RC4 Enrichment Algorithm Approach for Selective Image Encryption

Pramod Kumar, Pushpendra Kumar Pateriya

Lovely Professional University Phagwara, India

Abstract
This paper is introduces new self Enrichment Algorithm Approach for selective image encryption. This approach is derived from the standard RC4 algorithm. RC4 algorithm is already used for image encryption and also for the selective image encryption. Currently RC4 is vulnerable. Lots of cryptanalytic found the lots of weakness, vulnerable point and attacks inside the RC4 algorithm. So in this concern, this paper has worked. This paper has designed the RC4 based new enrichment approach to making strong the RC4 algorithm, "PC1-RC4". This approach is based on new KSA and PRGA algorithm process, which are the two stages inside the RC4 algorithm.

Keywords:
Rivest Cipher 4 (RC4), PC1-RC4, Encryption, Decryption, Selective.

1. INTRODUCTION

Presently, the communication via multimedia components are the current demanded in most of the application. The text, images, video and audio are the component of the multimedia which used for the communication. In this paper, main concerned the image component of
multimedia. The image is also become the main component as text used for communication. The image is used in internet, multimedia systems, medical, and telemedicine, military for the purpose of communication [1].
Other side, question is, communication via the images is secure if the secret and sensitive images is transmitted over the network? The answer of this question is not secure because of the attacker and intruder may be attack on the images, secretes and sensitiveness of the images can be disclose to the unauthorized person.
Now from this concern, Encryption of the image is also required to making secure the secret image and maintains the confidentiality on the image. In this context the new area of encryption has introduced Image Encryption [2].
In the image encryption, we encrypt the image via used a cryptographic algorithm. In the image encryption, we encrypt the whole of the image to making secure the image data. If we want to encrypt for secure the some sensitive portion of the image then we all the time encrypt the whole of the image. In this case, lots of time utilized by the image encryption process. So to solve this problem, the new era of image encryption introduces known as "Selective image encryption".
In selective image encryption encrypt the sensitive or specific portion of the image rather than the whole of the image. This process is directly saving the time during the encryption as well as decryption of the image.
There are lots of cryptographic algorithms are available and most like: RS DES, AES, Chaotic System, DCT, and DWT are proposed and used for image encryption and selective image encryption [3].
The most proposed approach for the selective image encryption is RC4 stream cipher. The reason, RC4 stream cipher is speedy encrypt image, less resources used, less time and implementation complexity. But the RC4 algorithm is not secure. There are lots of vulnerability point detect inside the RC4 algorithm. Basically RC4 algorithm is the two stages process, KSA and PRGA. The attacks are found in both the stages.
This paper uses the RC4 on the selective image encryption but as per description in this paper about the attacks on RC4 so rather than to use RC4, in this paper, enhanced the RC4 algorithm and used it over the selective image encryption on the bases image become too secure.
This paper is introduce new self enrichment approach to making secure the RC4 algorithm and proposed to use over the selective image encryption. Also, in this paper practically applied the enhanced approach PC1-RC4 over the image encryption. This algorithm is design new KSA and PRGA algorithm process for both KSA and PRGA.

2. RC4 STANDARD APPROACH

Pardeep, Pushpendra [4], RC4 stream cipher most preferred Stream cipher algorithm. In the RC4 algorithm, there are two stages process during encryption as well as decryption. The algorithm is dividing into the two parts KSA (Key scheduling Algorithm) and PRGA (Pseudo Random Generator algorithm). KSA as the first stage of algorithm also knows as initialization of S (s is state

Manuscript received April 5, 2013
Manuscript revised April 20, 2013

vector) and PRGA known as stream generation in the RC4 whole process of algorithm, mean RC4 basically two stages process.

In the first stages of RC4 Stream Cipher algorithm on the bases of variable sized key from 1 to 256 a State Vector (State Table) of fixed length 256 bytes is generated, after on the base of State Table, we generate the key stream that XOR with plaintext and cipher text during encryption and decryption. During encryption the key stream is XOR with the plaintext and during decryption the cipher text XOR with key stream then convert into the plaintext. In the description of RC4, first we discussing the first stage of the algorithm known as KSA, in this stage following steps are done:

1. Inputting the variable length key of size from 1 to 256
2. Initialize the key matrix as per the size of the input key
3. Initialize the State table of fixed size 256 bytes from the value 0 to 255 in ascending order.
4. Using the key matrix of variable size done the permutation on the S table
5. Output of the KDA, the final prepare S table after shuffling operation.

