International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 12 | Dec-2017 www.irjet.net p-ISSN: 2395-0072

DECRYPT AND ENCRYPT THE IMAGE IN CRYPTOGRAPHIC ALGORITHM HS BASED RDH AND LSB BY USING ASYMMETRIC CRYPTOGRAPHY PUBLIC KEY CRYPTOSYSTEM

Mrs. S. Shanthi[1], Ms. R. Nandhini[2], Ms. A. Sivasankari[3].

[1]Assistant Professor, Dept of Computer Science and Applications, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India.
[2]Research Scholar, Dept of Computer Science and Applications, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India.
[3]Head of the Department(cs), Dept of Computer Science and Applications, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India.

Abstract - *Digital Image processing is process of images in order to improve its clarity and quality. We need security while sending the image to the receiver. Now a days we focus largely on reversible data hiding (RDH) in encrypt and decrypt the images, so it can maintain the first-rate quality of original image can be easily improved without any loss of pixels after embedded the image. All previous techniques embedded data by reversibly vacating room from the encrypted images, which may be cause of some flaws on data extraction and image restoration. So we propose a method by reserving room before encryption with a HS based RDH algorithm and LSB algorithm by using asymmetric cryptography known as public key cryptosystem and thus it is so simple for the user to embedded data in the encrypted image. In future the image is reversible that is, data extraction and image recovery without any loss of data(pixel). RDH algorithm and LSB algorithm, which can recuperate the original image without any loss from marked image after encrypts the data, have been mined. This RDH method can be embedded more than ten times as large contents for the same image clarity and restoration.*

***Key Words*: Digital image processing, Reversible data hiding, Lossless data, Image encryption, LSB, Asymmetric cryptography, Reserving room**

1. INTRODUCTION

Using public key anyone can encrypt and decrypt image with the asymmetric key encryption scheme. The secrecy of public key gives security. In many field data security problem arises. The field such as detective agencies, forensics, Medical imaging, social media, Military images need high security while data transmission. The data hiding used to hide sensitive data to give security. Data hiding method is lossless if the display of cover image containing embedded data is same as that of original cover image. Using encryption key we encrypt cover image to give security to the sensitive data. The content is scrambled gives security to file or a message by applying encryption. To unscramble the content by having right encryption key can be readable. After extraction the embedded image it has no loss in data or a pixels by using Reversible data hiding (RDH) image technique. The original cover image can be recovered without any loss. Misrepresentation occurs in simple data hiding but in RDH there is no misrepresentation of original cover image. In this implemented algorithm are Reversible Data Hiding (RDH), Least Significant Bit (LSB) algorithm and Histogram Shift (HS) algorithm. Used by the owner of the content, sender can reversibly embed data into encrypt image without encryption key. The sender can implement directly in embedded image without knowing the content in the image using this method. The content owner generate sequence of pseudo random bits as encryption key and use original image by bit wise operations. Then the encrypted image given to the data hider. The data hider divides the encrypted image into non overlapping blocks. It is sized by sXs. Each block is embedded with one data bit. Then by data hiding for each image block, it divides its pixel into two equal parts that is S1, S2. Embedding is the simple technique to implement stenography. It embedded the data into cover image. So casual observer can't detect the cover image. Some of the information of the given pixel with information from the data in the image are replaced by the working of techniques. It is possible to embed data into an image on any bit-plane. The embedding creates minimizes the colours in variation. The detection of LSB embedding, the first is visual attack and second is statistical attack. The first is simple visual attack which depand on the human eye. The second is statistical attack, which examines image in statistical manner Histogram shifting algorithm is based on the pixel values, which utilizes the redundancy of the host image statistical information to hide secret data, the sketch map.

2. PROPOSED SYSTEM

Proposed system is reversible means data extraction and image recovery is without any loss. In order of encryption and vacating room that is first vacate the room and then encrypt the image which is belong to owner this is called "reserving room before encryption (RRBE)" proposed system uses three algorithm that are-

- RDH Algorithm
- LSB Algorithm
- HS Algorithm

Advantages

1. In the back side of the image we can perform the data encryption as well as compression.
2. We can hide easily large amount of data in the background of the image and videos etc by using digital watermarking.
3. Without data loss we can give high performance.
4. Free from flaws.
5. There is no image misrepresentation.

