Separable Reversible Data Hiding Using Rc4 Algorithm

[1]Prof.Swapnil Wani, [2]Mr.Nikhil Patil, [3]Miss Juiely Rane, [4]Mr.Sagar Patare

[1]Asst.Professor,[2,3,4]UG Student,[1,2,3,4]Computer Engg. Dept. Shivajirao S.Jondhle College of Engineering & Technology, Asangaon, Maharashtra, India.

[1]swapnilwani24@hotmail.com, [2]pnikhil944@gmail.com, [3]rane.juiely@gmail.com, [4]s.patare11@gmail.com

Abstract- Separable reversible data hiding using RC4 algorithm is alluded to as a procedure of hiding data in the encrypted image. Unique theme for separable reversible information hiding in the encrypted image is proposed in the system. In the principal period of the system, a receiver encodes the underlying uncompressed image utilizing a cryptography key that utilizes RC4 cryptography algorithm. Then, an information-hider hides some confidential data using data-hiding key. On the receiver end, if the data-hiding key is available extraction of hidden information is possible but recognizing the image content is difficult. If recipient possess a cryptographic key, image can be decoded but the extraction of concealed data is difficult. Hence the proposed system exploits robust algorithm that provides both the keys at the receiver end. This is done by manipulating the spatial correlation in image.

Keywords- Least Significant Bit, Data Hiding, Data Extraction, Image Recovery.

I. INTRODUCTION

This work provides an extension to the scheme proposed as separable reversible data hiding[2] in encrypted images to hide data[3]. In the first stage, a receiver scrambles the initial uncompressed image utilizing RC4 secret key algorithm. After this, a data-hider uses data hiding key, to create in-component space for adding some confidential data. Finally, system generates encrypted image consisting additional data. On receiver side image recovery and data extraction take place independently without any loss. Depending on key availability there are three possibilities. In an event where the receiver possessing the data-hiding key, receiver can separate confidential data however recipient does not realize the image content. In the event that the recipient possess the encryption key, recipient can decrypt the data which is received to acquire an image like the first one, however cannot extract confidential data. In the event that the collector has both the data-hiding key and the encryption key, recipient can extract confidential data and regain the initial image content without any losses.

II. LITERATURE SURVEY

In this, a secret message is embedded so the original image contents can be exquisitely reestablished after extraction of the concealed data. Various reversible data hiding procedures are proposed, and can be commonly grouped into three sorts: lossless compression based strategies, Digital watermarking techniques and Difference expansion (DE) techniques. The lossless compression based LSB method performing lossless compression so as to make an additional room to oblige extra secret data.

Paper 1: Reversible Data Hiding

This paper displays a reversible data biding algorithm, which can recuperate the original image after mutilation from the checked image subsequently as the hidden data is separated. This algorithm uses the zero or the minimal factor of the histogram and somewhat alters the pixel esteems to implant data.[2]

Paper 2: Reversible Data Hiding in Encrypted Image

This work displays method for which after encoding the whole data of an uncompressed image by a stream cipher, the extra data can be inserted in the image by adjusting a small extent of encrypted data.[3]

Paper 3: Lossy Compression and Iterative Reconstruction for Encrypted Images

A pseudorandom modification is utilized to encrypt an initial image, and encoded data are methodically compressed by methods for disposing of the unreasonably extreme and exquisite information of coefficients produced from orthogonal transform. After receiving the compressed data, with the asset of spatial relationship in natural image, a receiver can remake the fundamental content of the original image through iteratively refreshing the

© 2019, IJREAM All Rights Reserved.

estimations of coefficient This way, the better the compression ratio and the smoother the original image, the better the nature of the recreated image.[4]

Paper 4: Separable Reversible Data Hiding in Encrypted Image with Classification Permutation

A classification permutation based in this work designed a classification modification encryption connecting with the XOR-encryption to improve the privacy of encrypted image. More important, it is possible for the data hider to find the smooth pixels in then encrypted image without the original content and the encryption key including the type-mark. As a result, the aspect of decrypted images is recovered.[5]

Paper 5: Reversible Data hiding in pairwisely encrypted images.

