International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

DATA OPTIMIZATION WITH BUILT IN SECURITY

Prof. Atul S. Joshi

Assistant Prof.

Department of Electronics and Telecommunication Engineering,

Sipna College of Engineering and Technology,

S.G.B.Amravati University

Amravati, India

Dr. P.R. Deshmukh

Prof. & Head of Department of CMPS & IT,

Sipna College of Engineering and Technology,

S.G.B.Amravati University

Amravat ,India

ABSTRACT

Network friendly media security refers to the security technologies that are specifically designed to cope with existing and future multimedia networking infrastructures

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

and technologies so as to ease the deployment and maintain or improve the quality of service performance of multimedia applications. It is especially useful for streaming and mobile multimedia applications where content adaptation is a necessity. In this paper, we analyze the various motivations behind network-friendly security solutions, review some of the most recent approaches, discuss some open issues, and suggest some potential solutions.

KEYWORDS

Compression, Encryption, error exponents, Source coding, System delay.

INTRODUCTION

In open networks, confidentiality is one of the primary concerns for commercial uses of multimedia communication. This issue is usually addressed by encryption. Recent advances in networking and digital media technologies have created a large number of networked multimedia applications. Those applications and services are often deployed in a distributed network environment that makes multimedia contents vulnerable to piracy and malicious attacks.[1] The security concerns, if not addressed appropriately, will potentially prevent or delay the wide dissemination of the multimedia applications [2]. As a result, securing multimedia contents has been an active research area in recent years

These unique properties of multimedia data and its distribution have posed significant challenges to conventional security technologies that were mainly designed for general data communication.[3]

In this paper, we give a survey of the encryption algorithms review some of the most recent approaches, discuss some open issues, present various rationales behind network-friendly security solutions and suggest some potential solutions. Also the consequences of reversing the order of encryption & compression are investigated.

PRECOMPRESSION, POSTCOMPRESSION &JOINT ENCRYPTION

Encryption algorithms from this class perform encryption before compression as shown in Fig(1) Note that these algorithms are inherently format compliant and generally inapplicable for lossy compression[4]. Finally, in most cases, performing encryption prior to compression causes bandwidth expansion which adversely impact compression efficiency[5]. Hence, this class of algorithms is generally not compression friendly.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

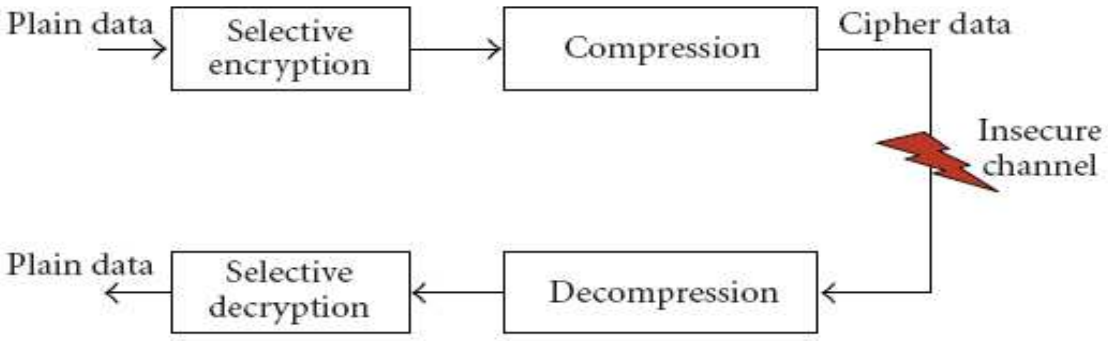

Fig (1) : PRECOMPRESSION APPROCH

Encryption algorithms from this class perform compression before encryption as shown in Fig (2). This class of algorithms is generally compression friendly; small overhead can be introduced to send the encryption key or some information about encryption. Encryption and decryption do not need modifications at encoder or decoder sides. Finally, it was suggested in [6] that post compression class is inherently no format compliant.

