ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

Image Encryption with RSA and RGB randomized Histograms

Gajendra Singh Chandel [1], Pragna Patel [2]

[1]Assistant Professor, Dept. of Computer Science and Information Technology, SSSIT, Sehore, India

[2]M.Tech Research Scholar, Dept. of Computer Science and Information Technology, SSSIT, Sehore, India

ABSTRACT*:* In this paper we have applied RSA algorithm to encrypt the image files to enhance the security in the communication area for data sending. The image file is first selected from the database then we first perform the splitting of the images. Then we apply the RSA algorithm on the split files. Then we apply the decryption mechanism on the same image and achieve the split image and combine it for forming original image. We are also considering the Histogram bins which are used for measuring the colour bins in the original and encrypted images. We are clearly showing this in the result section which shows the effectiveness of our approach. Finally we calculate the entropy of the original and encrypted image.

KEYWORDS: Image Encryption, RSA, RGB Histograms, Entropy

I.INTRODUCTION

In [1] author suggested that Encryption and decryption of original message is based on key value [1]. Very few algorithms like RSA, Quadratic residuosity, Phi-hiding assumption, etc. provides computational hardness [2] and it makes difficult to break a key by an adversary whose objective is to find the original message. Crux of cryptography was arrived in behalf of Loam Battle I to protect information from cryptanalyst.

In this day, facts capture recognize in internet is assuming, hence we attempt to ensure the secure data transfer. In addition, every cryptographic algorithm must satisfy the execution time and high level security channel according to selection of Advanced Encryption Standard (AES) [3]. In [4] author suggest that However, employing encryption in relay based cooperative wireless communication results in multiple drawbacks. First: encryption requires an extra-large amount of bandwidth because of the added overhead packets. Second: the performance deteriorates extensively due to the avalanche effect [5][6] in wireless fading channels, which tremendously reduces the effective bandwidth utilization. This is in addition to the delay caused by the processing time required by the encryption and decryption algorithms at the source and destination sides, respectively. At present, according to its own characteristics of the images, there are many encryption algorithms have been proposed [7]-[13]. Viewing from the point of transform domain they are divided into time-domain encryption and frequency domain encryption. In [14] author suggest RSA encryption for user cloud environment. Based on the above discussion we have applied RSA algorithm for image encryption.

The remaining of this paper is organized as follows. In Section 2 Literature Survey. In section 3 we discuss our proposed approach. Result Analysis is given in section 4 the conclusions and future directions are given in Section 5. Finally references are given.

II.LITERATURE SURVEY

In 2012, Long Baoa et al. [15] proposed chaotic system shows excellent chaotic behaviors. To demonstrate its application in image processing, a new image encryption scheme using the proposed chaotic system is also introduced. Computer simulation and security analysis demonstrate that the proposed image encryption scheme shows excellent encryption performance, high sensitivity to the security keys, and a sufficiently large key space to resist the brute attack. But in this paper random like nature of chaos is not considered. In 2012, Ahmad Abusukhon et al. [16]

