ROOTINDEXING
JOURNAL ABSTRACTING AND INDEXING SERVICE
INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
January-June 2023, Submitted in February 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

An Efficient and Improved RDH-EI

Jaideep Kumar, Dept. of Computer Science & Engineering, R.D Engineering College, Ghaziabad
Arti Sharma, Department of Electronics and Communication Engineering, R.D Engineering College, Ghaziabad

Abstract

With the improvement of data innovation the datas are put away in the cloud and it should be ensure the security of data and the executives of the data simultaneously. By these requests the reversible data hiding in encoded images (RDH-EI) draws in an ever increasing number of analysts consideration. Here propose a novel system for RDH-EI dependent on RIT (Reverse image Transformation). Herethe substance of the first image can be tansform to the substance of another image. Then, at that point the changed image, that resembles the target image, is utilized as the encoded image, and ship off the cloud. Subsequently, the cloud worker can implant data into the scrambled image by utilizing any RDH techniques for plaintext images. RDH-EI is a customer free plan and the data installing plan is irrelevent with both interaction encryption and decoding.

Keywords: ***Reversible Data Hiding, Reversible Image transformation, Cloud computing***

I. INTRODUCTION

The Reversible data hiding (RDH) may be a technique in image processing area for encryption, by which the first cover are often losslessly recuperated after the implanted message, is extracted. The RDH approach is widely utilized in life science , defense field and forensic lab, where there's no degradation of the first content is allowed. Since more research RDH method in recently. In hypothetical perspective rate-twisting model for RDH Kalker and Willems[2], through which they demonstrated the rate-bending limits of RDH for memory less covers , proposed a recursive code development which, nonetheless, doesn't move toward the bound. The recursive code advancement for equal covers and exhibited that this improvement can achieve the rate-mutilation bound as long as the pressing factor computation shows up at entropy, which develops the comparability between information pressure and RDH for paired covers. Numerous RDH procedures have arisen lately. Fridrich[2] et al developed an overall structure for RDH for strategy. By first extricating compressible highlights of unique cover at that point compacting them lossless, spare space are regularly put something aside for inserting helper information. A various RDH method is more popular is predicated on difference expansion (DE) [3] , during which the difference of every pixel group is expanded by various method or technique. Example, increased by 2, and along these lines the littlest sum critical pieces (LSBs) of the distinction are every one of the zero and may be used for embedding messages. Another solid methodology for RDH is histogram shift (HS), during which space is put something aside for information inserting by moving the containers of histogram of dim qualities. With respective to giving privacy to pictures, encryption is an efficient and popular means because it converts the first and meaningful content to non-readable one. Although there are scarcely any RDH strategies in encoded pictures are distributed at this point, there are some encouraging applications if RDH are often applied to encrypted images. Hwang et al. advocated a reputation-based trust management scheme enhanced with information shading (a method of inserting information into covers) and software watermarking, during which encoding and coloring offer opportunities for maintaining the substance proprietor's security and data integrity[6].In our system we provide the high quality image to the users. It also provides the more security of the info. The proposed system is reduces the time also as cost as compared to previous system.

II. LITERATURE REVIEW

The methods proposed in [6]-[8] are often summarized because the structure, "vacating room after encryption (VRAE)", as outlined in Fig.1(a). during this framework, a content owner