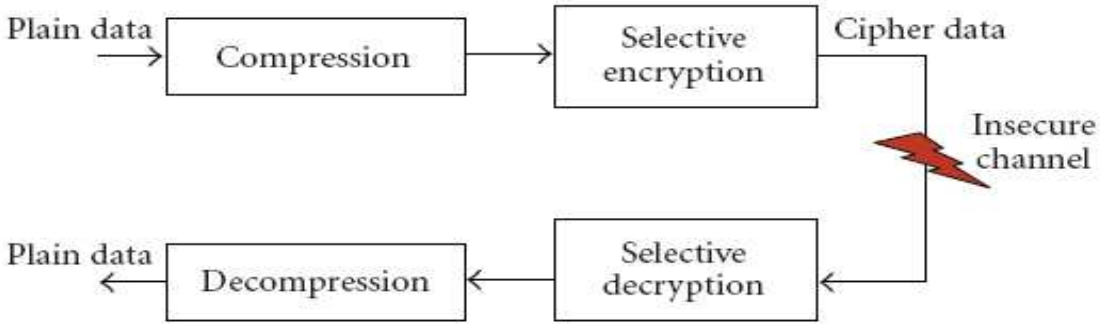

Fig (2): POSTCOMPRESSION APPROCH

Encryption algorithms from this class perform joint compression and encryption as shown in Fig ( ). Algorithms from this class imply modifications of both encoder and decoder which may adversely impact format compliance and compression friendliness.[7]

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

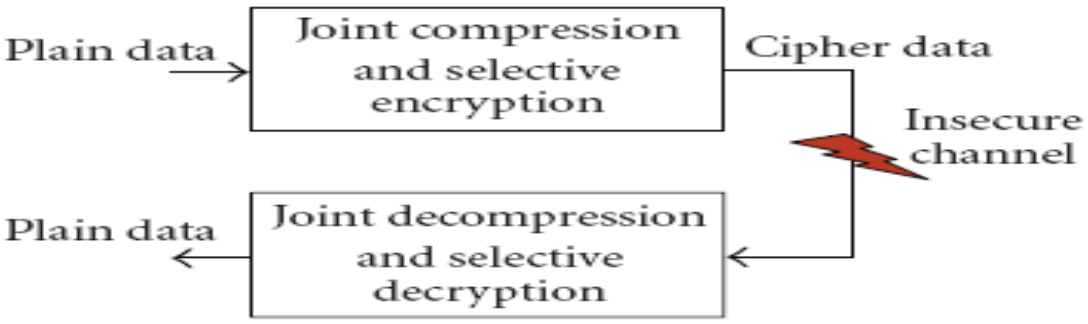

Fig (3): JOINT COMPRESSION & ENCRYPTION APPROCH

ENCRYPTION & COMPRESSIN OF STREAMING DATA

In this paper we have evaluated two architectures: the traditional compression-first approach depicted in Figure (4) and the encryption-first approach proposed in [8] and depicted in Figure (5)

In the traditional compression-first approach because of the lack of side-information compression can be modeled by having relevant error exponent with end-to-end delay is given by (11). The secret key can simply be used to XOR the rate R bit stream with a one-time-pad.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

