Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A New Approach of Compression and Encryption Algorithm

Alka P. Sawlikar
Dept. of Electronics Engineering
R.C.E.R.T. Chandrapur,
Maharashtra, India

Dr. Z. J. Khan
Dept. of Electronics & Power Engineering
R.C.E.R.T. Chandrapur
Maharashtra, India

Dr. S. G. Akojwar
Dept. of Electronics Engineering
R.C.E.R.T. Chandrapur
Maharashtra, India

Abstract: ***Tremendous data is all over the place, just take a look around us our Laptops, hard disks, computers, mobiles, everything is flooded with information and as the time passed by, data is tremendously increasing and Hence for transferring, saving and securing data it is becoming a complicated and troublesome work. To reduce the redundancy, storage requirements and to efficiently reduce communication costs data compression algorithms are used and to protect our data from eavesdropping and from unauthorized users, data encryption is used . Data compression offers an approach for reducing communication costs using available bandwidth effectively and at the same time we have to consider the security aspect of the data being transmitted which is vulnerable to attacks. Those encoding techniques are the best which offers high compression ratio so a module has to be developed for combining the operation of compression and encryption simultaneously on the same file of data and compare the combination of these outputs with the existing techniques or algorithms but in the secure compression module, the complete text file is preprocessed and then transform into some intermediate form so that it can be compressed with better efficiency and security. So in this paper we are presenting an optimized approaching encoding technique which offers high compression ratio which deals with both the issues of size and security. To improve the capability of algorithms and to compress the transmitted data an intelligent and reversible transformation technique is applied. The experimental results shows that our proposed method performs better than many existing techniques with respect to compression ratio, delay and the speed of Compression.***

Keywords: LZW, AES, RLE, DCT, DWT, ECC.

I. INTRODUCTION

Over a period of last consecutive years we have seen an unrivalled explosion in the amount of information or text data which is transmitted via many digital devices and for reducing the traffic ,there is a need to be compressed, so that large amount of information can be transmitted . For this a number of sophisticated compression algorithms have been proposed such as LZW,RLE,DWT,DCT,HUFFMAN. However, few of the above algorithms has been able to achieve best compression ratio[1][2].

Security of information and data has always been in demand since past few years and plenty of instances highlight the importance of the security of text data. As it is known cryptography is an art of hiding information and has been known from a long time,e.g.credit cards, debit cards, bank accounts, important documents and what not, everything needs protection. The most important issue in world today is the vast amount of valuable information that is passed among in various networks and present network development demands swap of information with more reduction and security in both the time for data transmission and the space requirement for data storage. This can be skilled by compression and encryption, such type of scheme is known as compression –crypto scheme[3][4]. That means ciphering/encryption is indeed a secure coding technique and data compression is a coding technique, whose purpose is to reduce both the space for data storage and the time for data transmission and hence compression ratio becomes an most important parameter which we have to always keep in mind [5][6]. So the data, which needs to be protected, is increasing on a rapid rate and can be handled a bit if we can remove the redundancy or can reduce its size and for this both encryption algorithm and *Compression* technique have to be combined and *made them work on data* so that our valuable information or message or file will be of compressed and encrypted form and is easy to handle and secure because of its reduced size and encrypted form which extends many advantages like saves space, manageable, easily transferrable, practical, and feasible[7][8].

We observed around that the rapid adoption of network technologies and computing systems has brought newer risks and threats such as stealing , unauthorized access service ,interruptions and altering of information, and so on. This becomes more intense to suggest the importance of security and presents every organization with the legal and ethical responsibility to correctly secure its information by using appropriate processes and measures. Imposing security at all states promises that information is processed, stored, or transmitted with integrity,reliability , authenticity and available to all authorized entities.

For a reduced and protected transfer of text information, the algorithms of encryption on text data must be able to be combined with the algorithms of compression of text data. The techniques of compression removes the redundancies contained in the text file in order to reduce the amount of information and on the other hand, the techniques of encryption

aim to guarantee a level of optimum safety to avoid the chosen plaintext attacks and brute-force attack which are the famous problem[11][12].

II. PROPOSED COMPRESSION AND ENCRYPTION ALGORITHM

Following is the proposed algorithm which compresses and encrypts the message :

Step 1: Prepare a Table for encoding the input symbols.

The upper limit and lower limit of each new symbol can be calculated or values can assigned

a) Initially load lower limit =0, upper limit =1
b) Encode all the symbols like a,b,c,d…..
c) Find new values for current range, upper limit and lower limit
   Current range = upper limit - lower limit
   Upper limit = lower limit + (current range * upper limit of new symbol)
   Lower limit = lower limit + (current range * lower limit of new symbol)

Step 2:- The string can be encoded by taking any value within the range of probability and after that convert the output decimal number into its binary format.