encrypts the primary image employing a typical cipher with an encryption key. In the wake of delivering the encoded picture, the substance proprietor surrenders it to an information hider (e.g., a data set director) and along these lines the information hider can implant some assistant information into the scrambled picture by losslessly emptying some room as per an information concealing key. Then, at that point a beneficiary, perhaps the substance proprietor himself or an authorized outsider can remove the inserted information with the information concealing key and further recover the primary image from the encrypted version consistent with the encryption key. altogether methods of [6]-[8], the encrypted 8-bit gray-scale pictures are produced by scrambling each bit-planes with a stream figure. the tactic in [6] segments the encrypted image into sort scale pictures are produced by scrambling each piece planes with a stream cipheof non-covering blocks estimated by a X a; each square is utilized to convey one extra piece. to attempt to this, pixels in each square are pseudo-haphazardly isolated into two sets S1 and S2 as indicated by an information concealing key. On the off chance that the extra piece to be inserted is 0, flip the three LSBs of each scrambled pixel in S1, in any case flip the three encoded LSBs of pixels in S2. For data extraction and picture recovery, the beneficiary flips all the three LSBs of pixels in S1 to make a replacement unscrambled square, and flips all the three LSBs of pixels in S2 to outline another new square; one of them are getting the opportunity to be decoded to the fundamental square. in view of spatial association in standard pictures, special square is endeavored to be a ton of smoother than intruded block and embedded piece are often taken out correspondingly. Nonetheless, there is a danger of rout of touch extraction and picture recuperation when partitioned block is generally little (for example a=8) or has a lot of fine-point by point surfaces. Hong et al. [7] diminished the blunder pace of Zhang's technique [6] by completely abusing the pixels in computing the perfection of each square and utilizing side match. The extraction and recuperation of squares are performed reliable with the dropping request of totally the perfection contrast between two applicant hinders and recuperated squares can additionally be wont to assess the perfection of unrecovered blocks, which is referenced as side match. Zhang's strategy in [8] pseudo-arbitrarily permuted and partitioned scrambled picture into assortment of gatherings with size of L. The P LSB-planes of each gathering are compacted with an equality check grid and accordingly the emptied room is utilized to install information. for instance , indicate the pixels of 1 gathering by x1,… ,xL, and its scrambled P LSB-planes by c that comprises of P . L pieces. the data hider creates an equality check framework G estimated, (P . L - S) X P.L and packs c as its disorder s such s = G . c. Since the length of s is (P . L - S), S pieces are accessible for information convenience. At the recipient side, 8 - P the premier huge pieces (MSB) of pixels are acquired by unscrambling straightforwardly. The recipient then, at that point gauges xi ($1 \leq I \leq L$) by the MSBs of adjoining pixels, and gets an expected variant of c indicated by c ' . On the contrary hand, the recipient tests every vector having a place with the coset Ω(s) of disorder s, where Ω(s) = {u |G.u = s} .On the contrary hand, the beneficiary tests every vector having a place with the coset Ω(s) of condition s, where Ω(s) = {u |G.u = s}. From every vector of Ω(s), the collector can get a reestablished form of c, and pick the one most practically actually like the assessed adaptation c ' in light of the fact that the reestablished LSBs.

III. EXISTING SYSTEM

Most of the current RIDH algorithms are planned plaintext domain, to be specific, the message pieces are implanted into the first, un-scrambled pictures. The early works for the most part used the lossless pressure calculation to pack certain picture highlights, to vacate room for message installing

Reversible Data Hiding(rdh)

Reversible data hiding in pictures is a procedure that shrouds data in computerized pictures for secret correspondence. It is a method to shroud extra message into cover media with a