2.1 RDH ALGORITHM

Until now, large amount of images are in the internet with rapid development of IT. Such as very important data we need to provide the some kind of authentication. At the point when the sender transmits the picture to the beneficiary, there might be interlopers introduce in the middle of who may catch the picture. Subsequent to catching the picture the picture the gatecrasher may see the important substance in the picture. This may not be the issue sometimes. However, in the event that we consider medicinal and military pictures then such misrepresentation is unsatisfactory. In watermark technique we can classify by two different types. The one of the type is visible watermarking. And second technique is based on the image and videos we can apply watermark. This is invisible to human eye. This technique is called digital watermarking. It is used to give copywriter protection to the films and videos and wide range of applications. The digital watermarking is more protected and secures the information that cannot be viewed with the outside. So if the intruder views the content of the image he will not be aware of the watermark which is already present in the image. The receiver make modification in the image can give an original message hidden in the file or an image. This modification can know only to the receiver. Watermarking procedure can be made more secure by scrambling the watermarked picture. Different techniques for encryption can be utilized to encode the picture. Encryption is a method by which the picture is changed or adjusted by utilizing keys. The encryption system can be ordered into two sorts i.e. Symmetric key encryption in which a similar key is utilized for encryption and unscrambling and uneven key encryption in which distinctive keys are utilized for encryption and decoding. Sender will utilize the general population key for encryption and recipient will utilize the private key for unscrambling. However, whatever system is utilized, the first nature of the picture must be recouped at the collector i.e. the beneficiary must get the first picture subsequent to expelling the watermark and in the wake of decoding the scrambled picture.

2.2 REVERSIBLE DATA HIDING:

The hidden data are extracted before reversing the process that the marked media back to original cover media.

Requirements

In data and cover media there is no error.

Applications

- Secure medical image data system
- Law enforcement
- E-government
- Image authentication

2.3 RETRIEVAL ALGORITHM:

Step 1:

Scan the whole marked image.
The order must be as same as embedding.
If it met the maximum point of grey value, the value is intact.
Eg. 155 the "0" is retrieved.
If altered the value. Eg., 156 the "1"is retrieved.
In this way, we can retrieved the embedded data.

Step 2:

Scanned the whole image once again.
The pixel of the grey value once reached between the peak point (eg. 155) and zero point (eg., 255) met (intervals [156,255]), the gray value of those pixel will be subtracted by 1.
Like this, without any misrepresentation the original image can be recovered.

Result:

Data Error rate is equal to 0, image error rate is equal to 0.

Retrieval Algorithm is inverse to the embedded process to retrieval data to check the number of pixels in gray value from right to Left to Center. (4,5),(-3,-4),(2,3) these pairs are embedding process. To get original cover image use expansion function.

2.4 LEAST SIGNIFICANT BITS (LSB) INSERTION

To convert an analog image to digital image format, these are the three choice to go with. We can choose between the different ways of colour representation.

24 bit Colour: Every pixel can have one in 2^{24} (2^24) colours, and these are represented as different quantities of three basic colours represent as RBG i.e., Red(R), Blue(B),Green(G) given by 8-bits (256 values)each.

8-bit colour: Each pixel may have one in total 256 colours that is (2^8) colours.

8-bit gray-Scale: Each pixel may have one in shades of gray colour that is 256 (2^8) colours.

This technique modifies the LSBs in 24-bit images of having each colour, or LSBs of 8-bit image is 8-bit value.

These examples represents that 1-LSB insertion usually has a 50% chance to change a LSB every 8-bits, adding little noise to the original image.

For 24-bit images the modification can goes to second or even third LSBs extended sometimes. Without being visible. To choose the colours in 8-bit images have much more limited space. So it is possible to change of LSB only without modification being detected.

Data Rate:

The most fundamental of LSBs inclusion for 24-bit pictures embeds 3 bits/pixel. Since each pixel is 24 bits, we can hide

3 hidden_bits/pixel/24 data_bits/pixel = 1/8 hidden_bits/data_bits

So for this case we hide 1 bit of the implanted message for each 8 bits of the cover picture.

In the event that we pushed the inclusion to incorporate the second LSBs, the formula would change to:

6 hidden_bits/pixel/24 data_bits/pixel = 2/8 hidden_bits/data_bits

Also, we would conceal 2 bits of the inserted message for each 8 bits of the cover picture. Including a third-piece inclusion, we would get:

9 hidden_bits/pixel/24 data_bits/pixel = 3/8 hidden_bits/data_bits

Gaining an information rate of 3 embedded bits each 8 bits of the picture.

3. ROBUSTNESS

LSB addition is exceptionally powerless against a great deal of changes, even the most innocuous and normal ones. Lossy compression, e.g. JPEG, is probably going to annihilate it totally. The issue is that the "openings" in the Human Visual System that LSB addition tries to misuse - little affectability to included flaws - are a similar that lossy compression calculations depend onto have the capacity to diminish the information rate of pictures. Geometrical changes, moving the pixels around and particularly dislodging them from the first framework, are probably going to pulverize the inserted message, and the special case that could permit recuperation is a straightforward interpretation.