Step 3:- Limit the number of bits by using the formula and anyways can ceil it or floor it or put it in bracket also:-

No of bits=log [2/upper limit of last encoded symbol - lower limit of last encoded symbol]

Step 4:-In this way compression can be done and the number of bits are used to reduce the number of bits obtained in step2.

Step 5:- Now for encryption choose any one binary key pad and EX-OR it with above.

Step 6:- Then rotate right less than 4 bits.

Step 7:- Convert above result into decimal format again.

We will get output which is floating point number and that is corresponding to the input symbol.

Now here is the algorithm which decompresses and decrypts the text

Step 1:- Convert the received data into binary form.

Step 2:- Rotate bits to left.

Step 3:- Selected binary key pad and EX-OR it with above result.

Step 4:- Convert the result back into decimal form, note this will encoded value.

Step 5:-Encoded_ value=Encoded input

Still string is not fully decoded so match the symbol containing encoded value within its range

Current range = upper limit of new symbol - lower limit of new symbol

encoded value = (encoded value - lower limit of new symbol) ÷ current range

At the output we will found the original string.

III. MATHEMATICAL ANALYSIS OF ALGORITHM:

To explain the above algorithm in a better way we will consider following example.

Table I: Representation of characters along with its probability occurrence

Symbol	Probability	Range(lower limit,upper limit)
a	40%	(0.00, 0.40)
l	15%	(0.40 , 0.55)
k	25%	(0.55, 0.80)
p	20%	(0.80, 1.00)

Compression and Encryption has been done in a following manner:

Data to be encoded and encrypted is “alkp”

Step 1:- Encode 'a'

current_ range = 1 - 0 = 1

upper bound = 0 + (1 × 0.4) = 0.4

lower bound = 0 + (1 × 0.0) = 0.0

Encode 'l'

current range = 0.4 - 0.0 = 0.4

upper bound = 0.0 + (0.4 × 0.55) = 0.22

lower bound = 0.0 + (0.4 × 0.4) = 0.16

Encode 'k'

current range = 0.22-0.16 = 0.06

upper bound = 0.16 + (0.06 × 0.8) = 0.208

lower bound = 0.16+ (0.06 × 0.55) = 0.193

Encode ‘p’

current range = 0.208-0.193 = 0.015

upper bound = 0.193 + (0.015 × 0.90) = 0.2065

lower bound = 0.193+ (0.015 × 0.80) = 0.205

Step 2:-
The string "alkp" may be encoded by any value within the range [0.2065, 0.205].
Now output is 0.20425 and its binary equivalent= 0.001101001001001101110 1
Step3:- No_ of_ bits= [log_2/0.0015]=[log1333.33]=8bits
Step4:- So after reducing number of bits binary value is 0.00110100.
Step5:- Our One time pad is – 0.10101010
Data- 0.00110100 from step 4.
After EX-ORing the output is 10011110
Step6:- Rotate 4 bits right the result is 11101001
Step7: 0 .11101001 in decimal is 0.91015625
Decompression and Decryption has been done in a following manner:
Step 1:- Received data is 0.91015625 and binary format of received data is 0.11101001
Step2:- Apply 4 left shifts to result of step1 the result is 10011110
Step3:- Apply selected one time pad i.e 10101010 and EX-OR it with the result of step2 the result is 0.00110100
Step4:- convert 0.00110100into decimal i.e. 0.203125
Step5:- Using the probability ranges from table decodes the four character string encoded as
0.203125
Decode first symbol 'a'
0.20312 5is within [0.00, 0.40)
0.203125encodes 'a'
Remove effects of 'a' from encode value
Current _range = 0.40 - 0.00 = 0.40
Encoded _value = (0.203125- 0.0) ÷ 0.40 = 0.50775
Decode second symbol 'l'
0.50775is within [0.40, 0.55)
0.50775 encodes 'l'
Remove effects of 'l' from encode value
current range = 0.55 - 0.40 = 0.15
encoded value = (0.50775 - 0.40) ÷ 0.15 = 0.71833
Decode third symbol 'k'
0.71833is within [0.55, 0.80)
0.71833encodes'k'
Remove effects of 'k' from encode value
current range = 0.80 - 0.55 = 0.25
encoded value = (0.71833-0.55) ÷ 0.25=0.67332
Decode third symbol 'p'
0.67332 is within [0.80, 0.90]
0.67332 encodes 'p'

IV. CONCLUSION

If both compression technique and encryption algorithm are combined and made them work on data then that will be compressed encrypted form i.e. it will be easy to handle and secure because of its reduced size and encrypted form. Such combination presents many advantages. It saves space, manageable, easily transferrable, practical and feasible, shielded. Compression and encryption of large text data gives an efficient way of handling it. Combination of these techniques reduces the size first and then makes the reduced size secured, which is a less time consuming process. Such methods can be helpful in saving memory and transfer of data. Propose method provided good results by combining own compression and technique.

