ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY Volume-2, Issue-6, 1643 – 1647

JOINT BINARY CODE COMPRESSION AND ENCRYPTION

Prof. Atul S. Joshi[1], Dr. Prashant R. Deshmukh[2], Prof. Aditi Joshi[3]

[1]*Associate Professor, Department of Electronics and Telecommunication Engineering,Sipna COET Amravati, Maharashtra, India* ***atuljoshi27@rediffmail.com***

[2]*Professor & Head of Department of Computer Science and Engineering Sipna COET Amravati, Maharashtra, India,* ***pr_deshmukh@yahoo.com***

[3]*Assistant Professor Department of Computer Science Narsamma Arts, Commerce & Science College Amravati , Maharashtra, India,* ***joshiadi23@rediffmail.com***

Abstract

Joint Compression and Encryption has gained increased attention from past four years to reduce the computational complexity & to provide encryption of multimedia content. In proposed algorithm Encryption prior to compression will improve the compression efficiency. The algorithm is based on Hamming distance between input binary bit steam & randomly generated key. Input bit stream divided into the chunk of either 32 or 64 bits. Encrypted message is generated depend on the Hamming distance. Codebook is generated according to Hamming distance & the index of codebook entry is then transmitted as a compressed code. We are using Polygram method for ciphering & codebook method for compression. Problem of similar bits in plaintext can also handled by proposed scheme by assigning special entries in the codebook. In proposed algorithm the technique used for encryption of input data is different for all chunks depend on the parity of sequence of input bit stream. This offers good encryption strength. Hamming distance of two are indexed using three bits & these bits used for compression. Computation is required to find out these numbers & hence computational cost of the said algorithm is less. The savings in computational steps of the proposed algorithm results into simplification process of decompression at the receiver end. Algorithm is tested with the help of MATLAB simulation tool. Results are taken for 32 bits & 64 bits of randomly generated key. It is observed that text data is compressed more as compare to image data. As compare to Key size of 32 bits compression is more pronounced in case of 64 bits key. This algorithm is more suitable for Text input as compare to Image input. Appreciable results are obtained for the random key of 64 bits.

Index Terms: *Compression, Encryption, Random Key, Computational Cost, Text, Image.*

---------- *** ----------

1. INTRODUCTION

Multimedia has wide variety of application today. Code compression promising for reducing the required Bandwidth, whereas encryption methods are widely used for the purpose of security applications [1]. Joint Compression and Encryption has gained increased attention from past four years to reduce the computational complexity & to provide encryption of multimedia content [2]. The conventional way to transmit data with consideration of conservation of Bandwidth & data security is to compress the data, up to its entropy and then encrypt it. At the receiver, received bit stream then decrypted and then decompress as shown in fig 1. In this paper we have reverse the order of compression & encryption & it is joint paradigm. The new approach of Symmetric Key algorithm is presented with randomly generated key of 32 & 64 bits. Test results are provided with Text as well as Image inputs .This paper is organized as below. Section 2 describe proposed scheme. Section 2.1 describe problem of similar bits. Section 3 & 4 describe degree of encryption & saving in computation respectively. Section 5 is result & discussion . Finally, Section 6 describes the conclusion of this work.

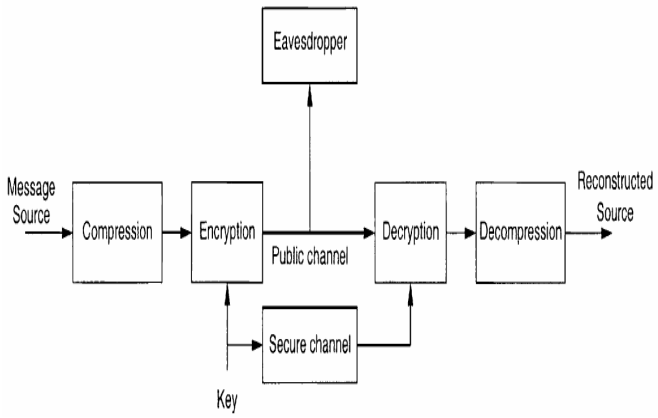

Fig-1: Conventional System

ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY Volume-2, Issue-6, 1643 – 1647

2. PROPOSED SCHEME

The proposed algorithm is based on Hamming distance. Hamming distance is calculated in between input binary bit steam & randomly generated key. Input bit steam generated from the message source is divided into the chunk of either 32 or 64 bits which is depend upon the size of the Key. Key is then compared with plaintext block to calculate the Hamming distance. Encrypted message is generated depend on the Hamming distance. Codebook is generated according to Hamming distance & the index of codebook entry is then transmitted as a compressed code. We are using Polygram method for ciphering & codebook method for compression.

