International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Secure Data Hiding using Reversible Image Transformation

Farisa T S, Anaha Ashokan, Eldo P Elias

Abstract: ***In today's era, the large amount of data's are stored in cloud. But nowadays securely storing data to the cloud is an important task. But the unauthorized parties are tries to decrypt the data from the cloud. So, the data stored in cloud should be secure from any malicious activities. Based on these requests, we propose a framework named reversible data hiding (RDH). It mainly works on encrypted images based on reversible image transformation (RIT). The server insert data into the cloud. On that time, he will add some additional information for the protection of data. In the given framework, the original data can be embedded in another image named carrier image with equal size. So, the hacker tries to pullout the data, he will only get the carrier image. So we can accommodate more data's into a single storage space. The method picks the data to be hide and a carrier image with equal size. The cover image is embedded into the original image based on the LSB insertion algorithm. i.e., the original data's are dissolved into the carrier image using a secret hiding key. The cover image is encrypted using blow fish encryption algorithm. It includes normal RDH method and RDH with RIT. Using RIT, it gives high visual quality and security. The technique is mainly used in medical imagery, military imagery for reliable data storage.***

Keywords : Carrier image, Original image, RDH, RIT

I. INTRODUCTION

In today's era, the large amount of data's are stored in cloud. But nowadays securely storing data to the cloud is an important task. The server insert data into the cloud. On that time, he will add some additional information for the protection of data. Obviously, the provider has no proper right to launch the permanent distortion when embedding data into another carrier image. Therefore, RDH is required which allows the original image to be retrieved after the cover data has been extracted. The system is mainly used in medical imaging, military imagery and forensic control, where high security of original data is needed. So far a number of techniques for RDH have been proposed on the images and text. Essentially, all of these techniques can be interpreted as a technique of semantic compression, where in additional statistics are reserved to be inserted with the aid of lossless compression of the original data. Compressed image in semantic compression should be near the original cover image, so you can get high quality image. Because the residual component of artifacts such as the errors of prediction has low entropy and can be easily compressed. Nearly all the new RDH procedures produce errors first because the host sequence reversibly integrates the message into the host sequence with the aid of editing the message. The histogram is edited with the techniques such as histogram shifting or distinction expansion, etc. Currently Zhang ET suggested the finest RDH histogram updated by estimating the optimum probability of modifications. On the opposite side, cloud storage carrier makes protecting the privacy of photo content difficult. For example, most private images of the Hollywood actress recently leaked out of iCloud. Although RDH helps control the stored data, it cannot safeguard the probity of data. Encryption is one of the popular technique used to protect privacy. Therefore, it is essential to implement RDH in encrypted data, whereby the server can inject data into the image. But the intruder cannot obtain any knowledge about the picture material. Inspired by the privacy needs, many methods for applying RDH techniques to the domain of encryption that have been suggested. As far as compression is concerned, RDH is mainly based on two methods: "booking room before encryption (RRBE)" and "vacating room after encryption (VRAE)" respectively. In the VRAE system, the server insert some statistics through the use of the concept of compressing encrypted images by vacating room from the encrypted data. Compression of statistics may be considered as supply coding at the decoder with side information. RDH is a mechanism for reversible-based hiding of data. The hiding is mainly done on encrypted images. The system allows the user to convert the original data content into another equally sized carrier file. So the hacker is trying to decrypt the data which will only get the picture of the carrier. Here the original data can be retrieved losslessly after removing the embedded code. The method can hide a data on a different image; so we can fit more data in a single storage space. The system is mainly used in medical imaging, military imagery and forensic control, where high security of original data is needed. The method picks the data to be hide and a carrier image with equal size. Using insertion of LSB, the secret data is inserted into the carrier image.

Revised Manuscript Received on March 17, 2020.
* Correspondence Author
Farisa T S*, Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Ernakulam, India. Email: farisafari1996@gmail.com
Anaha Ashokan, Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Ernakulam, India. Email: anu22ashok1997@gmail.com
Prof. Eldo P Elias, Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Ernakulam, India. Email: eldope@gmail.com

The hidden message is hard to identify in the process of insertion into LSB. We take care of hiding the message, based on the process. i.e., secret data is enter first and then it is represented in a binary form. LSB is overwritten with a carrier image for each bit. Then encrypt the cover image using blow fish encryption algorithm.