Some other sort of picture change, such as obscuring or different impacts, ordinarily will pulverize the shrouded information.

Al lines all, LSB addition is a next to no vigorous strategy for information stowing away.

3.1 Simplicity of recognition/extraction

There is no hypothetical exceptional sign of LSB inclusion, if not a little increment of foundation commotion.

It's simple, rather, to extricate LSBs even with straightforward projects, and to check them later to discover on the off chance that they mean something or not.

3.2 Appropriateness for steganography or watermarking

Above all else, since it is a so powerless system notwithstanding for straightforward handling, LSB addition is practically futile for computerized watermarking, where it must face malignant endeavors at its decimation, in addition to ordinary changes like pressure/decompression or transformation to simple (printing or perception)/ transformation to advanced (scanning). Its nearly high information rate can point it as a decent method for

steganography, where heartiness isn't such an important constraint.

3.3 Issues and conceivable solutions

Having expressed that LSB addition is useful for steganography, we can endeavor to enhance one of its significant downsides: the simplicity of extraction. We don't need that a malevolent attackers have the capacity to peruse all that we are sending.

3.4 This is normally refined with two complementary methods

Encryption of the message, so who extricates it should likewise decrypt it before it makes sense.. Randomizing the situation of the bits utilizing a cryptographical irregular capacity (dissipating), so it's practically difficult to revamp the message without knowing the seed for the arbitrary function. In this way, the message is ensured by two distinctive keys gaining substantially more classification than before. This approach secures likewise the respectability of the message, being significantly more troublesome (we could say in any event computationally infeasible) to fake the message. Anyway, since we don't need our message to be just an encoded and mixed message, we should backpedal to the reason for making the correspondence covered up for communication hidden.

The two most important issues in this problem are:

- the choice of images
- the choice of the format (24-bit or 8-bit, compressed or not)

The cover picture above all else must appear to be easygoing, so it must be picked between an arrangement of subjects that can have motivation to be traded between the source and the receiver. At that point it must have very fluctuating hues, it must be "noisy", so that the additional commotion will be secured by the officially display one. Wide solid colour territories amplify especially any little measure of noise added to them.

Second, there is an issue with the file size, which includes the decision of the format. Surprisingly enormous files traded between two associates, truth be told, are probably going to emerge doubt.

How about we ascertain, for example, what the size would be for a 500x300 image (150,000 pixels), very basic for pictures on the Internet, with the distinctive colour representations: 24-bit colour: 150,000 pixels x 24 bits/pixel/8 bits/byte = 90,000 Bytes ~= 440KB

• 8-bit colour/grayscale (the inhabitance is the same): 150,000 pixels x 8 bits/pixel/8 bits/byte = 150,000 bytes ~= 146KB

Taking a gander at the size, we can see that a 24-bit uncompressed picture is of a very extraordinary size, since it's extremely interesting that the sender didn't compress it, a training that is generally utilized and wouldn't have intensified the picture quality to such an extent.

To tackle this issue, with as been examined an adjustment to the JPEG algorithm that supplements LSBs in a portion of the lossless stages or pilots the adjusting of the coefficients of the DCT used to compress the picture to encode the bits.

Since we need little picture document sizes, we should resort in utilizing 8-bit images on the off chance that we need to impart utilizing LSB insertion, on the grounds that their size will probably be considered as would be expected.

The issue with 256 colour images is that they make utilization of a listed palette, and changing a LSB implies that we change a pixel from a position to a neighboring one. In the event that there are neighboring contrasting colours in the palette, it can happen that a pixel in the picture changes its colour suddenly and the concealed message ends up visible obvious.

To take care of this issue distinctive techniques have been examined, such as reworking the palette with the goal that contiguous colours don't differentiate so much, or even lessening the palette to fewer colours and repeating a similar section in the table in adjoining positions, so the distinction after the embedding of the message isn't unmistakable in any way. In addition for most images the diminishment of colours from, for example, 256 to 32 is not really unmistakable.
Most of the specialists, at any rate, encourage to utilize 8-bit grayscale images, since their palette is significantly less shifting than the colour one, so LSB inclusion will be difficult to identify by the human eye.

4. HISTOGRAM SHIFTING ON PIXEL DIFFERENCES

1. HS for single layer embedding
2. HS for multi-layer embedding

4.1 HISTOGRAM SHIFTING ALGORITHM

4.1.1 Traditional histogram shifting Algorithm (HS)

Traditional histogram shifting algorithm depends on the pixel values, which uses the repetition of the host picture factual data to conceal secret information, the draw sketch map appeared as takes after.

1) The extraction is performed in the switch arrange as the embedding procedure.
2) The side data (peak/zero points) ought to be furthermore transmitted to the receiver for reversible recuperation.— — No visually impaired
3) The histogram shifting is reached out to the pixel contrasts or prescient mistakes to enhance the execution.