reversible way so the first cover substance can be consummately reestablished after extraction of the secret message. Customarily, data hiding is utilized for secret correspondence. In certain applications, the implanted transporters are additionally encoded to keep the transporter from being dissected to uncover the presence of the installation. Different applications could be for when the proprietor of the transporter probably won't need the other individual, including data hider, to know the substance of the transporter before data hiding is really performed, like military pictures or secret clinical pictures. For this situation, the substance proprietor needs to encode the substance prior to passing to the data hider for data insertion. The recipient side can extricate the installed message and recuperate the first picture. Numerous reversible data hiding techniques have been proposed as of late .As is notable, encryption is a compelling and mainstream methods for security insurance. To safely impart a mysterious picture to other individual, a substance proprietor may encode the picture before transmission. In some application situations, a second rate colleague or a channel overseer desires to affix some extra message, like the beginning data, picture documentation or verification data, inside the encoded picture however he doesn't have the foggiest idea about the first picture content. For instance, when clinical pictures have been scrambled for ensuring the patient protection, a database head may mean to implant the individual data into the relating encoded pictures. It very well might be likewise cheerful that the first substance can be recuperated with no blunder after decoding and recover of extra message at collector side. Customarily, data hiding is utilized for secret correspondence. In certain applications, the inserted transporters are additionally encoded to keep the transporter from being dissected to uncover the presence of the implant. Different applications could be for when the proprietor of the transporter probably won't need the other individual, including data hider, to know the substance of the transporter before data hiding is really performed, like military pictures or classified clinical pictures. For this situation, the substance proprietor needs to encode the substance prior to passing to the data hider for data implant. The recipient side can separate the inserted message and recuperate the first picture. A significant ongoing pattern is to limit the computational prerequisites for secure mixed media dispersion by particular encryption where just pieces of the data are scrambled. There are two degrees of safety for advanced picture encryption: low level and undeniable level security encryption. In low-level security encryption, the encoded picture has debased visual quality contrasted with that of the first one, yet the substance of the picture is as yet apparent and reasonable to the watchers. In the undeniable level security case, the substance is totally mixed and the picture simply looks like arbitrary commotion. For this situation, the picture isn't justifiable to the watchers by any means. Specific encryption targets keeping away from the encryption of all pieces of a computerized picture but guaranteeing a protected encryption. Reversible data hiding is a procedure to insert extra message into some twisting unsatisfactory cover media, like military or clinical pictures, with a reversible way so the first cover substance can be consummately reestablished after extraction of the secret message. As a viable and mainstream implies for security assurance, encryption changes over the conventional sign into in understandable data, with the goal that the overall sign preparing commonly happens before encryption or after unscrambling. In any case, in certain conditions that a substance proprietor doesn't confide in the specialist organization, the capacity to control the encoded data when maintaining the plain substance mystery is wanted. At the point when the restricted information to be communicated are encoded, a channel supplier with no information on the cryptographic key may pack the scrambled data because of the restricted channel asset. Encryption is a compelling methods for security assurance. To impart a mysterious picture to other individual, a substance proprietor may encode the picture before transmission. Now and again, a channel overseer needs to add some extra message, like the beginning data, picture documentation or validation data, inside the encoded picture anyway he doesn't have the

foggiest idea about the first picture content. It could be likewise expected that the first substance can be recuperated with no mistake after decoding and recover of extra message at beneficiary side. That implies a reversible data hiding plan for encoded picture is alluring. Data hiding is alluded to as an interaction to shroud data (addressing some data) into cover media. That is, the data hiding measure joins two arrangements of data, a bunch of the installed data and another arrangement of the cover media data. Much of the time of data hiding, the cover media gets misshaped because of data hiding and can't be rearranged back to the first media. That is, cover media has perpetual bending even after the secret data have been taken out. In certain applications, for example, clinical conclusion and law implementation it is wanted that the first cover media can be recuperated effectively with no misfortune. The checking methods fulfilling this necessity are alluded to as reversible, lossless, mutilation free or invertible data hiding strategies. Execution of a reversible dataembedding calculation Reversible data implanting, which is additionally called lossless data inserting, installs imperceptible data (which is known as a payload) into an advanced picture in a reversible design. As a fundamental prerequisite, the quality debasement on the picture after data inserting ought to be low. An energizing element of reversible data installing is the reversibility, that is, one can eliminate the implanted data to reestablish the first picture. Reversible data inserting shrouds some data in an advanced picture so that an approved gathering could translate the secret data and furthermore reestablish the picture to its unique state. The presentation of a reversible data-inserting calculation can be estimated by the accompanying • Payload limit • Visual quality • Complexity The twisting free data installing is the inspiration of reversible data implanting. Data will positively change the first substance by implanting some data into it. Indeed, even an exceptionally slight change in pixel esteems may not be attractive, particularly in delicate symbolism, like military data and clinical data. In such a situation, all of data is significant. From the application perspective, since the contrast between the inserted picture and unique picture is practically unnoticeable from natural eyes, reversible data installing could be thought as a mysterious correspondence channel since reversible data implanting can be utilized as a data transporter.

Disadvantages

. As the source coding with side data at the decoder requires a criticism channel, this plan would confront serious difficulties in numerous commonsense situations, e.g., secure distant detecting, where the input channel could be exorbitant. The installing limit of this kind of technique is fairly restricted and the caused twisting on the watermarked picture is extreme.