In this manner the KDA generate the State Table (State Matrix) of 256 bytes.

Now let's discuss the algorithm of the KDA as following

KSA

1. for i=0 to N-1
2. s[i]=1
3. j=0
4. for i=0 to N-1
5. j=(j+s[i]+k[i]) mod N
6. swap(s[i],s[j])

Now we going to discuss the second stager of the algorithm known as PRGA

These stages basically used to generate the output key stream that used to encrypt and decrypt the data by XORed operation.

The algorithm description the algorithm as following

PRGA

1. i=j=0
2. Loop
3. i=(i+1) mod N
4. j=(j + s[i]) mod N
5. swap(s[i],s[j])
6. output= s[s[i] + s[j]] mod N]

From the last long time there are lots of weaknesses and attack to be found over the RC4 algorithm, some of the weaknesses detect in the KSA and some of the weakness is detect in PRGA of the algorithm.

3. WEAKNESS AND ATTACKS OVER RC4

Pardeep and Pushpendra [4], In 1994 the RC4 algorithm was disclosed in to the market and then experts start to analyze the RC4 algorithm and find out the lots of weaknesses in both the stages of the algorithm KSA and PRGA. Many cryptanalysis of the algorithm was divided into the two parts, analysis of the initialization of RC4 which focuses on the initialization of KSA and analysis of the output key stream generation which focuses on the internal state and the round
operation of PRGA [5].

Mantin and Shamir [6], was find out the weakness in the second round the probability of Zero output bytes as the major weakness of the algorithm.

Fluher et al. [7], was discovered the big weakness in the RC4, if anyone now the portion of the secret key than possible to attack fully over RC4.

Paul and Maitra [8], was discovered the secret key by using the initial state table. They generated some equation on the bases of initial state table and they select some of the bytes of secret key on the bases of guess and remain secret key find out by using the equation. So we know that the security of RC4 depends on the security of the secret key and the internal states of S-box, so many attacks focus on resuming the secret key of the internal states of the S-box. And also there is lot of other weaknesses and attacks are to be found over the RC4 algorithm. To making secure the RC4 that capable to stand against the attack, lot of research done over RC4 to enhancing the security of RC4.

4. PC1-RC4

a. Introduction: This is the self designed algorithm, "PC1-RC4", to enhance the security of the RC4 stream cipher algorithm. This approach basically designed to making strong to the RC4 algorithm against the various attacks and weaknesses.

This algorithm basically based on the two way encryptions as well as decryptions. This algorithm provides the new algorithm process for both KSA and PRGA.

b. Algorithm:

PC1_RC4
N=256
KSA:
Input single Key (Key Length)(base key)
Generate two sub keys
if(k1%2==1)
{

```
        k1=k1+1;
        }
subkey1=subkey2=k1/2;
initialize the two Key[length]  // generate on the bases of two sub keys
For i=0 to length
Key1[i]=random value;// (secret key1)
End for
For i=0 to length
Key2 [i] =random value ;//( secret key2)
End for
Initialize the Two Temporary Matrix
For i=0 to N
Temp1[i]= value
Temp2[i]= value
End for
initialize the State Matrix
For i=0 to N
S1[i]=i;
S2[i]=i;
End for
Permutation on State Matrix
j1=j2=j3=0
For i=0 to N
J1=(j1+s1[i]+s1[j1]+temp2[i]+temp2[j1]+temp2[j2])%N;
J2=(j2+s2[i]+s2[j2]+temp1[i]+temp1[j1]+temp1[j2])%N;
swap(s1[i],s1[j1])
swap(s2[i],s2[j2])
End for
PRGA:
Generate the random values used for encryption
i=j1=j2=0
while(True)
i=i+1 % N
j1=j1+s1[i]+s2[j1]+s2[j2] % N
j2=j2+s2[i]+s1[j1]+s1[j2] % N
swap(s1[i],s1[j1])
swap(s2[i],s2[j2])
index1=(s1[i]+s1[j1]) % N
index2=(s2[i]+s2[j2]) % N
output1= s1[index1]
output2= s2[index2]
CT= PT1 XOR output1
CT1= CT XOR output2
Swap(s1[s2[i]],s1[s2[j1]])
Swap(s2[s1[i]],s2[s1[j2]])
Wend( End While)
```