2.1 Similar Bits Problem & Its Resolution

If plaintext blocks having similar bits then algorithm fails. This is because for the similar bits corresponding key changing techniques of the algorithm get confuse. Proposed scheme can handled this matter by assigning special entries in the codebook. This is explained as below.

Let

$X \rightarrow$ Input binary data of 8 bits

$Y \rightarrow$ Randomly generated binary Key of 8 bits

$Z_E \rightarrow$ Encrypted binary output

$Z_C \rightarrow$ Compressed binary output

$W_C \rightarrow$ Decompressed binary output

$W_D \rightarrow$ Decrypted binary output

$X = \{Xi\}$ & $Y = \{Yi\}$ Where i = 0 to 7

$\sum_{i=0}^{1} Xi \cdot 2^i = \Delta (Y_1\ Y_0)$

$\sum_{i=2}^{3} Xi \cdot 2^i = \Delta (Y_3\ Y_2)$

$\sum_{i=4}^{5} Xi \cdot 2^i = \Delta (Y_5\ Y_4)$

$\sum_{i=6}^{7} Xi \cdot 2^i = \Delta (Y_7\ Y_6)$

$Z_E = \Delta Y = \{\Delta Yi\}$ - - - - - - - - **ENCRYPTION**

$H_d [\Delta(Y_1\ Y_0), (Y_1\ Y_0)] = 1$

$H_d [\Delta(Y_3\ Y_2), (Y_3\ Y_2)] = 1$

$H_d [\Delta(Y_5\ Y_4), (Y_5\ Y_4)] = 1$

$H_d [\Delta(Y_7\ Y_6), (Y_7\ Y_6)] = 1$

Thus $H_d [\Delta(Y_3Y_2Y_1Y_0), (Y_3Y_2Y_1Y_0)]$

$= H_d [\Delta(Y_7Y_6Y_5Y_4), (Y_7Y_6Y_5Y_4)]$

$= 2$

Let S is the set of Index of Hamming Distance between ΔY& Y. Since total numbers of 4-bit number having Hamming distance of Two, are Six, they can be index by using 3-bits.Thus the resultant code is the pair of Two 3-bits numbers (Total Six bits) that results into compression.
Hence

$S = \{Si\} = \{ 001,010,011,100,101,110 \}$

Thus $Z_C = (Z_C'' Z_C')$ - - - - - - - - **COMPRESSION**

Where Z_C'' & $Z_C' \in S$

$W_C = (W_C'' W_C')$

Where $W_C' = f [Z_2', (Y_3Y_2Y_1Y_0)]$

$W_C' = \sigma \Delta(Y_3Y_2Y_1Y_0) \sim [Z_2', (Y_3Y_2Y_1Y_0)]$ &

$W_C'' = \sigma \Delta(Y_7Y_6Y_5Y_4) \sim [Z_2', (Y_7Y_6Y_5Y_4)]$

i.e. $W_C' = \Delta(Y_3Y_2Y_1Y_0)$ &

$W_C'' = \Delta(Y_7Y_6Y_5Y_4)$ ------ **DECOMPRESSION**

$W_D = \{W_{Di}\}$

$= \Delta Yi \cdot 2^i = X_i$

Thus $W_{D\,i} = X_i$

Hence $W_D = X$ ---------- **DECRYPTION**

If $X_1\ X_0 = X_3\ X_2$ OR/AND $X_5\ X_4 = X_7\ X_6$

i.e $X_1\ X_0 = X_3\ X_2 = X_5\ X_4 = X_7\ X_6$= 00,01,10,11

Then S_1 = {aaaa, bbbb, cccc, ddddd}

Where aaaa → 00

bbbb → 01

cccc → 10

dddd → 11

Z_C € $\mathbf{S_1}$

Let S_2 = {00, 01, 10, and 11}

Z_D € $\mathbf{S_2 \sim S_1}$

W_C € $\mathbf{S_1 \sim S_2}$

Thus $W_D = X_i$

Hence $W_D = X$

3 DEGREE OF ENCRYPTION

The key size and the randomness of the encrypted plaintext are two major factors to analyze the degree of security. The amount of time that required breaking a cryptosystem can be measured by

