A Survey on Various Encoding, Encryption and compression Techniques

A.Devi, K.Mani

Abstract— **This paper reports about the survey of various techniques available in an encryption and also in compression technique. It is mainly analyzing the existing encoding and compressed cryptosystem together as a literature survey. It is also discussed about the security issues of using various encryption technique and compression technique to reduce the size of plain text as well as to increase the transmission speed of plain text from one end to other end. This survey analyses several encryption technique, compression technique and also various literature paper so that it provides an idea for efficient integrated methods using compressed crypto system for future work .**

***Index Terms*— Arithmetic encoding, BWT, Huffman Algorithm, RC4, RSA.**

I. INTRODUCTION

Security is an important concern while transferring the plain text from one end to other end. In order to protect the plain text from unauthorized person, the cryptographic methods namely public key and symmetric key methods are used. The symmetric key is otherwise called single key or private key cryptography.

As the increasing demand of information storage during data transfer, the data compression is very important to reduce the file size. The technique, data compression is used to reduce the file size. When large files are to be transferred over networks, the compression technique is very useful if the file size is more than the capacity of data storage. Before compression the encoding of plain text will protect the file from hacking or damaging the plaintext.

The two common entropy encoding techniques are Huffman encoding and Arithmetic encoding.

Huffman coding is a lossless data compression algorithm in which the length of assigned variable-length codes are based on the frequencies of corresponding characters. The most frequent character gets the smallest code and the least frequent character gets the largest code.

Arithmetic coding is a lossless data compression in which it is used in the form of entropy encoding. It differs from other forms of entropy encoding, such as Huffman coding. It encodes the entire message into a single number, a fraction n where $(0.0 \leq n < 1.0)$.

To enhance the strength of cryptosystem, public key and private key encryption techniques can be used in an efficient way. It is used to encrypt the plain text which is converted into cipher text and the cipher text will be decrypted into original plain text when it reaches the other end. RSA is a well known public key algorithm to encrypt the plain text and the private key algorithm uses a single key for both encryption and decryption whereas public key algorithm uses encryption key and decryption key.

II. LITERATURE SURVEY

Tarek M.Mahmoud [1] proposed an efficient technique of hybrid compression with encryption for securing of SMS in symbian operating system. This technique uses the compression and encryption technique so that SMS sent through mobiles can be made secure. Here, RSA based encryption technique is used to reduce the eavesdropping but encryption increases the size of the text message, hence bandwidth is not utilized.

Cheng-Kang Chu, Wen Tao Zhu [2] proposed technique regarding secure subscription of mobile in sensor-encrypted data. In SMS-SED, a node or a mobile device stores a secret key of size independent of the total number of sensor nodes and time periods.

Muhammad Fahad Khan, Saira Beg and Humayun Rehman[3] implemented a new technique of transmission of compresses audio through SMS. SMS cannot be used for transfer of audio data since SMS may contain less bandwidth. Hence the idea is to compress the audio signal data into text and compresses so that it will not take much of the bandwidth and data is transferred to the receiver through SMS.

Anita Singhrova, Dr.Nupur Prakash[4] provides a new technique in the field of mobile communication. In this technique, analysis of various security protocols in mobiles has been proposed. The various encryption and authentication technique needed during the transmission of data from mobiles has been implemented.

Stephan Rein, Clemens Guhmann[5] implemented compression of text data in mobiles. It provides a low complexity based arithmetic coding compression of the text transferred through Mobiles.

Abu Shamim Mohammad Arif[6] implemented an enhanced static data compression on short messages. It explains a new technique of data compression on Bengali short messages for the small devices using the concept of masking and dictionary. The technique implemented here is an efficient technique especially for the short Bengali messages.

Manuscript received Jan, 2018.

A.Devi, *Department of Computer Science, Bangalore University/ Karnataka College of Management and Science . Bangalore, India..Mobile No.:+(91)9945270104.*

K.Mani, *Department of Computer Science, Bharathidasan University Nehru Memorial College, Trichy ,India. Mobile No+(91)9443598804.*

Iwan Handoyo Putro, Petrus Santoso [7] proposed a new technique of data compression which is based on arithmetic encoding. It explains the limitations of the message length is presented and a solution of how we can send more than 160 characters in the message.

Dorward and Quinlan [8] proposed a robust data compression of network packets with different compression algorithms to improve the performance of packet networks. They concluded that speed is important when compressing network packets, especially if the bandwidth is large when compared to the available computational capacity.

Shanmugasundaram and Lourdusamy [9] described different statistical compression algorithms as well as benchmarks comparing the algorithms. They focused with algorithms based on LZ77 and LZ78.

The Linear Feedback Shift Register (LFSR) is one of the most popular encryption techniques widely used in communication [10]. But the main disadvantage of LFSR based structure is its vulnerability to attack due to inherent linearity in the structure .

Majid Bakhtiari and MohdAizainiMaarof [11] , designed an efficient stream cipher algorithm to generate 115 random bits in one round of process which increase the resistance of process in front of Berlekamp-Massey, algebraic and correlation attacks. But, many computers are not able to generate random bits efficiently.