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

suggested that in cryptographic application, the data sent to a remote host are encrypted first at the source machine using an encryption key then the encrypted data are sent to the destination machine. This way the attacker will not have the encryption key which is required to get the original data and thus the hacker will be unable to do anything with the session. They propose a novel method for data encryption and our method is based on the transformation of a text file into an image file on both client and server machines. They analyze our algorithm by calculating the number of all possible key permutations. In 2012, Anal Paul et al. [17] suggest that some chaos based algorithms are working well and resists many type of crypto analysis attacks, but it takes lot of time for encryption and decryption. Some of chaos based algorithms are very fast but their strength to resist attack is questionable. So these have motivated us to design a crypto system which will take less amount of time for encryption and decryption and it should resist all type of crypto analysis attacks. They have developed an advanced image encryption scheme by using block based randomization and chaos system. Here we discuss a block based transformation algorithm in which image is divided in to number of blocks. Then these blocks are transformed before going through a chaos based encryption process. At the receiver side after decryption, these blocks are re- transformed in to their original position. The main advantage of this approach is that it reproduces the original image with no loss of information during the encryption and decryption process in a reasonable amount of time, and due to sensitive chaos system becomes it more secure and reliable over the network. In 2012, Vinay et al. [18] presents securing the transmission of medical images. The presented algorithms will be applied to images. Their work presents a new method that combines image cryptography, data hiding and Steganography technique for denoised and safe image transmission purpose. In This method they encrypt the original image with two shares mechanism encryption algorithm then embed the encrypted image with patient information by using lossless data embedding technique with data hiding method after that for more security. They apply steganography by encrypted image of any other medical image as cover image and embedded images as secrete image with the private key. In receiver side when the message is arrived then they apply the inverse methods in reverse order to get the original image and patient information and to remove noise we extract the image before the decryption of message. In 2013, Mohammad Ashiqur Rahman et al. [19] suggest that the risk analysis is an important process for enforcing and strengthening efficient and effective security. Due to the significant growth of the Internet, application services, and associated security attacks, information professionals face challenges in assessing risk of their networks. The assessment of risk may vary with the enterprise's requirements. Hence, a generic risk analysis technique is suitable. Moreover, configuring a network with correct security policy is a difficult problem. The assessment of risk aids in realizing necessary security policy. Risk is a function of security threat and impact. Security threats depend on the traffic reachability. Security devices like firewalls are used to selectively allow or deny traffic. However, the connection between the network risk and the security policy is not easy to establish. A small modification in the network topology or in the security policy, can change the risk significantly. It is hard to manually follow a systematic process for configuring the network towards security hardening. Hence, an automatic generation of proper security controls, e.g., firewall rules and host placements in the network topology, is crucial to keep the overall security risk low. They first present a declarative model for the qualitative risk analysis. They consider transitive reachability, i.e., reachability considering one or more intermediate hosts, in order to compute exposure of vulnerabilities. Next, we formalize our risk analysis model and the security requirements as a constraint satisfaction problem using the satisfiability modulo theories (SMT). A solution to the problem synthesizes necessary firewall policies and host placements. They also evaluate the scalability of the proposed risk analysis technique as well as the synthesis model. In 2013, Manoj Kumar Ramaiya et al. [20] suggested that Image steganography is a technique for hiding information into a cover image. Least Significant-Bit (LSB) based approach is most common steganographic technique in spatial domain due to its easiness and hiding capacity. All of existing methods of steganography focus on the embedding strategy with less concern to the pre-processing, such as encryption of secrete image. The conventional algorithm does not provide the preprocessing required in image based steganography for better security, as they do not offer flexibility, robustness and high level of security. Their proposed work presents a unique technique for Image steganography based on the Data Encryption Standard (DES) using 64 bit block size of plaintext & 56 bits of Secrete key. The preprocessing provide high level of security as extraction of image is not possible without the knowledge of mapping rules of S –Box and secrete key of the function. Attack Detection in Watermarked Images with PSNR and RGB Intensity are also suggested in [21]. An optimized fast encryption scheme based on chaotic signal with multi key is justified for video frame is suggested in [22]. Their Simulation results show that the proposed chaotic encryption scheme outperforms the existing scheme in terms of considerable reduction in encryption and decryption time. The security of the proposed

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

scheme is also analyzed by various cryptanalysis attacks.

III.PROPOSED ALGORITHM

The figure 1 shows the working process of our algorithm. We are using some images from [23][24] the famous Wang database. Although our algorithm is working on the entire image database.

First we consider the images from the dataset. Then we apply the splitting algorithm on the image so that the image will be split in several parts and the image items are separated. The purpose of splitting is to enhance the security in two ways. First by splitting and second by encryption. Then we apply RSA encryption on the split data and it will be decrypted by the intended user and join all the split data by applying the reverse mechanism which is also bared by security key. So we are applying two key securities first for split data and second for encryption.

Algorithm: IERSA
Step 1: Select the image.
Step 2: Split the images.
2.1 rows = 3;
2.2 cols = 3;
2.3 chunks = rows * cols;

2.4 Columns:chunkWidth = image.getWidth()
2.5 determines the chunk width and height
Rows: int chunkHeight = image.getHeight()
2.6 count = 0;
2.7 Image array to hold image chunks
2.8 BufferedImage imgs[]
for x = 0; x < rows; x++
{
for int y = 0; y < cols; y++
{
imgs[count] = new BufferedImage(chunkWidth, chunkHeight, image.getType());
2.9 draws the image chunk

Then we apply Rivest-Shamir-Adleman (RSA) algorithms is one of the most popular and secure public-key encryption methods [25][26]. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.
Using an encryption key (*e*,*n*), the algorithm is as follows:
Step 3: Represent the message as an integer between 0 and (*n*-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
Step 4: Encrypt the message by raising it to the *e*th power modulo *n*. The result is a ciphertext message C.
Step 5: To decrypt ciphertext message C, raise it to another power *d* modulo *n*
The encryption key (*e*,*n*) is made public. The decryption key (*d*,*n*) is kept private by the user.

