International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 7, Issue 12, December 2018)

An Improved Encryption Algorithm to Secure SMS Data

Nikhil[1], Nitin Choudhary[2]
[1]M.Tech Scholar, [2]Assistant Professor, Computer Science & Engineering, Kopal Institute of Science & Technology

Abstract: **Utilization of effective data transfer capacities plays an imperative job on SMS messages in versatile correspondences. At the same time securing SMS information is likewise a critical one. In the present digital world huge volumes of information is transferring between end users as SMS (Short Message Service) through mobile devices. Each SMS data mostly is comprised of simple text characters which are sent in the form of plain text. Mobile devices also place a limit on each SMS up to 160 characters. SMS data sent by subscriber A is stored at service center of service provider before it is delivered to the subscriber B.**

To accomplish the desired task cryptography mechanism is implemented which gives better security on SMS data. I have first implemented FECTSD [22] algorithm and found that author did not use any compression technique and the algorithm is easy to break or guess the keyword as avalanche effect of an algorithm is very low. The aim of this research work is to build up a powerful and secure cryptography algorithm against various sorts of attacks. The strength and security in expanded by Generation of Random number by adding ASCII value of key character followed by modulo of key length. Appropriately an effective plan is created here that are having better execution time and avalanche Effect against a broad assortment of assaults. The outcomes appear that our proposed security algorithm has less complexity as compare to A Fast Encryption and compression technique on SMS data (FECTSD) (2018)

Keywords **- Encryption, decryption, plain text, cipher text, symmetric key and Block cipher.**

I. INTRODUCTION

Nowadays, cryptography plays a major role in protecting the information of technology applications. Information security is an important issue, for some applications. Have the top priority such as ecommerce, e-banking, e-mail, medical databases, and so many more, all of them require the exchange of private information. For instance, let us consider an individual named Alice a sender who needs to send an information message which has a length of characters to a recipient called Bob. Alice utilizes an unbound correspondence channel. Which could be a phone line, PC organize, or some other channel. In the event that the message contains secret information, they could be blocked and perused by programmers. Additionally they may change or alter the message amid its transmission so that Bob would not have the capacity to find the change.

In this review a different method for encryption is seen and has been looked at, and many of examples have been given.

In the present computerized world immense volumes of data is exchanging between end clients as SMS (Short Message Administration) through cell phones. Every SMS information generally is included basic content characters which are sent in the form of plain text. Cell phones likewise put a limit on every SMS up to 160 characters. SMS information sent by Sender A is firstly stored at service centre of service provider then after it is delivered to the receiver B. The expansion of SMS information likewise puts huge an impact on the storage system present at service centre and furthermore on data transmission channels. On the off chance that information is exhibited just in the type of plain text then at that point there is security risk. SMS information can be helpless against security assaults by an Eavesdropper during transmission of text messaged at service center where data or text is stored through channels. compression with Cryptography are two zones which can give solution for manage security problem .

The word cryptography originates from the Greek word "Kryptos", that implies covered up, what's more, graphikos" which implies writing.

When talking about information security and cryptography, it is common to divide the field into four main categories [12]. These categories are symmetric encryption, asymmetric encryption,data integrity algorithms and authentication protocols.

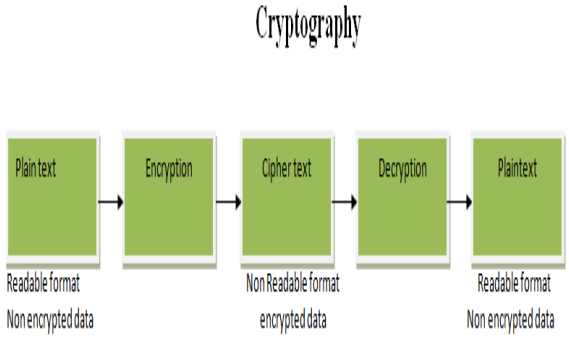

Figure 1: Cryptography

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 7, Issue 12, December 2018)

1.2 Cryptographic Algorithm categories

There are main two types of cryptographic algorithm.

- Symmetric key
- Asymmetric key

1.2.1 Symmetric key

- Symmetric encryption schemes lets two parties communicate secretly by being possession of the same secret key that only they know. Both parties will use the same secret key to encrypt and decrypt the messages exchanged between them. Sender and Receiver share a same key.

