Research Article

International Journal of Advanced Computer Research, Vol 6(24)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.2016.624019

Block based text data partition with RC4 encryption for text data security

Rajni Tiwari [1*] and Amit Sinhal[2]
M.Tech Scholar, Computer Science and Engineering, TIT, Bhopal, India[1]
Associate Professor, Computer Science and Engineering, TIT, Bhopal, India[2]

Received: 12-April-2016; Revised: 22-May-2016; Accepted: 27-May-2016

Abstract
There are several different encryption standards along with different mechanism are used for text data security. In this paper an efficient text data encryption technique has been proposed based on RC4. In this approach the text is divided into different blocks according to the block division mechanism. The block division is based on the number of bytes. Then the divided block is encrypted with RC4 and then each block is converted into an image and sends to the receiver. The receiver received the images and applied different keys. The numbers of keys are depending on the block. If the block is five then the receiver will apply the five keys for the data decrypted and then join the images by the join key. The results are compared by the histogram, key size, number of blocks, key length and number of keys. The results of our approach are efficient in terms of enhancing security by block division, number of keys and key size.

Keywords
RC4, Block division, Histogram, Number of keys, Key size.

1.Introduction
Data security has become an important concern today for the successful operations of different requirement of any organization. The information security is the real concern and shielding an association's data resource from security risks [1] [2]. With an eye to scene division procedures are ensign for countermeasures against various security dangers of the authoritative data. The varied perspectives of dangers and vulnerabilities make threatening condition for the data administrator [3] [4]. It is now a challenging task for the enterprises as all the communication and business relies on the data as it is the core part of any organization [5] [6].

There are several cryptography techniques, which are useful in data security, for example, private or secret key cryptography, public key cryptography, digital signature and hash function [7]. Private key cryptography, a private key is used. Advanced encryption standard (AES), Blowfish, CAST5, Grasshopper, RC4 and 3DES are the examples of private key cryptography.

This requires meander if all else fails part convey offering an impersonation of the key and the key be struck by be passed do without a safe channel to the next individual [8]. Private-key cryptography is level indestructible and effectively actualized for data security. In this way they are more than once for mass measurements encryption. Public key cryptography uses a public and private pair for data encryption. RSA, elliptic curve cryptography (ECC) and Diffie–Hellman key exchange. There are other techniques like to produce digest hashing the message and can encrypt the digest to produce digital signature [9] [10].

Due to generally utilizing content as a part of correspondence procedure, it is vital to shield the secret content information from others that is not authorized for the concern data [11] [12]. To scramble text information one needs to encode the data that is pertinent to every pixel, since pixels are the essential building piece of image data [13] [14]. The encoded content could contain great properties that pass the vast majority of the testing criteria so method of content encryption ought to be sufficiently strong. The encoding procedure will change the information into indiscernible structure and lessening the extent of the information, document or expand the span of the record [15]. So for enhancing the security a method has been proposed to convert the text data

*Author for correspondence

into images, and encrypts it by RC4 and generate the keys according to the block. The numbers of keys generated are equal to the number of blocks.

2.Related study

In 2012, Bao et al. [16] proposed a chaotic framework having the capability of high sensitivity to the security keys, and a sufficiently large key space. They have suggested that it can resist the brute force attack. In 2012, Abusukhon et al. [17] has been proposed an encryption method based on the transformation of a text file into an image file which can be replicated and rely on the client and server. They have analyzed the possible key permutations also. In 2012, Zhang et al. [18] proposed a multi-beneficiary time signcryption concern, and front criss-cross the signcryption are out of it, however the learning was turned out to be acquire not worth the purposeless prophet show, the plan doesn't fulfill privacy and unforgeability of signcryption. Clearly, they almost the like move, and to beat the not defenseless defects, only we mean the relating enhanced technique.