ACKNOWLEDGMENT

I express my sincere gratitude to my guides Dr. Z. J. Khan, Professor & Head Dept. of Electronics &Power Engineering and Dr. S. G. Akojwar Professor & Head Dept. of Electronics Engineering for their valuable guidance & keen interest in this work. I am very much thankful for their help & encouragement for the fulfillment of this paper.

REFERENCES

[1] Frank H.P. Fitzek Stephan Rein Morten V. Pedersen (2006), *Low Complex and Power Efficient Text Compressor for Cellular and Sensor Networks.* IST Moblie Summit.pp 1-5.

[2] Handoyo Putro, Petrus Santoso, Maya Basoeki (2012), *A Short Text Compression Scheme based on Arithmetic Coding*,1st International Conference on Recent Advances in Information Technology (RAIT), pp 285 – 289.

[3] S. Haykin(2001), *Fundamental Limits of Information Theory* Book: Communication Systems, John Wiley & Sons Inc, 4th ed.,, pp 578–581.

[4] Made Agus Dwi Suarjaya(2012), *A New Algorithm for Data Compression Optimization*, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.8,pp 14-17.

[5] Gagandeep shahi , Charanjit singh,(2013), *Securing and Compressing Transmission over LAN by using Public Key Cryptography*,.International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 1, Issue 7, pp-2320-9798.

[6] A.Makki Sagheer, M. Shaban Al-Ani, Omar Adil Mahdi(2013) ,*Ensure Security of Compressed Data Transmissi*, IEEE Computer Society of India, Sixth International Conference on Developments in eSystems Engineering , ISBN:978-1-4799-5263-2,pp270-275.

[7] Patil, M.Sahu, V. Jain(2014) , *SMS text Compression and Encryption on Android O.S*, International Conference on Computer Communication and Informatics (ICCCI), , ISBN:978-1-4799-2353-3,pp 1 – 6.

[8] Nivedita Bisht, Sapna Singh(2015) , *A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithm*,.International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3, March, ISSN-2347 – 6710, pp.1028-1031.

[9] Imai H., Hanaoka G., Shikata J., Otsuka A., Nascimento A.C(2002) Cryptography with Information Theoretic Security. Information Theory Workshop, Proceedings of the IEEE. Print ISBN:0-7803-7629-3.

[10] N. Khanna, J. Nath, J. James, A. Chakrabarti, S. Chakraborty A. Nath (2011) *New symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm.*, NJJSAA symmetric key algorithm. International Conference on Communication Systems and Network Technologies, p 126-127.

[11] A.Nadeem,(2006*),A performance comparison of data encryption algorithms,* IEEE information and communication technologies.pp 87-89.

[12] Idrizi, Florim,Dalipi, Fisnik & Rustemi , Ejup(2013*) ,Analyzing the speed of combined cryptographyic algorithms with secret and public Key* , International Journal of Engineering Research and Development,e-ISSN:2278-067X,ISSN:2278-800X, Volume 8,Issue 2 ,p.45.

[13] Abdul D S, Eliminaam ,Kadar H M A and Hadhoud M M (2008), *Performance Evaluation of symmetric Encryption Algorithms*, IJCSNS International Journal of Computer Science and Network Security , VOL.8 No. 12.pp 1028-1031.

[14] Vishwa Gupta, Gajendra Singh, Ravindra Gupta(2012*).Advance Cryptography algorithm for improving data security*, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X Volume 2, Issue 1..pp 1-5.

[15] Prashanti.G, Deepthi .S & Sandhya Rai.K(2013*).A Novel Approach for Data Encryption Standard Algorithm* , International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume -2 Issue-5, p.264-267.

[16] M. Savari, M. Montazerolzohour and Y. E. Thiam(2012 *) Combining Encryption Methods in Multipurpose Smart Card*, IEEE International conference CyberSec ,p. 43-48.

[17] A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung,C. Wachter(2012), *Public keys* ,Springer Crypto, volume 7417 of LNCS, pp 626-642.

[18] B. B. Brumley and R. M. Hakala(2009) ,*Cache-timing template attacks* , Springer- ASIACRYPT, volume 5912 of LNCS, pp 667-684.

[19] Behrouz A. Forouzan Debdeep M ukhopadhyay, *Cryptography and network security*,2edition, Mc Graw Hill Education (India) Private Limited.

[20] N. Sangwan (2013) ,*Combining Huffman text compression with new double encryption algorithm*,IEEE International Conference on Emerging Trends in Communication, Control, Signal Processing & Computing Applications (C2SPCA), ISBN:978-1-4799-1082-3,pp 1 – 6.