How to Determine Appropriate Values for *e*, *d*, and *n*

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as *p* and *q*.
2. Set *n* equal to *p* * *q*.
3. Choose any large integer, *d*, such that GCD(*d*, ((*p*-1) * (*q*-1))) = 1
4. Find *e* such that *e* * *d* = 1 (**mod** ((*p*-1) * (*q*-1)))

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

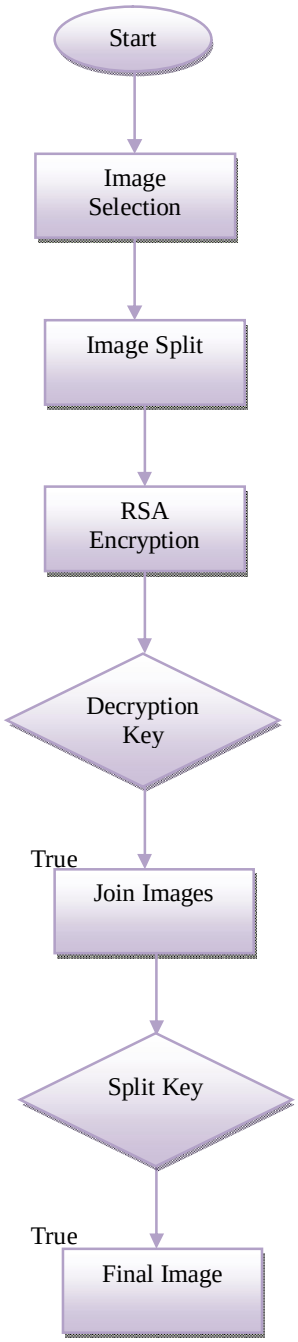

Figure 1: Flowchart

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

For better understanding our methodology, we have considered the rose example in figure 2. We first apply splitting technique then we apply RSA on the splitted files and then RSA encryption will be applied on the encrypted files. Then It will be decrypted by the key and merge by the key for providing security.