In 2013, Paul et al. [19] proposed an image encryption method based on block based randomization and chaos system. The aim of this method is to achieve less amount of time for encryption and decryption and capable of resisting crypto analysis attacks. In 2013, Rahman et al. [20] analyzing, and endeavor the procedure for authorizing and reinforcing proficient and successful Attach. Opportune to the cumbersome storing up on the internet, importune upkeep, and related fasten attacks, data experts face challenges in surveying shot of their systems. The obligation of scene might change with the endeavor's necessities. In 2013, Ramaiya et al. [21] proposed a method for image steganography, which is based on the data encryption standard (DES) capable of using 64 bit block size of plaintext and 56 bits of secret key. They have suggested that this method is able to provide a high level of security because image extraction is not possible without the knowledge of mapping rules of S -Box and secret key. In 2013, Ahirwal et al. [22] suggested a signcryption method which is based on elliptic curve cryptography (ECC). The main feature of this method is an elliptic curve is used for both encryption and signature generation. The transmitted message is sent in this method in the form of point which is embedded in elliptic curve which is efficient and safe.

3.Methods

In this section the method used along with the working principle has been discussed. In this framework the admin has the authority of sending data to the concern client. Admin can generate new clients and approve it. The data sending process are divided into five parts.

1. Block division based on the file size
2. RC4 Encryption
3. Block and Join Key generations
4. Image Conversion
5. Data Receive

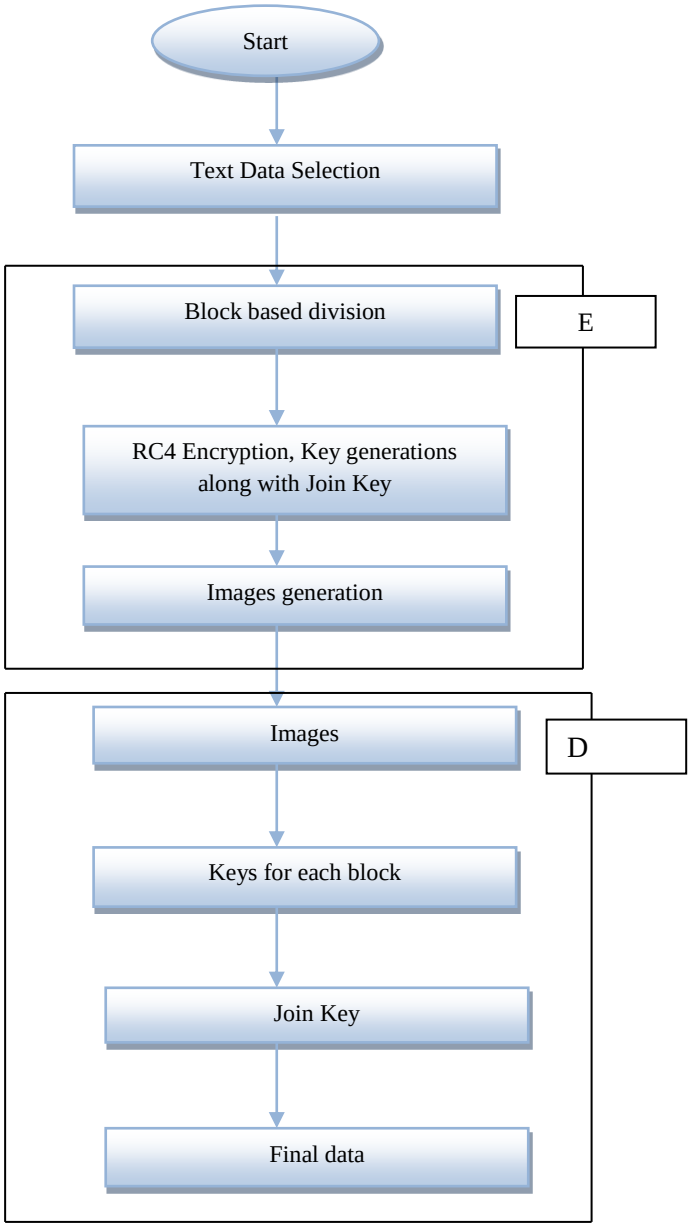

Figure 1 Process flowchart

In the first part the data are divided into different blocks according to a data block division algorithm. A maximum 8 block can be generated. Here size represents the number of data bytes.

