sequence from secrete key.
- First H (Header) pixels of permuted image area unit accustomed hide parameters of data hiding. The parameters though of area unit MAX-MIN component values & variety of MAX-MIN pairs. Let there are S MAX-MIN pairs. Then, the number of pixels needed to hide the parameter are given by

  $$H = 2^* S + 1 * 8$$

  Significant once, eight bits area unit accustomed represent a value.
- Generate histogram of the remaining N-H pixels and notice the utmost (MAX) and minimum (MIN) points. A scoop purpose is that the color value having the utmost variety of pixels within the image. A MIN purpose is that the color

value having minimum variety of pixels within the image. Data hiding with one try solely explained here. From the observations in most of the cases, MAX<MIN. information area unit embedded into pixels with color value capable scoop. The pixel positions with color value capable MIN area unit keep as overhead info and can be hidden into the image alongside pure information.

- The N-H pixels used for generating the histogram area unit scanned within the sequent order. The color values of these pixels within the vary [MAX+1, MIN-1] area unit incremented by one, by deed the MAX+1 slot empty. This method is named histogram shifting.
- Let there be p pixels corresponding to the color value MAX. These p pixels area unit accustomed hide the information. information to be embedded is converted to binary bit stream. The N- H pixels area unit scanned within the sequent order. Whenever a component with color value MAX is encountered, check the bit to be embedded. If the corresponding bit to be embedded into that component is "1", the component price is incremented by 1. If the bit to be embedded is "0", the component value remains unchanged.
- The parameters of data hiding specifically, variety of MAX- MIN pairs and MAX-MIN component values, area unit hidden into the image by substitution the LSB of initial H pixels. the first H LSBs also are hidden as overhead info along with pure data.
- Perform inverse permutation on the image.

The higher than steps complete data hiding method. it's determined that data hiding capability of the strategy is (P-O-H) bits, wherever O is that the overhead info due to MIN Positions. Increased data hiding capability are often achieved by exploitation multiple MAX and MIN pairs as explained in [11].

C. Data Extraction and Image Recovery

When the receiver has only secrete key and encrypted image containing hidden information, he should be ready to extract the hidden information, however mustn't be ready to read the original image.

In order to extract the hidden information, the receiver might first pseudo randomly permute the image using secrete key as in data hiding phase. Then, extract the LSB of 1st eight pixels to find the amount of MAX-MIN pairs S. LSB of next 2*H* 8 pixels square measure then extracted to seek out the MAX-MIN combine values. Receiver then scans the image pixels in sequent order. If a pixel price with color value easy MAX + 1 is encountered, a bit "1" is extracted. If a pixel value MAX is encountered, a bit "0" is extracted. The extracted bits are concatenated to get the hidden data. Thus, the pure data as well as overhead information are exactly extracted.

In order to recover the original pixel values when data extraction, the whole image is scanned once more in sequent order. The LSB of 1st H pixels square measure replaced by the primary H bits of extracted overhead info.

For the remaining pixels, if the pixel value is within the vary [MAX+1, MIN], the pixel value is decremented by one. The extracted overhead info conjointly contains the original pixel positions with MIN value. Replace these pixels with MIN value. when data extraction, inverse permutation is performed to get the encrypted image with none hidden information.

The receiver will decrypt the encrypted image containing hidden data by using the secrete key only. For this, he generates same random sequence as in encryption phase using (1) and therefore the initial conditions. The logistic map is generated by sorting the sequence in ascending order. Using the logistic map, pixels of the encrypted image are rearranged to their original position to induce the decrypted image.

The decryption process will bring back all the pixels to their original position. only distortion within the decrypted image could be a difference of 1 in color value for those pixels used for data hiding. The lower bound of Peak Signal to Noise Ratio (PSNR) of this decrypted image will be verified to be larger than 48.13 dB as follows.

PSNR (Original Image) = 77.00331

PSNR(Recover Image) = 75.78108

The resultant lower bound of PSNR is much higher than that of reversible data hiding in encrypted image techniques,[2], rumored within the literature.

When the receiver have only secrete key, he first extracts the

hidden data using secrete key and this will recover the original value of distorted pixels due to data hiding. Then, the receiver decrypts the image. Thus, the hidden information is extracted exactly and therefore the original image is recovered completely.

