International Journal of Grid Distribution Computing
Vol.7, no.3 (2014), pp.189-198
http://dx.doi.org/10.14257/ijgdc.2014.7.3.19

Multiple Selective Regions Image Cryptography on Modified RC4 Stream Cipher

Mahfuzulhoq Chowdhury[1], Md. Moniruzzaman[1] and Parijat Prashun Purohit[1]

[1]*Department of Computer Science & Engineering, Chittagong University of Engineering & Technology, Chittagong, Bangladesh.*
mahfuz_csecuet@yahoo.com, monircse50@gmail.com, parijat2009@gmail.com

Abstract

Cryptography is the technique which is utilized for secure communication over the network. By using Cryptography technique readable information is converted into an unreadable form. Cryptography is used to protect data from unauthorized access. Universality of security in modern internet based application is an explicit motivation to contribute in the area of Information Security. Multimedia data contain different types of data that include text, audio, video, graphic, images. This paper gives an initiation of an amending technique for multiple selective region image cryptography based on both RC4 stream cipher and chaos. This approach is derived from the standard RC4 algorithm. But Currently RC4 is vulnerable. So for making image encryption technique more secure, we have proposed RC4 with chaos. We have shown that, our proposed method will boost image security over any type of network with several types of attack.

Keywords: *Digital Image Processing, Image Cryptography, Computer Security*

1. Introduction

Cryptography means "study", respectively is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, cryptography is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects of information security such as data confidentiality, data integrity, authentication, and non-repudiation. Cryptography plays a significant role in the disciplines of mathematics, science & engineering. Cryptography is widely used in an electronic based transaction where ATM card password used. Encryption is a common technique to uphold image security in the storage and transmission of digital images are exchanged over network types. Image encryption has application in various fields include Internet communication, multimedia systems, medical imaging and Tele-medicine and military communication. The information security has become more important to the progress in the exchange of data and various encryption systems to encrypt and decrypt image and no single encryption algorithm which is satisfied different types of image. 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 the text used for communication. The image is used in internet, multimedia systems, medical, and telemedicine, military for the purpose of communication [2]. Traditionally developed an encryption algorithm such as RSA, DES is suitable for text encryption, but not suitable for image encryption directly because of two reasons [1]. One is that the image size is larger than

ISSN: 2005-4262 IJGDC
Copyright ⓒ 2014 SERSC

that of the text, so the traditional crypto systems take much time to directly encrypt the image data. The other reason is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image, a decrypted image containing small distortion is acceptable due to human perception. The RC4 algorithm is most used stream cipher algorithm. Different protocol standard used this algorithm to make secure networks. Some of the names of the standard protocols are WPA (Wi-Fi Protected Access), SSL (Secure Socket Layer Protocol), and WEP (Wired Equivalent Privacy) [2]. On the other hand Chaos-based encryption has become an attractive research topic today [3]. Chaos system is used in cryptography for three reasons:

- The nature of chaos is sensitive to initial conditions of the system,
- Random chaotic behavior, and
- The values do not have a period of chaos.

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 resolve 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. Image cryptography may contribute significantly in the field of image security if the proposed method can be applied properly.

Our paper is organized in a way that initially introduces the background and related works of the problem in the past and present time. Then detailed methodology and implementation is described. Experimental results and analysis have given sequentially. Finally, we conclude the goal that we achieved in by completing our work. Also, some recommendation is given for further research in this field.

2. Background and Related Works

Image Encryption can become an integral part of the image delivery process if encryption is the process of transforming the information to ensure its security with the huge growth of computer networks and the latest advances in digital technologies. A quite of works has been done in this field. Our work mainly depends on the previous done in [1],[2],[3],[4]. Most them has some limitations either in types of image or selecting regions and most often the execution time. P. Kumar et al [1] developed a method for the selected image cryptography which is quite satisfactory but the main limitation is that they developed their process for only single region. Only one single region makes image data more vulnerable if we can select image by multiple parts then it can be more secured. What if the analyst can guess the cipher by the existing portions? P. K. Pateriya et al. [2] found a method that only has the application of RC4 algorithm. But now a day no standalone algorithm is secure because of various attacks. There need to be addition of other somewhat algorithm. Gautam and Dr.P.R [3] Gupta proposed a method where they used the block based cipher for full image encryption. They got the output that takes much times. Although the got a significant result but the complexities for the block based cipher is huge and again execution time is quite high. Dongming et al. [4] published a research work which is based on chaos although the chaos is a good algorithm but Chaotic Image Encryption technique does not have any compression scheme and authenticity verification. Their method gives output for only gray scale image. Here should be an addition of RGB. So an algorithm is required that can perform operation both on RGB and gray scale images.