$$T = 2k\text{-}1\ t$$

Where k is the size of the encryption key, t is the amount of time needed for encryption of plaintext. It is true that size of the key is not very large as compare to other algorithm with the key size of 128 bits. However we are using the here the concept of one time pad. Key generation is random according to Shannon's Distributed Source Coding techniques[3].& it is independent of input bit stream. Symmetric key [4] is used to process the data results into fast encryption as compare to asymmetric key algorithms. In proposed algorithm the technique used for encryption of input data is different for all chunks. Encryption method changes depend on the parity of sequence of input bit stream. This offers good encryption strength in proposed algorithm[5].

4. SAVING IN COMPUTATION

Speed of both compression and decompression is important. For example when the users send compressed data over the network, it is important that both the sender and receiver can process the data in an acceptable time. This implementation achieves a lossless compression ratio of about 65 % with saving in compression & decompression time. Although other implementations with varying degrees of compression are possible require higher computational cost. In the AES algorithm, 128 bit blocks of data are arranged in a 4×4 matrix [6]. This matrix of data undergoes initial key addition and substitution. Each of the round functions that follow consists of a diffusion layer implemented by the row shifting and column mixing operation followed by the addition of a round key and substitution. In the proposed scheme, compression is based on Hamming distance of 'Two' bit key & encrypted data. Total Six numbers with Hamming distance of two are indexed using three bits & these bits used for compression. In short because of Joint scheme [7] only computation is required to find out these numbers & hence computational cost of the said algorithm is less. The savings in computational steps of the proposed algorithm results into simplification process of decompression at the receiver end.

5. RESULT & DISCUSSION

Proposed algorithm is tested with the help of MATLAB simulation tool. Results are taken for 32 bits & 64 bits of randomly generated key.

5.1 32 BIT KEY SIZE

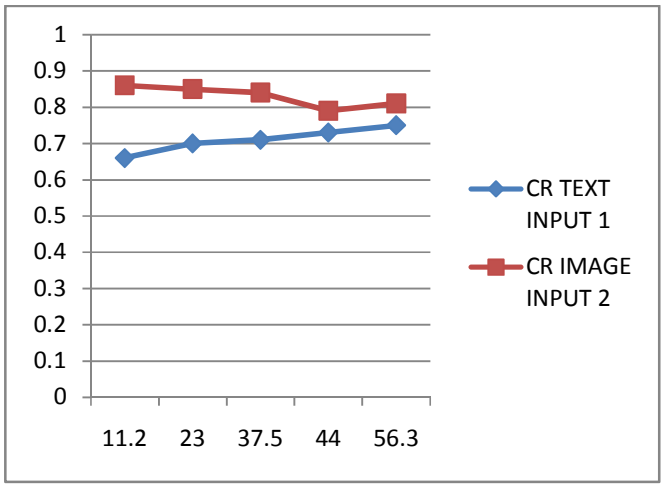

Fig-2: 32bits Key Size

Compression ratio is plotted against the file size in KB of Text & Image in fig 2. Results are taken by generating a random Key of 32 bits. It is observed that text data is compressed more as compare to image data.