III. EXPERIMENTAL RESULTS & ANALYS

Table I. shows the PSNR (peak signal to noise ratio) and MSE (mean square error) value of Original and Recovered Image

Table 1 EXPERIMENTAL RESULT FOR SOME COMMONLY USED IMAGES

S.NO	IMAGE		MSE	PSNR(dB)
1.	101201.jpg	Recover Vs Origi	0.0019621	75.2375
		Original Vs Steago	0.0033856	72.8684
2.	101702.jpg	Recover Vs Origi	0.0014609	76.5187
		Original Vs Steago	0.0013283	76.9317
3.	102901.jpg	Recover Vs Origi	0.0020272	75.0957
		Original Vs Steago	0.0012217	77.295
4.	108901.jpg	Recover Vs Origi	0.0025901	74.0316
		Original Vs Steago	0.0010945	77.7726
5.	110801.jpg	Recover Vs Origi	0.0018698	75.4468
		Original Vs Steago	0.0005375	80.861
6.	128900.jpg	Recover Vs Origi	0.001168	77.4902
		Original Vs Steago	0.00049334	81.2334
7.	129003.jpg	Recover Vs Origi	0.0017425	75.7532
		Original Vs Steago	0.0027713	73.738
8.	126808.jpg	Recover Vs Origi	0.0013616	76.8243
		Original Vs Steago	0.0012324	77.2572
9.	2.jpg	Recover Vs Origi	0.001442	76.5751
		Original Vs Steago	0.0012796	77.0939
10.	4.1.03.jpg	Recover Vs Origi	0.0021513	74.8377
		Original Vs Steago	0.0020811	74.9819

- Average PSNR value for Recover Image = 75.78108
- Average MSE value for Recover Image = 0.00177755
- Average PSNR value for Original Image = 77.00331
- Average MSE value for Original Image = 0.001542534