 Copyright ⓒ 2014 SERSC

3. Motivation

Presently the area of networking and communication of computer science develops too widely. Different types of communication and networks use practically as per the different organizational and industry requirement, like: Wireless, Sensor, Internet and so on. The common concern regards these all the networks are Security. To make secure the secret data and information during transmission from unauthorized access. So, to solve this problem, Cryptography concept is available [12]. The concept of Cryptography provides the various algorithms for confidentiality purpose. One of the most used algorithms is RC4 stream cipher. If the image cryptography technique can be implemented then it could be useful in medical image processing, picture messaging on Cell Phones, Military sectors, Government documents *etc*. Selective region image cryptography will make the image contents secure in less time that'll be helpful for faster encryption and decryption process. If the multiple regions can be encrypted then the cryptography process will be more secure ever.

4. Methodology

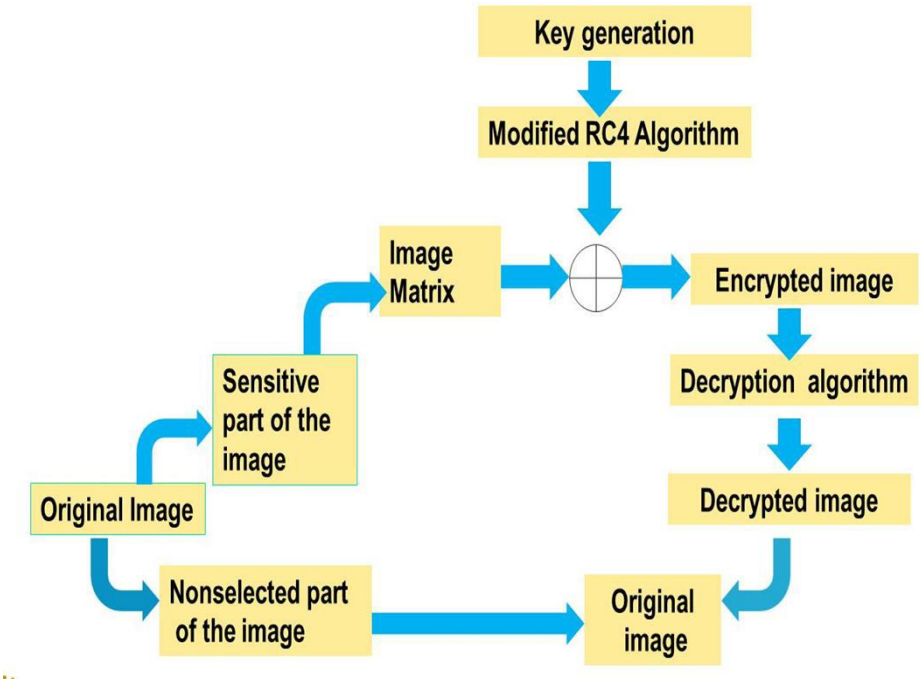

Figure 1. Procedure of Encryption & Decryption

Normally cryptography begins with taking an image as an input and then applying the required algorithm encrypting the image that is called encrypted image. But for selected image encryption first we need to specify the regions we are going to encrypt. Then the encryption algorithm works. With the help of the algorithm the selected parts of the image is being encrypted and the other parts remains the same. After the end of this process we got the encrypted image. By applying the same algorithm we again decrypt the selected regions. After the end of this step we again got the original image back. The overall procedure is shown in Figure 1.

Copyright ⓒ 2014 SERSC

4.1. Key Generation

Figure 2.1. Main Input Image

25	25	25	25	25	25	25	25	25
25	25	25	25	25	25	25	25	25
26	26	25	25	25	25	25	25	25
25	26	24	25	25	26	26	25	25
26	23	24	25	25	26	26	25	25
31	26	25	26	26	24	25	25	25
64	38	28	26	24	26	23	25	27
151	111	76	38	26	23	28	27	28
188	183	176	128	57	29	25	26	25
166	172	183	190	158	82	29	24	23
140	144	158	170	180	165	99	45	26
131	132	136	141	139	171	170	96	48
136	141	141	136	118	132	178	165	99
130	148	155	146	134	128	148	185	173

Figure 2.2. Image Matrix

184	175	182	187
179	172	182	188
180	173	181	186
186	179	183	184
186	180	181	179

231	231	234	237
236	234	235	238
241	240	237	240
239	238	240	240
239	238	239	239
239	239	239	239