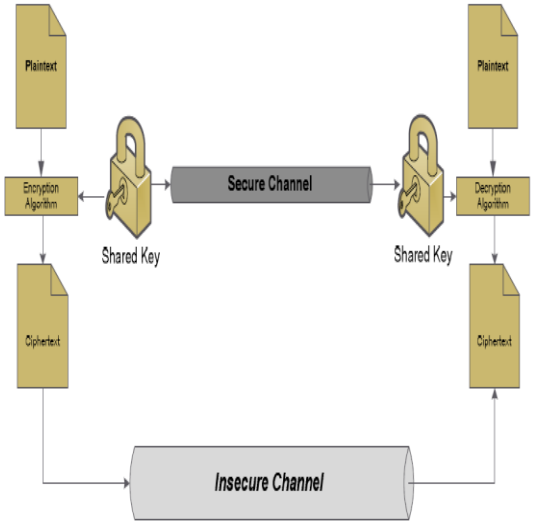

Figure 2: Simplified model of Symmetric Key Encryption

1.2.2 Asymmetric key:

- Asymmetric encryption schemes, synonymous with public key encryption schemes, are able to solve the key exchange problem of symmetric encryption. Specifically, in asymmetric encryption, both parties possess their own unique key pair. The key pair consists of one secret key that only they know and a public key that they can publish for anyone to see.

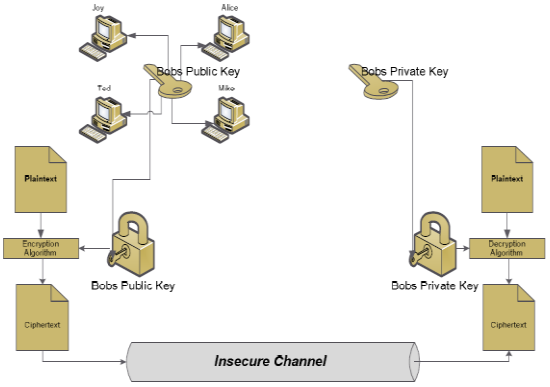

Figure 3: Simplified model of Asymmetric Key Encryption

1.3 Cryptography Goals

By using cryptography many goals can be achieved, These goals can be either all achieved at the same time in one application, or only one of them, These goals are:

1. Confidentiality: it is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.

2. Authentication: Authentication: it is the way toward demonstrating the identity that guarantees the imparting element is the one that it professed to be, this implies the client or the framework can demonstrate their very own characters to different gatherings that don't have individual information of their personalities. (The essential type of host to have verification on the Internet today is name-based or address-based; and the two are famously frail).

3. Data Integrity: its guarantees that they got message has not been modified at all from its unique frame, This can be accomplished by utilizing hashing at the two sides the sender and the beneficiary so as to make a special message process and contrast it and the one that got.

4. Non-Repudiation: it is system used to demonstrate that the sender truly sent this message, and the message was gotten by the predefined party, so the beneficiary can't guarantee that the message was not sent.

5. Access Control: it is the process of preventing an unauthorized use of resources. This objective controls who can approach the assets, if one can access, under which limitations and conditions the entrance can be happened, and what is the consent dimension of a given access

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 7, Issue 12, December 2018)

1.4 Application of cryptography

- Secrecy in Transmission
- Secrecy in Storage space
- Integrity in message Transmission
- Integrity in Storage
- Authentication of Identity
- Credentialing Systems
- Electronic Signatures
- Electronic Cash
- Threshold Systems
- Systems Using Changing Keys
- Hardware to Support Cryptography