RC4[12] is an important stream cipher in software application. The first weakness of RC4 is that a large number of bits of initial permutation which is determined by a small subset of key bytes. The second weakness is a key vulnerability, if a part of key is exposed to the attacker.

Biham and Seberry[13], presented a method called Rolling Arrays which contain variable rotations and permutations. But, the disadvantage is that the total 256 keys must be accumulated for initial permutation and the plain text is not encoded. The key stream is not depending on the plain text to be encrypted.

An efficient key-pooled RC4 stream cipher is suggested by Kim et al.[14] for secure transmission of multimedia files in the wireless mobile network. In this method, a IBM-sized key stream pool is used with 32,768 key stream frames for every client device in the registration step is generated. It is more secured than the normal RC4. But, the drawback is the number of keys to be stored is huge.

In[15], Sreelaja and Pai recommended an Ant colony optimization(ACO) method for creation of key stream which is used to distribute the characters in the plain text for encryption. Artificial Ant's which do not discover counterparts with real ants and the encryption time is higher due to the phenomenon deposition is problem dependent. It does not reproduce real ant's performance.

Data Compression Methodologies for Lossless Data and Comparison between Algorithms presented by S.Porwal, Y.Chaudhary, J.Joshi, M.Jain[16]. They compared the performance of Huffman and Arithmetic encoding. After comparison of two techniques they concluded that the compression ratio for arithmetic encoding is better than the Huffman encoding and also found that the channel bandwidth and time is reduced much better than Huffman encoding. But the compression speed is very less in arithmetic encoding than the Huffman coding.

U.Khurana and A.Koul[17] provides Text Compression And Superfast searching and they proved that it is an efficient technique providing high compression ratios and faster search through the text.

S.Kaur and V.S.Verma[18] implemented a Design and Implementation of LZW Data Compression Algorithm.The author has implemented a finite state machine by using LZW data compression algorithm and he proved that text data is effectively compressed.

A Data Compression using Huffman based LZW Encoding Technique is presented by Md. Rubaiyat Hasan[21] for transmitting a digital image from a digital data source to a digital data receiver. The author has proved that it provides better transmission speed and saves time.

Rajan.S.Jamgekar et.al[19] implemented a File Encryption and Decryption Using Secure RSA. It shows that MREA algorithm is used to encrypt files and transmit encrypted files to other end where it is decrypted. But it works for smaller file size whereas it takes more time for larger file size.

In [20], Monisha Sharma et.al described about a novel Approach of Image Encryption and Decryption by using partition and Scanning Pattern. The author has proposed a lossless encryption of image and also gives access to variable lengths of the encryption keys.

In [22], Imad Khaled Salah et.al analyzed that no attack algorithm can break RSA cryptosystem in efficient manner. Most attacks appear to be result of misuse of the system or bad choice of parameters.

Fenwick.P[23],describes that the use of conventional pre-defined variable length codes or universal codes and shows that they too can give excellent compression. The paper also describes a 'sticky Move-to-Front' modification which gives a useful improvement in compression for most files. They proved that higher the compression ratio, more efficient is the algorithm.

Moumita Pal, P.Maji[24], shown that the image compression has proved to be a valuable technique as one solution and also the images those are compressed by A Block-sorting Lossless Data Compression Algorithm technique called Burrows-Wheeler Algorithm. Based on the result, it can be specified that after the decompression of the algorithm the data which compressed by the algorithm can be returned at almost lossless condition to their original data.

R.R.Baruah,V.Deka1,M.P.Bhuyan[25], shows that the performance analysis of BWCA transformation algorithms along with the proposed method are done for different text files of different size. They proved that higher the compression ratio, more efficient is the algorithm.

III. CONCLUSION

From the existing literature, it is found that no authors have proposed an integrated approach for encoded compressed cryptosystem, thus an integrated approach termed as **LECCRS (Lucas Encoding based Compressed CRyptoSystem)** is proposed for future research wherein which for encoding a new Lucas coding is analyzed for encoding the plain text to create an intermediate plain text, for compression the lossless variable length Huffman coding

is considered and in performing encryption, RSA encryption with varying block size to enhance the security.

