ISSN 2277–5528
Impact Factor- 4.015

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

SPACE AND SECURITY EFFICIENT DYNAMIC KEY GENERATED HYBRID BLOCK CIPHERING METHOD FOR ENCRYPTION

Kirti Singh Chouhan* and Jai Mungi
Department of Computer Science & Engineering, SIRTE, Bhopal, (M.P.) – India
kirti.chouhan739@gmail.com, jaimsirt@gmail.com

Abstract

We proposed our new encryption algorithm with reduce space complexity and increase security. There are two most important parameter or characteristics space and security. This proposed work is all about the new encryption and decryption process. Encryption process is based on two concepts: First dynamic key generation and second one is block encryption. Key generation and block encryption will be done in .NET and we will measure the effectiveness of the proposed work on the parameters like: memory complexity and security. Memory complexity is measured in KB and security of work will be measure through Avalanche Effect. This work will be very effective. In this proposed work data security will be increase and space capacity should be reduce. It is the establishment of all data security focuses. The systems used to this end have wound up being powerfully numerical of nature. Set up cryptosystems is immediate, effortlessly acknowledged and simple to be broken. We proposed a new cryptographic algorithm based on symmetric key block cipher that provides better security and reduce space complexity.

Keyword: Encryption, Cryptography, Security, Avalanche Effect, Memory Complexity, Dynamic Key

Introduction

Cryptography has many commercial applications. The main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication. Presently continuous researches on the new cryptographic algorithms are going on. We have already known that they must consider many factors like: security, the features of algorithm, the time complexity and the space complexity**.** We present the fundamental issues by talking about the issue of encryption with the fast improvements and the data interchanges, a lot of concerns have been brought up in the security of information transmitted or put away over open channels. Particularly at the levels of the text and picture information. As indicated by [1] there are three fundamental routines for secured correspondence accessible in particular, cryptography, steganography and watermarking. Among these three, the first one, cryptography [2]-[3], manages the improvement of procedures for changing over data in the middle of understandable and incomprehensible structures amid data trade. Steganography [4]-[5], then again, is a procedure for concealing and separating data to be passed on utilizing a transporter signal [1]. The third one, watermarking [6]-[7], is a method for creating legitimate strategies for concealing restrictive data in the perceptual information.

This obliges meander if all else fails part convey offering an impersonation of the key and the key be struck by be passed swear off a safe channel to the next individual. Private-key calculations are level indestructible and effectively actualized in equipment. Along these lines they are over and again second-hand for mass measurements encryption. The vast please of the all-around adjusted encryption rely on upon plaintext, encryption calculation, key and unscrambling calculation. The plaintext is the size ahead requiring the encryption calculation. It is joining of the inputs to the encryption calculation. The encryption calculation is the calculation used to continue on b deal with the information stranger plaintext to figure relieve. The mystery key is a comparable to repel of the encryption calculation and of the plaintext and it is associate of the encryption's inputs calculation.

Related Work

Security and space both are very important issues because of theft and congestion on network . In [3] author shows that how much space is needed by symmetric key encryption algorithm and gave their idea to reduce the size of encryption data.Author says that we can perform only XOR operation so it is not more efficient and more secure. In [7] authors have proposed and encryption algorithm using wavelets transform technique for image encryption .Archana V.S Nair has proposed an encryption algorithm using arithmetic coding but author say that using arithmetic coding there is problem in decryption it is not easy to find accurate character when digits are rounded . If we have use arithmetic coding to reduce the size of cipher text but it makes algorithm to slow and there is needed to use extre memory space and the performance would be very slow. Existing algorithm such as AES, DES, TDES, and Blowfish need some extra space for encrypted data. In 2013, Praloy Shankar De et al. [9] try has been made to focus on a count of cryptography that was made by using old rationalities. DEDD Symmetric-key cryptosystem is the better approach to manage symmetric key estimation. By this strategy they can doubly scramble and doubly translate the message. It infers the sender will create the figure content from the plain substance twice. The recipient will in like manner need to disentangle the figures for two times and a short time later the correspondence between them will be done. For making the key, they will take the message length in first encryption and in second encryption they will apply moving framework. In 2015, Li et al. [15] coordinated the idea of session key foundation and broadened confused maps for the satisfaction to permit information senders and information recipients to build up a protected normal session key through a trusted server over a frail channel. They proposed a protected three-party confirmed key trade convention (3PAKE) which depends on amplified turbulent maps away administration without utilizing savvy card and timestamp. It requires neither long haul mystery keys nor symmetric cryptosystems. It satisfy the assurance necessity against different assaults. Their proposed convention is more secure and commonsense for genuine situations.