II. Literature Survey

Many existing researchers have proposed various methods to secure SMS data. Substitution and transposition are two major operations of cryptography which provide security of data. Substitution changes the symbol with another one whereas Transposition interchanges the position of symbol Various Cryptographic techniques were discussed in [1]. SMS security for Smartphone [2] dependent on creamer cryptographic arrangement uses AES and RC4 strategies to give security. SMS encryption estimation [3] gives security features reliant on hyper violent structure. Cryptography procedures [4], [5] use elliptic twist framework for tying down SMS and MMS data which endeavor to give approval with minimal key and in small handling time. A protected short message correspondence tradition [6] executes an application tradition over SMS correspondence tradition dependent on key understanding and open key approval. Proposed a showcase for mooring SMS [7] gives confirmation, security moreover, reliability by executing balanced RSA-2048 and SHA-256. Secure short message conveyed tradition [8] is in perspective of TLS which is a client gadget for interfacing with server in safe path and after that approves correspondence. Weight hopes to decrease input data measure and is of two classes lossless and lossy [9]. In lossless weight, recipient can reproduce revise data from stuffed data where it is altogether used for compacting artistic data. In lossy weight little proportion of data gets lost at decompressing stage which is associated fundamentally for pictures. Huffman Coding [10] is an outstanding weight system that uses tree thought for making prefix codes where by and large as frequently as conceivable happened pictures get shorter prefix codes and less routinely happened pictures get greater prefix codes.

An assortment of Huffman coding is presented as Dynamic Huffman Coding [11] where a tree is created meanwhile as scrutinizing the information pictures, unlike Huffman coding. Various subgroup data weight [12] uses Huffman coding on three subgroups (letters all together, numbers, heads and other phenomenal pictures) where it attempts to crush Adaptive Huffman Coding [11].

Another approach of memory beneficial Huffman tree depiction [13] hopes to lessen Huffman coding tree gauge by showing a powerful memory framework to store the Huffman tree using extra bits to address a tree structure. Profitable Test Example Compression Techniques [14] is another assortment of Huffman coding which relies upon perceiving supplement esteems. Run Length Encoding [15] sees reiterating pictures what's more, puts a picture and its check in the place of repeating plan. Math Coding [16] performs weight by applying numerical calculations. It takes stream of data pictures and replaces with a single bona fide regard. Lossless substance weight using word references [17] packs by keeping up meal based vocabularies and word based word references. A Validated Bit Shifting and Stuffing Methodology [18] change eight bytes into seven bytes by setting eight byte in the past seven bytes. A couple of strategies join weight besides, encryption steps. An indirect encryption using weight [19] alters [18] and changes over into encryption instrument as well. Cryptanalysis of some blended media encryption designs [20] discusses systems which do weight and encryption. We present another instrument that in the meantime performs weight and encryption meanwhile of examining input pictures. Proposed approach incorporates no utilization of exorbitant data structures and does not comparing to the present circumstance complex logical formulae. It packs and scrambles at more conspicuous speed which is an obvious prerequisite require condition in present propelled world. As opposed to various systems, the route toward checking input pictures, doing encryption + weight and making pressed + encoded pictures to yield record is done in a lone development. Our tests reveal that it does encryption and weight at a conventional rate in smart time limits.

III. Proposed Method

3.1Proposed Algorithm:

3.1.1 Encryption Process:

Encryption Algorithm steps are given below

Step-1 Generation of Random number by adding ASCII value of key character followed by modulo of key length.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 7, Issue 12, December 2018)

Step-2 Generate 6 different Keys

a.Key1 = Binary Conversion of Key

b. Key2 = Leftrotate Key1 by RN value

c.Key3 = XORing Key1 and Key2:

d. Key4 = XORing Key3 by its circular front RN bit

e.Key5 = XORing Key3 and Key4

f. Key6 = = Leftrotate Key5 by RN value

Step-3 Now, Shuffling of Keys by following process:

```
if (RN % 6 == 0)
{
  K0 = Key1;
  K1 = Key2;
  K2 = Key3;
  K3 = Key4;
  K4 = Key5;
  K5 = Key6;
}
else if (RN % 6 == 1)
{
  K0 = Key2;
  K1 = Key4;
  K2 = Key6;
  K3 = Key3;
  K4 = Key1;
  K5 = Key5;
}
else if (RN % 6 == 2)
{
  K0 = Key3;
  K1 = Key5;
  K2 = Key1;
  K3 = Key2;
  K4 = Key4;
  K5 = Key6;
}
else if (RN % 6 == 3)
{
  K0 = Key4;
  K1 = Key6;
  K2 = Key1;
  K3 = Key3;
  K4 = Key5;
  K5 = Key2;
}
else if (RN % 6 == 4)
{
  K0 = Key5;
  K1 = Key1;
  K2 = Key3;
  K3 = Key2;
  K4 = Key6;
  K5 = Key4;
}
else if (RN % 6 == 5)
{
  K0 = Key6;
  K1 = Key2;
  K2 = Key4;
  K3 = Key1;
  K4 = Key3;
  K5 = Key5;
}
```

Step-4 Pad ‘0’ to make plaintext multiple of 128

Step-5 Divide the plaintext into small chunks of 128 bits size.