Figure 2.3. Selected Part matrix

Figure 2. Image with its Selected Part Matrix

The key-scheduling algorithm is used to initialize the permutation in the array "S". "key length" is defined as the number of bytes in the key and can be in the range $1 \leq$ key length $\leq$ 256, typically between 5 and 16, corresponding to a key length of 40 – 128 bits. First, the array "S" is initialized to the identity permutation. S is then processed for 256 iterations in a similar way to the main PRGA, but also mixes in bytes of the key at the same time.

```
for  i from 0 to 255
S[i] := i
endfor
j := 0
for i from 0 to 255
j := (j + S[i] + key[i mod keylength]) mod 256
swap values of S[i] and S[j]
endfor
```

Here the key required for the process is generated and then the key is encrypted by a function, i.e. state1=randi(1000)
Encrypted key= randseed(state1,1,1,30,80);

The above statement says that the key will be multiplied by any number between 30 to 80. The receiver needs to decrypt the key by algorithm.

4.2. Sensitive Part Selection

We used an image 320*320 size. This image will produce an image matrix of 320*320. Hence term comes to define the sensitive part. I worked on fixed RGB or Gray Scale image. Make more than one selected regions. Then the size of the matrix decreased. Figure 2 shows the details along with image matrix.

4.3. Encryption Part

Apply the confusion and diffusion on selected part and XOR it with randomly generated pseudo code and replace the pixel value of the selected portion's matrix. Now we get the selected regions encrypted.

 Copyright ⓒ 2014 SERSC

4.4. Decryption Part

In this part the hidden portion of the image is restored by using the same algorithm. Finally we get the original image. We have taken the benefit of symmetric key algorithm to decrease the complexity of the operation and protect the data in a reasonable computational cost and these properties make the scheme suitable for real-time applications. We described the concept of selective encryption technique. Selective encryption technique is one of the most promising solutions to increase the speed of encryption as compared to the full encryption. Selective image after encryption becomes more secure against the attacks. Selective encryption is advantageous for the multimedia content like images, video and audio. Selective encryption is faster as compared to the full encryption of the data.

5. Experimental Results

5.1. Histogram Analysis

An image histogram is a type of histogram that acts as a graphical representation of the tonal distribution in a digital image.[14] It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance. The horizontal axis of the graph represents the tonal variations, while the vertical axis represents the number of pixels in that particular tone.[14] The left side of the horizontal axis represents the black and dark areas, the middle represents medium grey and the right hand side represents light and pure white areas. The vertical axis represents the size of the area that is captured in each one of these zones. Thus, the histogram for a very dark image will have the majority of its data points on the left side and center of the graph. Conversely, the histogram for a very bright image with few dark areas and/or shadows will have most of its data points on the right side and center of the graph. Histogram shows distribution of pixel intensities of an image. Using histogram an attacker does frequency analysis to deduce the secret key or plain-pixels. This kind of attack is called statistical attack. To prevent statistical attack, histogram of plain-image and histogram of cipher-image should not have a similarity statistically. Therefore, histogram of cipher-image should be relatively flat or statistically have an uniform distribution. Relatively uniform distribution of the cipher-image is an indication that the image encryption algorithm has a good quality [11].For different Image files Histogram result is shown in Figure 3.