II. RELATED WORKS

All sectors require secure storage of the data. In many instances, data hiding scenarios have some distortion across the cover object, and cannot transfer it back to the original data. It can be mainly done, because even after the secret information has been removed a few parameters can be skewed over the cover item. But in RDH, after the message is removed the original cover item is recovered correctly. The RDH technique is commonly used in medical, military fields etc. no alteration of the original object is permitted here.

A. RDH with Distributed Source Encoding (DSE) in Encrypted Images

RDH used DSC in encrypted images in 1966. After the content provider uses a stream cipher to leverage the original data, the hider squeezes a chain of selected bits taken from the encrypted image. Here a space is created for original facts. Low density parity check (LDPC) codes are used to encode the agreed on bit array. In case the receiver only has the encryption key, using an algorithm for image estimation, it can recover the original material with visual quality approximately. If embedding and encryption keys are visible to the receiver using the open source encoding, the original data can be retrieved perfectly. The proposed method outperforms formerly published ones. Because estimating MSB is far more accurate than evaluating the LSB planes, the original records of MSB plane [6] can be retrieved with appropriate deciphering via DSC interpretation. First of all the original image is encrypted in this process. After encryption the owner of the content sends the encrypted data to the hider of the documents. The statistics hider first break down the encrypted fact F into 4 sub-facts F(1), F(2), F(3) and F(4) to insert some additional data into the image, with each size blunders portability M/2N/2.Bits of planes of the F(2), F(3), and F(4) sub-snap shots are obtained, and produces 3MN/4 bits total. The hider arbitrarily choose L bits (1L3MN / four) from them using a selection key KSL, and shuffles the selected bits. The shuffling is done through a key. The secret records may be retrieved using the embedding key with the specified encrypted file. And the original image can be restored roughly using the encryption key, or the use of either key can be retrieved losslessly. The receiver removes the hidden information contained based on the key and the values.

Split X into four subsets X(1), X(2), X(3) and X(4). Assemble all bits inside the planes of the MSB and pick L bits according to the key of choice. Shuffle the selected bits based on the use of the KSF key, and cut the shuffled segments into K departments, each with n bits. The hidden statistics can thus be replicated by combining bits from all K classes, and decrypted using the key to the plain text letter. If each receiver has the encryption key and embedding keys, he / she can successfully takeout the hidden information, and perfectly boost the original data. The beneficiary takes the L agreed on bits in the MSBs of the sub-images using the embedding key. The receiver generates an estimated image of the use of the estimation algorithm with the encryption key. The proposed device features include the probability of error calculation of the plane. It can be less than calculating alternate flights. Extraction of the larger implant records and restoration of the image is separable inside the container, using DSC [5] can be accomplished. Health at extraction can also be assured. And it enhances the payload embedding, too. The system's drawbacks are mainly on image restoration, though some noise may occur when the marked encrypted images are directly decrypted. Compression performance and estimation of plane LSB is inadequate. So to eliminate the noise at some stage in the image recovery, we proposed reversible information hiding the usage of reversible image transformation. From this paper for the mission the technique for extraction safety is followed. The technique for decreasing the payload is likewise implemented within the challenge.

B. Separable RDH Method in Encrypted Data

It's a singular method for RDH in encrypted pictures. Within the first section, a content man of affairs encrypts the initial uncompressed data supported by the usage of associate degree cryptography key. Then the insufficient amount bits of encrypted knowledge is compressed by the record hider. It'll be done exploitation associate degree information-hiding key. It's principally accustomed offer some storage space for a few extra knowledge. Once the encrypted information includes extra records and the recipient has the hiding key, certain extra details will be taken out while the image material is not known. The receiver decipher the collected knowledge once he has the primary cryptography key [7]. The encrypted image is close to the primary image, however he cannot pullout the additional knowledge to be extra. Once the receiver has the primary cryptographic key, then he deciphers the accumulated information. The encrypted image is similar to the primary image, but he can't extract the extra knowledge. If the beneficiary has the key to cryptography, he must decode the information obtained to trigger a picture just like the original. He can't pull out the extra records though. If the receiver has each the key to conceal statistics and the key to cryptography, the additional facts will be leveraged. Then, with no mistakes, it will find that the initial content is higher. As a consequence of the big fashion of additional information is not too growing, it is helpful for the tool to leverage the spatial connection in natural image at the same time. The proposed strategy is made from embedding details about picture encryption and phases of facts-extraction /photo-recovery. The owner of the content encrypts the uncompressed picture based on using a key to deliver an encrypted image.

