Research Article

International Journal of Advanced Technology and Engineering Exploration, Vol 4(31)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2017.431002

Text data partitioning and image based RC5 encryption with block based key generation

Sonu Kumar[1*], Kailash Patidar[2], Rishi Kushwah[3] and Sudeesh Chouhan[3]
M.Tech Scholar, Department of Computer Science & Engineering, SSSUTMS, Sehore, India[1]
Head and Assistant Professor, Department of Computer Science & Engineering, SSSUTMS, Sehore, India[2]
Assistant Professor, Department of Computer Science & Engineering, SSSUTMS, Sehore, India[3]

Abstract

Data security is very important aspects in different areas of communication. This paper deals with text data encryption as maximum of the data communication is basically depends on text data. In this framework first the text data is loaded in the framework. Then it is partitioned into different blocks. The data is encrypted by RC5 method and keys are generated according to the blocks. Then an addition join key is generated for joining the blocks. Finally the results are compared based on the histogram, key lengths, variations in keys and image conversion. The comparative study shows the effectiveness of our approach.

Keywords

RC5, Text data, Histogram, Key variability.

1.Introduction

Information security has turned into a critical concern today for the fruitful operations of various prerequisite of any association. The data security is the genuine concern and protecting an affiliation's information asset from security dangers [1, 2]. With an eye to scene division techniques are ensign for countermeasures against different security perils of the definitive information. The fluctuated points of view of perils and vulnerabilities make undermining condition for the information executive [3, 4]. It is currently a testing assignment for the ventures as all the correspondence and business depends on the information as it is the center piece of any association [5, 6].

There are a few cryptography strategies, which are helpful in information security, for instance, private or mystery key cryptography, open key cryptography, advanced mark and hash work [7]. Private key cryptography, a private key is utilized. Progressed encryption standard (AES), Blowfish, CAST5, Grasshopper, RC4, RC5 and 3DES are the cases of private key cryptography. This requires wander as a last resort part pass on offering a pantomime of the key and the key be struck by be passed manage without a sheltered channel to the next individual [8]. Private-key cryptography is level indestructible and adequately completed for information security. Along these lines they are more than once for mass estimations encryption. Open key cryptography utilizes an open and private combine for information encryption. RSA, elliptic curve cryptography (ECC) also, Diffie–Hellman key trade. There are other strategies jump at the chance to deliver process hashing the message and can encode the process to create computerized signature [9, 10].

Because of by and large using content as a piece of correspondence strategy, it is fundamental to shield the mystery content data from others that is most certainly not approved for the worry information [11] [12]. To scramble content data one needs to encode the information that is germane to each pixel, since pixels are the basic building bit of picture information [13, 14]. The encoded substance could contain extraordinary properties that pass most by far of the testing criteria so technique for content encryption should be adequately solid. The encoding strategy will change the data into confused structure and decreasing the degree of the data, archive or extend the traverse of the record [15].

[*] Author for correspondence

2.Related work

In 2009, Juan et al. [16] suggested that the Bluetooth is a low-cost short-range wireless communications medium. Thy suggested security is greater concern in these devices. They have applied DES algorithm to enable Bluetooth technology for military purposes.

In 2011, Murthy et al. [17] focused on encrypting the data based on stream cipher method. The data considered was between the mobile stations and base stations. The keys are generated using genetic algorithm. This genetic algorithm technique gives the best or optimal key for encryption. Before we single point cross over technique is used in generating optimal key for encryption but this paper emphasizes on genetic algorithm technique for different sizes of population and different number of iterations considering multi point crossover. The plain text which is to be encrypted along with the key are encoded using the arithmetic coding technique. Encryption is done to convert the plain text into cipher text.

In 2012, Kester et al. [18] contributed in the area of cryptography application. They have developed a cipher algorithm to produce the ciphered image and also to decrypt ciphered image. The calculation at last makes it feasible for encryption and unscrambling of the pictures in light of the RGB pixel the calculation was actualized utilizing MATLAB.

In 2012, Jing et al. [19] suggested that the text encryption method is capable in information security. On the premise of dissecting the parallels between content watermarking and content encryption, a content encryption calculation in view of common dialect handling is proposed. Three semantic changes in normal dialect preparing are presented. At long last, the necessities and the procedure of the content encryption calculation are given.

In [20-22] authors have suggested different encryption techniques with different file formats have been applied in server and client communication security and provided a practical overview and their implications. The results suggest that their techniques are capable in securing server data.