Methodology

PROPOSED METHODOLOGY

There are two aspect of proposed encryption work. These are as follows:

1. Dynamic Key Selection
2. Proposed Encryption

Dynamic key

Dynamic keys is a one time forming a sequence of keys in symmetric cryptographic keys. Similar in nature to one time pad, every message in the system is encrypted by different cryptographic key. Dynamic key stratagies is more secure as compare to static key.

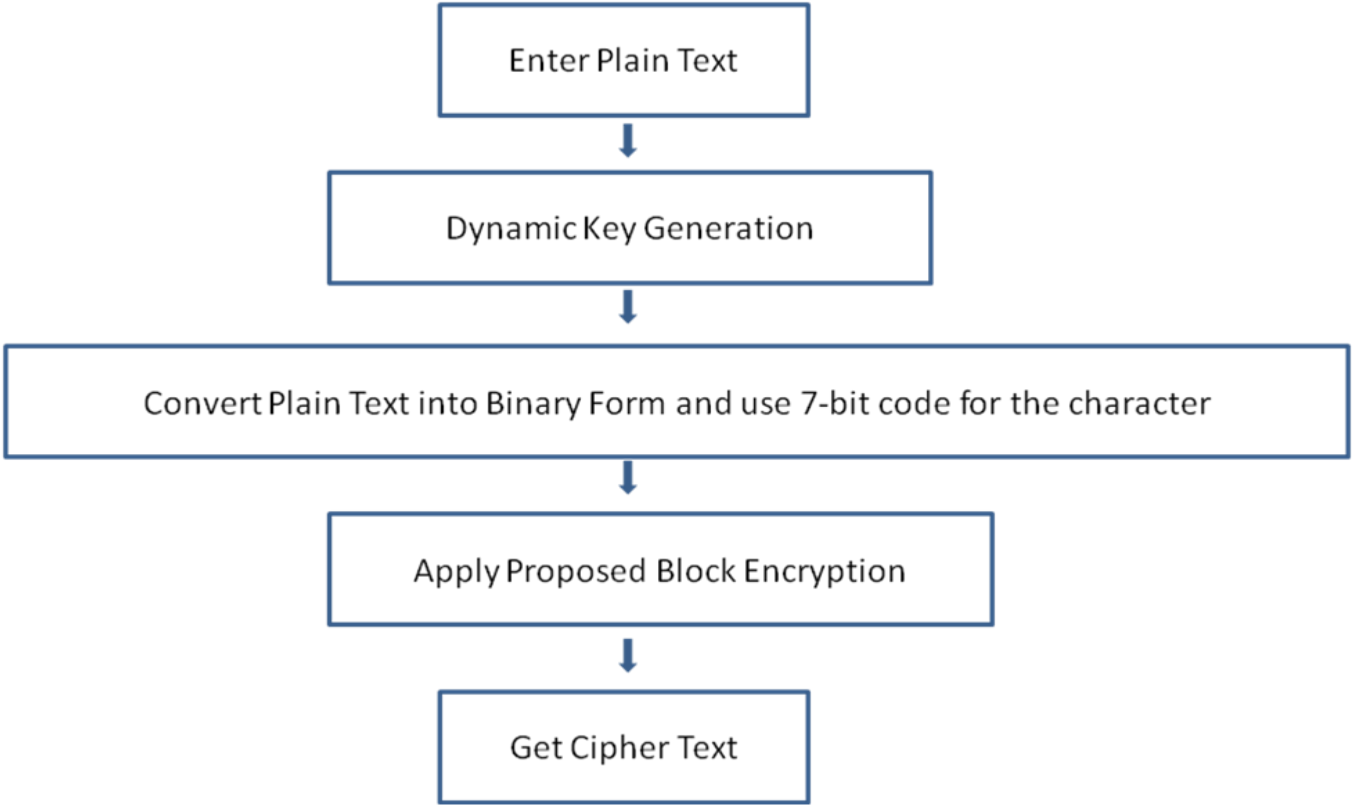
Enter Plain Text
Dynamic Key Generation
Convert Plain Text into Binary Form and use 7-bit code for the character
Apply Proposed Block Encryption
Get Cipher Text