Then the hider squeeze the encrypted image with the smallest amount of substantial bits of LSB. Use of an information-hiding key to make the additional data a sparse place to deal with. The records embedded within the generated space will be easily retrieved results from the encrypted photo with extra information at the receiver point.

The information is normal with the information-hiding key. Puzzling over the very fact that the statistics embedding handiest infect the LSB of decryption with the key may also additionally find yourself in an exceedingly picture rather like the preliminary version. While the use of each of the encryption key and data hiding keys would effectively remove the hidden additional facts and thus the first image will be retrieved flawlessly using the natural image spatial correlation.

In an uncompressed form, the data in the image format is encrypted via the initial image with a time n1x n2 and pixel value with gray charge is formulated by eight bits. Several boundaries are stored in a small form of encoded pixels. The LSB of chance of encoded pixels is compressed to allow a proximity to fit the additional data. The first place statistics were occupied by the values of parameters. The facts-hider pick up the pixels to keep with an information-hiding key which can be delivered through the parameters. Here, Np is also a tiny low high-quality. It is a first-rate integer divided into businesses, each of which contains L pixels [3]. With an encoded data containing added records and the recipient has only the hiding key. Then he may additionally moreover first accumulate the values of the parameters. So one or later of this device two instances decryption takes place. It includes region of the decryption of original photo and decryption of carrier photograph. The gain of the machine is that it makes use of a straightforward approach of know-how hiding. The two encryption keys are furnished for records security however the effort is that it's a time consuming technique with two encryption and decryption respectively. So to lower the tactic of experience hiding and decryption we put into effect reversible records hiding based on the usage of reversible image transformation. The normal encryption method is followed from this paper and a way to hide a photograph from an interior image is studied and understood from this paper.

C. A Secure Approach for RDH Using Virtual Cryptography

Data is the central bit of correspondence among sender and beneficiary. So it must be secure and confirmed. Recently there are many methods for securely storing the data. The methods includes Cryptography, Steganography etc. Cryptography implies the examination of logical methodologies and related pieces of information. Security is like data characterization, uprightness and affirmation. RDH is getting some portion of essentials. RDH is just securely transmitting data inside a cover image. The ultimate objective is that data and spread record can be suitably recovered at the beneficiary. This paper offers a key less reversible technique of hiding data before encryption of images to make hiding strategy of data easy. Today, there is no area of particular endeavor for all intents and purposes that is not affected in any way by taking care of cutting edge image. The uses of taking care of cutting edge pictures are so vast. The suggested strategy works on five rule steps; clearing data inserting space, embedding data in spared relinquished space, image encoding, picture recovery, and extraction of data[8]. Device isolates an image into individual sections of the RGB. Then it stores each component in the portions concerned. So firstly we are detaching the pixel regard into three sections, so the chase space we get is on different occasions are more. The purpose of the suggested system is to equip all out reversibility with the least amount of calculation using cryptography. Saving space for data embedding involves

Splitting one of a kind image into separate RGB pieces and finding the base value pixels using DE system among the pixel sets. In addition, it can be used to oblige data. The fact is to be in exhausted domain by then after the introduction stage. This image will be combined before and after the data is inserted using SDS computation. SDS count combines the three fundamental Sorting, and Shuffling progresses. Sieving involves riddle of the joined sections of RGB into particular parts of R, G and B. The resulting stage involves parceling the sections R, G and B into shares in the wake of filtering through the primary image into R, G, and B bits. Modification of categories inside separate deals. The pieces are generally modified using bit cutting and bits shift. We dive into four proportional offers no. of uncertain ideas. The unpredictable offers delivered autonomously don't give any information about the riddle picture, anyway all self-assertive offers would be needed to retrieve the substance of an image. In wake of recollecting all the unpredictable modified data shares, special picture redoing can be performed. In picture recouping stage, the primary picture incorporates sieving the discretionary offers and reviewing all the reworked shares. Further from these individual improved offers the main picture can be made and data is recuperated as well. In addition to these individually enhanced deals, the main picture can be made, and data is also recovered. The newly determined pixel look is considered in data extraction organize and distinction is resolved again using the same technique of Difference Expansion [2] in switch demand. The record location of those squares and the pixel sets circumstance; where the data has been stored, it is necessary to losslessly delete remarkable material. The advantage of the structure is that it uses a keyless encryption, so the amount of steps in picture encryption is diminished. In any case, the security of one of a kind picture is diminished. So to give all out security of special picture we like to execute reversible data disguising using reversible picture change. From this paper get the procedure for randomly cutting and moving of bits that is required in our endeavor.