IV. PROPOSED SYSEM

In this work, we propose a scrambled domain RIDH conspire by explicitly taking the as of late referred to plan inclinations into thought. The proposed strategy installs message through a public key regulation instrument, and performs information extraction by abusing the measurable noticeability of encoded and non-scrambled picture blocks. Since the interpreting of the message bits and the chief picture is composed, our proposed technique has a spot with the classification of non-divisible RIDH arrangements Compared with the condition of expressions of the human experience, the proposed approach gives higher embedding limit, and can achieve ideal redoing of the principal picture similarly as the embedded message bits. Wide exploratory results on test pictures support the transcendent show of our arrangement.. 3.1. Benefits Enabling us to together disentangle the inserted message and the first picture signal consummately. It give higher security and have higher implanting limit. Likewise it giving higher security to information and picture.

1) Reversible Image Transformation

RIT produces a encrypted picture E(I), which enjoys the benefit of keeping a significant type of the picture contrasted with conventional encryption strategies. In this way, it is free for the cloud worker to utilize any old style RDH on the encoded picture. Choosing what sort of

RDH strategy relies upon if to keep the picture quality. In this part we basically embrace two RDH techniques, one is a customary RDH that keeps the nature of pictures and the other is a brought together data inserting and scrambling strategy that may extraordinarily debases picture structures for implanting huge payload.

2) Transformation

Transformation is a capacity. A capacity that guides one set to another set in the wake of playing out operations.

3) Digital Image Processing system.

We have effectively found in the starting instructional exercises that in computerized picture preparing, we will foster a framework that whose info would be a picture and yield would be a picture as well. Furthermore, the framework would play out some preparing on the info picture and gives its yield as a handled picture. -function applied inside this computerized framework that interaction a picture and convert it into yield can be called as transformation function

B. Image transformation.

Think about this condition

$G(x,y) = T\{ f(x,y) \}$

In this condition,

F(x,y) = input picture on which transformation function must be applied.

G(x,y) = the yield picture or handled picture.

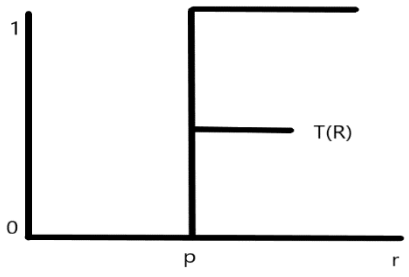
T is the transformation function.

This connection between input picture and the handled yield picture can likewise be addressed as.

$s = T(r)$

where r is really the pixel worth or dim level force of f(x,y) anytime. What's more, s is the pixel worth or dim level power of g(x,y) anytime. The essential dim level transformation has been examined in our instructional exercise of fundamental dim level transformations. Presently we will talk about a portion of the essential transformation functions.

1) Examples



Consider this transformation functio n.

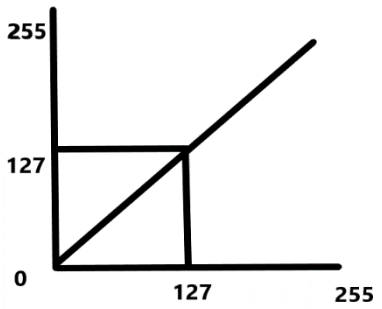
Lets take the guide r toward be 256, and the direct p toward be 127. Believe this picture to be a one bpp picture. That implies we have just two degrees of powers that are 0 and 1. So for this situation the transformation appeared by the diagram can be clarified as.

All the pixel force esteems that are under 127 (point p) are 0, implies dark. And all the pixel power esteems that are more prominent then 127, are 1, that implies white. However, at the specific mark of 127, there is an abrupt change in transmission, so we can't tell that at that careful point, the worth would be 0 or 1.

Numerically this transformation function can be signified as:

$$g(x,y) = \begin{cases} 0 & f(x,y) < 127 \\ 1 & f(x,y) > 127 \end{cases}$$

Consider another transformation like this



Presently on the off chance that you will take a gander at this specific diagram, you will see a straight change line between input picture and yield picture.
It shows that for every pixel or force worth of info picture, there is an equivalent power worth of yield picture. That implies the yield picture is careful reproduction of the info picture.
It very well may be numerically addressed as:
$g(x,y) = f(x,y)$
the input and output picture would be for this situation are appeared underneath.