Fig. 1: Proposed Architecture

Proposed Encryption

Encryption is a process which is converted plaintext data into ciphertext .it is a process of encoding a message so that its meaning is not obvious.

Plaintext to ciphertext: encryption

$$C=E(P)$$

Cryptography

Cryptography addresses the above issues. It is the establishment of all data security focuses. The systems used to this end have wound up being powerfully numerical of nature. Set up cryptosystems is immediate, effortlessly acknowledged and simple to be broken. New sorts of cryptography came after the far reaching progress of PC correspondences. In information and impart correspondences, cryptography is key when giving over any depended medium. In the most recent couple of decades, notwithstanding, the illustration has been on setting cryptography onto a sound numerical structure. This cutting edge center has started the change of the field from a workmanship into a science, which solidifies fundamentally any structure, especially the web. This change runs with present day cryptography (MC) really starts with Claude Shannon clearly the father of coherent cryptography. He flowed a related paper, "Correspondence Theory of Secrecy Systems", in 1949. These, notwithstanding his differing handles data and correspondence hypothesis built up a strong theoretical clarification behind cryptography and for cryptanalysis. Moreover, with that, cryptography for all intents and purposes vanished into puzzle government correspondences relationship, for example, the NSA and accomplices somewhere else. Today's cryptographic systems have changed into the instigate react in due request in regards to secure data against untouchables. These structures required that information and data ought to be blended with some kind of coherent number where just the social events that shares the data could conceivable interpret to utilize the data.

Encryption/Decryption Algorithm Architecture

Pseudo Code:

```
1. Calculate Random Number by adding all the 1's of a binary Key
```

Code Example:

```
Set RN = 0;
for (int i = 0; i < Key.Length; i++)
        {
          RN += Key[i];
        }
return RN;
```

```
2. Now, Convert the key into 7 bit binary format
```

Code Example:

```
        Key = con_binary_7(Key);
```

```
3. Next generate 3 Different keys equal to 126 bit by using following Steps:
   Step1:
       a. If RN is Even
               i.   Key1 = Xor All bits of key RN position + 2 bit respectively
               ii.  Key2 = Xor Key1 with input Key
               iii. Key3 = Circular Left Rotate by 2 bits
       b. If RN is Odd
               i.   Key1 = Xor All bits of key RN position + 1 bit respectively
               ii.  Key2 = Circular Left Rotate by 2 bits
               iii. Key3 = Xor Key2 with input Key
   Step2:
       If Division of RN by 4 gives remainder 1 than
               i.      Key1 = Key2
               ii.     Key2 = Key3
               iii.    Key3 = Key1
       If Division of RN by 4 gives remainder 1 than
               i.      Key1 = Key3
               ii.     Key3 = Key2
               iii.    Key2 = Key1
       If Division of RN by 4 gives remainder 1 than
               i.      Key1 = Key1
               ii.     Key2 = Key3
               iii.    Key3 = Key2
```