Security is considered as most huge essential factor in any correspondence structures. Issues in such security structures are decency, insurance, affirmation and non-repudiation, such issues must be dealt with warily. Here the security destinations are specifically: protection, openness and dependability that can be undermined by security attacks. So to shield the main information from such attacks the data covering methodologies are completed. Data hiding frameworks embeds remarkable data which we would incline toward not to disclose into spread media by introducing slight palatable changes. It is significant to embed the data into a propelled media to pass on the secret messages. The owner can change the main substance of the media using pictures, with the objective that the introduced data is concealed. If we can apply RDH to scramble picture,

by then some incredible applications can be made through it. This technique can be comprehensively used in various fields, for instance, clinical, military and law wrongdoing scene examination, where reshaping of the primary spread isn't allowed. RDH technique is used to embed additional fact into spread media, for instance, picture or video. Starting late various new RDH methods are made which gives normal structure for RDH. It works by first turn out the properties of the primary spread media and a short time later pressing them without mishap, extra room can be saved by introducing partner data. Focus of this system is to achieve strategy for ensured about transmission of significantly sensitive information over the web. Encryption is the most well-known technique for making sure about security. So executing RDH in mixed pictures is charming, by which the server can insert data into the another picture anyway can't get any data. Animated by the security defense needs, different systems have been shown to loosen RDH methods into space for encryption.

III. METHODOLOGY

Redistributed cut off by cloud changes into an obviously even more striking help, primarily for natural media records requiring extra space for monsters. To handle the re-appropriated data, the server can install some additional facts into the original data, such as picture course of action and documentation details, and use such information to perceive possession or, of course, to test image reliability. The cloud has no benefit in displaying unceasing bending in the re-appropriated images during information embedding. RDH progression is therefore needed, by which the critical image can be retrieved on the extraction of data. This technique is also used widely in clinical symbolism, military symbolism and criminology of law, where no twisting of the fundamental spread is permitted. Numerous RDH techniques on pictures have been proposed up to this point. Essentially, these systems can be seen as a technique for semantic lossless weight, in which storage is saved by lossless squeezing the picture to provide additional information. Now it deduces that the stuffed image should be similar to the first one, and right now it can get a ventured image with amazing visual quality. Since standing by some portion of the images, e.g. the longing bungles (PE), has hardly been available.

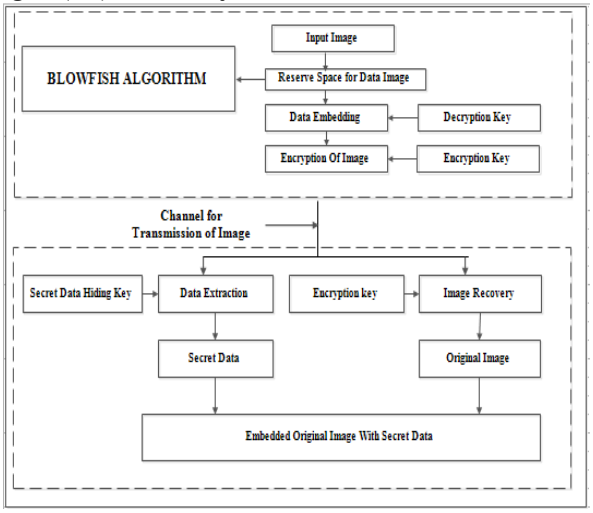

Fig. 1. System architecture [5]