Block division algorithm
Step 1: Calculate the file size.
Step 2: if (size<=256)
len= (int) f. length () /2;
Step 3: else if (size<=512)
len= (int) f. length () /4;
Step 4: else if (size<=1024)
len= (int) f. length () /6;
Step 5: else
len= (int) f. length () /8;
Step 6: Final blocks

Then we have applied RC4 encryption algorithm. This algorithm support block based encryption and based on the number of blocks same number of keys is generated. The keys are randomized by Java random classes in each new process.

RC4 algorithm [23]
Step 1: An array which consists of 256-byte array S. It contains a permutation of 0 to 255 bytes stored in the array.
Step 2: So the total possible states is 256! ~2^{1700}
Step 3: Let two index name I and J
Step 4: Initialize i = j = 0
i = (i + 1) (mod 256)
j = (j + S[i]) (mod 256)
Step 5: swap (S[i], S[j])
Step 6: (S[i] + S[j]) (mod 256)
Step 7: for i = 0 to 255 do
S [i] = i
j = 0
Step 8: for i = 0 to 255 do
j = (j + S[i] + k[i mod L])(mod 256)
Step 9: swap (S[i], S[j])
Step 10: Final cipher text data

Then in the next phase join key is generated to join the images.

In the next step the text blocks are converted into images. As the text data are encrypted and converted into different images. It is hard to apply brute force attack for the data recovery and in the second level joining the image to form the final data is also not easy as the recovery of images and placing it in the right position is not so easy.

and finally it is sent to the receiver. The Receiver first applies the decryption key, then join key is applied to convert it into a single file. This process is better understood from *Figure 1* also.

4.Results and discussion

The results, based on our approach are shown in this section and capable to show the effectiveness of our approach. In the previous approach [17] the authors have suggested that the approach with multiple keys and text to image converted data is better for text data encryption. Our approach extends their work. In our approach the data are divided and encrypted in block wise as per the data size. It is shown in *Figure 2-4*. Then it is converted into an image as shown in *Figure 5*. So our approach provided tri-security mechanism. Each block is decrypted by an individual key, the entire block is joined by different key and finally there is an illusion of an image. The results, based on key length, block and histogram are shown in *Figure 6-8*. The variations in key length and block based variations support the randomization process. *Table 1* shows the comparison of different previous methods and found to be better in key sizes (40–2048) bits; block based key generation up to 8 keys and key length varies.