In 2013, Saraireh et al. [23] proposed a secure system for communication. Their algorithm combined cryptographic algorithm together with steganography. It helps in providing robust and strong communication system to protect from the attackers. Thy have used filter bank cipher to encrypt the secret text message. Then a discrete wavelet transforms (DWT) based steganography is adopted to hide the encrypted message in the cover image by modifying the wavelet coefficients. Their result suggests that it provides high level security.

In 2016, Park et al. [24] deals with two security problems between the cloud computing service and trusted platform module (TPM). They suggested the first problem is the social issues from inside attackers. For this they suggested encrypted DB retrieval system. They suggested the second problem is that cloud computing has limitless computing resources. To conquer the shortcoming and create synergic impacts between the two advancements, we join two applications (cloud datacenter benefit, TPM chip) as a portable concurrent innovation. The principle strategies are TPM-security-customer and veiled keys. With these techniques, the genuine keys are put away in TPM and the faked keys (covered keys) are actualized for calculations rather than genuine keys. Accordingly, the consequence of the faked keys is the same as the genuine keys. So their framework is secure against both of the insiders and pariahs, the distributed computing administration can enhance security shortcomings.

3.Proposed work

The proposed framework allows the client to register in this framework and authenticated by the admin. After authentication clients can received the data from the admin. The whole process is divides in the following manner:

1.File partitioning

This is the first phase. In this phase the available data is divided into different block as per the block division algorithm. The maximum 8 blocks are permitted.

2.RC5 encryption

Then RC5 encryption and decryption algorithm have been applied for data encryption and decryption purpose. It provides the key sizes between 0 to 2040 bits and block sizes of 32, 64 and 128 bits.

3.Key productions

Our method provided block based encryption and decryption which is applied on the number of blocks. The numbers of keys generated are the same as the number of blocks.

4.Image conversion

In this phase the blocks are then converted into images to show it in the encrypted form. To join it to the final version the join key is also generated.

5.Image received by the receiver

The data is send to the client along with the keys. The receivers first apply the decryption key and then apply the join key to join it to form the complete data.

It is pictorial represented by the flowchart as shown in *Figure 1*.

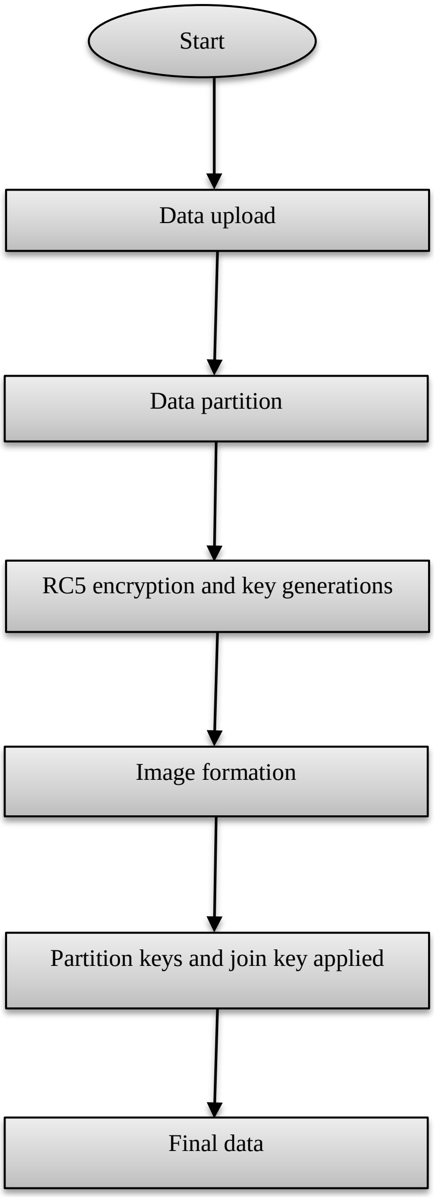

Start
Data upload
Data partition
RC5 encryption and key generations
Image formation
Partition keys and join key applied
Final data

Figure 1 Working flowchart

RC5 algorithm [25]