Step-6 Repeat the following process for each chunk:

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 7, Issue 12, December 2018)

a. PT = leftrotate(PT, RN)

b. PT = xor(PT, K0)

c. PT = XOring PT by its circular front RN bit

d. PT = xor(PT, K1)

e. PT = leftrotate(PT, RN)

f. PT = xor(PT, K2)

g. Divide PT in two half PTL and PTR and swap them.

PTL = PT.Substring(64, 64)

h. PTR = PT.Substring(0, 64)

i. PTL = xor(PTL, PTR)

j. PT = xor(PT, K3)

k. PT = XOring PT by its circular front RN bit

l. T = xor(PT, K4)

m. PT = leftrotate(PT, RN)

n. PT = xor(PT, K5)

Step-7 Result of each chunk is cipher text of that chunk finall merge all to get final ciphertext and convert to character format.

3.1.2 Key generation block diagram

3.1.2.1 Key Generation Part-I

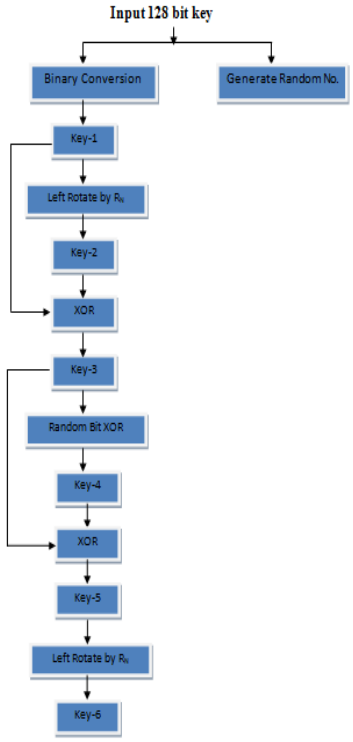

Figure 4: Key generation Block Diagram Part-I

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 7, Issue 12, December 2018)