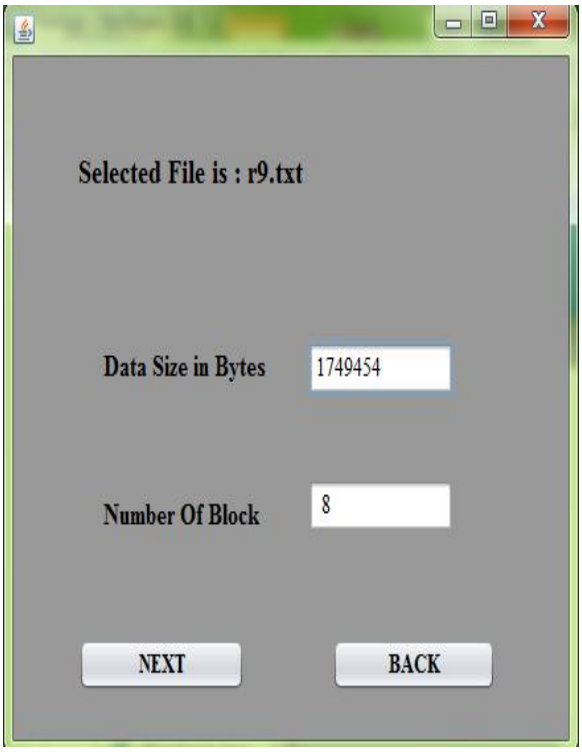

Figure 2 Block based division of the file

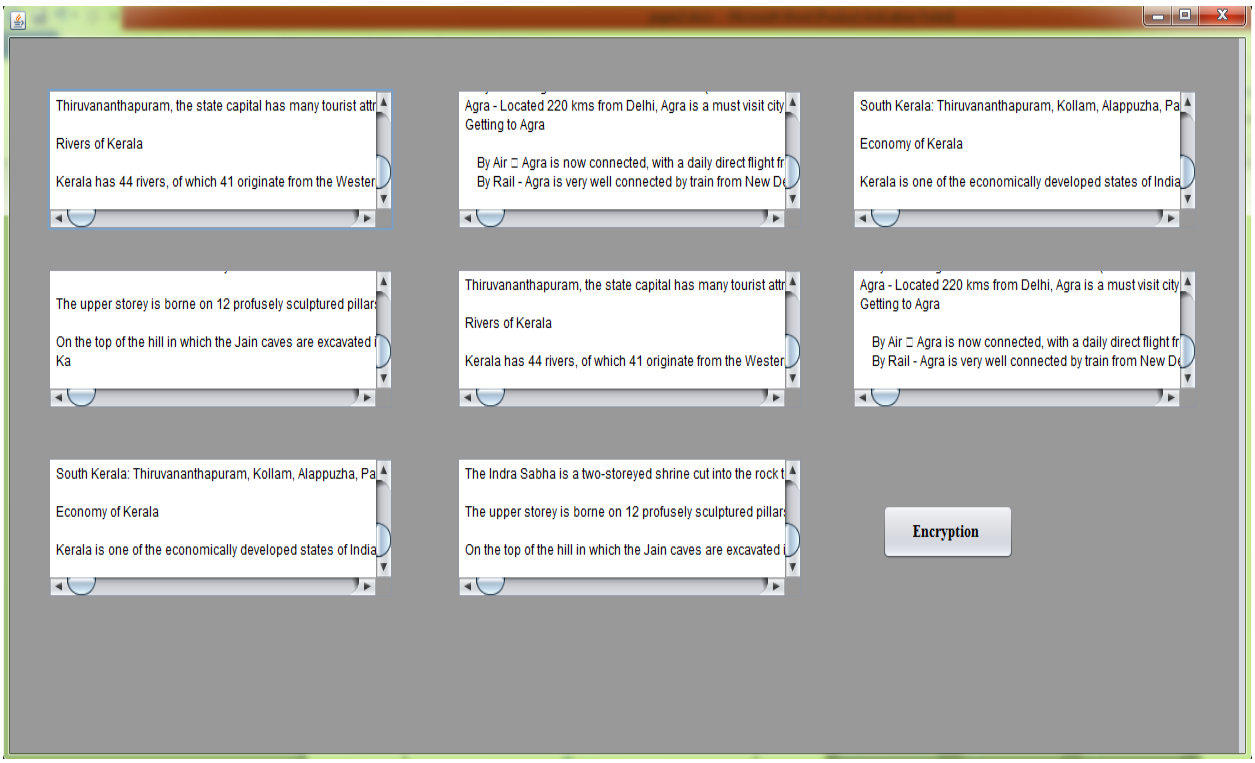

Figure 3 Divided blocks

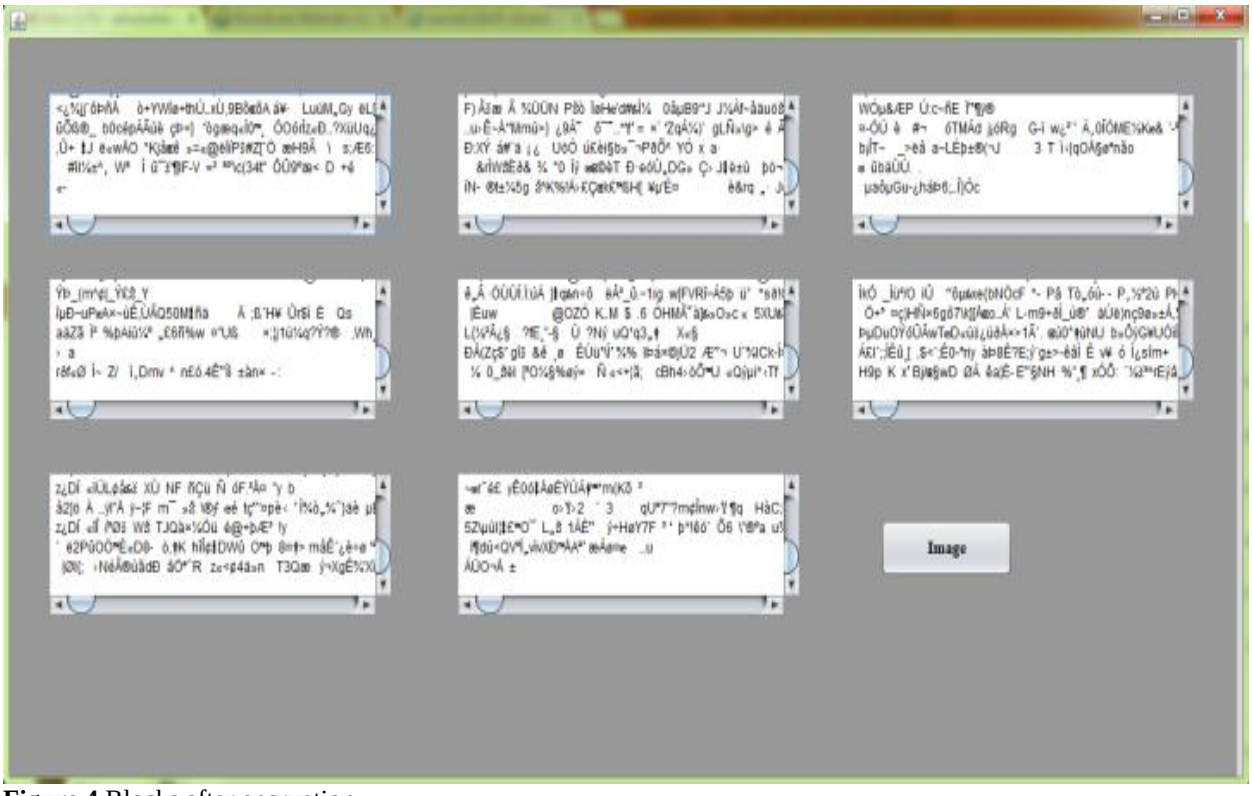

Figure 4 Blocks after encryption

Figure 5 Blocks after encryption and image conversion

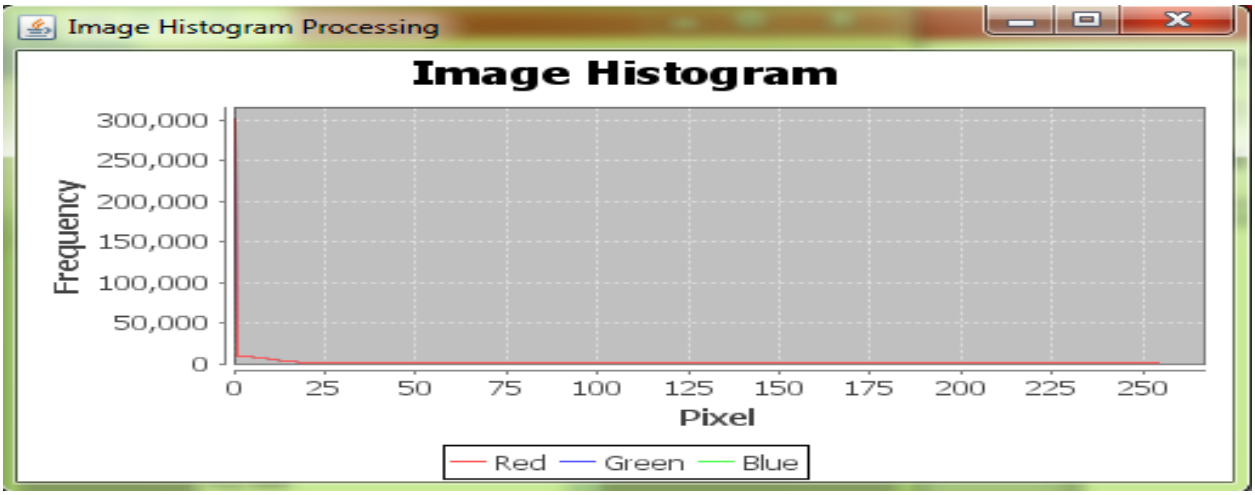

Figure 6 Image histogram

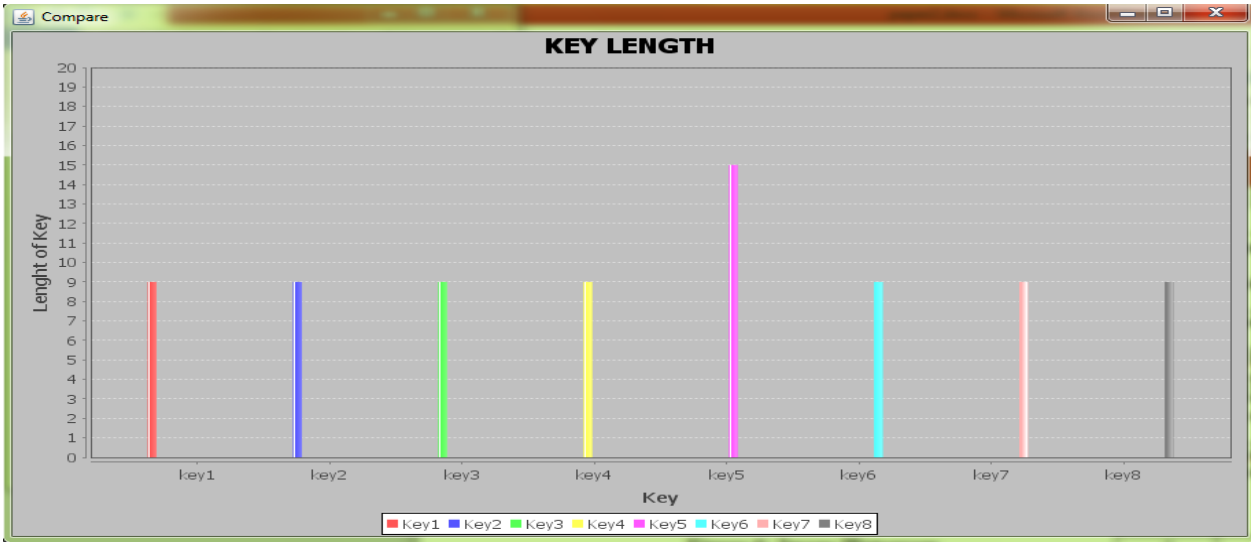

Figure 7 Key length variations

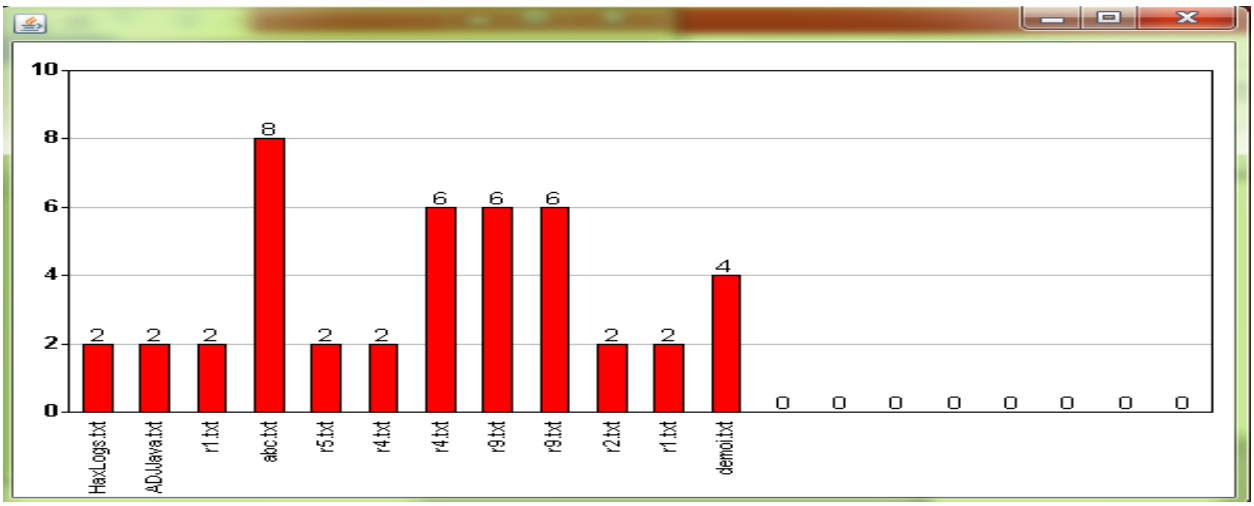

Figure 8 Block based variations

Table 1 Overall comparison

S.No	Author	Proposed method	Result
1	Ren et al.[24]	DES and RSA	key space is 256