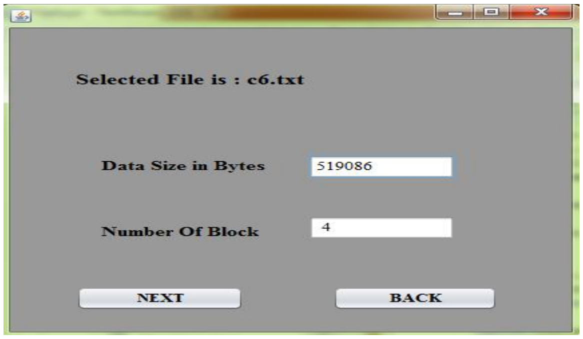
The following terminology has been used in this algorithm:

w – Word length (Example: 16, 32 or 64)
u = w/8 word length (bytes)
b – Key length (bytes)
K[] – Key array
c – Key length (words) (1, if b = 0)
L[] – Temp array
R – Number of rounds
t = 2(r+1) (number of required round)
S[] – Sub key array
Pw – First constant
Qw – Second constant
A, B – Word block

```
Step 1: K is divided into words.
u = w / 8
c = ceiling( max(b, 1) / u )
Step 2: L is a temporary array initially with a c-length list.
i = b-1 to 0
L[i/u] = (L[i/u] << 8) + K[i]
Step 3: S array is initialized. Initially it is 2(r+1) length list
S[0] = Pw
i = 1 to t-1 do:
S[i] = S[i-1] + Qw
Step 3: Key scheduling follows the below loop
i = j = 0
A = B = 0
do 3 * max(t, c) times:
A = S[i] = (S[i] + A + B) <<< 3
B = L[j] = (L[j] + A + B) <<< (A + B)
i = (i + 1) % t
j = (j + 1) % c
Step 4: Encryption
A = A + S[0]
B = B + S[1]
for i = 1 to r do:
A = ((A ^ B) <<< B) + S[2 * i]
B = ((B ^ A) <<< A) + S[2 * i + 1]
Step 5: Decryption
for i = r to 1 do:
B = ((B - S[2 * i + 1]) >>> A) ^ A
A = ((A - S[2 * i]) >>> B) ^ B
B = B - S[1]
A = A - S[0]
```

4.Result analysis

To validate the results the produced results have been compared with the previous method [26]. The strength of this approach is providing different keys according to blocks and an additional key for joining it. The partitioning, number of blocks and encryption as shown in *Figure 2*, *Figure 3* and *Figure 4*. The number of blocks is converted to images as shown in *Figure 5*. The other results for the key length comparison block and histogram comparisons are shown in *Figure6*, *Figure 7* and *Figure 8*.

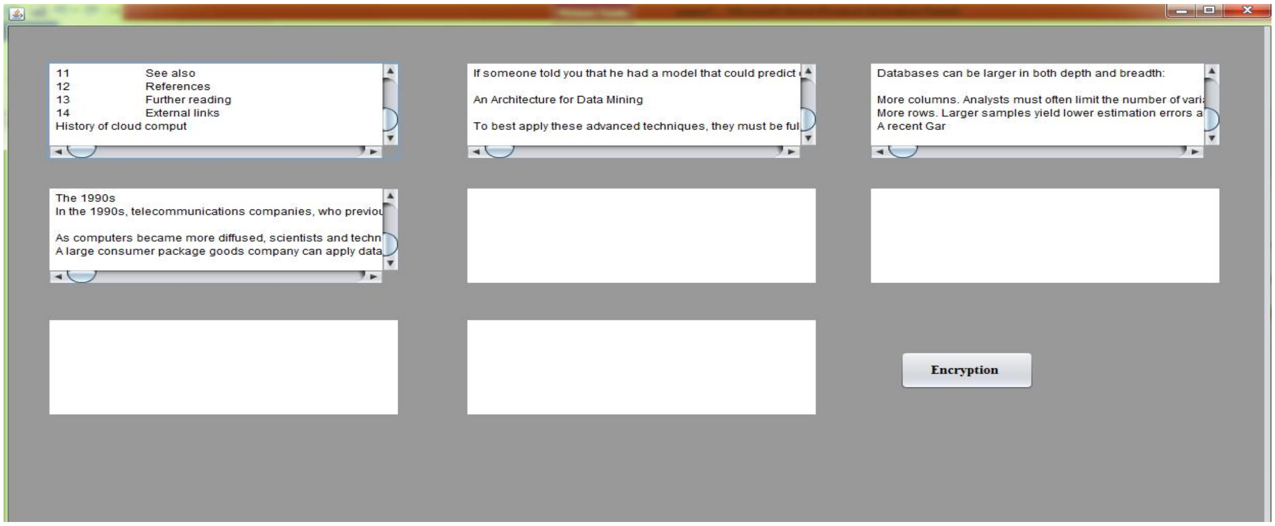


Selected File is : c6.txt

Data Size in Bytes: 519086

Number Of Block: 4

Figure 2 File sizes and number of blocks



```
11              See also
12              References
13              Further reading
14              External links
History of cloud comput
```

```
If someone told you that he had a model that could predict

An Architecture for Data Mining

To best apply these advanced techniques, they must be ful
```