A. Reversible Data Hiding

The framework shows a reversible data anticipating count, which can recover the primary picture without mutilation from the stepped picture after the hid data have been expelled. This estimation utilizes the zero or on the other hand the base reason for the histogram and to some degree changes the pixel regards to introduce data. It can embed more data when diverged from most by far of the existing reversible data hiding estimations. Reversible Information Covering up (RDH) is where the first picture can be recovered with no mishap after the covered message is recuperated. Right now, is performed by the sender, by embedding's the data hider, what's more, data extraction or possibly picture restored by the beneficiary. The story plot which is RDH in pictures using Blowfish Algorithm improves the security level of picture encryption. The genuine spread picture is sent to the data hider where it packs a gathering of supported least vital bits investigated the image to exhaust the spot for the puzzle data to be concealed. By then the data embedded picture is being mixed using the square figure methodology which is the blowfish count. At the recipient end, the covered message can be recouped on the off chance that the recipient has recently the embedding key which is the private key. Accept the recipient has recently the encryption key for instance the secret key, the recipient can recover the veritable picture with no bending. If the beneficiary has both the private and riddle keys, the gatherer can recoup the concealed data and ideally recuperate the genuine picture with high security level.

B. Blowfish

The proposed Blowfish is structured utilizing a memory based method to improve its presentation. This plan is broadly assessed dependent on three zones. The principal territory is the design parameter, which is utilized to get a base equipment necessity that can prompt a littler structure size. The subsequent zone is a high-throughput plan to do an encryption/unscrambling as quickly as conceivable. At long last, the third region is the low force structure, which looks to limit power utilization no matter what. This examination can help specialists settle on the chance of executing Blowfish for a safe remote correspondence rather than AES. As the usage of the Blowfish configuration is directed to decrease the center size and timing delay, the proposed memory based S-box strategy is advanced as represented in Fig. 2. In light of the Verilog structure module. In the current technique employments a read-just memory (ROM) that contains 1024 32-piece input information of addr. In the proposed technique we lessen the read-just memory (ROM) that contains 512 32-piece input information of addr, to diminish the territory and deferral of the current strategy. The addr speaks to the information of four 32-piece S-boxes with 256 passages each. The 32-piece yield information are perused from the ROM at a positive clock edge. The proposed technique can likewise decrease the aggregate of cuts utilized by the Blowfish structure. A cut contains a set number of look-into tables (LUTs), FFs, and multiplexers. Consequently, less rationale assets are utilized to perform rationale,

number-crunching, and ROM works that can prompt a quicker encryption/unscrambling process. Then again, cloud administration for redistributed capacity makes it trying to ensure the security of picture substance. Blowfish is mainly used for symmetric key encryption. It is mainly used as an expansion of DES algorithm For example, as of late numerous private photographs of Hollywood entertainer spilled from iCloud. In spite of the fact that RDH is useful for dealing with the redistributed pictures, it can't secure the picture content. Encryption is the most well-known method for ensuring security. So it is fascinating to actualize RDH in encoded pictures (RDH-EI), by which the cloud server can reversibly install information into the picture however cannot get any information about the picture substance. Motivated by the necessities of security assurance, numerous techniques have been displayed to stretch out RDH strategies to encryption area. From the perspective of pressure, these strategies on RDH-EI have a place with the following two structures Framework I "abandoning room after encryption (VRAE)" and Framework II "saving room before encryption (RRBE) ".In the system "clearing room after encryption (VRAE)", the cloud server inserts information by losslessly emptying room from the scrambled pictures by utilizing compacting encoded pictures . Pressure of encoded information can be detailed as source coding with side data at the decoder. Normally the side data is the connection of plaintexts that is misused for decompression by the decoder.

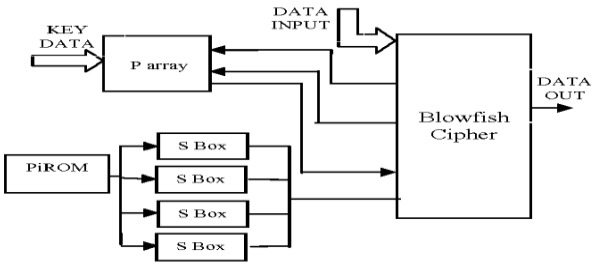

Fig. 2. Blowfish algorithm [8]

IV. EXPERIMENTAL RESULT

A. Registration Page

Register to the system using our valid details. Enter the details like Name, Place, and email-id and set a username and password.

Fig. 3. Registration page

B. Login Page

If already registered in to the system, login to the system using valid username and password. Otherwise sign-up to the system with valid details and then login to the system.

