International Journal of Engineering Research and General Science Volume 3, Issue 4, July-August, 2015
ISSN 2091-2730

An Advanced Text Encryption & compression System based on ASCII values and arithmetic encoding to improve data security

Veerpal Kaur, Ramanpreet Kaur

Baba Farid Group of Institution, Bathinda, Punjab

Veerpalkaur100@ymail.com , ramanpreetbrarbfgi397@gmail.com

Contact no 98788-26316, 95011-15397

Abstract: Cryptography is the art and science of study of designing or generating the secret message code or ciphers of the original message for the secure communication between sender and the receiver. The main goals of cryptography are (1) Authentication, (2) Privacy, (3) Integrity, (4) Non-repudiation and (5) Access Control This research paper present the symmetric key encryption technique to encrypt the variable length text data and modified Huffman algorithm to compress and decompress the data, using fix length key which is randomly generated by the system to encrypt the data.

Keyword: AES (Advanced Encryption standard), RSA, DES (Data Encryption Standard), TCP (Transmission Control Protocol), RC4 (Rivest Cipher 4), IDEA (International Data-Encryption Algorithm), LZW (Lempel-Ziv-Welch)

INTRODUCTION

Cryptography is the art and science of study of designing or generating the secret message i.e. code or ciphers of the original message for the secure communication between sender and the receiver. A cryptographic algorithm is a mathematical functions and unchanging set of steps to perform encryption and decryption of the original data. The main objective of every cryptographic algorithm is to make it as difficult as possible to decrypt the generated cipher text without using the key. If a really good cryptographic algorithm is used, then there is no technique significantly better than methodically trying every possible combination of key.

PROPOSED WORK: There is a complete range of different data compression techniques available both online and offline working such that it becomes really difficult to choose which technique serves the best. Here comes the necessity of choosing the right method for text compression purposes and hence an algorithm that can reveal the best tool among the given ones. A data compression algorithm is to be developed which consumes less time while provides more compression ratio as compared to existing techniques.

Proposed Algorithm

Step I : Input the text data to be compressed.

Step II : Find the number of unique symbols in the input text data.

Step III : Assign the numeric code to the unique symbols found in the step II.

Step IV : Starting from first symbol in the input find the binary code corresponding to that symbols from assigned numerical codes and concatenate them to obtain binary output.

Step V : Add number of 0's in MSB of Binary output until it is divisible by 8.

Step VI : Generate the ASCII code for every 8 bits for the binary output obtained in step V and concatenate them to create input for second phase.

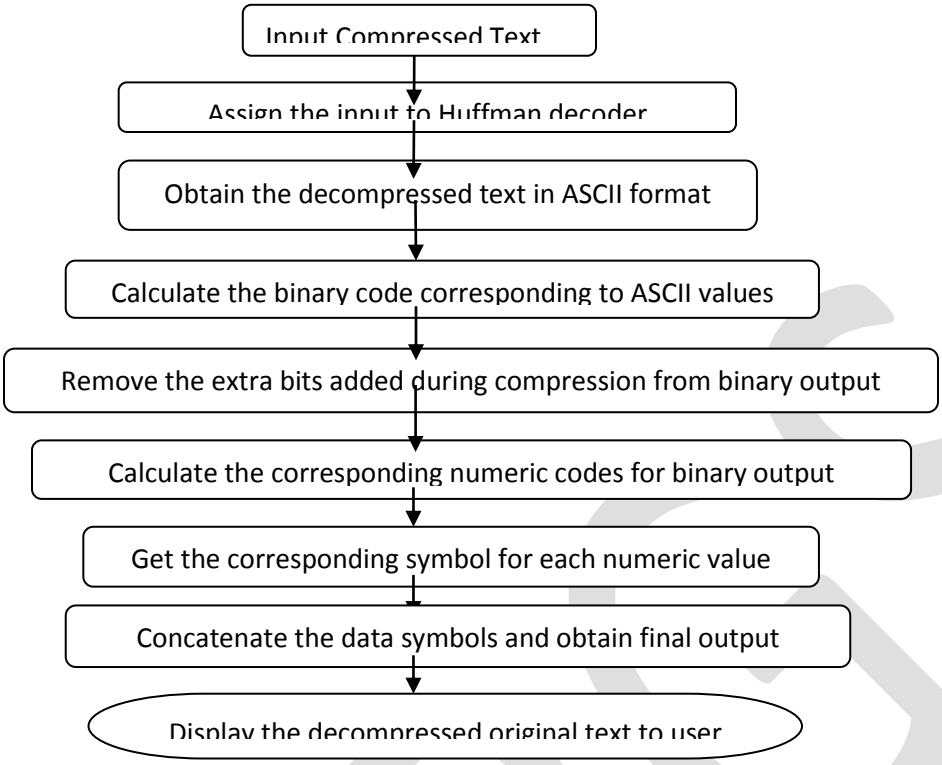
[Step VI is the result of dynamic bit Reduction Method in ASCII format]