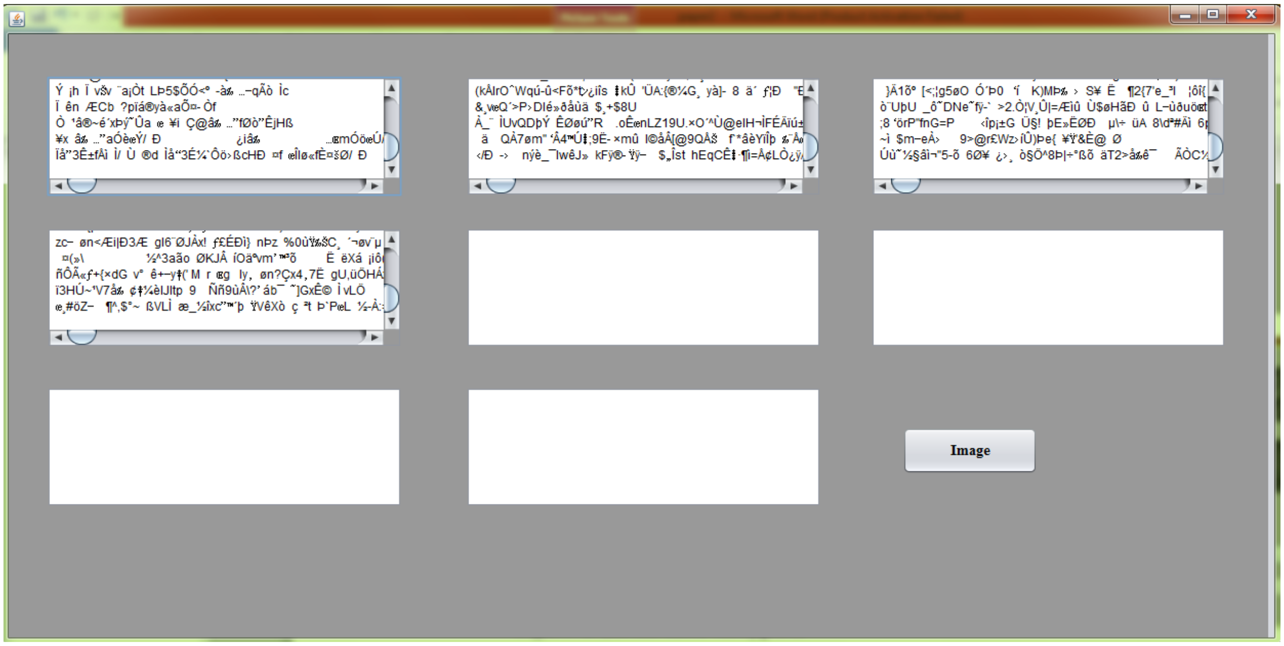
```
Databases can be larger in both depth and breadth:

More columns. Analysts must often limit the number of vari
More rows. Larger samples yield lower estimation errors a
A recent Gar
```

```
The 1990s
In the 1990s, telecommunications companies, who previou

As computers became more diffused, scientists and techn
A large consumer package goods company can apply data
```