2	Li et al.[25]	Advanced Encryption Standard (AES) and Elliptic Curve Cryptosystems (ECC)	high computing speed and anti-attack capability
3	Chen et al. [26]	AES-128	Encryption Time 61573618 for 1021kb
4	Chen et al. [26]	Chaos-AES-128	Encryption Time 65164900 for 1021kb
5	E et al. [27]	chaos encryption and hybrid encryption	Information Entropy is 5.15996 for original entropy 5.15996.
6	Ahmad et al. [15]	Private Key Encryption	Two keys are generated for the send message
7	Proposed work	RC4 based data encryption	Key sizes 40–2048 bits
8	Proposed work	RC4 based data encryption	Block based key generation up to 8 keys
9	Proposed work	RC4 based data encryption	Key length variations

5.Conclusion and future work

The proposed approach is an efficient way of textual data encrypted as it provides different layers of security. It provides data security by RC4 keys. Different keys are needed for each block and a separate key is needed for joining the image. Then it is converted into images. Means each block is represented by an image. So it is much more secure than the traditional mechanism.

The future work of this approach is as under:

1. Time taken in partitioning in our approach is high, so there can be some mechanism in the future by which it can be reduced.
2. The type of data used for this experiment is text only in future different data type like images and video can be included.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Stoneburner G, Goguen AY, Feringa A. Sp 800-30. Risk management guide for information technology systems. 2002.

[2] Steve E. An Introduction to information system risk management.2007.

[3] Rahman MA, Al-Shaer E. A declarative approach for modeling and verification of network access control policies. 12th IM 2011.

[4] Jaquith A. Security metrics: replacing fear. Uncertainty and Doubt. Addison Wesley; 2007.

[5] Noel S, Jajodia S, O'Berry B, Jacobs M. Efficient minimum-cost network hardening via exploit dependency graphs. In proceedings of annual computer security applications conference 2003 (pp. 86-95). IEEE.