Step VII : Give the output generated by Step VI to Huffman tree to further compress the data and obtain the result in compressed binary output form.

Step VIII: Display the final result obtained in step VII.

[Output from step VIII is final compressed output]

Flowchart for Decompression Process



RESULTS:

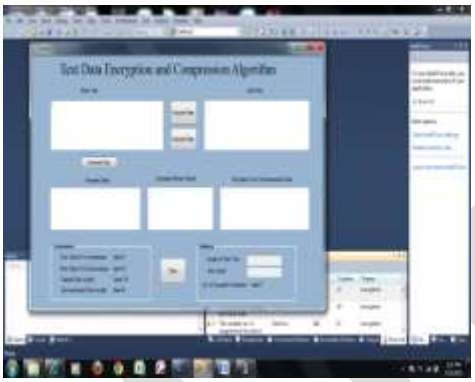


Fig 1. Output of basic environment

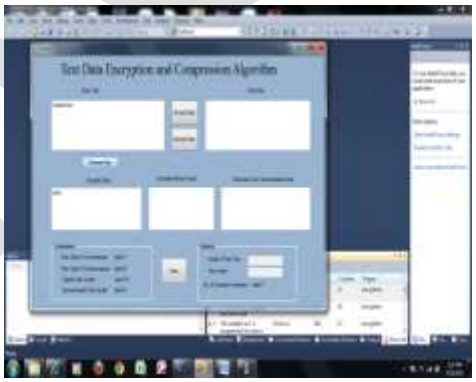


Fig. 2 Generate Key of 4 characters

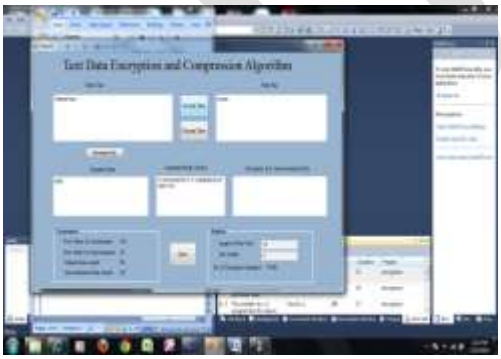


Fig. 3 Encryption of Data

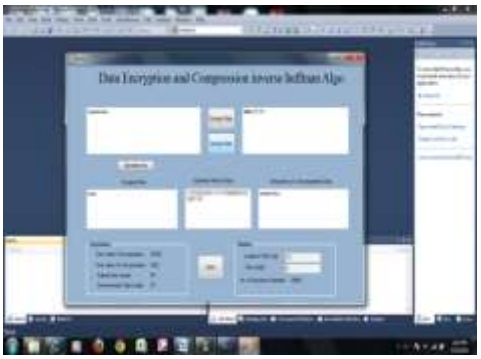


Fig. 4 Decryption of Data

Table of results generated by proposed system:

Input data (Plain Text)	Symmetric Key (generated by system)	Output Data (Cipher Text)
Abcd	Acbc	Cbee
Vcdhcdeasd	Gdeg	Yfdifgebvgab
Qwertyuioplkjhg	Ffeh	Txfrwzvirqmkmiha
Zxcvbnmlkjhgfdsaqwer	Bhgd	|xi{dnsqmjnlhdyfswkw
zaqwsxcderfvtgbnhyujmkiol	Gfeh	}crwvzddhtgvwicnk{vjpmjoocba

Table 1 the table which shows the result of the input data

Above table shows the results obtained by our proposed algorithm. We use input data of various lengths with fixed length key to generate the cipher text. The system is adequate to generate cipher text with this variable length input data.

Comparison between previous approach and our approach

Previous approach	Our approach
(1) Key is of variable length. (2) Key is generated manually. (3) Key is dependent on length of input data. (4) More memory is required. (5) Not efficient for large data	(1) Key is of fixed length. (2) Key is randomly generated by the system. (3) Key is not dependent on length of input data. (4) Less memory is required. (5) No limit on data length.

Table 2: Comparison between previous approach and our approach.

CONCLUSION:

The purposed system is showing good results for encryption and compression. The purposed system uses ASCII values of text data to encrypt the data. In the proposed system,It decrease the execution time. As the size of key is small, so that it occupies less memory due to compression algorithm. The scope of the system can be further improved by using variable length key. System can be made to encrypt the data on the basis of Unicode values. It also can be improved for to decrypt and compression the sentence form of data. so that it can be accepted globally

REFERENCES:

[1] Akanksha Mathur,"An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms,International Journal on Computer Science and Engineering (IJCSE),Vol. 4 No. 09 Sep 2012"
[2] Ajit Singh and Upasana Jauhari," Data Security by Preprocessing the Text with Secret Hiding, Advanced Computing: An International Journal (ACIJ), Vol.3, No.3, May 2012"
[3] Dr. Anwar Pasha Abdul Gafoor Deshmukh, Dr. Riyazuddin Qureshi," Transparent Data Encryption- Solution for Security of Database Contents, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011"
[4] Matthew M. Shannon,"Forensic Relative Strength Scoring:ASCII and Entropy Scoring,International Journal of Digital Evidence Spring 2004, Volume 2, Issue 4"
[5] Anupam Kumar Bairagi,"ASCII based Even-Odd Cryptography with Gray code and Image Steganography: A dimension in Data Security,COPYRIGHT © 2011 IJCIT, ISSN 2078-5828 (PRINT), ISSN 2218-5224 (ONLINE), VOLUME 01, ISSUE 02, MANUSCRIPT CODE: 110112"
[6] Kush Jain,Vaishali Ingale, Ashwini Sapkal"Kunal Secure Astro-Encryption- Data Encryption and Compression Using Planar Geometry,International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS),IJETCAS 12-342; © 2013,"
[7] Tarun Narayan Shankar G.Sahoo, "Cryptography by Karatsuba Multiplier with ASCII Codes, ©2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 12"
[8] Tanisha , Reema Gupta, Dr. Rajesh Kumar," File Security in Cloud using Two-tier Encryption and Decryption, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013 ISSN: 2277 128X"
[9] Verma, Sharad Kumar,Ojha, D. B.,"An application of data encryption technique using random number generator, International Journal of Research Studies in Computing 2012 April, Volume 1 Number 1, 35-42"
[10] Majdi Al-qdah, Lin Yi Hui,"Simple Encryption/Decryption Application International Journal of Computer Science and Security, Volume (1) : Issue (1)"
[11] R.S. Brar and B.Singh, "A survey on different compression techniques and bit reduction algorithm for compression of text data" International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) Volume 3, Issue 3, March 2013
[12] S. Kapoor and A. Chopra, "A Review of Lempel Ziv Compression Techniques" IJCST Vol. 4, Issue 2, April - June 2013