The input image is encrypted first via a pairwise encryption scheme. Then the data bits can be inserted into the pair wisely encrypted image by the well-known difference expansion technique. In this manner, the steady the original image and the greater the compression ratio , the better the quality of the recreated image.[6]

III. EXISTING SYSTEM

In separable scheme, the initial image is encrypted utilizing an encryption key and the supplementary data are implanted into the encrypted image utilizing a data-hiding key. With an encrypted image consisting of additional data which is hidden, when the recipient has just the data-hiding key, user can separate the extra data t however not realize the image content. User can decrypt the received data to achieve an image like the original cover media, if user has just the encryption key, but cannot remove the implanted additional data using that key. In the event that the recipient possess both the keys the user can regain the initial image with almost no error and extract the additional data.

IV.COMPARATIVE STUDY

Table no.4.1: Comparative Study

Sr No.	Paper Title	Author's Name	Encryption	Data Hiding	Description
1.	Reversible Data Hiding	Nirwan Ansari, Wei Su	Pseudo-random permutation	Histogram modification	In this technique data is pseudo-Randomly embedded into histogram of the image.
2.	Reversible Data Hiding in Encrypted Image	Xinpen g Zhnag.	Pseudo-random permutation	LSB	This technique embeds secret data in the least significant bit of encrypted image.
3.	Reversible Data Hiding in pairwisely encrypted images.	Jen Chun & Yun Hong	Pseudo-random permutation	Orthogonal Transform	This technique uses orthogonal transform for lossy compression and on the receiver side after data extraction image will be recovered iteratively.
4.	Separable Reversible Data Hiding in encrypted image with classification Permutation.	Bangxu Yin & Fan Chen	Permutation & EXOR encryption	LSB	This technique embeds secret data in the least significant bit of encrypted image
5.	Reversible Data hiding in pairwisely encrypted images	Jen Chun & Yun Hong	Pairwise encryption	Difference Expansion	The proposed technique scheme obtains much better embedding capacity.

V. PROBLEM STATEMENT

Reversible data hiding in all the images is an effective new technique cause it is has privacy-preserving requirements for cloud data. Past strategies execute RDH in encrypted images utilizing encryption and decryption. This is achieved with the help of reserving space before encryption. The proposed strategy can exploit all traditional RDH strategies for any plain random images and accomplish great execution not losing perfect secrecy. The novel method can accomplish real reversibility. Separate data extraction can greatly improve quality of assigned decrypted images. The previous RDH techniques used for encrypted and decrypted the image, also considers a new algorithm of encryption and decryption of images. Ceaser Cipher algorithm is used for this algorithm, along with concept of mixing the rows random generation manner and Huffman Encoding. The image which is encrypted and decrypted by this algorithm insulate the image from an unofficial connection. This Algorithm provides high security to an image and occupies less memory space. And for data embedding process , by using the Integer Wavelet Transform minimizing the mean square exaggeration along the original and watermarked image and also to boost Peak signal to noise ratio. Also all these experiments are done in the gray scale images. The proposed method also used in color images. The two peaks

© 2019, IJREAM All Rights Reserved.

in histogram are elected for data embedding in form to accomplish histogram leveling performed by repeating the procedure. The results that the image contrasts can be upgraded by splitting various histogram peaks combination by combination. The enhanced contrast enhancement can be used in the proposed techniques. The 2 peaks in the histogram can be calculated from the pixel values of the given images.

VI. PROPOSED SYSTEM

In the architectural design of the proposed system, initially, the mage Undergo encryption stage. RC4 secret key algorithm is used for encryption. Encryption key (e1) is taken as input. After image encryption secret data is inserted into encrypted image providing data hiding key (e2) as input. On the reception side, if user has data hiding key (e2) then user is able to extract secret data, although user is inadequate to decrypt image. If receiver side has encryption key (e1), user is capable to decrypt image yet the image will contain less amount of secret data. If recipient has both keys then the user can extract secret data along with decrypting the image without any error.

VII. ALGORITHM

The general idea of working of proposed system algorithm is given as follow: The RC4 encryption algorithm has the following steps:

1. Get the Original image array and key.
2. Create two string arrays.(A & B)
3. Initialize one array(A) with numbers from 0 to 255.
4. Fill the other array(B) with key.
5. Randomize the first array(A) based on the array of the key.
6. Randomize the first array(A) within itself to attain the final key stream.
7. XORing the conclusive key stream with initial image array to give encrypted image.

RC4 has an 8×8 S-box: S0, S1,..., S255.

