**PERFORMANCE ANALYSIS OF AN IMPROVED RESERVING ROOM BEFORE ENCRYPTION ALGORITHM IN IMAGE STEGANOGRAPHY**

 M.HemamaliniMCA., M.Phil.,SET.,Ph.D.

 Assistant Professor, Department of Computer Science, A.V.C College(Autonomous), Mannampandal,Mayiladuthurai, Tamilnadu, India, maliniavcce@gmail.com

ABSTRACT: Cryptography is used to protect digital information and converting the contents from readable format to non-readable format. Steganography is the process of hiding data by embedding data within others. An Improved Reserving Room before Encryption Algorithm is used to hide text using unused bits in an image file into image without damaging the original image. The analysis shows that the size of encrypted image is same as the original image. The quality of the image is also kept unchanged in this technique.

keywords*s*: BitMap Image Steganography, Reversible Data Hiding.

**INTRODUCTION**

Steganography is the process of hiding data by embedding messages within other, apparently undistributive messages. The hidden message is not seen even if the encryptedfile is cracked[1].

These techniquesare used to protect varying secret data from text and images.They protectdata by encrypting them into unreadable cipher text. The message can be decrypted into plain text by using secret key. Sometimes encrypted messages can be broken by cryptanalysis although recent cryptography techniques are unbreakable[2].

Visual cryptography is branch of cryptographic technology.Visual information can be encrypted and decrypted by the human.Visual Cryptography scheme is used to encrypt and decrypt images without complex computation. The accuracy of algorithms calculated with some merits such as no of share images created during encryption processof the size of encrypted images[3].

Visual cryptography that restructures the image y stacking significant images together is called Extended Visual Cryptography.That allows the contrast enlargement by broadening the concept of error and by applying encryption and half toning consecutively[4].

1. **RELATED WORK:**

Tripta Deendayal et al [5] used Digital watermarking technique to encrypt the image. Error diffusion techniques are used to improve the quality of the images. Retrieve the secret information, the images. To retrieve the secret information, the image should be stacked to any K number of decrypted shares. Renders the halftone image reduces the color sets and chooses the color.

Nagaraj V.Dharwakhar et al [6] proposed another VSC method for the color image which applies the error diffusion dithering on color channel. This paper illustrates the methods to enhance the size of encrypted image and quality of the output image.

Musheer Ahmed et al [7] proposed for color Images using chaotic mapping. In this method, the ideais tochange the gray values of the image pixels and shuffle the pixels positions.

Naor et al [8] proposed the visual Cryptography scheme for binary images and color image.

1. **EXISTING SYSTEM:**

The two approaches used in RDH are as follows:

* Reserving Room After Encryption.
* Reserving Room Before Encryption

**RESERVING ROOM AFTER ENCRYPTION (RRAE):**

The data hider will hide the secret data into the detailed coefficient after image encryption. The encryption process affects the entropy of an image[9].



**Figure1. Reserving Room After Encryption Framework**

**IMAGE STEGANOGRAPHY:**

Steganography on images are most acceptedmethod of Steganography as image frequently occur at website, as email attachments, etc. There is minimum cause for distrust when digital image is used [10]. There are simple watermarking, direct Cosine Transformation,Least Significant Bit and Wavelet Transformation.

**RESERVING ROOM BEFORE ENCRYPTION (RRBE):**

This algorithm proves the performance of rate distortion model for binary covers.The reconstruction approach of this algorithm achieves the rate distortion. Thus to achieve higher accuracy the data security is increasing important and so, RRBE used.



**Figure2. Reserving Room Before Encryption Framework**

**PROCESS OF RESERVING ROOM BEFORE ENCRYPTION:**

* Vacating Room in Image
* Image Partitioning
* Self Reversible Embedding
* Creation of Encrypted Images
* Data Hiding
* Data Encryption and Image Recovery
* Extracted data from Encrypted Image
* Extracted data from decrypted Image.
* **Vacating Room in Image**

Image can be distributed in two parts,image portioning and reversible embedding**.**

* **Image Partitioning**

The LSB planes are used for the Reserving Room operation. The image partitioning is to build a smoother area. The Performance is improved by using the standard RDH algorithms.

* **Self Reversible Embedding**

The process is to embed the LSB planes of A into B where A as Block pixel, B as white pixel.

* **Creation of Encrypted Images**

There are three main steps in encrypted image such as image encryption, image partitioning and self reversible embedding.

* **Data Hiding**

The data hider needs the encrypted image E. The first step is tofind the encrypted version of A. To formulate marked encrypted image encrypt data with the key.

* **Data Encryption and Image Recovery**

Data extraction is completely independent from image decryption.

* **Extracting Data From Encrypted Image**

To protectthe information of client, the database manager may have rights to access the key and operate the data.

1. **PERFORMANCE ANALYSIS OF AN IMPROVED RESERVING ROOM BEFORE ENCRYPTION ALGORITHM**

An Improved Reserving Room Before Encryption algorithm works by replacing bits of unused data with bits of our data. The data will be the plain text that is needed to hide.The Least Significant Bit (LSBs) in the image pixels is the unused data.

The steps in the algorithm are

Step 1: R RGB for each pixel read

Step 2: Makes LSB to 0 for each of R G and B

Step 3:NoC=Count (giventext)

Step 4:char C=getCharacter(i)

Step 5:Number N=ConvertToint(C)

Step 6: hide 8 bits of in RGB of consecutive pixels

Step 7:I=i+1

Step 8:if I <No C do step 4

Where

NoC stands number of Character

C stands Character

N stands Number of Given Character

iStands for character

Based on the length of the text, the text can be hidden in a small part of the image .