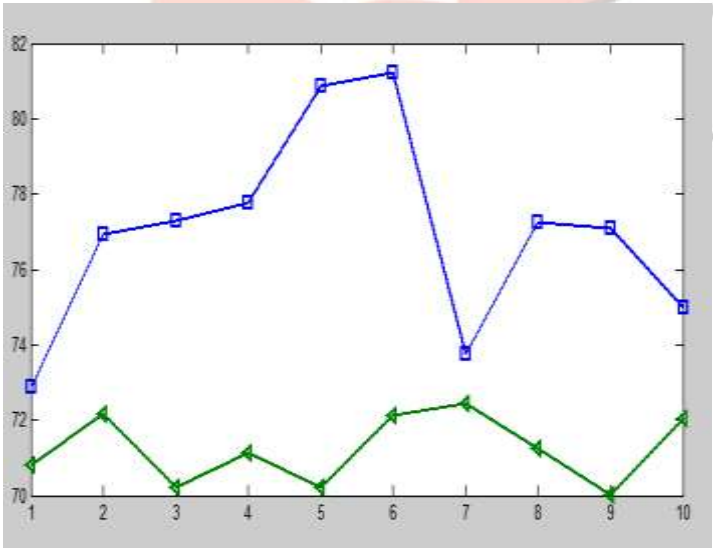

Fig.4.Graph of PSNR (peak signal to noise ratio) for Original Image

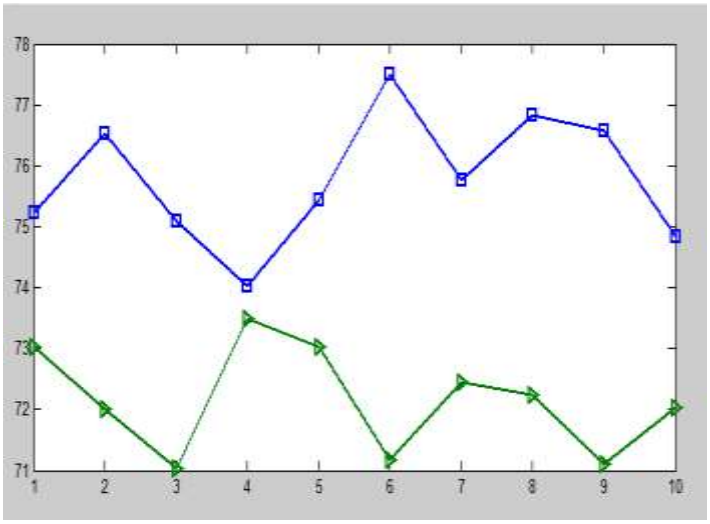

Fig.5.Graph of PSNR (peak signal to noise ratio) for Recover Image

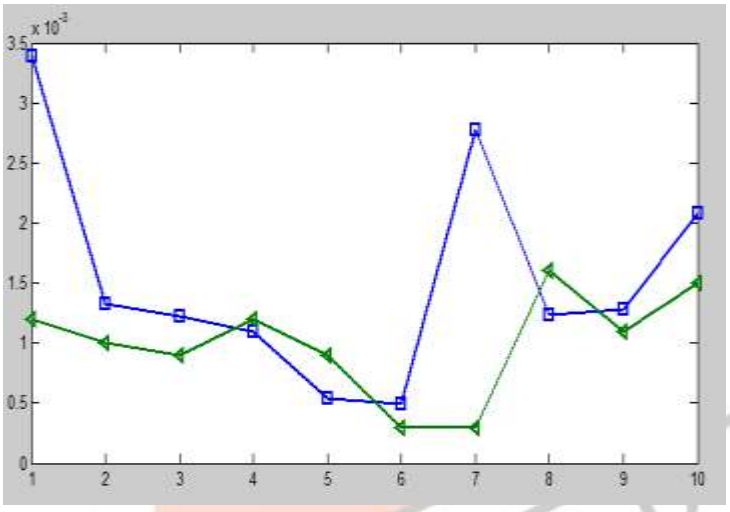

Fig.6.Graph of MSE (mean square error) for Original Image

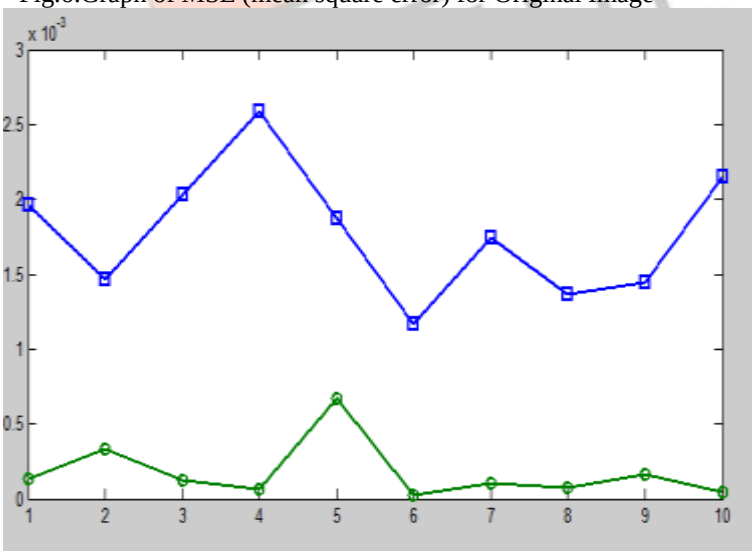

Fig.7.Graph of MSE (mean square error) for Recover Image

III. CONCLUSION

We planned a completely unique dissociable reversible data hiding in encrypted image with improved performance. The method consists of image encryption, data hiding , and data extraction and image recovery phases. within the initial section, owner of the image encrypts the image by random permutation exploitation secrete key. the data hider while not knowing the initial content will hide data into the encrypted image exploitation secrete key. For this histogram modification based mostly methodology is used. Data hiding capability of this methodology is way beyond that of {the information|the info|the information} activity strategies utilized in existing reversible data hiding in encrypted image techniques. At the receiver aspect, data extraction and image recovery are performed during a separable manner. The receiver with secrete key solely will extract the hidden information, however cannot decode the image. The receiver with secrete key solely will generate a picture similar to the initial image by cryptography, however cannot browse the hidden information. The bound PSNR of this decrypted image is 75.78108 dB and Original image PSNR 77.00331 dB that is way beyond that of existing reversible data activity techniques in encrypted image. If the receiver has secreted key, he will extract the info and recover the initial image utterly.

IV. ACKNOWLEDGMENT

The authors would like to sincerely thank the editors and anonymous reviewers for their valuable comments.

REFERENCES

[1] Chinmaya Kumar Nayak, Anuja Kumar Acharya, Satyabrata Das, "Image encryption using an enhanced block based transformation algorithm", International Journal of Research and Reviews in Computer Science, vol. 2, No. 2, Apr. 2011.

[2] Jun Tian, "Reversible data embedding using a difference expansion", IEEE Trans. on Circuits and Systems for Video Technology, vol. 13, No. 8, Aug. 2003.

[3]Hao-Tian Wu, Jean-Luc and Yun-Qing Shi,"Reversible Image Data Hiding with Contrast Enhancement", IEEE signal processing letters, vol 22, no.1,January 2015.

[4] Arun K Mohan, Saranya M R , K Anusudha, "An algorithm for Enhanced Image Security with Reversible Data Hiding", 978-1-4799-6629-5/14/$31.00_c 2014 IEEE.

[5] K. Ma, W. Zhang, X. Zhao, N. Yu, F. Li, Reversible data hiding in encrypted images by reserving room before encryption, IEEE Trans. Inf Forensic Secur. 8(3) (2013) 553-562.

[6] W. Zhang, K. Ma, N. Yu, Reversibility improved data hiding in encrypted images, Signal Process. 94 (2014) 118–127.

[7] Rintu Jose, Gincy Abraham, "A separable reversible data hiding in encrypted images with improved performance", International conference on Microelectronics, Communication & Renewable energy, Nov, 2013.

[8] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, "Design and implementation of image encryption algorithm by using block based symmetric transformation algorithm", International Journal of Computer Technology and Electronics Engineering, vol. 1, Issue 3.

[9] Weiming Zhang, Kede Ma, Nenghai Yu,"Reversibility improved data hiding in encrypted images", Elsevier Signal Processing letter, vol. 94, (118-127), Jun 2014.

[10] Xiaotian Wu, Wei Sun, "High capacity RDH in Encrypted Images by prediction error", IEEE Signal Processing Letters, vol. 18, No. 4, Apr. 2011.