Figure 3 Number of blocks with data



```
Ý ¡h Ï vŠv ¯ajÒt LÞ5$ÕÓ<º -â‰ …–qÃò Ìc
Ï ên ÆCb ?pïá®yà«aÕ¤- Òf
Ò ¹â®~é´xÞÿ˜Ûa œ ¥i Ç@â‰ …"fØò"ÊjHß
¥x â‰ …"aÓèœÝ/ Ð              ¿iâ‰              …œmÓöœÚ/
Ïå"3Ê±fÂì Ì/ Ù ®d Ìå"3É¼`Ôö›ßcHÐ ¤f œÎlø«fÈ¤šØ/ Ð
```

```
(kÅlrO^Wqú-û<Fõ*ƀ¿iîs ǂkÛ 'ÜA:{®¼G¸ yà]- 8 ä´ ƒ¦Ð  "E
&¸wœQ´>P›Dlé»ðåùä $¸+$8U
À_¨ ÌUvQDþÝ ÊØøú"R   .oÊœnLZ19U.×O´^Ù@eIH¬ÌFÉÄïú±
 ä   QÀ7øm" 'Â4™Ú‡;9Ë-×mû l©åÂ[@9QÅš  f*âèYïÎþ ‰¯Å
‹/Ð ->   nýè_¯lwêJ» kFÿ®-Ÿÿ–   $„Îst hEqCÊ‡·¶ï=Â¢LÒ¿ÿ
```

```
}Ä1õº [<;¦g5øO Ó´Þ0  ˜í   K)MÞ‰ › S¥ Ë   ¶2{7'e_ª|  ¦ôî{
ò¯UþU _ô˜DNe˜fÿ-` >2.Ò¦V¸Û|=Æïû ÙSøHãÐ û L–ùðuöœ
;8 'örP"fnG=P      ‹îp¡±G Ü§! þE»ËØÐ   µ\÷ üA 8\dª#Äì 6
~ì $m–eÂ›     9>@r£Wz›íÛ)Þe{ ¥Ÿ&È@ Ø
Úù˜½§âì¬"5-õ 6Ø¥ ¿›¸ ò§Ö^8Þ|÷ºßõ äT2>å‰ê¯    ÃÓC½
```

```
zc– øn<Æi|Ð3Æ gI6¯ØJÀx! ƒ£ÉÐì} nÞz %0ùŸ‰ŠC¸ ´¬øv¨µ
 ¤(»\              ½^3aão ØKJÂ íOäºvm'™³õ        Ë ëXá ¡iô
ñÔÃ«ƒ+{×dG v°  ê+–y‡('M r œg  ly,  øn?Çx4,7Ë gU,üÖHÁ
ï3HÚ~'V7å‰ ¢‡¼èIJltp 9   Ññ9ùÂ\?'áb¯ ˜]GxÊ© Ì vLÖ
œ¸#öZ–  ¶^,$°~ ßVLÌ æ_½îxc"™´þ ŸVêXò ç ªt Þ`PœL ½-À:
```