The data are a blend of numbers 0 through 255, and the blend is a function of the variable-length key. It has two counters, p and q, initialized to zero. To generate a random byte follow the following pseudo code

```
p= (p + 1) mod 256
q = (q + Sp) mod 256
swap Sp and Sq
t = (Sp + Sq) mod 256
```

M = St The ciphertext is generated by XORing the byte M with the plaintext, for encryption.

VIII. MATHEMATICAL MODEL

Set theory approach has been adopted to design a mathematical model for the
designed system.
Let I be a set of input image file.
Let F be the set of functions used for the implementation.
Let O is the output generated
Such that S= {I, F, O} Where,
I represent the set of inputs:
I= Input image file.
And F is the set of functions:
F= {F1, F2, F3, F4}
F1 = Encrypt image by using RC4 algorithm.
F2 =Inserted additional data in encrypted image utilizing LSB technique.
F3 = Decrypt image file using RC4 algorithm.
F4 = Extract additional data without any loss.
And O is the set of outputs:
O = v, d
v = Output image after decryption.
d= Output data after data extraction.

Functions

F1: Encryption of image file by applying RC4 algorithm.
If x = encryption key.
F(x) = Generate encrypted image.
F2 = Embed additional data by applying LSB technique.
X: data hiding key and additional data.
F(x) = generate encrypted image consisting of additional data.
F3 = Decryption of image file consisting of additional data.
X: encryption key.
F(x) = Generate decrypted image visually look like original image file
F4 = Extract additional data.
X: data hiding key.
F(x) = Extract additionally embedded data.

IX .SYSTEM ARCHITECTURE

Figure demonstrates the architectural structure of the proposed framework. At first, the image undergo encryption stage. Encryption takes place using RC4 secret key algorithm, encryption key (e1) is taken as input.

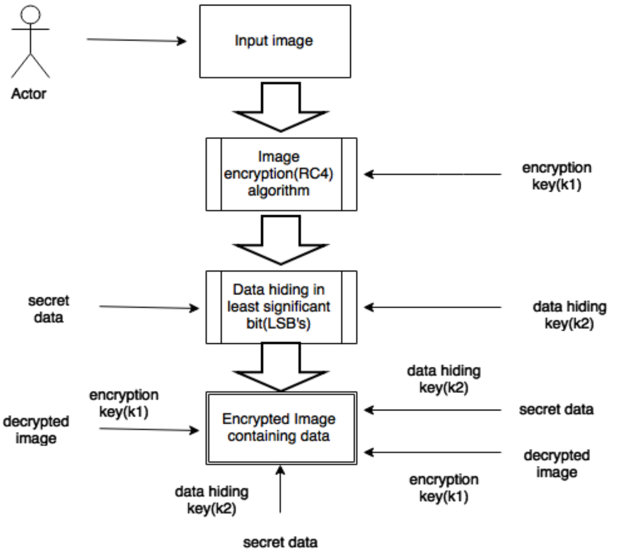


Fig.9.1: System Architecture

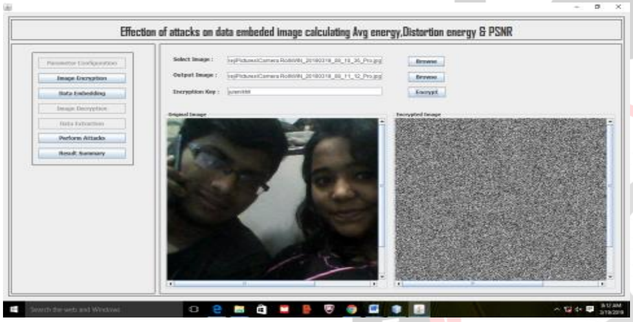
After image encryption secret data is installed into encrypted image proving data hiding key (e2) as input. If recipient has data hiding key (e2) then recipient can extract secret data, however recipient is not able to decrypt image. Recipient can decrypt image if recipient has encryption key (e1), however the image contain little amount of secret data. If receiver has both keys, recipient can extract secret data as well as decrypt image without any error.

X. ADVANATGES

1) Decryption algorithm not required. So an individual obscure to cryptography can decrypt the message.
2) Lower computational expense since the secret message is perceived only by human eyes and not cryptographically processed.
3) Context Awareness.