3.1.2.2 Key Generation Part-II

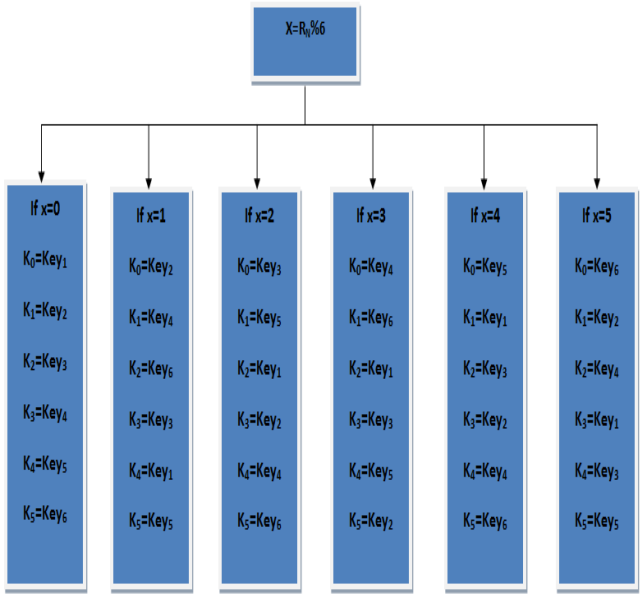

Figure 5: Key Generation Block diagram of part -II

Block diagram of Plaintext to Cipher text Conversion

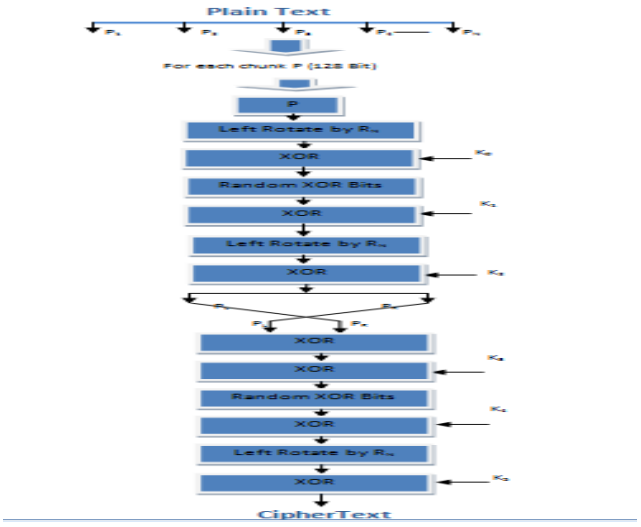

Figure 6 :Block diagram of encryption algorithm

3.1.2 Decryption Process:

Decryption algorithm is just a reverse process of encryption algorithm.

IV. Result Analysis

There are multiple researchers that work on many encryption and decryption algorithm to make it better in terms of security, space & time evaluation. Here I experimentally evaluate FECTSD algorithm [22] and Proposed algorithm and compare it in terms of throughput, time and space complexity.

4.1 Experimental Analysis of FECTSD[22], standard DES & Proposed algorithm

Encryption algorithm plays a very important role in network information security. It is essential to evaluate the performance of encryption algorithms. Usually the evaluation includes two parts: security and time efficiency. We analyzed the FECTSD **algorithm** [22], standard DES and proposed algorithm on these two parameters. In this section, we discussed the experimental results on FECTSD **algorithm** [22],standard DES and **proposed algorithm** on these two parameters with comparison graph.

A. Evalaution of Encryption time

The encryption speed is considered the computation quantity that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption speed is used to measure the throughput per unit time of an encryption scheme. The encryption speed is calculated as the total plaintext in bytes divided by the encryption time. The main work for encryption speed evaluation is to observe the performed time of encryption for certain plaintext. Table 1 show the encryption time of FECTSD algorithm [22], standard DES and Proposed algorithm on different file size.

Table1
Encryption Time of FECTSD Algorithm, standard DES and proposed algorithm

File Size in KB	Encryption Algorithm (Execution Time in Second)		
	FECTSD [22]	**Proposed Algorithm**	**Standard DES[23]**
10 KB	0.015	0.14	0.764
20 KB	0.046	0.374	1.709
40 KB	0.156	1.201	4.339

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 7, Issue 12, December 2018)

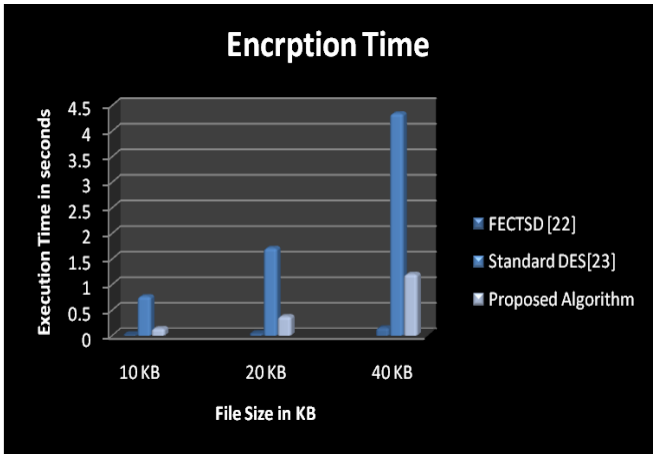

Figure 6: Encryption Time of FECTSD algorithm[22] ,standard DES[23] and Proposed Algorithm

Here, it is clearly seen that as file size increases, the encryption speed (throughput) of algorithm decreases. Our algorithm shows the better results as compared to FECTSD and standard DES algorithm.

B. Encryption Security

Encryption security considers the strength of encryption algorithm. As discussed, key strength of FECTSD[22] is not powerful as compare to standard DES and our proposed Algorithm . For analyzing the strength of encryption algorithm, Avalanche Effect is calculated. According to the avalanche effect, on changing the single bit in key 50% bits of cipher text must change. The algorithm close to avalanche effect is more secure against cryptanalysis. Table 2 shows the avalanche effect of FECTSD algorithm [22] ,standard DES and proposed algorithm.