Code Example:

```
if (RN % 2 == 0)
        {
          K1 = R_Ran_xorbits(Key, RN + 2 % 126);
          K2 = xor(K1, Key);
          K3 = leftrotate(K2, 2);
        }
else
        {
          K1 = R_Ran_xorbits(Key, RN + 1 % 126);
          K2 = leftrotate(K1, 2);
          K3 = xor(K2, Key);
        }
int S = RN % 4;
if (S == 1)
        {
          temp = K1;
          K1 = K2;
          K2 = K3;
          K3 = temp;
```

```
         }
elseif (S == 2)
         {
           temp = K1;
           K1 = K3;
           K3 = K2;
           K2 = temp; ;
         }
elseif (S == 3)
         {
           temp = K2;
           K2 = K3;
           K3 = temp;
         }
```

4. Now, divide the plain text equal to chunks of 126 bit, if the last chunk has less bits than convert the key of chunk length by just elemineting the last bits (Key transformation will be done only when last chunk under process),
5. Next, repeat the following operations for each chunk:
    a. Set PT = XOR PlaintText$_i$ with Key1
    b. PT = Circular Left Rotation of PT by RN bits
    c. PT = XOR PlaintText$_i$ with Key2
    d. PT = Circular Left Rotation of PT by RN % 4 bits
    e. Divide PT in two parts and swap them
    f. PT = XOR all bits by RN bit position
    g. PT = XOR PlaintText$_i$ with Key3
    h. PT = XOR all bits by RN % 4 bit position

   Result is ciphertext of input chunk

   Code Example:

```
PT = xor(PT, K1);
           PT = leftrotate(PT, RN%PT.Length);
           PT = xor(PT, K2);
           PT = leftrotate(PT, RN % 4);
           temp = PT.Substring(0, PT.Length / 2);
           PT = PT.Substring(PT.Length / 2) + temp;
           PT = R_Ran_xorbits(PT, RN % PT.Length);
           PT = xor(PT, K3);
           PT = R_Ran_xorbits(PT, RN%4);
           CipherText += PT;
```

6. Convert the resultant cipher text in to 8 bit character format

Flow Diagram

Dynamic Key Selection

Calculate Random Number by adding all the 1's of a binary Key

Pseudo Code :

```
Start Procedure keyGeneration
         Set RN = 0;
         for (int i = 0; i < Key.Length; i++)
         {
           RN += Key[i];
         }
         return RN;
End Procedure
```

