International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Security Enhanced RDH Image Steganography by RRBE

Saranya .M[1], Aswani .K[2]

[1]M.Tech Scholar, ECE Department, MEA Engineering College, Perinthalmanna, Kerala, India

[2]Assistant Professor, ECE Department, MEA Engineering College, Perinthalmanna, Kerala, India

Abstract: ***These Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication and Reversible Data Hiding (RDH) in images is a technique by which the image can be retrieved back after extracting the secret messages embedded in it. The present methods involves reserving room for the secret message before encrypting the message into the cover image. so that the cover image can be effectively retrieved after extracting the secret message by the receiver. But the method involves some disadvantages which reduces the efficiency of this method. The primary disadvantage that the key generation used in Reversible data hiding method is by using random value. When the random value is used in key generation, it can be effectively regenerated by the invaders. So this proves to be inefficient in security. In this paper we propose a new method in which we make use Rivest-Shamir-Adleman algorithm for the key generation which effectively increase the security as the key generation is difficult. This method can also be used to encrypt the message in the video also. The security is highly improve in the new method which is proved by using various experiments.***

Keywords: Reversible data hiding, Steganography, Rivest Shamir adleman algorithm, Rhombus**,** Peak signal to noise ratio.

1. Introduction

Steganography is data hiding in image for secure communication. The idea used here is novel approach. And it expressed in two ways. First we are giving importance to image in the case of medical application. And second we are giving importance to data hided in military purpose. In military application, data is highly confidential. And we want to securely transmit this data to other Centre so data hiding in image. In the case of medical application the patient privacy must maintained by the hospital. So we want to securely store this image in data base of data Centre of the hospital.

In previous years we use the technology vacating room after encryption where data hider vacate room after encryption for embedding data. It has many drawback such as error probability is very high and PSNR changes, MSE is very less and also in previous case, the keys are generated using random value.The proposed system using the technique is reserving room before encryption

2. Existing work

The proposed system is based on hospital application, here the patient's privacy must be maintained by the hospital. For this, the doctor first generate public key and private key by using RSA algorithm. So the medical images of any patient will be first encrypted by the doctor's public key which is known to him only. After that he send this to the data Centre of the hospital. The data hider in the data Centre of the hospital will place name and other details over the encrypted image to identify the respective person. Then data hider again encrypted this marked encrypted image using data hiding key. Data hiding key is generated by using random value. This data hiding key must be shared between the doctor. So that he could any time retrieve the image from the database of datacenter of the hospital using both keys. This is main concept of this paper.

Figure 1: Original image

RRBE consists of four stages such as (1). Generation of encrypted image, (2). Data hiding in encrypted image,(3). Data extraction, (4) Image recovery.

3. Generation of encrypted image

To construct the encrypted image, the first stage can be divided into three steps such as image partition, self-reversible embedding and it followed by image encryption.

3.1 Image partition

The main goal of Image partition method is to construct a smoother area B, on which RDH method can achieve better performance. Original image C is an 8 bits gray-scale image with its size M*N and pixels $C_{ij} \in [0,255]$, $1 \leq I \leq M$, $1 \leq j \leq N$ divides into two parts A and B. For this first original image is considered as different blocks then we can calculate the F for each block based on below equation

$$F = \sum_{u=2}^{m} \sum_{v=2}^{N-1} \left| c_{u,v} - \frac{c_{u-1,v}+c_{u+1,v}+c_{u,v-1}+c_{u,v+1}}{4} \right|$$

If F is maximum that area is considered as non-smooth and said to be A. And remaining part is smooth area is said to be B.

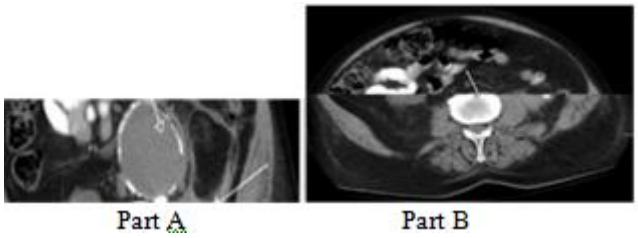

Figure 2: Image partition

Then concatenate the image A followed by B.