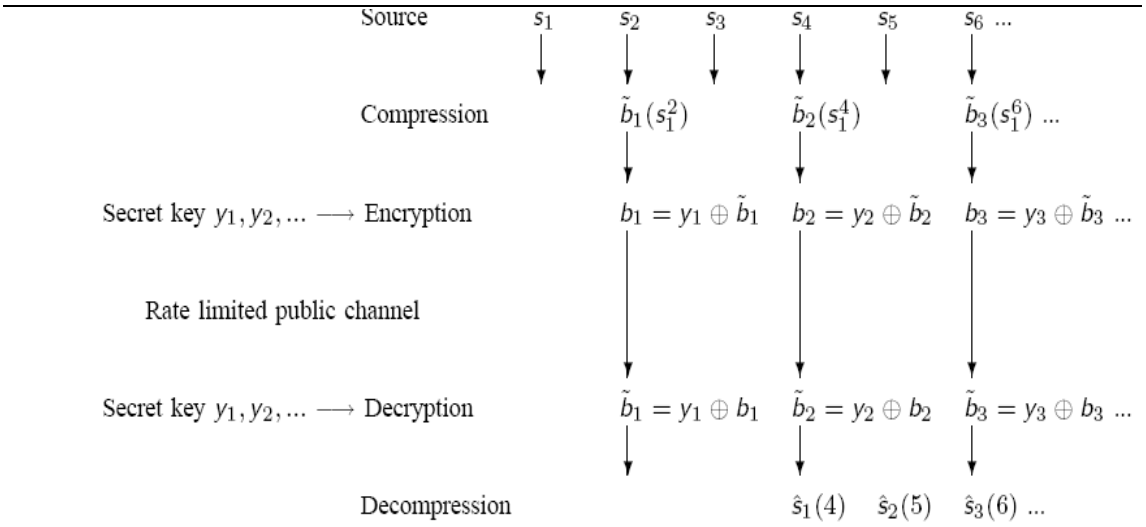

Fig (4): APPROCH OF COMPRESSION FOLLOWED BY ENCRYPTION

For this approach of [8], the secret key is used at a rate of log2 |S| bits per source-symbol to generate uniform virtual side-information The virtual source is generated in the Abelian group modulo |S|. From the encoded data bits, the eavesdropper learns nothing about the source symbols.

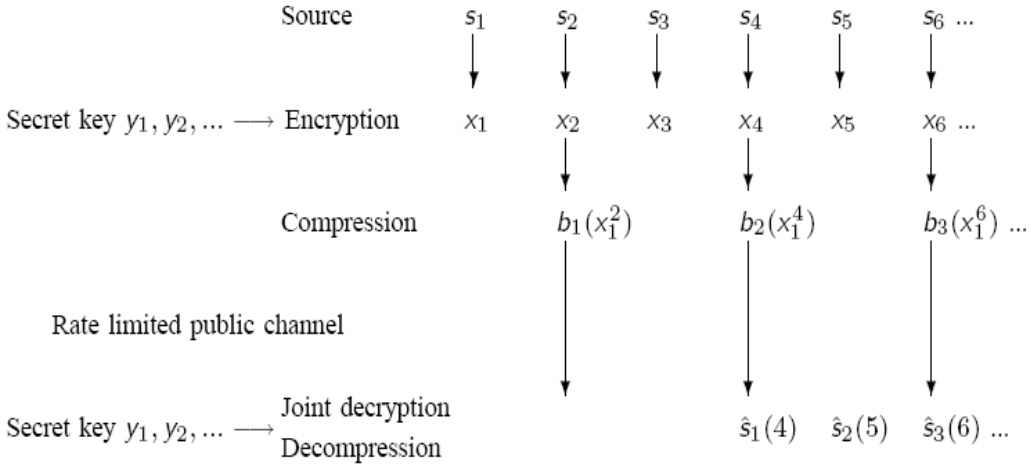

Fig (5): COMPRESSION OF ALREADY ENCRYPTIED STREAMING DATA

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

Meanwhile, the marginal distributions for both the encrypted data and the secret key are uniform. Since the the upper bound on the error exponent with delay is guarantees that a sequential random binning strategy can achieve the exponent This means that nothing higher than the fixed-block-length error exponent for source coding can be achieved with respect to end-to-end delay if the encryption-first architecture is adopted with the requirement that nothing about the true source be revealed to the compressor.

In practical terms, this means that if both the end-to-end delay and acceptable probability of symbol error are constrained by the application, then the approach of encryption followed by compression can end up requiring higher-rate bit-pipes.

ASYMPTOTIC PERFORMANCE OF SOURCE CODING SYSTEM

Asymptotic performance of different source coding systems is plot for Error exponent & Ratio of delay against rate R. We also plot the Error probability of source symbol against End to end delay.