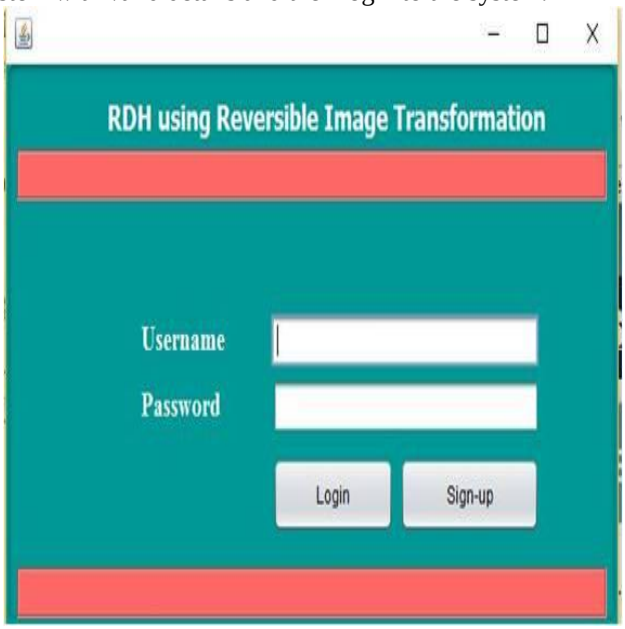

Fig. 4. Login page

C. Home Page

The home page includes two methods: i.e.; Normal data hiding and RDH method. In normal data hiding the carrier image is expose to others. In RDH, we have two options such that image and text. Select the option then click the"Go" button.

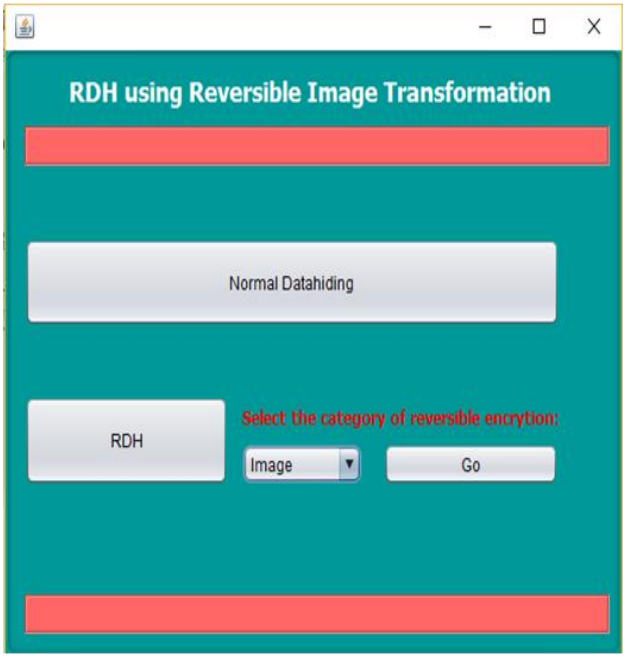

Fig. 5. Home page

D. Normal Data Hiding

In normal data hiding, first select a carrier image and then enter the text to be hide. Then hide the text in a location. Unhide the text using carrier image.