Table 2:
Avalanche Effect of FECTSD, standard DES & Proposed BEE algorithm

Single bit change in key	Avalanche Effect		
	FECTSD[22]	**Proposed Algorithm**	**Standard DES**
	.69 %	49.076	48.67%

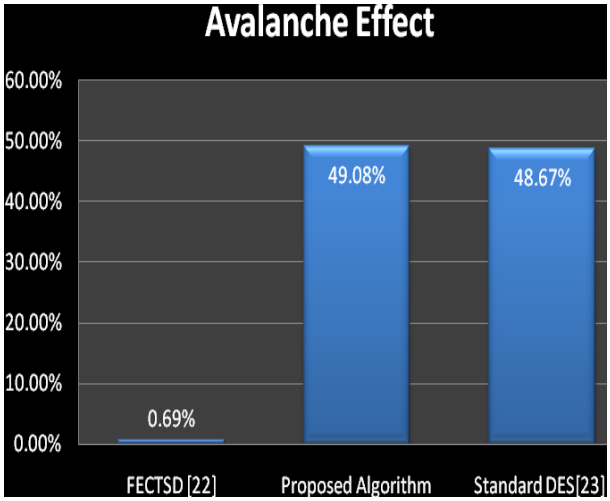

Figure 7: Avalanche Effect of FECTSD algorithm[22], standard DES[23] and Proposed Algorithm

Here, on analyzing the avalanche effect, it is clear from table 2 and figure--- that robustness of the FECTSD algorithm is very low as compared to standard DES and our proposed algorithm.

V. Conclusion & Future Scope

We have introduced a new mechanism that implements encryption methods on SMS data. The set of characters placed in the table and their order plays key role in encryption. In this work I have studied lots of cryptographic algorithms based on SMS data and proposed an improved algorithm and analyzed it with **FECTSD**[22]. Cryptography has been known and practiced for centuries. Previously, people would use manual methods for encrypting data. But after the arrival of variety of techniques, the entire method of data hiding has been modified. Cryptography has totally overtaken the old traditional methods in recent world of computers and internet. Also with the arrival of new methods, the attackers have invented newer techniques to break the code. This in turn gives rise to invention of more secure methods which are even more complex. This paper aims to develop an algorithm which provides more security to the confidential data by first encrypt it by applying a new secure encryption algorithm.

- The encryption speed (throughput) of algorithm not decreases as file size increases.
- Avalanche effect showed that the key strength of Proposed is very much powerful.

Results prove that our proposed algorithm shows the better security as compared with standard DES and FECTSD [22]

The proposed algorithm can be used in many application such as image security and real time application such as banking services and online payment gateway.

Future scope of this research work:

- This security system encrypts and embeds a confidential message into which is essentially a text document. Now if this cipher message might be further encrypted and sent as a secret message, the attacker would not be able to retrieve the original message.
- Secondly, this method could also be improved to compress the original secret message file and then encrypt more than one small compressed secret message files and embed them randomly.

REFERENCES

[1] Sophia Yakoubov, Vijay Gadepally, Nabil Schear, Emily Shen, and Arkady Yerukhimovich, A survey of cryptographic approaches to securing big-data analytics in the cloud," in 2014 IEEE High Performance Extreme Computing Conference (HPEC), pp. l–6, Year: 2014.

[2] Ali Makki Sagheer, Ayoob Abdulmunem, Abdul hameed, and Mohammed Adeeb AbdulJabbar, "SMS Security for Smartphone," in 2013 Sixth International Conference on Developments in eSystems Engineering, Year: 2013, pp. 281–285.

[3] Ayadi Wael and Seddik Hassene, "A new SMS encryption algorithm based on hyper chaotic system," in 2016 Second International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Year: 2016, pp. 57–62.

[4] Shraddha N. Karale, Kalyani Pendke, Prashant Dahiwale, "The survey of various techniques & algorithms for SMS security," in 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Year: 2015, pp. 1–6.

[5] B. N. Jagdale, R. K. Bedi, and Sharmishta Desai, "Securing MMS with high performance elliptic curve cryptography," International Journal of Computer Applications, vol. 8, no. 7, pp. 17–20, Oct. 2010.

[6] Chao-Wen Chang, Heng Pan, and Hong-Yong Jia, "A secure short message communication protocol," International Journal of Automation and Computing, vol. 05, no. 2, pp. 202–207, Apr. 2008.