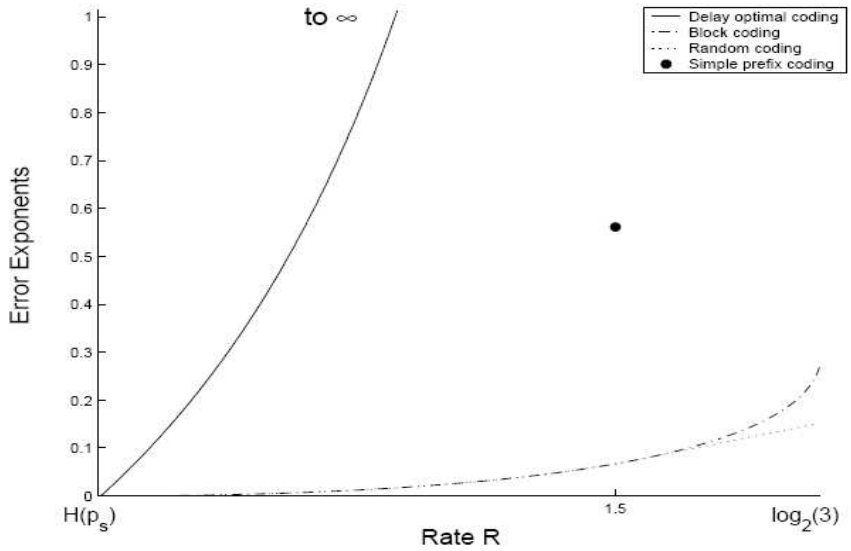

Fig (6): VERIOUS SOURCE CODING ERROR EXPONENT

It is clear from the above plot that Error exponents govern the asymptotic performance of delay systems with and without side information[9].

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

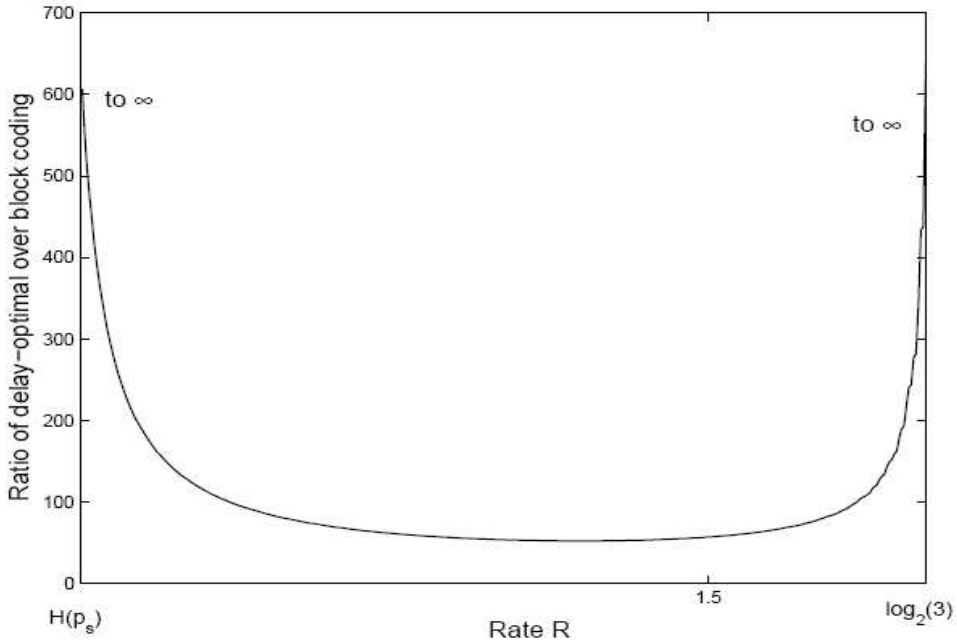

Fig (7): RATIO OF FIXED DELAY ERROR EXPONENT OVER BLOCK CODING

Figure (7) plots the ratio of the source uncertainty-focusing bound over the fixed-block-length error exponent. The ratio tells asymptotically how many times longer the delay must be for the system built around an encoder that does not have access to the side-information [10]. The smallest ratio is around 52 at a rate around 1.45.

From the above two plots it is very clear that even non-optimal codes can outperform optimal codes.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