ISSN 2277–5528
Impact Factor- 4.015

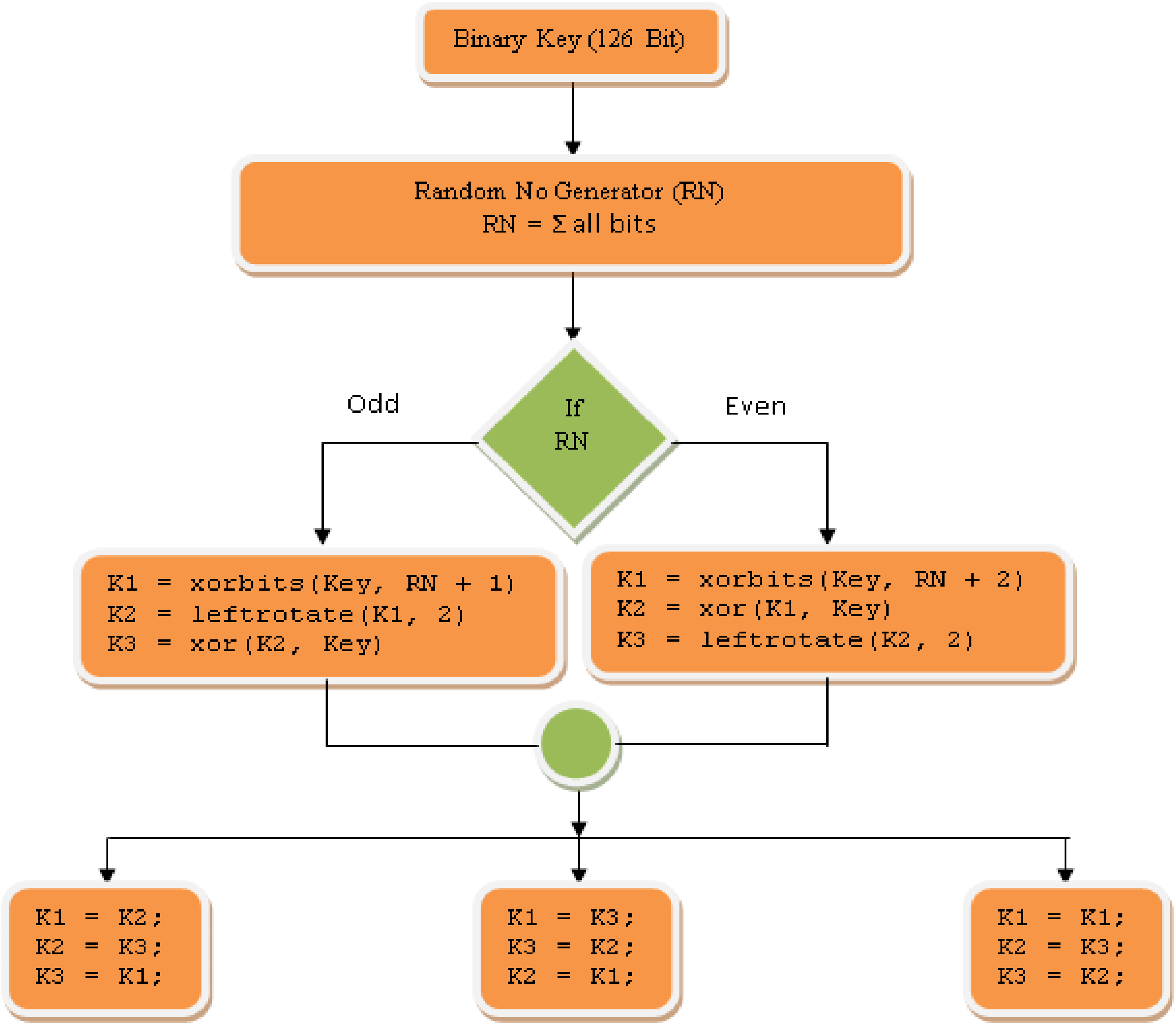

Fig. 2: Dynamic Key Selection

Flow Chart: Proposed Block Encryption

- Conversion of Plain text to Binary text:

  All_Text = con_binary_7(All _Text);

Pseudo Code:

```
Start Procedure encryption Algorithm
Step 1:     PT = xor(PT, K1);
Step 2:     PT = leftrotate(PT, RN%PT.Length);
Step 3:     PT = xor(PT, K2);
Step 4:     PT = leftrotate(PT, RN % 4);
Step 5:     temp = PT.Substring(0, PT.Length / 2);
Step 6:     PT = PT.Substring(PT.Length / 2) + temp;
Step 7:     PT = R_Ran_xorbits(PT, RN % PT.Length)
Step 8:     PT = xor(PT, K3);
Step 9:     PT = R_Ran_xorbits(PT, RN%4);
Step 10:    CipherText += PT;
End Procedure
```