REFERENCES

[1]. Tarek M.Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahmed,"Hybrid Compression Encryption Technique for Securing SMS", IJCSS, Vol. 3. Issue 6, 2010.
[2]. Cheng-Kang Chu, Wen Tao Zhu, Sherman S. M. Chow,"Secure Mobile Subscription of Sensor Encrypted Data", ACM, March 2011.
[3]. Muhammad Fahad Khan,Saira Beg and Humayun Rehman, "Transference of Compressed Audio through SMS Using Prediction by Partial Matching Technique", *IJAST*, Vol. 41, April 2012.
[4]. Anita Singhrova, Dr.Nupur Prakash, " Performance Analysis of Mobile Security Protocols: Encryption and Authentication", IJS, Vol. 1, Issue 1, 2007.
[5]. Stephan Rein, Clemens Guhmann, Frank H.P. Fitzek,"Low- Complexity Compression of Short Messages", 2006.
[6]. Abu Shamim Mohammad Arif, Asif Mahamud, Rashedul," An Enhanced Static Data Compression Scheme of Bengali Short Message", IJCSIS, Vol. 4, No.1&2, August 2009.
[7]. Iwan Handoyo Putro1, Petrus Santoso, Maya Basoeki,"A Short Text Compression Scheme based on Arithmetic Coding", 2007.
[8]. S.Shanmugasundaram and R.Lourdusamy,"A Comparative Study of Text Compression Algorithms," *International Journal of Wisdom Based Computing*, vol. 1 (3), December 2011, pp. 68–76.
[9]. https://en.wikipedia.org/wiki/Linear-feedback_shift_register.
[10]. Majid Bakhtiari, MohdAizainiMaarof,"An Efficient Stream Cipher Algorithm for Data Encryption",*IJCSI International Journal of Computer Science Issues*, Vol. 8, Issue 3, No. 1, May 2011 ISSN (Online): 1694-0814, www.IJCSI.org.
[11]. Scott Fluhrer,ItsikMantin and Adi Shamir, "weaknesses in the Key Scheduling Algorithm of RC4", (1).Cisco Systems,Inc,170 West Tasman Drive, SanJose,CA95134.(2).Computer Science department, The WeizemannInstitute, Rehovot 76100, Israel.
[12]. https://www.vocal.com/cryptography/rc4-encryption-algorithm
[13]. Biham E, Seberry J, Py(Roo): "A fast and secure stream cipher.", Research Online, 2005.
[14]. Kim HG, Han JK, Cho S,"An efficient implementation of RC4 cipher for encrypting multimedia files on mobile devices", SAC 07 Proceedings of the ACM Symposium on Applied Computing, 2007, pp. 1171–5.
[15]. Sreelajaa N.K, Paib GAV,"Stream cipher for binary image encryption using Ant Colony Optimization based key generation.", Journal of Applied Soft Computing, 2012,12(9):2879–95.
[16]. S.Porwal, Y.Chaudhary, J.Joshi, M. Jain ,"International Journal of Engineering Science and Innovative Technology (IJESIT)", Volume 2, Issue 2, March 2013.
[17]. U.Khurana and A.Koul, "Text Compression And Superfast Searching", Thapar Institute Of Engineering and Technology, Patiala, Punjab, India-147004.
[18]. S.kaur and V.S.Verma," Design and Implementation of LZW Data Compression Algorithm", *International Journal of Information Sciences and Techniques (IJIST)* ,Vol. 2, No.4, July 2012.
[19]. Rajan.S.jamgekar, Geeta shantanu joshi ,"File Encryption and Decryption using secure RSA" ,*International Journal of Emerging Science and Engineering (IJESE)*, ISSN: 2319–6378, Volume 1, Issue 4, February 2013.
[20]. M Sharma, C Kamargaonkar, A Gupta,"A Novel Approach of Image Encryption and Decryption by using partition and Scanning Pattern", *International Journal of Engineering Research & Technology (IJERT)*,Volume 1,Issue 7,September 2012, ISSN:2278-0181.
[21]. Md.Rubaiyat Hasan,"Data Compression using Huffman based LZW Encoding Technique", *International Journal of Scientific & Engineering Research*, Vol. 2, Issue 11, November-2011.
[22]. Imad Khaled, salah, Abdullah Darwish, and Saleh oqeilli, "Mathematical Attacks on RSA Cryptosystem", *Journal of Computer Science* 2(8), pp:665-671, 2006, ISSN 1549-3636.
[23]. Fenwick.P,"Burrows Wheeler Compression with Variable Length Integer Codes", Software – Practice and Experience, 32(13), 1307–1316, 2002.
[24]. Moumita Pal, P.Maji, "An Approach to Image Compression Using Burrows-Wheeler Algorithm", *International Journal of Science, Technology & Management*, Volume No.04, Issue No. 03, March 2015.
[25]. R. R. Baruah, V.Deka1, M.P.Bhuyan, "Enhancing Dictionary Based Preprocessing For Better Text Compression", *International Journal of Computer Trends and Technology (IJCTT)*, volume 9, number 1, Mar 2014.

First Author Devi. A received her MCA and M.Phil. from Bharathidasan University, Trichy, India in Computer Science Applications. During 2004-2016(April), she had been with the Department of Computer Science at the Lowry Memorial College, affiliated to Bangalore university, Karnataka, India where she was working as an Associate Professor. During 1998-2001, She was working as a programmer in different software companies. She is currently working as a Professor in Karnataka College of Management and Science, affiliated to Bangalore University, Karnataka, India. She has reviewed around 4 research papers for InderScience and 1 research paper for Elsevier Journal. She is pursuing her PhD in Compressed Cryptosystem, Bharathidasan University.

Second Author Mani. K received his MCA and M.Tech. from the Bharathidasan University, Trichy, India in Computer Applications and Advanced Information Technology respectively. Since 1989, he has been with the Department of Computer Science at the Nehru Memorial College, affiliated to Bharathidasan University where he is currently working as an Associate Professor. He completed his PhD in Cryptography with primary emphasis on evolution of framework for enhancing the security and optimizing the run time in cryptographic algorithms. He published and presented around 15 research papers at international journals and conferences.