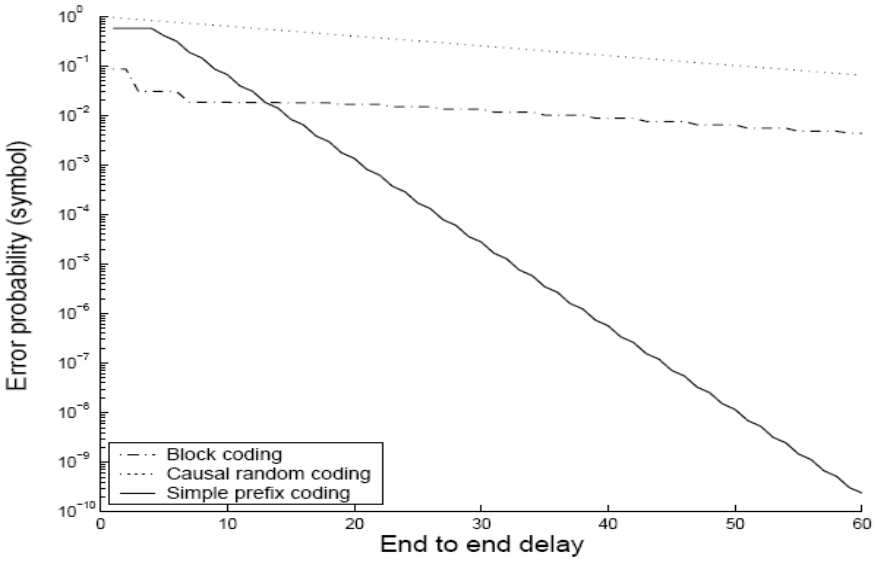

Fig (8): ERROR PROBABILITY VS DELAY

Figure (8) compares three different coding schemes in end to end delays and moderate probabilities of error. The slope of the curves indicates the error exponent governing how fast the error probability goes to zero with delay. Although smaller than the delay optimal error exponent Es(R), this simple coding strategy has much higher fixed-delay error exponent than both sequential random coding and optimal *simplex* block coding[11]. A simple calculation reveals that in order to get a 10−6 symbol error probability, the delay requirement for our simple scheme is 40, for causal random coding is around 303, and for optimal block coding is around 374.

CONCLUSIONS

This paper has shown that fixed-block-length and fixed-delay lossless source-coding behave very differently. Fixed-block-length systems do not usually gain substantially in reliability with encoder access to the side-information, fixed-delay systems can achieve very substantial gains in reliability. This means that if an application has a target for both end-to-end latency and probability of symbol error, then depriving the encoder of access to the side-information will come at the cost of higher required data rates.

End-to-end delay provides a framework to understand this and thereby compare different approaches. Comparing both sets of results shows how feedback in channel coding is very much like encoder access to decoder side-information in lossless source coding. The

main difference is that source coding performance is generally better at high rates while channel coding is better at low rates.

REFERENCES

[1] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *IEEE Trans. Inform. Theory*, vol. 49, pp. 626–643, Mar. 2003.
[2] B. Girod, A. Aaron, S. Rane, and D. Rebollo-Monedero, "Distributed video coding," *Proc. IEEE*, vol. 93, pp. 71–83, 2005.
[3] D. Socek, H. Kalva, S. S. Magliveras, O. Marques, D. Culibrk,and B. Furht, "New approaches to encryption and steganography for digital videos," *Multimedia Systems*, vol. 13, no. 3, pp.191–204,2007
[4] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Processing*, vol. 52, no. 10, pp. 2992–3006, 2004.
[5] C. Chang and J. Thomas, "Effective bandwidth in high-speed digital networks," *IEEE J. Select. Areas Commun.*, vol. 13, no. 6, pp. 1091–1114, Aug. 1995.
[6] T. M. Cover and M. Chiang, "Duality between channel capacity and rate distortion with two-sided side information," *IEEE Trans.Inform. Theory*, vol. 48, pp. 1629–1638, June 2002.
[7] J. Meyer and F. Gadegast, "Security mechanisms for multimedia data with the example MPEG-1 video," Project Description of SECMPEG, Technical University of Berlin, Germany, May 1995.
[8]C.-P. Wu and C.-C. J. Kuo, "Efficient multimedia encryption via entropy codec design," in *Security and Watermarking of Multimedia Contents III*, vol. 4314 of *Proceedings of SPIE*, pp.128–138, San Jose, Calif, USA, January 2001.
[9] A. Sahai, "Why block-length and delay behave differently if feedback is present," *IEEE Trans. Inform. Theory*
[10] C. Chang and A. Sahai, "Error exponents with delay for joint source channel coding," in *Forty-fourth Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Sept. 2006.
[11] 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.

AUTHOR INFORMATION

Prof. A. S. Joshi is currently working as a Assistant Professor in Department of Electronics and Telecomm. Engineering, Sipna College of Engineering & Technology, Amravati (India) since 2001. He is also pursuing

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

his Phd in Electronics. His areas of interest are Communication Enginering, Communication Network & Electronic Circuits Design.

DR. P. R. Deshmukh is currently working as Head of CMPS & IT Department, Sipna College of Engineering, Amravati (India). He has completed his Ph.D. in the faculty of Electronics Engineering From SGB Amravati University, Amravati (India). His areas of interest are Digital Signal Processing, VLSI Design and Embedded Systems.