[6] Ou X, Govindavajhala S, Appel AW. MulVAL: a logic-based network security analyzer. In USENIX security 2005.
[7] Zaidan BB, Zaidan AA, Al-Frajat AK, Jalab HA. On the differences between hiding information and cryptography techniques: An overview. Journal of Applied Sciences. 2010; 10:1650-5.
[8] Singh A, Gilhotra R. Data security using private key encryption system based on arithmetic coding. International Journal of Network Security & its Applications. 2011; 3(3):58-67.
[9] Kumar MK, Azam SM, Rasool S. Efficient digital encryption algorithm based on matrix scrambling technique. International Journal of Network Security & its Applications. 2010; 2(4): 30-41.
[10] Lakhtaria KI. Protecting computer network with encryption technique: a study. In ubiquitous computing and multimedia applications 2011(pp. 381-90). Springer Berlin Heidelberg.
[11] Raviraj P, Sanavullah MY. The modified 2D-haar wavelet transformation in image compression. Middle-East Journal of Scientific Research. 2007; 2(2):73-8.
[12] Blackedge JM, Ahmed M, Farooq O. Chaiotic image encryption algorithm based on frequency domain scrambling. School of Electrical Engineering Systems Articles, Dublin Institute of Technology. 2010.
[13] Kharate GK, Ghatol AA, Rege PP. Image compression using wavelet packet tree. ICGST-GVIP Journal. 2005; 5(7):37-40.
[14] Walnut DF. An introduction to wavelet analysis. Springer Science & Business Media; 2013.
[15] Ahmad M, Alam MS. A new algorithm of encryption and decryption of images using chaotic mapping. International Journal on Computer Science and Engineering. 2009; 2(1):46-50.
[16] Bao L, Zhou Y, Chen CP, Liu H. A new chaotic system for image encryption. In international conference on system science and engineering, 2012 (pp. 69-73). IEEE.
[17] Abusukhon A, Talib M. A novel network security algorithm based on Private Key Encryption. In 2012 international conference on cyber security, cyber warfare and digital forensic (CyberSec) 2012 (pp. 33-7). IEEE.
[18] Zhang J, Chen Z, Xu M. On the security of ID-based multi-receiver threshold signcryption scheme. In international conference on consumer electronics, communications and networks (CECNet) 2012 (pp. 1944-8). IEEE.
[19] Paul A, Das N, Prusty AK. An advanced gray image encryption scheme by using discrete logarithm with logistic and HEH64 chaotic functions. In IEEE 3rd international advance computing conference (IACC) 2013 (pp. 1114-20). IEEE.
[20] Rahman MA, Al-Shaer E. A formal approach for network security management based on qualitative risk analysis. In international symposium on integrated network management 2013 (pp. 244-51). IEEE.
[21] Ramaiya MK, Hemrajani N, Saxena AK. Improvisation of security aspect in steganography applying DES. In international conference on communication systems and network technologies (CSNT) 2013 (pp. 431-6). IEEE.
[22] Ahirwal R, Jain A, Jain YK. Signcryption scheme that utilizes elliptic curve for both encryption and signature generation. International Journal of Computer Applications. 2013; 62(9): 41-8.
[23] Rivest R. RSA Security response to weaknesses in key scheduling algorithm of RC4. Technical note, RSA Data Security, Inc. 2001.
[24] Ren W, Miao Z. A hybrid encryption algorithm based on DES and RSA in Bluetooth communication. In second international conference on modeling, simulation and visualization methods (WMSVM) 2010 (pp. 221-5). IEEE.
[25] Li X, Chen J, Qin D, Wan W. Research and Realization based on hybrid encryption algorithm of improved AES and ECC. In international conference on audio language and image processing (ICALIP) 2010 (pp. 396-400). IEEE.
[26] Chen Y, Chen H, Chen H, Cheng X. Research on data encryption techniques for distributed interactive simulation network. In Computer Application and System Modeling (ICCASM), 2010 International conference on 2010 (pp. 676-9). IEEE.
[27] Xu E, Shao L, Cao G, Ren Y, Qu T. A new method of information encryption. In ISECS international colloquium on computing, communication, control, and management 2009 (pp. 583-6). IEEE.

Mrs. Rajni Tiwari hails from Damoh and was born on 28th August 1989. I did my schooling from the Saraswati shishu mandir higher secondary school Damoh ,and completed my graduation in stream of computer science and Engineering from Ojaswani institute of management and technology Damoh with 69.20 %. I am a PG Scholar at Technochrats institute of technology Bhopal, and pursuing M.Tech in Computer Technology and Application. My research area is network security.
Email: rajni.rajniti.tiwari@gmail.com