c. Description: In this algorithm, in the KSA, first inputs one keylen (basic key) in between the size of 1 to 256. Then, this algorithm divides the single keylen into the two keylens (two basic keys). After this process, this algorithm generates the two secret keys as equal the length of the two subkeys which contain the random values. After generating the two secret keys, end for step is to generate the two temp1 [] and temp2 [] matrices of size 256 that contain random values on the bases of secret key and secret key2. End for step to initialize the two state matrix s1[] and s2[] of size 256 with inserting the values from 0 to 255 bytes in ascending order.

End for step is to done the shuffling on the both state matrix, where different process to be follow.

Let's take a look over these lines,

J1=(j1+s1[i]+s1[j1]+temp2[i]+temp2[j1]+temp2[j2])%N;
J2=(j2+s2[i]+s2[j2]+temp1[i]+temp1[j1]+temp1[j2])%N;

In this lines, this algorithm generates the confusion by generating j1 random index location pointer on the bases of temp2[256] that used to do swapping over the s1[256] state matrix and also same as PC-RC4 algorithm provides the randomness on the index level by used the j1 and j2 at the index level. Same in this manner, swapping process has done over the s2[256] state matrix. In this algorithm, used state[256] matrix to provide the randomness through using the s1[j1], s2[j1], s1[j2] and s1[j2] values. The output of the KSA is the random two state matrix s1 and s2.

This algorithm is also providing the different process for the PRGA. In this stage, the PRGA stage is having 2 state matrices of random values from 0 to 255 bytes values. Then In this stage, on the bases of this two state matrices, generated j1 and j2, two index location indicators, on the based attempt the swapping and further output byte generated output1 and output2, use to two times encryption on the given data.

In this PRGA, this algorithm provides the tough level of randomness by using the s2[j1], s2[j1] with relate to the s1[] and using s1[j1], s2[j2] with relate to the s2[].

And also in the end of the PRGA algorithm, is adding additional swapping in inside the PRGA to create the more confusion inside the PRGA algorithm. By using the following lines have to done swapping over the state matrix.

Let us take a look on these lines

Swap(s1[s2[i]],s1[s2[j1]])
Swap(s2[s1[i]],s2[s1[j2]])

5. METHODOLOGY

a. Introduction: In this section, this paper is introduces the selection algorithm to select the specific portion of the image. This paper is uses two algorithm one for selection of image part and second for encryption of the image describes in the previous section of this paper. For selection a part of an image we provide GUI on the action of mouse double click with variable size (resize). The algorithm is using for the selection describe in the following as follow:

b. Algorithm to select a portion of an image [8]:

Step1. Import the origin image for the transmission.
I=imread(img);
Step2. Choose the way for selection (Rectangle free/ Rectangle centre)
Step3. Call the array file of image.
ROI = imSelectROI (fnames (I));
Step4. For i: length (fname);
Step5. Store the image in array form "image".
Image =imread(fname(I));
Step6. Select the part of the image with X, Y parameter.
Selection=image (ROI.Xrange, ROI.Yrange);
Step7. Store the selected image
SelectImg=imwrite (selection);

c. Method of encryption and selection:
The following figure1: describe the methodology of the encryption and selection of the portion of the image in the process of selective image encryption. The description process is done in the reverse order of the encryption process.

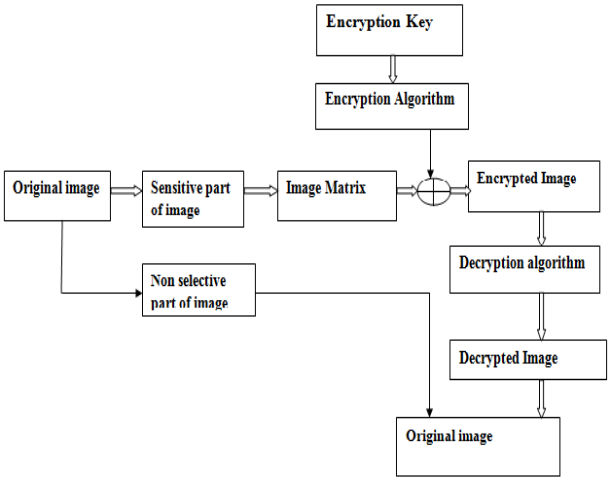

Figure 1: Method of Selective Image Encryption

6. SIMULATION AND RESULT

In this section, this paper shows the simulation and result including the performance analysis by taking different sized images by the using selective image encryption and full image encryption. This paper uses the proposed algorithm to done the encryption over the selective portion of the image. And image selection is done by using the selection algorithm describes in this paper.