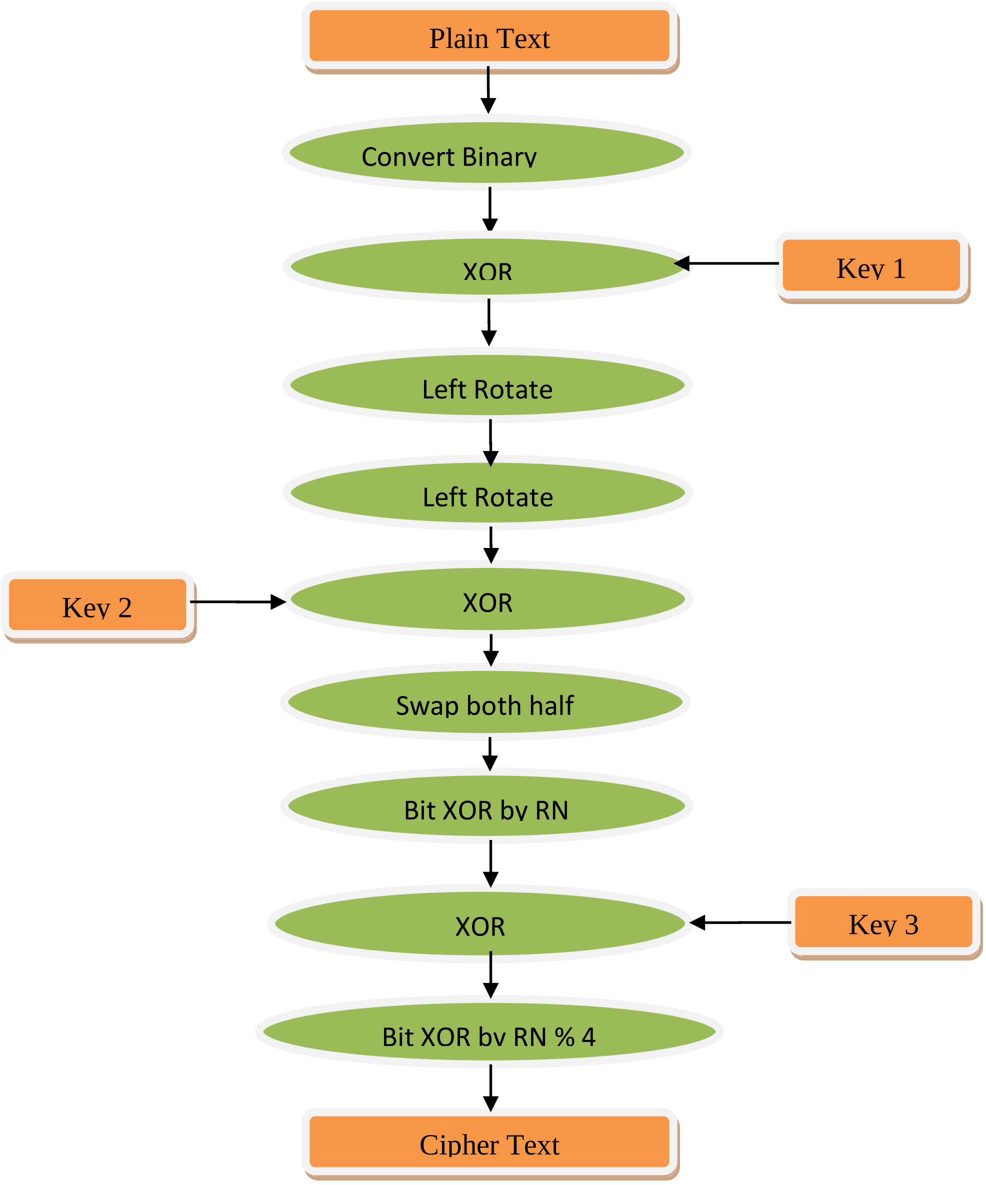

Fig. 3: Proposed Block Encryption

Results and Discussion

Avalanche Effect

- It is quantity which shows the effectiveness of the work in terms of security. The avalanche effect is satisfied if:
- The output changes significantly (e.g., half the output bits flip) as a result of a slight change in input (e.g., flipping a single bit)
- In "quality" block ciphers, such a small change in either the key or the plaintext should cause a strong change in the cipher text.
- Both of above features allow small changes to propagate rapidly through iterations of the algorithm, in such a way that every bit of the output should depend on every bit of the input before the algorithm terminates.
- Avalanche Effect is ratio of Number of change bit in cipher text to Number of bit in cipher text