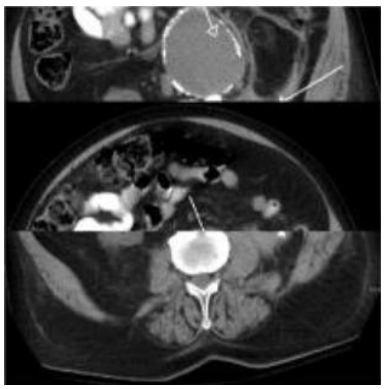

Figure 3: Concatenated image A and B

3.2 Self – reversible embedding

The main goal of Self-reversible embedding is to LSB of A are reversibly embedded into B with a standard RDH algorithm called Rhombus method[2] and also here room is reserved for embedding data.. So that here LSB of A can be used for accommodating messages.

Rhombus Method

To predict the pixel value position Uij .Neighboring four pixel of Uij are used in the form of rhombus. Here this five pixel comprise a cell which is used to hide one bit of data. Even and odd pixels are used for data embedding.

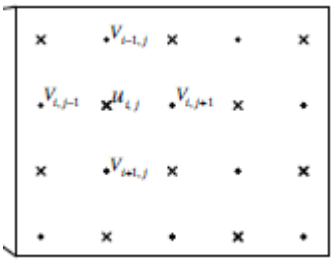

Figure 4: Prediction pattern

1. Here first we calculate Uij',
   $U_{ij}' = U_{i,j-1} + U_{i+1,j} + U_{i,j+1} + U_{i-1,j}/4$
2. Based on the value Uij' then we calculate error e computed as $e = U_{ij} - U_{ij}'$
3. The error e expanded to hide information and applied LSB replacement
   E=2e
   M=E + Bit
   $V_{ij} = M + U_{ij}'$
4. After data hiding the original value U_{ij} is changed to V_{ij}

3.3 Encryption

After self- reversible embedding, the image encrypts to construct the encrypted image using encryption key. RSA algorithm is used for the key generation which effectively increase the security as the key generation is difficult.

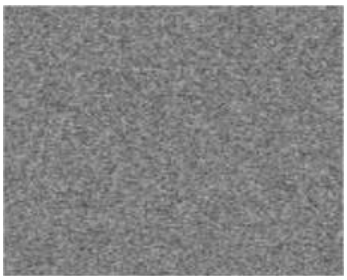

Figure 5: Encrypted image

RSA Algorithm

RSA is good public key cryptosystem and it is widely used for secure data transmission. In this algorithm the encryption key and decryption key is generated. In RSA algorithm for the key generation

1. Choose two distinct prime numbers are p and q.
2. Compute n by multiplying p and q.
3. Compute Ø(n)=(p-1)*(q-1), this value kept as private.
4. Choose an integer *e* such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$. Where *e* and $\varphi(n)$ are co-prime.
5. Using e then we determine d, d*e mod Ø(n) = 1
6 Then we calculate Public key = {e,n) and Private key={d,n}
7. To Encrypt the image we use $c=m^e$ mod n and for decryption $m=c^d$ mod n

3.4 Data Hiding in Encrypted Image

Here data hider will hide the data into the reserved place on the encrypted image that is LSB of A. It again encrypted using data hiding key and get marked encrypted image and it stored in the data base of the data center of the hospital.

3.5 Data Extraction and Image Recovery

At the receiver side the data extraction is completely independent from image decryption. After some time doctor can retrieve the data using data hiding key. In data extraction reverse rhombus method is used. Here first V_{ij} changed to original value U_{ij} and then calculate

$M = V_{ij} - U_{ij}'$
M= Bit + E
To retrieve the hiding data we calculate
Bit = M mod 2
E=M-Bit
e=E/2
$U_{ij} = e + U_{ij}'$

After the data extraction LSB of B can reversibly embedded into A.so we can recovered Original image using decryption

key. Decryption key is also generated by using RSA algorithm.