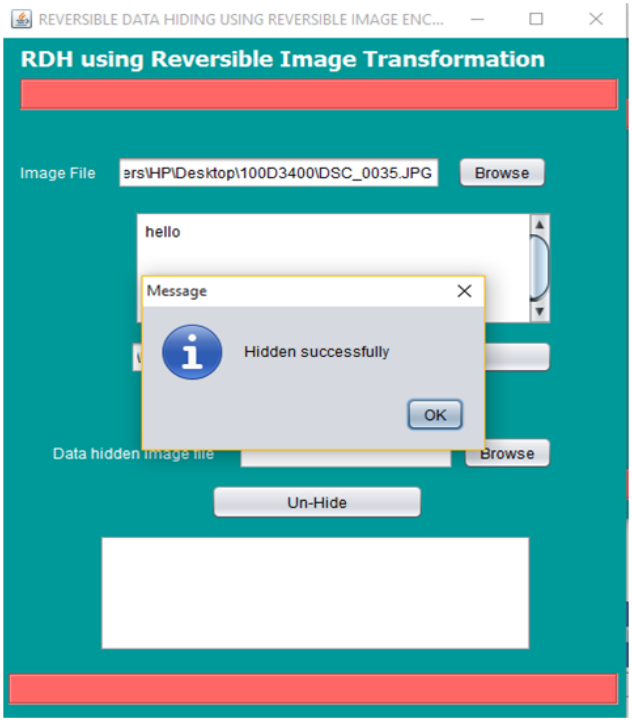

Fig. 6. Normal data hiding

E. RDH with text

In RDH with text first choose a carrier image that text has to be hide the text. Enter the data to be hided. Then hide the text in a carrier image. Encrypt the hided data and decrypt it from the carrier image. It only shows the carrier image and then unhide the text from carrier image. The original data is secured in a carrier image. When a hacker tries to decrypt the data it only gets the carrier image.

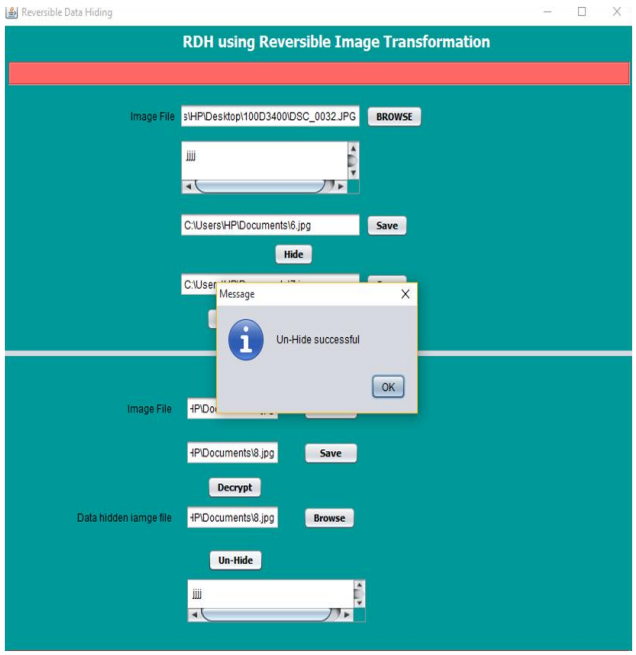

Fig. 7. RDH with text

F. RDH with image

Choose a carrier image to hide the original image. Browse the image to be hided. The original image is saved in a location and then hided successfully. So the original image is secured in a carrier image. After the encryption the original and carrier image is does not expose to any other users.

Fig. 8. Hide the image using carrier image

Encrypt the hided data and decrypt it from the carrier image. It only shows the carrier image and then unhide the image from the carrier image.

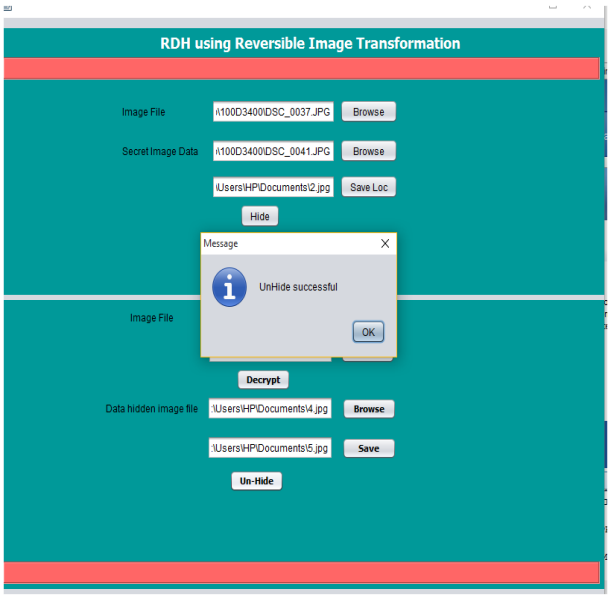

Fig. 9. Unhide the image

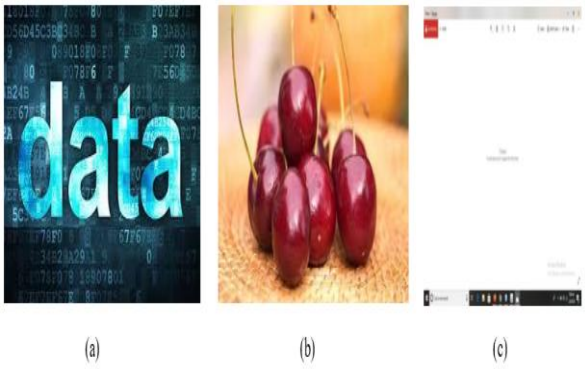

Fig. 10. (a)Original Image (b) Carrier Image (After hide the original image) (c) Encrypted image