Copyright ⓒ 2014 SERSC

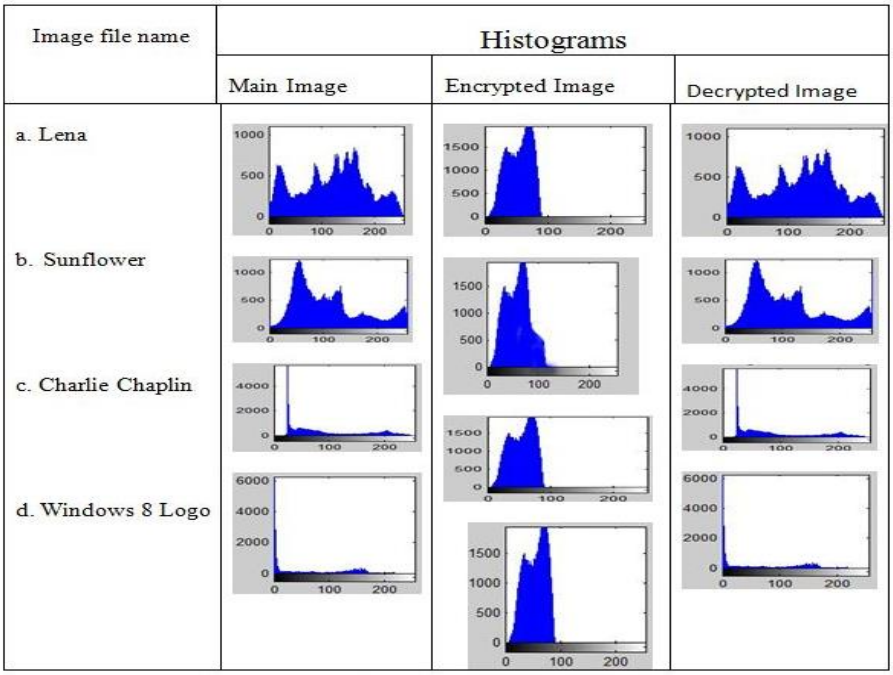

Figure 3. Histogram Analysis of Various Images

5.2. Entropy Analysis

Refer to information theory, entropy states degree of uncertainty in a system. Entropy of message m is calculated by equation described in [12]. Entropy is expressed in units of bits. Random messages should have an ideal entropy equal to 8, while in less random messages entropy is less than eight. If the entropy is less than eight, here are degrees of predictability, which is a threat to security. Cipher-images can be viewed as random images, so the entropy should ideally 8. In the grayscale image there are 256 gray values (m0 = 0, m1 = 1... m255 = 255) and probability of each grey value is calculated from its histogram. Without loss of generalization, we calculate entropy for gray scale image only. Here we got the average entropy (7.8799) is very close to 8 which means that the proposed selective encryption algorithm is safe from entropy attack that predict information in the image. Entropy Analysis is shown in Table1 for sample images.

Table 1. Entropy Analysis

Image File Name	**Entropy Existing Method(P. Kumar et al's Method [1])**	**Entropy Proposed Method**
1. Lena	7.4564	7.9760
2. Charlie Chaplin	7.7323	7.9987
3. Sunflower	7.7650	7.9501
5. Windows 8 logo	7.6597	7.8967

Copyright ⓒ 2014 SERSC

5.3. Peak signal-to-noise ratio (PSNR) Analysis

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (*e.g.*, for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content. PSNR result is shown in Table 2.

Table 2. PSNR Values

Image File Name	**PSNR**
a. Lena	14.7272
a. Sunflower	13.5867
a. Charlie Chaplin	12.5839
a. Windows 8 Logo	10.3319

5.4. Attack Analysis

Attack analyses were also done for sample images and results are shown in Table 3.

Table 3. Attack Analysis for Images

Attack Name	**PSNR [5]**	**PSNR(Proposed Method)**	**NCC [5]**	**NCC (Proposed Method)**
Sharpening	11.8549	13.8356	1.00	1.00
Gamma Correction	10.9943	12.8906	1.00	1.00
Cropping	13.5673	15.9056	0.9769	0.9846
Salt & Pepper Noise	12.5690	13.9567	0.9800	1.00

- Proposed method provides less complexity, fast and secures approach of image cryptography.
- It provides a high PSNR and NCC (≈1.00) value that ensures the reliability of the proposed method.
- All the performance analysis demonstrates that the proposed method any can be applicable for image security over any network

Copyright ⓒ 2014 SERSC

5.4. Processing Time

When we are talking about image encryption process, we mean whole image encryption. But there are some recent works [5] where partial image encryption is discussed. But they had only the single selected region. Our proposed method is about multiple regions. It's quite normal that multiple regions will take more processing time than single regions. Again the processing time for selected is smaller than the full image encryption process. So there will be a quite difference in the time interval. There is a table follows which illustrates the time for whole process-

Table 4. Processing Time for Various Regions

Image File Name	Single Region	Multiple Regions	Entire Region
Lena	0.2345	0.4587	0.5904
Sunflower	0.3245	0.5678	0.6231
Charlie Chaplin	0.0988	0.5005	0.3589
Windows 8 logo	0.1934	0.5421	0.6598