Figure 4 Number of blocks with data in encrypted form

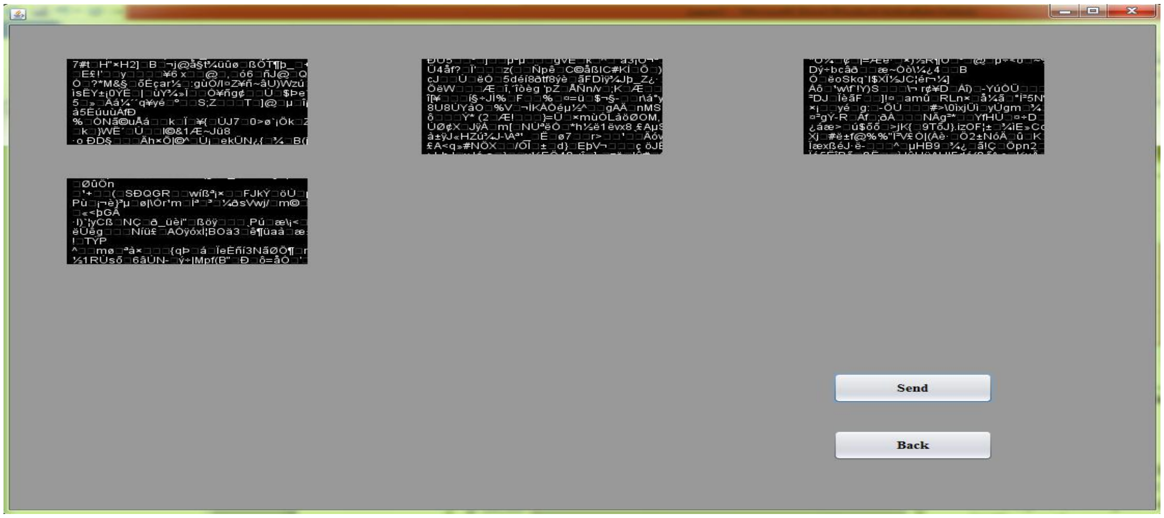


Figure 5 Number of blocks with image form

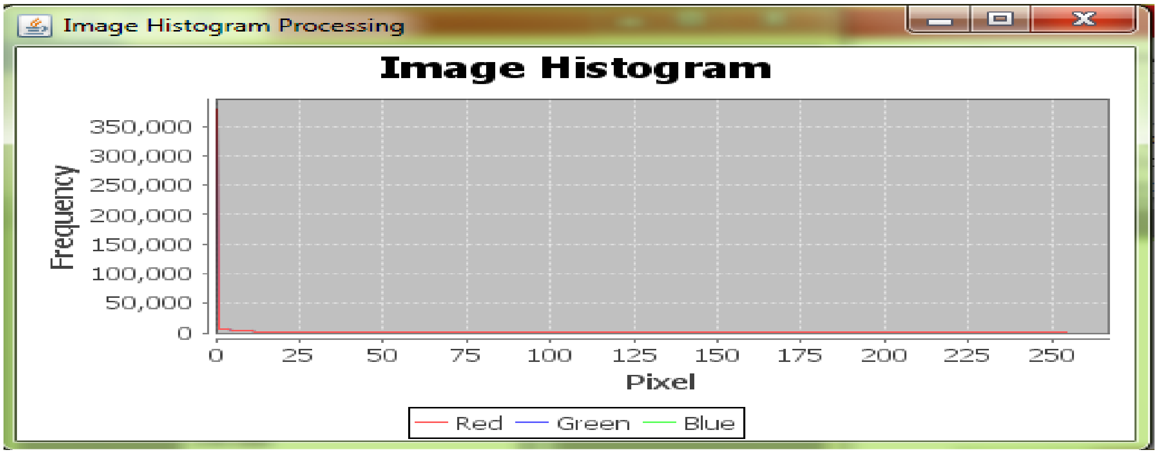


Figure 6 Image histogram

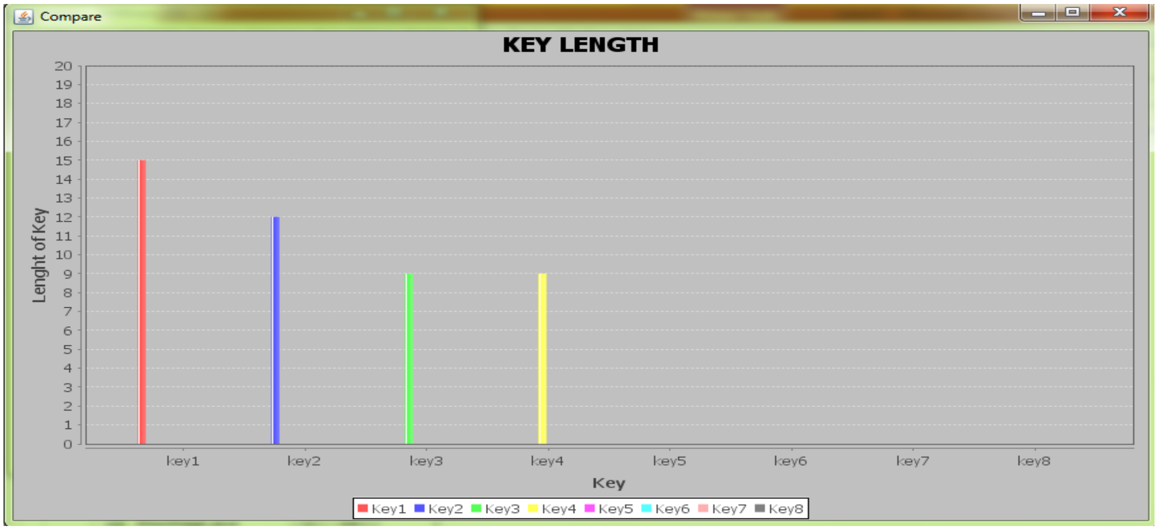


Figure 7 Variations in key length

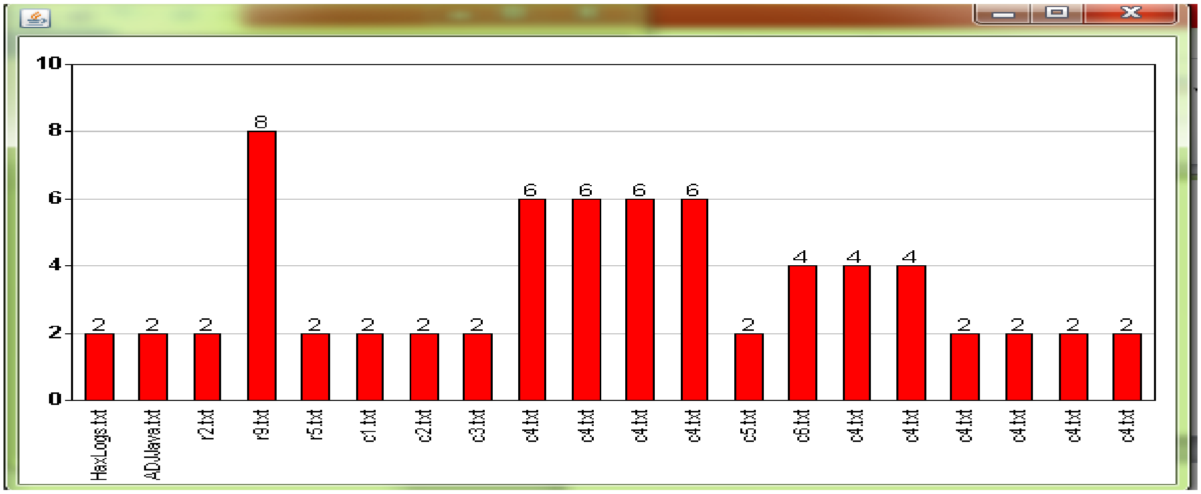


Figure 8 All files variations

5.Conclusions

In this approach a multiple key approach with textual data have been proposed with block division along with block key join approach. It provides the data security in three ways first it partition the data and convert the data in the encrypted form block wise then all the blocks are converted into different images and finally all the blocks needed different security keys. After applying the security keys we needed a join key also to combine the data. So the complete security in our approach is improved. The effectiveness is also shown by the image histogram and all files variations.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Kumar B, Boaddh J, Mahawar L. A hybrid security approach based on AES and RSA for cloud data. International Journal of Advanced Technology and Engineering Exploration. 2016; 3(17):43.

[2] Kumar B, Boaddh J. A meta-analysis on secure cloud computing. International Journal of Advanced Technology and Engineering Exploration. 2016; 3(15):15.

[3] Lee HM, Lee TY. Analysis of algorithm of cipher text containing data and key in network security. In international conference on innovative computing, information and control 2007 (pp. 439-439). IEEE.

[4] Jaquith A. Security metrics: replacing fear, uncertainty, and doubt. Upper Saddle River: 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 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 symposium 2005 (pp. 8-8).

[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 and 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 international conference on 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] Juan L, Bin C, Kun L. Study on the improvement of encryption algorithm of Bluetooth. In international conference on networking and digital society 2009 (pp. 89-92). IEEE.