V. SYSTEM ARCHITECTURE

Since losslessly emptying room from the mixed pictures is moderately troublesome and in some cases wasteful, for what reason would we say we are still so fixated to discover novel RDH methods turning out straightforwardly for encoded pictures? On the off chance that we turn around the request for encryption and abandoning room, i.e., holding room going before picture encryption at content proprietor side, the RDH errands in encoded pictures would be more trademark and much easier which drives us to the novel framework, "saving room before encryption (RRBE)". As demonstrated in Fig. 1(b), the substance proprietor first hold adequate room on unique picture and afterward changes over the picture into its scrambled rendition with the encryption key. Presently, the information implanting measure in encoded pictures is intrinsically reversible for the information hider just necessities to oblige data into the additional room past released out. The data extraction and picture recuperation are indistinguishable from that of Framework VRAE. Clearly, standard RDH calculations are the ideal executive for saving room before encryption and can be effortlessly applied to Framework RRBE to accomplish better execution contrasted and strategies from Framework VRAE. This is on the grounds that in this new structure, we follow the standard thought that first losslessly packs the excess picture content (e.g., utilizing incredible RDH procedures) and afterward scrambles it concerning ensuring protection. Then, we elaborate a functional strategy dependent on the Framework "RRBE", which fundamentally comprises of four phases: age of mixed picture, data concealing in encoded picture, data extraction and picture recuperation. Note that the saving activity we receive in the proposed strategy is a conventional RDH approach.

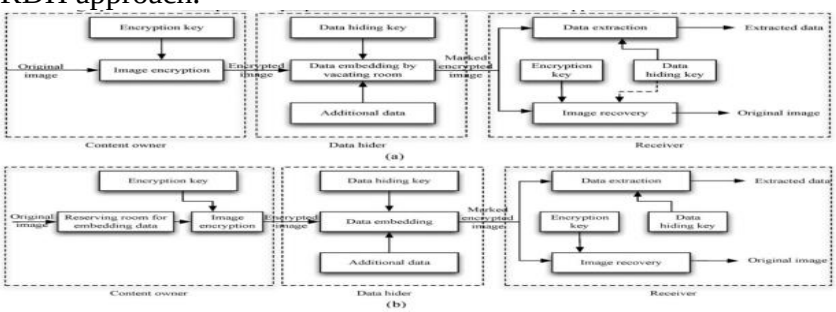


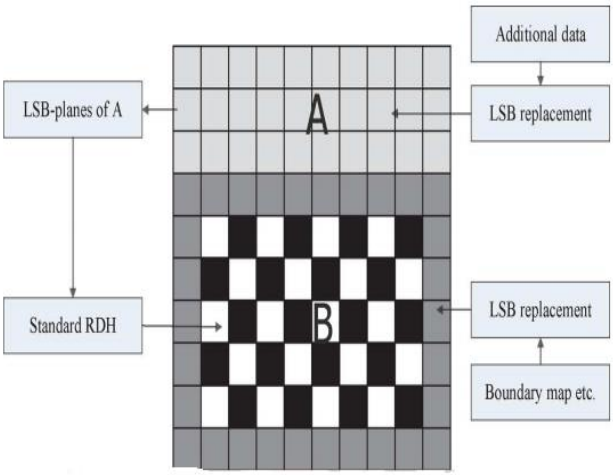
Fig-1: Framework: "vacating room after encryption (VRAE)" versus system: "reserving room before encryption (RRBE)." (Dashed line in (a) states that the need of information concealing

key in picture recuperation fluctuates in various pragmatic techniques). (a) Framework VRAE. (b) Framework RRBE.