6. Conclusion & Future Recommendations

Selective image after encryption becomes more secure against the attacks. Selective encryption is advantageous for the multimedia content like images, video and audio. Selective encryption is faster as compared to the full encryption of the data. For securing large visual data with requirements of real-time communication and use in resource constrained applications such method would be in demand in the future as well. Through the discussion over the paper, we discussed first the basis behind the Cryptography, then later in the discussion move to the Symmetric Stream Cipher, one of the most important and most used classes of the Symmetric algorithm. We also discuss the survey over the performance of the various stream cipher algorithms and RC4 stream cipher is proved to be better than among all. We have proposed our algorithm and verified that our algorithm would work better in any kind of attack discussed in attack analysis. So in the remainder of the composition, we discussed the RC4 stream cipher algorithm in detail and talked about the various applications where we used the RC4 for the security purpose, basic algorithm, attacks and the various enhancements on RC4, is introduced by some of researcher to increase the protection of the RC4 stream cipher against the attacks and weaknesses. So in this manner, we simply consider the enhancement over the RC4 stream cipher done by the different experts to increase the security of the RC4 stream cipher. Still plenty of research to be done to improve the security of the RC4. Again in our proposed method we used the image type of RGB and Gray Scale, but future modification can be made out in any type of the image. It can be modified for the PNG or BMP image. Again, we trust we would able to apply the algorithm for video encryption.

 Copyright ⓒ 2014 SERSC

References

[1] P. Kumar et al. "RC4 Enrichment Algorithm Approach for Selective Image Encryption", International Journal of Computer Science & Communication Networks, vol.2, no.2 (**2012**), pp. 181-189.
[2] Pardeep, Pushpendra, "A Pragmatic Study on Different Stream Ciphers and on Different Flavors of RC4 Stream Cipher", IJCSNS, vol.12, no.3 (**2012**), pp. 37-42.
[3] A. Gautam, P.R Gupta "A New Image Encryption Approach Using Block Based Transformation Algorithm ", International Journal of Advanced Engineering Sciences and Technologies, vol.8,no. 1(**2011**),pp 090-096.
[4] C. Dongming, Z. Zhiliang, Y. Guangming, "An Improved Image Encryption Algorithm Based on Chaos." in Proceedings of IEEE International Conference for Young Computer Scientists,(**2008**). pp. 2792-276.
[5] S. Sasidharan and D. S. Philip, "A Fast Partial Image Encryption Scheme with Wavelet Transform and RC4", International Journal of Advances in Engineering & Technology, ISSN: 2231-1963, vol.1, no.4 (**2011**), pp. 322-331.
[6] Jian Xie, Xiaozhong Pan, "An Improved RC4 Stream Cipher", International Conference on Computer Application and System Modeling, (**2010**).
[7] I. Mantin, A. Shamir "A practical Attack on Broadcast RC4", Fast Software Encryption (M.Matsui,ed.), Springer-Verlag,(**2001**), pp. 152-164.
[8] S.Fluthrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", SAC2001 (S. Vaudenay, A. Youssef, eds.), col. 2259 of LNCS, Springer- Verlag, (**2001**), pp. 1-24.
[9] G. Paul, S.Maitra, "RC4 state in formation at Any Stage Reveals the Secret Key ", In proceedings of SAC (**2007**), http://eprint.iacr.org/2007/208.pdf.
[10] Kamlesh Gupta and Sanjay Silakari, "A Chaos Based Image Encryption Using Block-Based Transformation Algorithm", IJCNS, December (**2009**).
[11] Rinaldi Munir, "Security Analysis of Selective Image Encryption Algorithm Based on Chaos and CBC-like Mode", 7th International Conference on Telecommunication Systems, Services, and Applications (**2012**).
[12] Alireza Jolfaei, Abdul Rasoul Mirghadri, "An Image Encryption Approach Using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology, (**2010**).
[13] Atul Kahate, "Cryptography and Network Security", pp- 123-125, (**2008**).
[14] Web link, http://www.mathworks.com.
[15] Wikipedia, the free encyclopedia, en.wikipedia.org/wiki/Image_histogram.

Authors

Mahfuzulhoq Chowdhury, received the B. Sc. Engineering Degree in computer science and engineering from Chittagong University of Engineering and Technology, Bangladesh, in 2010. From September 2010 onwards he has been serving as a faculty member in the Department of Computer Science and Engg., Chittagong University of Engineering and Technology (CUET), Chittagong, Bangladesh. His major researches include Human Computer interaction, Cognitive Radio Networks, Cryptography, Wireless Sensor Networks etc.

Md. Moniruzzaman received the B. Sc. Engineering Degree in Computer Science and engineering (CSE) from Chittagong University of Engineering and Technology (CUET), Bangladesh, in 2013. His major research interests include image Encryption, Pattern Recognition etc.

Copyright ⓒ 2014 SERSC

Parijat Prashun Purohit is pursuing the B. Sc. Engineering Degree in Computer Science & Engineering from Chittagong University of Engineering and Technology. His major research interests include Natural Language Processing, Wireless Communication Systems, and Cloud Computing etc.

Copyright ⓒ 2014 SERSC