****

**Figure3. Data Extraction and Image Recovery**

1. **RESULTS:**
* **PEAK SIGNAL NOISE RATIO - THE IMAGE QULITY METRICS**

The various image enhancement algorithm can be analyzed. From this analysis shows that an Enhanced Reserving Room Before Encryption Algorithm produce a better results.

The mathematical representation of the PSNR.

$$MSE=(1/(m\*n))\*sum(sum\left(\left(f-g\right).^{\^2}\right))$$

$$PSNR=20\*log{\left(max\left(max\left(f\right)\right)\right)}/{\left(\left(MSE\right)^{\^0.5}\right)}$$

Where f indicatesthe original image.

g stands for degraded image.

m indicates the number of rows of pixels of the image.

i represents the index of that row.

n represent the number of columns of pixel image.

j indicates the index of that column.

f is the maximum signal value of the image.

* PSNR (in db)
* CAPACITY (in bits)
* Image Size (in bytes)
* Size of Embedded Data (in KBs)

* **RGB PIXEL PLANE USING POSSIBLE COLORSAND FILE TYPE**

Thetrue image is kept as an m-by-n-by-3 data arrayin MATLAB. The RGB pixel Plane using possible colors and File Types is shown in Table 1.

**Table 1: RGB Pixel Plane using possible colors and File Type**

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Byte per pixel | Possible Color | File Type |
| 24 bit RGB | 3 byte per pixel( one byte for each of RGB) | 16.71 million colors the normal picture | JPG,TIF,PNG |
| 48 bit RGB | 6 byte per pixel | 2.81 trillion color | JIF , PNG |

******

**Figure3. RGB Pixel Plane Image**

* **CAPACITY COMPARISON OF IMAGE IN (bits)**

The value of MSE between two identical images will be 0. The PSNR will be undefined division by0.

**Table 2: Capacity Comparison of Image (in bits)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Image Name | Total number of pixels | Number of Secret Message Embedded (in bits) | pixel used for embedding(in percentage) | Originality retension in stego image(in percentage) |
| Existing Method | Proposed Method | Existing Method | Proposed Method |
| Desert | 35947 | 17320 | 48.18 | 15.75 | 51.82 | 84.25 |
| Horse | 3000 | 1480 | 49.33 | 18.75 | 50.67 | 81.23 |

* **COMPARATIVE ANALYSIS USING PSNR WITH VARIABLE IMAGE DIMENSIONS**

**Table 3: PSNR with Variable Image dimensions**

|  |  |
| --- | --- |
| ImageSize (in bit) | Peak Signal Noise Ratio in (Db) |
| LSB | An Improved Reserving Room Before Encryption Algorithm in Image Steganography |
| 128 | 65 | 66 |
| 256 | 50 | 73 |
| 512 | 38 | 89 |
| 124 | 42 | 87 |



* **COMPARATIVE ANALYSIS USING PSNR WITH VARIABLE AMOUNT OF EMBEDDED CIPHER**

**Table 4:PSNR with Variable amount of Embedded Cipher**

|  |  |  |
| --- | --- | --- |
| Data Size (in KBs) | Existing Method (PSNR in db) | Proposed Method (PSNR in db) |
| 2 | 52 | 66 |
| 4 | 51 | 60 |
| 6 | 53 | 59 |
| 8 | 50 | 60 |

 

There is no noise of all tests. The data embedding capacity and the marked image versus the original image can be adjusted. The Peak Signal Noise Ratio represents the measurement of the image quality.

1. **CONCLUSION:**

The main aim of Stegnography is that the Encrypted text must be decrypted only by system. It was achieved in this Improved RRBE model. From the analysis, it shows that bitwise hiding text concept produces the better decrypted images. The analysisshows that an improved reserving room before encryption algorithm makes the better quality of image.

**REFERENCES:**

1. Mizuho Nakajima and Yasushi Yamaguchi, “Extended Visual Cryptography”, *ICCSI Journal*, Vol 2 Issue 2, 2008.
2. N. K. Pareek, V. Patidar, K. K. Sud, “Image encryption using chaotic logistic map.” *Image and Vision Computing*, Vol. 24, No. 9, pp. 926–934, 2006.
3. C. Dongming, Z. zhiliang and Y. Guangming, "An Improved Image Encryption Algorithm Based on Chaos", *IEEE International Conference for Young Computer Scientists*, pp. 2792-2796, 2008.
4. Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson. “Extended capabilities for visual cryptography”, *Theoretical Computer Science*, Vol. 250, No 1-2, pp. 143–161,Jan 6, 2001.
5. Tripta Deendayal and Ch.Sunitha , “Enhanced Visual Cryptography Using color Error diffusion and Digital Watermarking”,*International Journal Computer Technology & Applications*, Vol. 3, Issue.1, 261-264, 2012.
6. Nagaraj V. Dharwadkar, B. B. Amberker, Sushil Raj Joshi, “Visual Cryptography for Color Image Using Color Error Diffusion”, ICGSI *– GVIP Journal*, Vol. 10, No. 1, 2010.
7. Musheer Ahmad and M. Shamsher Alam, “A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping”, *International Journals of Computer Science and Engineering*, Vol. 2, No. 1, pp. 46-50, 2009.
8. M. Naor and A. Shamir, “Visual cryptography,” *Advances in Cryptology-Eurocrypt*, pp. 1–12, 1994.
9. Kede Ma and Wei Zhang, :Reversible data hiding in encrypted images by reserving room before encryption,” *IEEE International Trans,* Vol. 18, No.3, pp. 398–404,Jan 6, 2013.
10. Shatnawi M. “A new novel method in image steganography with improved image quality:,*IEEETransactions on information security*, Vol.4,No.5,pp.173-178.