Figure 2: Rose Data

Figure 3: Split Rose File

Figure 4: Encrypt all Split Files

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

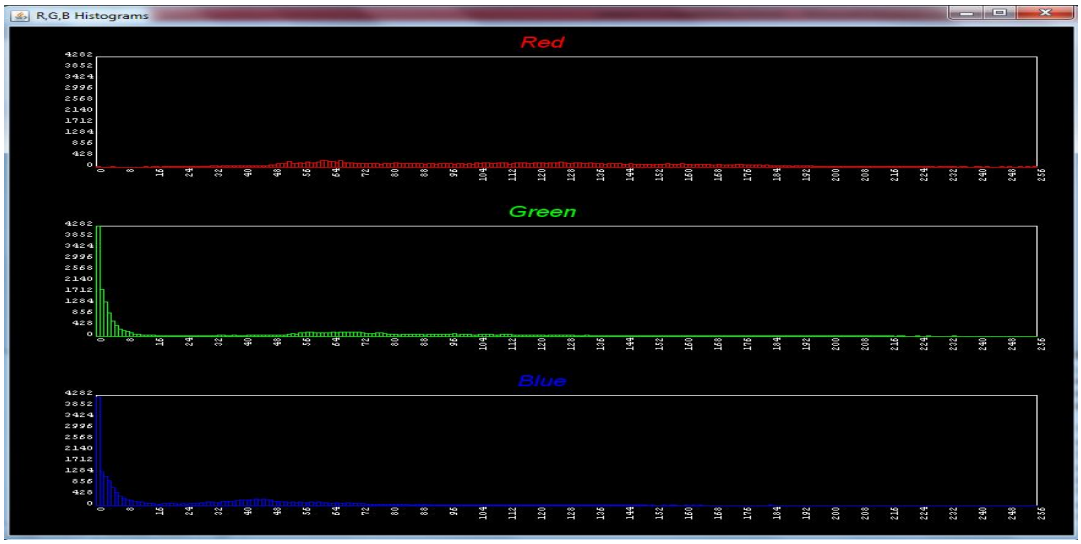

Figure 5: Original Image Histogram

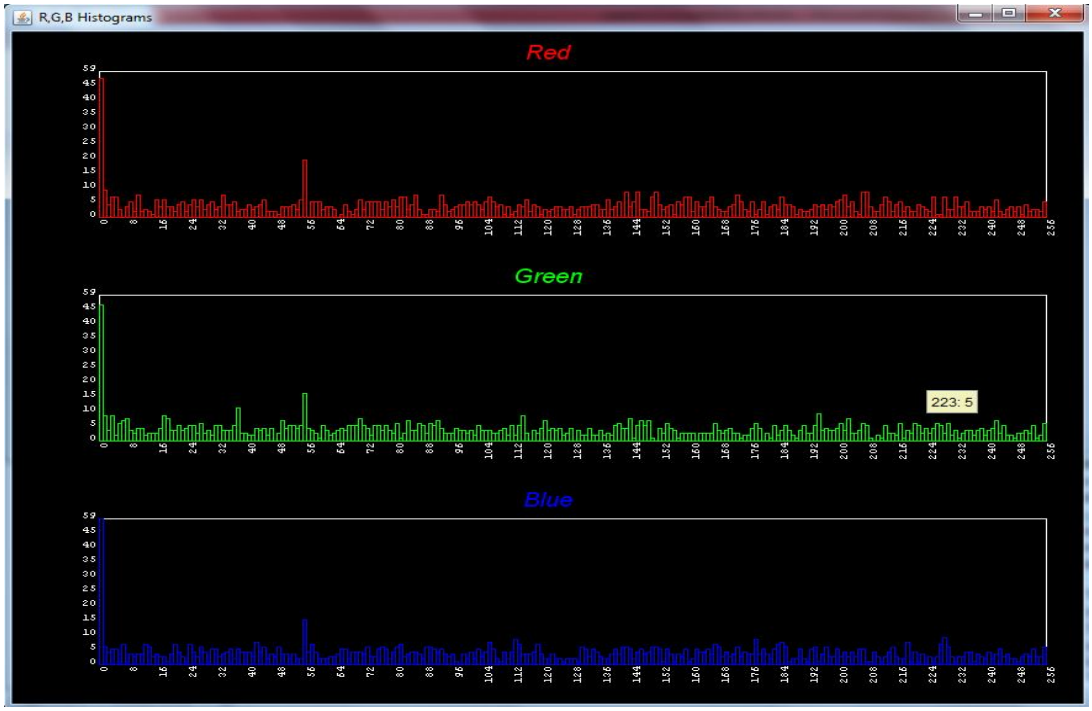

Figure 6: Encrypted Image Histogram

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

IV.RESULT ANALYSIS

In figure 5 and figure 6 we are analyzing our results by the help of histograms also. The above pictures clearly showed the significant changes in the original and in the encrypted image. After studying and observing several research works we compare the result discussions by our techniques.

For this we are using entropy implications as the amount of "disorder" of a system.

- Probability of symbol in string

$$\sum_{i=1}^{N} p_i = 1$$

And the value of Entropy (H) is: $\sum_{i=1}^{n} - p(s_i) \log_2 p(s_i)$

S. No	Data	Original Image (Entropy)	Encrypted Image (Entropy)	Difference
1	African Man	7.967	7.991	0.24
2	Rose	7.903	7.951	0.48
3	Leena	7.937	7.984	0.47
4	School	7.900	7.956	0.56
5	Elaine	7.929	7.980	0.51
6	College	7.912	7.960	0.48
7	Globe	7.807	7.937	0.13
8	River	7.758	7.900	0.14

As per the above table we clearly show that the difference in entropy is minimum in comparison to the previous technique adopted. It shows the effectiveness of our approach.

VI.CONCLUSION

In this paper we survey and analyze several image encryption and decryption techniques. On the basis of our study we find the problem formulation as well as analysis. So our study analyses and also provides future enhancement directions. Based on the above study we provide the following future directions which can be helpful in better detection:

1) We can use Powerful encryption technique like DES and RSA.
2) Need of Increasing RGB randomization and security key randomization for improving image security.
3) We can improve the block size or bit encryption standard like 128 bit and 256 bit.
4) Chaos-based ciphers should not be susceptible to traditional differential and linear cryptanalysis attacks so hybridization is the better possibility.