Figure 6: Original output image

4. Proposed work

In previous case, key generation used in RDH is by using random value. When the random value is used in key generation, it can effectively regenerated by the invaders. So this proves to be inefficient in security. To avoid this drawback, we modify the project here RSA algorithm is used for the key generation which effectively increase the security as the key generation is difficult also here we use RRBE method so it very useful in the case of medical imagery because where no distortion of the original cover is allowed.so high level of security needs to be ensured. So no error probability, less MSE and PSNR make constant.

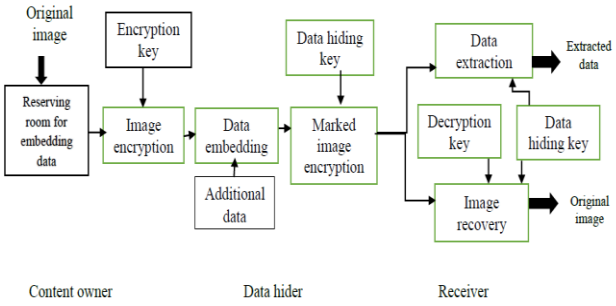

Figure 7: Proposed block diagram

5. Acknowledgment

The authors would like to thank all the faculties in ECE department in MEA Engineering College for all their support during the work. Also authors like to thank all unknown referees whose papers helped during this work.

6. Conclusion

The security enhanced RDH image steganography by RRBE in which we used RSA algorithm for the key generation which effectively increase the security as the key generation is difficult and also Here we used Reserving Room Before Encryption method is help to reduce error probability and make PSNR constant. This method can also be used to encrypt the message in the video also.

References

[1] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li,2013, "Reversible data hiding in encrypted images by reserving room before encryption" IEEE transactions on information forensics and security, VOL. 8, NO. 3

[2] v. Sachnev, h. J. Kim, j. Nam, s. Suresh, and y.-q. Shi, "reversible Watermarking algorithm using sorting and prediction," *ieee trans. Circuits syst. Video technol.*, vol. 19, no. 7, pp. 989–999, jul. 2009.

[3] z. Ni, y. Shi, n. Ansari, and s. Wei, "reversible data hiding," *ieee Trans. Circuits syst. Video technol.*, vol. 16, no. 3, pp. 354–362, mar.2006.

[4] D.m. thodi and j. J. Rodriguez, "expansion embedding techniques for reversible watermarking," *ieee trans. Image process.*, vol. 16, no. 3, pp. 721–730, mar. 2007

[5] Luo*et al.*, "reversible imagewatermarking using interpolation technique," *ieee trans. Inf. Forensics security*, vol. 5, no. 1, pp. 187–193, mar. 2010.

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

[7] w. Zhang, b. Chen, and n. Yu, "improving various reversible data Hiding schemes via optimal codes for binary covers," *ieee trans. Image process*, vol. 21, no. 6, pp. 2991–3003, jun. 2012

[8] w. Zhang, b. Chen, and n. Yu, "capacity-approaching codes for Reversible data hiding," in *proc 13th information hiding (ih'2011),Lncs 6958*, 2011, pp. 255–269, springer-verlag

[9] x. L. Li, b. Yang, and t. Y. Zeng, "efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *ieee trans. Image process.*, vol. 20, no. 12, pp. 3524–3533, dec. 2011.

[10] medical image. available:www.google.com

Author Profile

Saranya.M received B.Tech. Degree in Electronics and Communication Engineering from MEA Engineering college, Calicut university, Kerala, India in 2013. Currently, she is doing M.Tech in Communication engineering in Calicut University, Kerala.

Aswani.K received B.Tech. Degree in Electronics and Communication Engineering from MES Engineering college, Calicut university, Kerala, India , ME in Communication systems from Mahendra engineering college,nammakal, India and currently she is working as Assistant Professor in the Department of Electronics and Communication in MEA Engineering college.