A. Encrypted Image Generation

Encrypted Image Generation In this module, to develop the scrambled picture, the primary stage can be partitioned into two stages. Picture Partition and Self Reversible Embedding followed by picture encryption. Toward the start, picture parcel step isolates unique picture into two sections An and B; at that point, the LSBs of An are reversibly inserted into B with a standard RDH estimation so LSBs of A can be utilized for obliging messages; finally, scramble the modified picture to produce its last form

The substance proprietor, thusly, chooses the specific square with the most elevated to be , and puts it to the front of the picture linked by the rest part with less finished regions,



B. Data Hiding In Encrypted Image

In this module, a substance holder encodes the first picture utilizing a standard code with an encryption key. Subsequent to creating the encoded picture, the substance proprietor gives up it to an information hider (e.g., a data set director) and the information hider can install some assistant information into the scrambled picture by lossless abandoning some room as per an information concealing key. At that point a collector, perhaps the substance proprietor himself or an approved outsider can remove the installed information with the information concealing key and further recuperate the first picture from the scrambled rendition concurring

C. Data Extraction and Image Recovery

In this module, the information extraction is totally not reliant upon picture decryption, thus this request suggests two unique methods of down to earth applications, for example,

1) Extracting Data From Encrypted Images:-

To oversee and refresh individual data of pictures which are encoded for ensuring customers' protection, a substandard data set administrator may just gain admittance to the information concealing key and need to control information in encoded area. At the point when the information base chief gets the information concealing key, he can decode and separate the extra information by straightforwardly perusing the unscrambled form. While mentioning for refreshing data of encoded pictures, the data set director, at that point, refreshes data through LSB substitution and encodes up dated data as per the information concealing key once more. As the entire cycle is altogether worked on encoded space, it maintains a strategic distance from the spillage

2) Extracting Data From Decrypted Images:-

For this situation, the client needs to decode the picture first and concentrates the information from the unscrambled picture when it is required. The accompanying model is an application for such situation. Expect Alice reevaluated her pictures to a cloud worker, and the pictures are encoded to secure their substance. Into the encoded pictures, the cloud worker marks the

pictures by installing some documentation, including the character of the pictures' proprietor, the personality of the cloud worker and time stamps, to deal with the encoded pictures. Note that the cloud worker has no option to do any

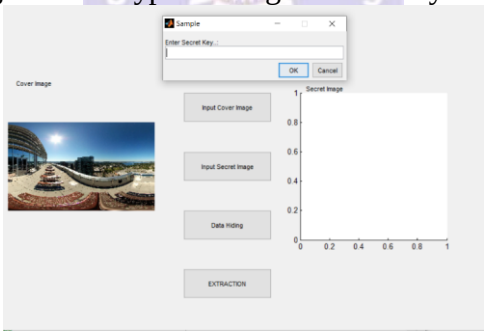
lasting harm to the pictures. Presently an approved client, Bob who has been shared the encryption key and the information concealing key, downloaded and decoded the pictures. Weave expected to get checked decoded pictures, i.e., unscrambled pictures actually including the documentation, which can be utilized to follow the source and history of the information. The request for picture decoding previously/without information extraction is completely appropriate for this case. All the more explicitly, the mutilation is presented by means of two separate ways: the implanting interaction by adjusting the LSB-planes of and self-reversible implanting measure by inserting LSB planes of into . The initial segment mutilation is very much controlled through abusing the LSB-planes of just and the subsequent part can profit by magnificent execution of current RDH proceduresof unique substance.

D. Data Extraction and Image Restoration

n this module, in the wake of creating the checked unscrambled picture, the substance proprietor can additionally remove the information what's more, recuperate unique picture. Reversible covering up permits extraction of the first host signal and furthermore the inserted message. There are two significant prerequisites for reversible information concealing procedures: the installing limit need to be huge; and contortion ought to be low. These two prerequisites struggle with one another. All in all, a higher implanting limit brings about a more serious level of contortion. An improved procedure inserts a similar limit with lower bending or the other way around.