REFERENCES

[1] D. Rajavel, S. P. Shantharajah," Cubical Key Generation and Encryption Algorithm Based on Hybrid Cube's Rotation", Pattern Recognition, Informatics and Medical Engineering, March 21-23, 2012.
[2] Stallings William, "Stalling Cryptography And Network Security", 4/E – 2006 Pearson Education, Inc.
[3] Michael R. Garey and David S. Johnson, "Computers and Intractability: A Guide to the Theory of NP-Completeness", W.H. Freeman (1979).
[4] National Institute of Standards (NIST): FIPS Pub 197: Advanced Encryption Standard AES (2001).
[5] Li Qian. Study on Color Image Encryption Algorithms Based on Scan Methodology And Chaotic Sequence. Computer Application and Software, 2008,25(7):237..239.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

[6] Liu Lijun. Image Encryption Algorithm Based on New Composite Chaotic Sequences.Computer and Digital Engineering, 2008,36(1):90 ..94.
[7] Li Peng.Image Encryption Algorithm Based on Super-Chaotic Sequences. Microelectronics and Computer, 2008, 25(3).
[8] Gao Jie.New Chaotic Image Encryption Algorithm Based on Hybrid Feedback. Computer Application, 2008,28(2):434..436.
[9] Chen G R,Mao Y B,Chui C K.A symmetric image encryption scheme based on 3D chaotic cat maps[J].Chaos Solution and Frctals,2004,21:749-761.
[10] Lv Feng. Informatics and Coding. The People's Posts and Telecommunications Press,2005.
[11] Man Young Rhee. Network Security Encryption Principle, algorithm and Protocol[M]. Peking: Tsinghua University Pres, 2007.
[12] Suri , P. R . ; Rani , S. Bluetooth security Need to increase the efficiency in pairing [J]. IEEE/ Southeastcon , 2008.
[13] Fengying Wang. Dynamic Key 3DES Algorithm of Discrete System Based on Multi-dimension Chaos[J]. Microelectronics and Computer, 2005, 7: 25-28.
[14] Ashutosh Kumar Dubey,Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava,"Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", CONSEG 2012.
[15] Long Bao, Yicong Zhou,C. L. Philip Chen," A New Chaotic System for Image Encryption", 2012 International Conference on System Science and Engineering June 30-July 2, 2012, Dalian, China.
[16] Ahmad Abusukhon and Mohammad Talib, "A Novel Network Security Algorithm Based on Private Key Encryption", IEEE 2012.
[17] Anal Paul, Nibaran Das and Agyan Kumar Prusty, "An Advanced Gray Image Encryption Scheme by Using Discrete Logarithm with Logistic and HEH64 Chaotic Functions", IEEE 2012.
[18] Vinay Pandey, Manish Shrivastava, "Medical Image Protection using steganography by crypto-image as cover image", International Journal of Advanced Computer Research (IJACR) Volume-2 Number-3 Issue-5 September-2012.
[19] Mohammad Ashiqur Rahman and Ehab Al-Shaer, "A Formal Approach for Network Security Management Based on Qualitative Risk Analysis", IEEE 2013.
[20] Manoj Kumar Ramaiya, Naveen Hemrajani and Anil Kishore Saxena, "Improvisation of Security aspect in Steganography applying DES", IEEE 2013.
[21] Neha Chauhan, Akhilesh A. Waoo, P. S. Patheja," Attack Detection in Watermarked Images with PSNR and RGB Intensity ", International Journal of Advanced Computer Research (IJACR) Volume-3 Number-1 Issue-9 March-2013.
[22] R. Tamijetchelvy, P. Sankaranarayanan," An Optimized Multikeying Chaotic Encryption for Real Time Applications", International Journal of Advanced Computer Research (IJACR) Volume-3 Number-4 Issue-13 December-2013.
[23] ia Li, James Z. Wang, ``Automatic linguistic indexing of pictures by a statistical modeling approach," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 9, pp. 1075-1088, 2003.
[24] James Z. Wang, Jia Li, Gio Wiederhold, ``SIMPLIcity: Semantics-sensitive Integrated Matching for Picture LIbraries," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol 23, no.9, pp. 947-963, 2001.
[25] Singhal, Mukesh and Shivaratri, Niranjan G., Advanced Concepts in Operating Systems, McGraw-Hill, p. 405.
[26] Rivest, R.L., Shamir, A., and Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol 21, No. 2, February 1978, p. 120-26.