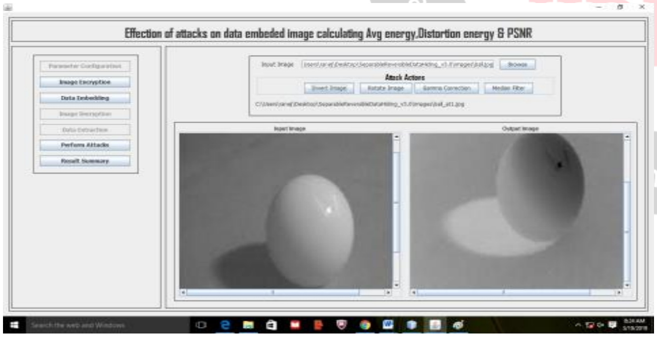
4) Simple to implement.

XI. DESIGN DETAILS


Effection of attacks on data embeded image calculating Avg energy,Distortion energy & PSNR

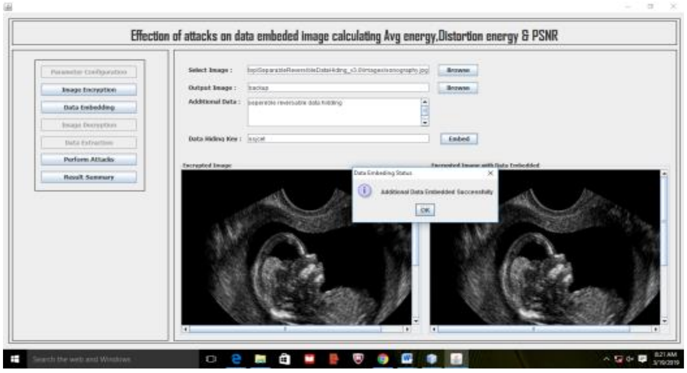
Select Image : \raj\Pictures\Camera Roll\WIN_20180318_08_10_36_Pro.jpg
Output Image : \raj\Pictures\Camera Roll\WIN_20180318_08_11_12_Pro.jpg
Encryption Key : [illegible]

Fig.11.1: Encrypting Image


Effection of attacks on data embeded image calculating Avg energy,Distortion energy & PSNR

Input Image [illegible]
C:\Users\[illegible]\Desktop\SeparableReversibleDataHiding_v3.0\images\ball_att1.jpg

Fig.11.2: Attack Performed


Effection of attacks on data embeded image calculating Avg energy,Distortion energy & PSNR

Select Image : top\SeparableReversibleDataHiding_v3.0\images\sonography.jpg
Output Image : [illegible]
Additional Data : separable reversable data hidding
Data Hiding Key : [illegible]

Data Embeding Status
Additional Data Embedded Successfully

Fig.11.3: Decrypting Image

XII. CONCLUSION

We have tired to implement paper on Xinpeng Zhang ,"Separable Reversible Data hiding in Encryption Image". A novel methodology incorporating using separable information concealment using reversible method is employed for the encryption process. The input data is encrypted by using a key. Data concealment key pads the LSB of the encrypted data for embedding the data. The lossy method based on Haar wavelet technique was not able to accomplish the retrieval of the image when correlated to the Run-Length Coding method. Both the methods of Image encryption & the keys used for hiding will be used for extracting the needed original content. he results prove that it is very similar to the Human Visual System (HVS) and with the best quality reports.

REFERENCES

[1] Xinpeng Zhang ,"Separable Reversible Data hiding in Encryption Image", IEEE transaction on information forensics and security, vol, 7,NO.2 april 2012

[2],Zhicheng Ni, Yun Q. Shi, Nirwan Ansari and Wei Su "Reversible Data Hiding", 0-7803-776\-31031$17.00 02003 lEEE

[3]Xinpeng Zhang," Reversible Data Hiding in Encrypted Image" IEEE SIGNALPROCESSING LETTERS,VOL.18,NO.4,APRIL2011

[4] Xinpeng Zhang," Lossy Compression and Iterative Reconstruction for Encrypted Image" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 1, MARCH 2011

[5] Jen-Chun Chang & Yun-Hong Chou & Cheng-Huai Ni & Hsin-Lung Wu " Reversible Data Hiding in Pairwisely Encrypted Images" 2016 Third International Conference on Computing Measurement Control and Sensor Network, IEEE

[6] Bangxu Yin, Fan Chen, Hongjie He, Shu Yan "Separable Reversible Data Hiding in Encrypted Image With Classification Permutation "2017 IEEE Third International Conference on Multimedia Big Data

© 2019, IJREAM All Rights Reserved.