4.1.2 PROBLEM FORMULATION

Our proposed system mainly divided into three parts:

1) Lossless Data Hiding Scheme
2) Reversible Data Hiding Scheme
3) Combined Data Hiding Scheme

4.1.3 Mathematical Model

System maintains its original histogram (H1) at sender and receiver side.

System = [RM, ENCRY, DE, DEX]

Where,
RM = Reserving Room
RM = [R1, R2, R3, R4]

Where,
R1 = Accepting original image from sender.
R2 = Partitioning the image.
R3 = Shifting bits of partitioned image.
R4 = Vacating the room to embed data.

ENCRY = Image Encryption
ENCRY = [E1, E2, E3]

Where,
E1 = Accept the vacating image.
E2 = Encrypt image with specific encryption key.
E3 = Forward encrypted image for data embedding process.

DE = Data Embedding
DE = [D1, D2, D3, D4]

Where,
D1 = Accept encrypted image
D2 = Find out vacate space
D3 = Embed data in a vacate space
D4 = Make an updated histogram (H2) for embedded data image.

DEX = Decryption and Data Extraction.
DEX = [O1, O2, O3, O4, O5, O6]

Where,
O1 = Accept image from sender.
O2 = Identify encryption key.
O3 = Decrypt according to particular encryption key.
O4 = Compare histogram H1 with H2.
O5 = Find if any loss in data, if so then again demand sender to send image.
O6 = If no loss, accept image and get data.

5. CONCLUSIONS

Using these techniques, total loss of data can be recovered as possible at the time of data extraction. This proposes the lossless of data, reversible and combined data hiding schemes for cipher text. Images encrypted by the public key cryptography. Here we can conclude that prevention of data attack is reduced and data security is extended highly. The data will be secrecy while transferred with high security level.

REFERENCES

[1] E. J. Delp and O. R. Mitchell, "Image compression using block truncation coding," IEEE Trans. Commun., vol. 27, no. 9, pp. 1335–1342, Sep. 1979.

[2] V. Udpikar and J. Raina, "BTC image coding using vector quantization," IEEE Trans. Commun., vol. 35, no. 3, pp. 352–356, Mar. 1987.

[3] Y. Wu and D. C. Coll, "BTC-VQ-DCT hybrid coding of digital images," IEEE Trans. Commun., vol. 39, no.

9, pp. 1283–1287, Sep. 1991.

[4] C. S. Huang and Y. Lin, "Hybrid block truncation coding," IEEE Signal Process. Lett, vol. 4, no. 12, pp. 328–330, Dec. 1997.

[5] Y.-G. Wu and S.-C. Tai, "An efficient BTC image compression technique," IEEE Trans. Consum. Electron, vol. 44, no. 2, pp. 317–325, May 1998.

[6] M. Lema and O. R. Mitchell, "Absolute moment block truncation coding and its application to color images," IEEE Trans. Commun., vol. 32, no. 10, pp. 1148–1157, Oct. 1984.

[7] J. M. Guo and M.-F. Wu, "Improved block truncation coding based on the void-and-cluster dithering approach," IEEE Trans. Image Process., vol. 18, no. 1, pp. 211–213, Jan. 2009.

[8] N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis, Digital Signal Processing, 20, pp. 16291636, 2010.

[9] J. Tian, Reversible Data Embedding Using a Difference Expansion, IEEE Trans. on Circuits and Systems for Video Technology

[10] M.U. Celik, G.Sharma, A.M.Tekalp, and E.Saber, Lossless Generalized LSB Data Embedding, IEEE Trans. On Image Processing, 14(2),pp.253266, 2005

[11] Neeta,D.;Snehal,K.;Jacobs,D., "Implementation of LSB Steganography and Its Evaluation for Various Bits," Digital Information Management, 2006 1st International Conference on, vol., no.,pp.173,178, 6Dec.2006doi:10.1109/ICDIM.2007.369349

[12] Joan Condell, Kevin Curran, Paul McKevitt, Digital image steganography: Survey and analysis of current methods, Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.

BIOGRAPHIES

MRS. S. SHANTHI
Assistant Professor,
Dept of Computer Science and Applications,
D.K.M. College for Women (Autonomous),
Vellore, Tamilnadu, India.

MS. R. NANDHINI
Research Scholar,
Dept of Computer Science and Applications,
D.K.M. College for Women (Autonomous),
Vellore, Tamilnadu, India.

MS. A. SIVASANKARI
Head of the Department(cs),
Dept of Computer Science and Applications,
D.K.M. College for Women (Autonomous),
Vellore, Tamilnadu, India