Retrieval Number: C6395029320/2020©BEIESP
DOI: 10.35940/ijeat.C6395.049420
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

V. CONCLUSION

The endeavor uses a novel structure for reversible data concealing in mixed picture (RDH-EI) in perspective on reversible picture change (RIT). Interesting according to past structures which scramble a plaintext picture into a figure content structure, RIT based RDH-EI shifts the semantic of interesting picture to the semantic of another image and right now the security of the special picture. Since the mixed picture has the sort of a plaintext picture, it will avoid the documentation of the curious cloud server and it is free for the cloud slice off to pick any of RDH systems for plaintext pictures to introduce watermark. Comprehend a RIT based procedure by improving the picture change framework in to be reversible. By RIT, can change the primary picture to an emotional picked target picture with a comparative size, and restore the main picture from the mixed picture in a lossless way. Two RDH systems tallying PEE-based RDH and UES are grasped to embed watermark in the mixed picture to satisfy different necessities on picture quality and embedding limit. A couple of entrancing issues can be viewed as later on, including how to improve the idea of the mixed picture and how to grow thought of RIT to sound and video.

REFERENCES

1. X. Cao, L. Du, X. Wei, et al., “High capacity reversible data hiding in encrypted images by patch-level sparse representation,” IEEE Trans. On Cybernetics, vol. 46, no. 5, pp. 1132-1143, May. 2016.
2. Y. Lee and W. Tsai, “A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformation,” IEEE Trans. on Circuits and Systems for Video Technology, vol. 24, no. 4, pp. 695-703, Apr. 2014.
3. X. Hu, W. Zhang, X. Li, N. Yu, “Minimum rate prediction and optimized histograms modification for reversible data hiding,” IEEE Trans. on Information Forensics and Security, vol. 10, no. 3, 653-664, Mar. 2015.
4. X. Hu, W. Zhang, X. Hu, N. Yu, X. Zhao, F. Li, “Fast estimation of optimal marked-signal distribution for reversible data hiding,” IEEE Trans. on Information Forensics and Security, vol. 8, no. 5, pp. 779-788, May. 2013.
5. Pradnya P. Mandlik, Samruddhi S. Mhatre, Hiding Data into Reserve Space before Image Encryption using Blowfish Algorithm, Volume 140 – No.10, April 2016.
6. Z. Qian, and X. Zhang, “Reversible data hiding in encrypted image with distributed source encoding,” IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 4, pp. 636-646, Apr. 2016.
7. W. Zhang, K. Ma and N. Yu, “Reversibility improved data hiding in encrypted images,” Signal Processing, vol. 94, pp. 118-127, Jan. 2014.
8. ChanchalD.Pande1,Prof.S.S.Mungona2 An Approach for High Speed Data Cryptography Technique of Blowfish Algorithm using VHDL, Vol. 4, Issue 5, May 2017.

AUTHORS PROFILE

Farisa T S received Bachelor of Technology in Computer Science and Engineering from KMEA Engineering College Edathala in 2018 and currently pursuing Master of Technology in Computer Science and Engineering from Mar Athanasius College of Engineering, Kothamangalam affiliated to APJ Abdul Kalam Technological University. Her research interest is in Computer Security.

Anaha Ashokan received Bachelor of Technology in Computer Science and Engineering from Christ Knowledge City Engineering College Mannoor, Muvattuppuzha in 2018 and currently pursuing Master of Technology in Computer Science and Engineering from Mar Athanasius College of Engineering, Kothamangalam affiliated to APJ Abdul Kalam Technological University. Her research interest is in Computer Security.

Prof. Eldo P Elias is currently working of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India. He received his B-Tech Degree in Computer Science and Engineering in 2003 from Bharathiar University, Coimbatore and M-Tech in Computer and Information Sciences from Cochin University of Science and Technology, Kochi in 2013. He has around 14 years of teaching and research experience in various institutions in India. His research interests include Computer Security, Computer Architecture, Operating Systems and Data Science.