Result Parameters To Enhance Security Through Avalanche Effect

Algorithm		
Avalanche Effect		
Sample	Base Paper	Proposed Algorithm

Sample-1	26.38	49.34
Sample-2	40.01	49.51
Sample-3	36.12	50.12

Table 1: Result Analysis Table

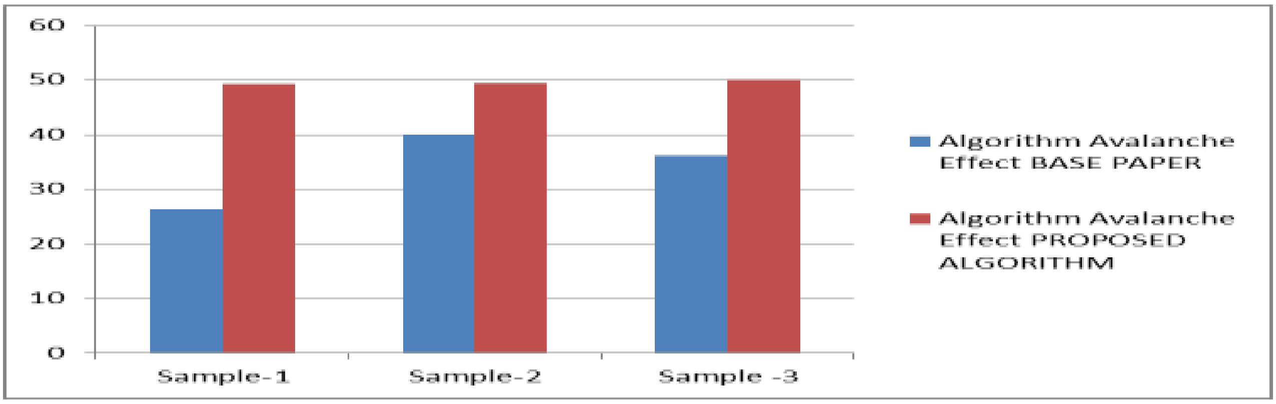

Fig. 4: Comparisons between Previous Algorithm and Proposed Algorithm Through Avalanche Effect

Memory Complexity

It is quantity which shows the effectiveness of the work in terms of memory required after execution of proposed encryption work. Its unit is Bytes. Which means it will calculate the Cipher text which comes after encryption of Plain Text in bytes.

Result Parameters to Reduce Size

Algorithm		
Memory Requirement		
Sample	Base Paper	Proposed Paper
Sample-1	5 KB	4.4 KB
Sample-2	10 KB	8.8 KB
Sample-3	20 KB	17.5 KB

Table 2: Result Analysis Table

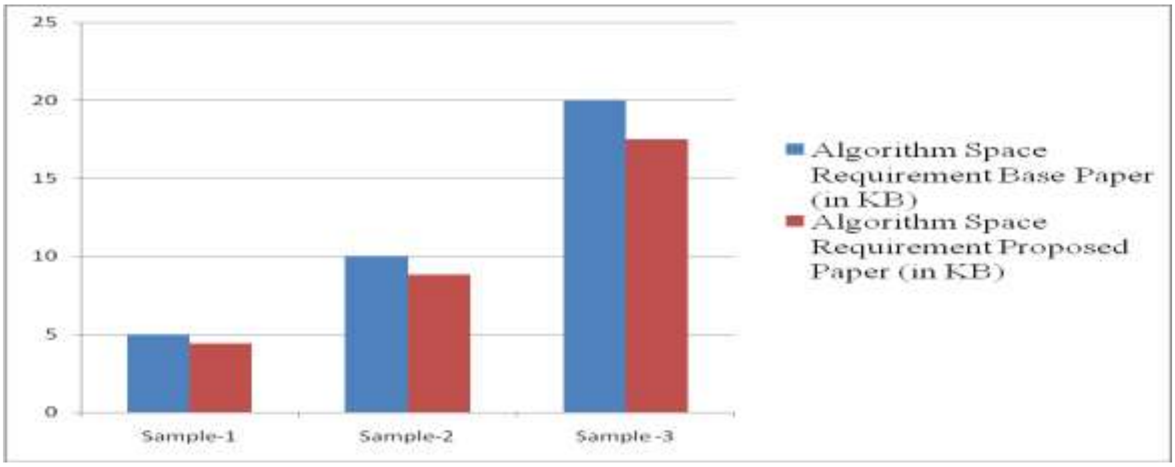

Fig. 5: Comparison between Previous Algorithm and Proposed Algorithm Reduce in Size