This simulation is does by using matlab 9 as tool for the simulation.

The selective image encryption shows in the follow figure 2:

Figure 2: selective image encryption process

In figure2: describe the selective image encryption. First, we inputs the original image and then we select and encrypt the selective portion of the image by using the selection algorithm describe in this paper and proposed encryption algorithm. In this simulation, we used the 256* 256 KB and 80 bits image.

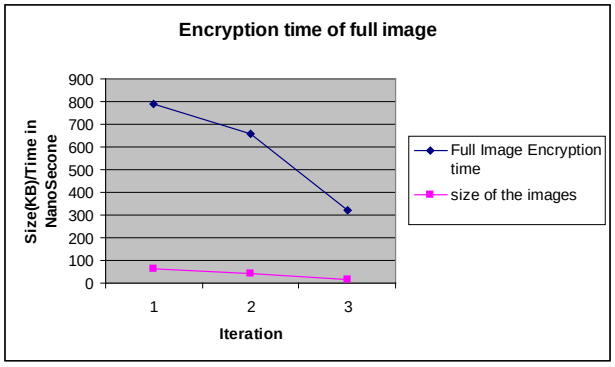

Figure 3: Encryption Time for Full Image

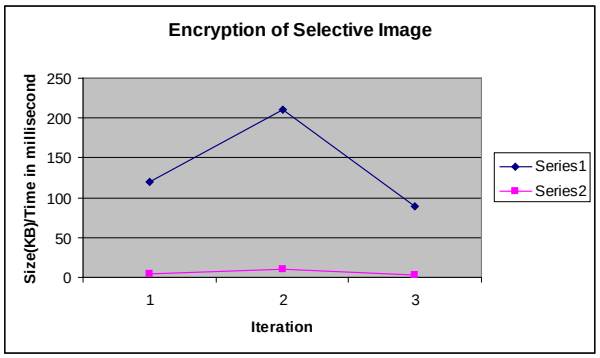

Figure 4: Encryption Time for selective Image

In Figure3 and Figure4, describes the performance analysis of the selective and full image encryption over the different sized images data. As shown in the result, selective image encryption takes less time then the full image encryption. And this shows the selective image encryption best to use from time concern.

7. CONCLUSION

In this manner, this paper describes the concept of selective image encryption. This paper is proposed new enrichment algorithm based on RC4 algorithm, to making secures RC4 against the attacks and applied it over the selective image encryption. So in this manner, provide the more security over the selective image and save time for the encryption of the image. Mean selective image after encryption becomes more secure against the attacks.

REFERENCE

[1] Rafael C. Gonzalez (2009), ”Digital Image Processing”.
[2] Sapna Sasidharan and Deepu Sleeba Philip, “A FAST PARTIAL IMAGE ENCRYPTION SCHEME WITHWAVELET TRANSFORM AND RC4”, 2011
[3] Hameed A. Younis*, Dr. Turki Y. Abdalla**, Dr. Abdulkareem Y. Abdalla*, “A Modified Technique For Image Encryption”.
[4] Pardeep,Pushpendra, “A Pragmatic Study on Different Stream Ciphers And On Different Flavors of RC4 Stream Cipher”, 2012.
[5] Jian Xie, Xiaozhong Pan, “An Improved RC4 Stream Cipher ”, International Conference on Computer Application and System Modeling (ICCASM), 2010.
[6] I. Mantin, A. Shamir “A practical Attackon Broadcast RC4”, FastSoftware Encryption 2001 (M.Matsui,ed.), pp. 152-164, Springer-Verlag, 2001.
[7] S.Fluthrer, I. Mantin, A. Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4”, SAC2001 (S. Vaudenay, A. Youssef,eds.), col. 2259 of LNCS, pp. 1-24, springer-Verlag, 2001.
[8] http://www.mathworks.com, web link