[17] Murthy YS, Satapathy DS, Srinivasu P, Saranya AA. Key generation for text encryption in cellular networks using multi-point crossover function. International Journal of Computer Applications 2011.

[18] Kester QA, Koumadi KM. Cryptographie technique for image encryption based on the RGB pixel displacement. In international conference on adaptive science & technology 2012 (pp. 74-7). IEEE.

[19] Jing X, Hao Y, Fei H, Li Z. Text encryption algorithm based on natural language processing. In international conference on multimedia information networking and security 2012 (pp. 670-72). IEEE.

[20] Qadri SI, Pandey K. Tag based client side detection of content sniffing attacks with file encryption and file splitter technique. International Journal of Advanced Computer Research. 2012; 2(5):227-33.

[21] Dubey A, Gupta R, Chandel GS. An efficient partition technique to reduce the attack detection time with web based text and PDF files. International Journal of Advanced Computer Research. 2013; 3(9):80-6.

[22] Gupta S. Secure and automated communication in client and server environment. International Journal of Advanced Computer Research. 2013; 3(4):263-71.

[23] Saraireh S. A Secure Data Communication system using cryptography and steganography. International Journal of Computer Networks & Communications. 2013; 5(3):125-37.

[24] Park HA. Secure chip based encrypted search protocol in mobile office environments. International Journal of Advanced Computer Research. 2016; 6(24):72-80.

[25] Rivest RL. The RC5 encryption algorithm. In international workshop on fast software encryption 1994 (pp. 86-96). Springer, Berlin, Heidelberg.

[26] Abusukhon A, Talib M. A novel network security algorithm based on private key encryption. In international conference on cyber security, cyber warfare and digital forensic 2012 (pp. 33-7). IEEE.