Conclusion

Cryptography is assuming a noteworthy part in information security in applications running in a system domain. It enables individuals to work together electronically without stresses of double dealing and trickiness notwithstanding guaranteeing the respectability of the message and genuineness of the sender. It has turned out to be more basic to our everyday life since a huge number of individuals cooperate electronically consistently; through email, online business, ATM machines, phones, and so on. This geometric increment of data transmitted electronically has made expanded dependence on cryptography and validation by clients. The whole proposed work is meant for achieving the data encryption by which we can get better efficiency to the proposed work. There are two aspects of the proposed work. In this First section of the proposed work we have used Dynamic key generation concept to secure the key and at the second part of the work we have used the new proposed encryption technique. The result section clearly shows that the proposed work is far better than existing work on two parameters:

1. Achieved Higher Security Through Avalanche Effect
2. Achieved Less Memory Requirement

Future Works

There are various enhancement which could be possible and part of my future work:

1. A Parallel algorithm can be designed which is equally secure and space efficient but more time efficient also. If any one succeed in doing this obviously, its algorithm is better than the existing algorithms.
2. Proposed Encryption work for Image and Video too.

References

1. A. Mitra, Y V. SubbaRao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science,vol. 1, no. 1, p.127, 2006.
2. A. J. Elbirt and C. Paar, "An Instruction-Level Distributed Processor for Symmetric-Key Cryptography," IEEE Trans. Parallel and distributed systems, vol. 16, no. 5, pp. 468-480, May 2005.
3. W. Stallings, Cryptography and Network Security. Englewood Cliffs,NJ: Prentice Hall, 2003.
4. E. Besdok, "Hiding information in multispectral spatial images," Int. J.Electron. Commun. (AEU) 59, pp. 15-24, 2005.
5. S. Trivedi and R. Chandramouli, "Secret Key Estimation in Sequential Steganography," IEEE Trans. Signal Processing, vol. 53, no. 2, pp. 746-757, Feb. 2005.
6. Y. Wu, "On the Security of an SVD-Based Ownership Watermarking,"IEEE Trans. Multimedia, vol. 7, no. 4, pp. 624-627, Aug. 2005.
7. Y. T. Wu and F. Y. Shih, "An adjusted-purpose digital watermarking technique," Pattern Recognition 37, pp. 2349-2359, 2004.
8. Ajit Singh and Rimple Gilhotra, "Data Security Using Private Key Encryption System Based On Arithmetic Coding", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.
9. Shivangi Goyal, "A Survey on the Applications of Cryptography", International Journal of Science and Technology Volume 1 No. 3, March, 2012.
10. Alexandra Boldyreva, Nathan Chenette, Younho Lee and Adam O'Neill, "Order-Preserving Symmetric Encryption", 2007.
11. Keiko Hashizume and Eduardo B. Fernandez, "Symmetric Encryption and XML Encryption Patterns", 2008.
12. Neha Garg & Partibha Yadav "Comparison of Asymmetric Algorithms in Cryptography", Neha Garg et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 1190-1196.
13. Ritu Tripathi & Sanjay Agrawal, "Comparative Study of Symmetric and Asymmetric
14. Cryptography Techniques" International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853.
15. Md Asif Mushtaque and Harsh Dhiman," Implementation of New Encryption Algorithm with Random Key Selection and Minimum Space Complexity," International Conference on Advances in Computer Engineering and Application, IEEE, 2015.s
16. Prof. Mukund R. Joshi, Renuka Avinash Karkade," Network Security with Cryptography," IJCSMC, Vol. 4, Issue. 1, January 2015.
17. Madhumita Panda," Security in Wireless Sensor Networks using Cryptographic Techniques," American Journal of Engineering Research (AJER), 2014.
18. M.Madhurya, B.Ananda Krishna, T.Subhashini," Implementation of Enhanced Security Algorithms in Mobile Ad hoc Networks," I.J.Computer Network and Information Security, 2014, 2, 30-37.
19. Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013.
20. Aniel Castro And Alan Mcquinn, "Unlocking Encryption: Information Security and the Rule of Law," Information Technology & Innovation Foundation, March 2016.