[7] Dr. Shaimaa H. Shaker, Dr.Hassan A. Jeiad, and Fatimah A. Hassan, "Propose a model for Securing SMS," International Journal of Scientific & Engineering Research, vol. 5, no. 4, 2014.

[8] Saurabh Samanta, Radhesh Mohandas, and Alwyn R. Pais, "Secure short message peer to peer protocol," International Journal of Electronic Commerce Studies, vol. 3, no. 1, pp. 45–60, 2012.

[9] Khalid Sayood, "Introduction to data compression," 4th edition, Morgan Kaufmann Series In Multimedia Information And Systems.

[10] J. Cox, M. M. Miller, and J.A. Bloom, Digital Watermarking,Morgan Kaufmann Publishers, "A method for the construction of minimum-redundancy codes," Proceedings of the I.R.E., Sept. 1952, pp. 1098–1102.

[11] http://wikipedia.org/wiki/DynamicHuffmanCoding.

[12] Piyush Kumar Shukla, Pradeep Rusiya, Deepak Agrawal, Lata Chhablani, Balwant Singh Raghuwanshi, "Multiple subgroup data compression technique based on huffman coding," in 2009 First International Conference on Computational Intelligence, Communication Systems and Networks, Year: 2009, pp. 397–402.

[13] M. Ramesh, B. Hemantha Kumar, and A. Srinagesh, "A novel blockcipher mechanism for information security in cloud system," in 2016 IEEE 6th International Conference on Advanced Computing (IACC), Year: 2016, pp. 524–528.

[14] Shyue-Kung Lu, Hei-Ming Chuang, Guan-Ying Lai, Bi-Ting Lai, Ya-Chen Huang, "Efficient test pattern compression techniques 1216 This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2017 conference. based on complementary huffman coding," in 2009 IEEE Circuits and Systems International Conference on Testing and Diagnosis, pp. 1–4,Year 2009

[15] http://en.wikipedia.org/wiki/Information_Theory.

[16] http://en.wikipedia.org/Arithmetic_Coding.

[17] Sushil Kumar, Sarita S. Bhadauria, Roopam Gupta, "A Temporal Database Compression with Differential Method," Journal of Computer Applications, vol. 48, no. 6, 2012, DOI: 10.5120/7356-0273.

[18] Ramesh Makala, "Quin Stage Bio-Cryptographic Technique for Informatin Security," in Procedings of International Conference on Research in Engineering, Computers and Techonology (ICRECGT-2016), NIT Trichy, Tamilnadu, India, Year: 2016, pp. 77–83.

[19] M. Ramesh, B. Hemanth Kumar, M. Surendra Babu, "An indirect encryption using compression with random bit stuffing," International Journal of Computer Science and Information Technologies, vol. 6, no. 3, pp. 2142–2144.

[20] Goce Jakimoski, K. P. Subbalakshmi, "Cryptanalysis of some multimedia encryption schemes," IEEE Transactions on Multimedia, vol. 10, no. 3, pp. 330–338, Year: 2008.

[21] Ramesh Makala, Venkateswarlu Bezawada and Ranganath Ponnaboyina "A Fast Encryption and Compression Technique on SMS Data" IEEE WiSPNET 2017 conference,2017

[22] Makala, Ramesh, Venkateswarlu Bezawada, and Ranganath Ponnaboyina. "A fast encryption and compression technique on SMS data." Wireless Communications, Signal Processing and Networking (WiSPNET), 2017 International Conference on. IEEE, 2017.

[23] Coppersmith, Don. "The Data Encryption Standard (DES) and its strength against attacks." IBM journal of research and development 38.3 (1994): 243-250.

[24] William, Stallings. "Cryptography and network security: principles and practice." Prentice-Hall, Inc (1999): 23-50.

[25] A. Forouzan.,: " Cryptography and Network Security ", First Edition. McGraw-Hill, (2007), USA

[26] S .Maret," Cryptography Basics PKI ", First Edition. Dimension Data SA, ., (1999):, Switzerland.

[27] W .Stallings, "Cryptography and network security, Principles and practices ", Fourth Edition.Pearson Prentice Hall, (2006), USA.