VI. IMPLEMENTATION

Step 1: Taking a cover image and encrypted using a Secret key as shown below:



Step 2: Choosing the image(Secret image) which you want to hide into cover image as shown below

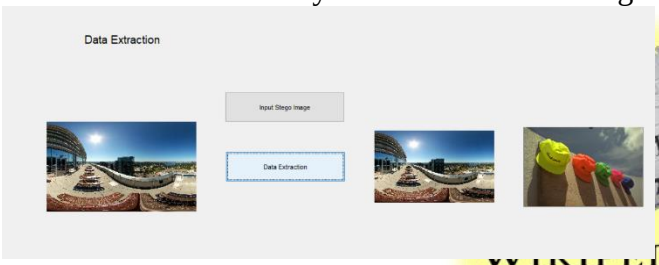
Step 3: Date hiding:

Then again, cloud administration for reevaluated capacity makes it trying to get the assurance of picture substance. For instance, actually various private photos of Hollywood entertainer spilled from iCloud Although RDH is useful for dealing with the rethought pictures, it can't secure the image content. Encryption is the most celebrated technique for ensuring security. So it is intriguing to execute RDH in encoded pictures (RDH-EI), by which the cloud laborer can reversibly introduce data into the image yet can not get any data about the image

substance. Impelled by the necessities of security assurance, numerous techniques have been introduced to stretch out RDH strategies to encryption region. From the point of view of pressing factor, these techniques on RDH-EI have a spot with the accompanying two structures Framework I "abandoning room after encryption (VRAE)" and Framework II "saving room before encryption (RRBE)

Step 4: Extraction

Enter the same secret key to revel the secret image as shown below



If the secret key doesn't match with the original key it replays as invalid secret key

VII. CONCLUSION

In this paper we propose a novel framework for reversible information laying by in scrambled picture (RDH-EI) in light of reversible picture change (RIT). Not quite the same as past systems which scramble a plaintext picture into a ciphertext structure, RIT-based RDH-EI shifts the semantic of remarkable picture to the semantic of another image and in this way secure the protection of the first picture. Since the scrambled picture has the sort of a plaintext picture, it will avoid the documentation of the curious cloud specialist and it is free for the cloud slice off to pick any of RDH procedures for plaintext pictures to introduce watermark. We comprehend a RIT based technique by improving the image change method in to be reversible. By RIT, we can change the main picture to a self-emphatic picked target picture with a comparable size, and restore the primary picture from the mixed picture in a lossless way. Two RDH procedures including PEE-based RDH and UES are gotten to embed watermark in the mixed picture to satisfy different necessities on picture quality and embedding limit.

REFERENCES

[1] T. Kalker and F.M.Willems, "Capacity bounds and code constructionsfor reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76

[2] J. Tian, "Reversible data embedding using a difference expansion,"IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.2010.Process., vol. 19, no. 4,pp. 1097– 1102, Apr. 2010.

[3] Z. Qian and X. Zhang, "Reversible data hiding in encrypted images with distributed source encoding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 4, pp. 636–646, 2016

[4] F. Huang, J. Huang, and Y. Q. Shi, "New framework for reversible data hiding in encrypted domain," IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2777–2789, 2016

[5] Z. Yin, A. Abel, J. Tang, X. Zhang, and B. Luo, "Reversible data hiding in encrypted images based on multi-level encryption and block histogram modification," Multimedia Tools and Applications, vol. 76, no. 3, pp. 3899–3920, 2017
[6] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," Signal Processing, vol. 144, pp. 134 – 144, 2018
[7] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang, "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 3, pp. 441–452, 2016
[8] Z. Yin, H. Wang, H. Zhao, B. Luo, and X. Zhang, "Complete separable reversible data hiding in encrypted image," Cloud Computing and Security: First International Conference, ICCCS 2015, pp. 101–110, 2015.
[9] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," Signal Processing, vol. 97, pp. 172 – 182, 2014.
[10] X. Liao, K. Li, and J. Yin, "Separable data hiding in encrypted image based on compressive sensing and discrete fourier transform," Multimedia Tools and Applications, vol. 76, no. 20, pp. 20 739–20 753, 2017
[11] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," Signal Processing, vol. 97, pp. 172 – 182, 2014.
[12] X. Liao, K. Li, and J. Yin, "Separable data hiding in encrypted image based on compressive sensing and discrete fourier transform," Multimedia Tools and Applications, vol. 76, no. 20, pp. 20 739–20 753, 2017