5.2 64 BIT KEY SIZE

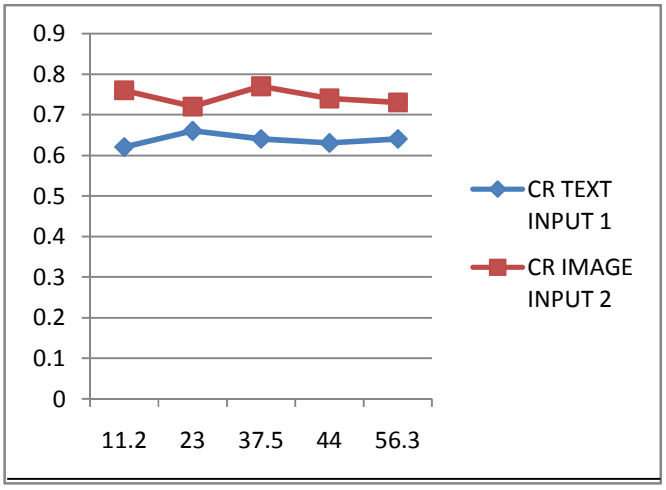

Fig-3: 64bits Key Size

As compare to Key size of 32 bits compression is more pronounced in case of 64 bits key. In latter case maximum compression ratio is 0.78. It means that increase in key size enhance the security of the data as well as compression performance. This is because as key size increases number of chunks of the input data decreases[8], hence codebook entries decreases . Comparatively lesser codebook entries can be coded with lesser bits. It results into more compressed bits.

CONCLUSION

In proposed scheme inspired the reversal of the order of compression & encryption i.e. encryption prior to compression without the loss of compression efficiency. Computational cost is low because of joint encryption & compression paradigm. High degree of security is possible due to variable encryption strategies, vary from data chunk to chunk. This algorithm is more suitable for Text input as compare to Image input. Appreciable results are obtained for the random key of 64 bits.

ACKNOWLEDGEMENT

First of all I would like to record my immense gratitude toward Respected Supervisor Dr.Prashant Deshmukh whose guidance and conclusive remarks had a remarkable impact on my work. I am also thankful to all my colleagues who supported me during this work. Last but not least, as always, I owe more than I can say to my exceptionally loving Guru Achyut Maharaj,my Parents & daughter Adya whose supports pave every step of my way.

REFERENCES

[1].Gred E.Keiser,“Local area network”, Tata Mc Graw Hill Edition , 1997, pp 443-497
[2].Seon-WonSeong, P.Mishra, “Bitmask based code compression for embedded system”, IEEE transaction on computer aided design of integrated circuit & system , vol. 27 , No. 4 , April 2008 , pp 673-685
[3].Daniel Hillel Schonberg, “Practical Distributed Source Coding & its application to the compression of
[4].S. Shani, B.C. Vemuri, F. Chenc Kapoor, “State of art image compression algorithm”, October 30, 1997.
[5].A. Wolf & A. Chanin, “Executing compressed program of embedded RISC architecture”, in poc. Int. symp. Micro, 1992,pp 81-91
[6].M.A. Haleem, K.P. Subbalakshmi , R. Chandramouli , Joint encryption & compression of correlated sources”, EURASIP Journal on Information Security , Jan. 2007
[7].Dr. V.K. Govindan , B.S. Shajee Mohan , “ IDBE – An intelligent Dictionary Based Encoding Algorithm for text data compression for high speed Data transmission ”, Proceeding of International conference on Intelligent signal processing , Feb 2004
[8].H.Lekats, J. Henkel, “Design of one cycle decompression hardware” , in pocd. Des. Conf. 2002 , pp 34-39
[9].R. L. Dobrushin, “An asymptotic bound for the probability error of Information transmission through a channel without memory using the feedback,” Problemy Kibernetiki, vol. 8, pp. 161–168, 1962.
[10].C.-P. Wu and C.-C. J. Kuo,“Efficient multimedia encryption via entropy code design,” in Security and Watermarking of Multimedia Contents III,vol.4314ProceedingsofSPIE, pp.128–138, January 2001.

BIOGRAPHIES

Prof. Atul Joshi is currently working as a Associate Professor in Department of Electronics & Telecommunication Engineering, at Sipna College of Engineering & Technology,Amravati (India). He is pursuing his PhD in Electronics. His areas of interest are Communication Engineering, Communication Network & Electronic Circuits Design.

Dr. Prashant Deshmukh is currently working as Head of CMPS & IT Department, at Sipna College of Engineering & Technology, Amravati (India). He has completed his Ph.D. in the faculty of Electronics Engineering from SGBAU Amravati University, Amravati (India). His areas of interest are Digital Signal Processing, VLSI Design and Embedded Systems.

Prof. Aditi Joshi is currently working as a Assistant Professor in Department of Computer Science, at Narsamma Arts,Commerce & Science college,Amravati(India.) She completed her MBA in 2011 . Her areas of interest are Image processing, & MATLAB Programmng.