Mathematical Problems of Computer Science 28, 2007, 18–33.

Random Coding Bound of Reversible Information Hiding E-capacity*

Mariam Haroutunian†, Smbat Tonoyan†, Oleksiy Koval‡, Svyatoslav Voloshynovskiy‡

† Institue for Informatics and Automation Problems of NAS of RA
e-mail: {armar, smbatt}@ipia.sci.am
‡University of Geneva, Switzerland
e-mail: {Oleksiy.Koval, svolos}@cui.unige.ch

Abstract

In this paper we consider the problem of reversible information hiding in the case when the attacker uses only discrete memoryless channels (DMC), the decoder knows only the class of channels, but not the DMC chosen by the attacker, the attacker knows the information-hiding strategy, probability distributions of all random variables, but not the side information.

We introduce the notion of reversible information hiding E-capacity, which expresses the dependence of the information hiding rate on the error probability exponent and the distortion levels for information hider, for attacker and for the host data approximation. The random coding bound for reversible information hiding E-capacity is found. When $E \to 0$ we obtain the lower bound for reversibility information hiding capacity.

In particular, we have analyzed two special cases of the general problem formulation, pure reversibility and pure message communications.

References

[1] A. V. Kusnetsov and B. S. Tsybakov, "Coding in a memory with defective cells", (in Russian), *Probl. Peredachi Informacii*, vol. 10, num. 2, p. 52-60, 1974.

[2] S. I. Gel'fand and M.S. Pinsker, "Coding for channel with random parameters", *Probl. Control and Inf. Theory*, vol. 9, num. 1, p. 19-31, 1980.

[3] M. Costa, "Writing on dirty paper", *IEEE Trans. on Information Theory*, vol. 29, num. 3, p. 439-441, 1983.

[4] H. C. Papadopoulos and C.-E. W. Sundberg, "Simultaneous broadcasting of analog FM and digital audio signals by means of adaptive precanceling techniques", *IEEE Trans. on Communicationsy*, vol. 46, num. 9, p. 1233-1242, 1998.

*The work was partially supported by the CRDF and NFSAT grant GRSP 09/06.

[5] F. M. J. Willems and T. Kalker, "Methods for reversible embedding," *Proc. 40th Annual Allerton Conference on Communication, Control, and Computing*, Allerton House, Monticello, Illinois, Oct. 2-4, 2002.

[6] T. Kalker and F. M. Willems, "Coding Theorems for Reversible Embedding," *DIMACS Workshop on Network Information Theory*, Rutgers University, Piscataway, NJ, vol. 66, March 2003.

[7] E. Martinian, G. W. Wornell and B. Chen, "Authentication with Distortion Criteria", *IEEE Trans. on Information Theory*, vol. 51, num. 7, p. 2523-2542, 2005.

[8] S. Voloshynovskiy, O. Koval, E. Topak, J. Vila and T. Pun, "Partially reversible data hiding with pure message communications", *IEEE Trans. on Information Forensics and Security*, submitted for publications.

[9] A. Sutivong, M. Chiang, T.M. Cover and Y.-H. Kim, "Channel Capacity and State Estimation for State-Dependent Gaussian Channels", *IEEE Trans. on Information Theory*, vol. 51, num. 4, p. 1486-1495, 2005.

[10] E. A. Haroutunian, "Upper estimate of transmission rate for memoryless channel with countable number of output signals under given error probability exponent" (in Russian), *III All-Union Conf. on Theory of Information Transmission and Coding, Uzhgorod, Publication House of Uzbek Academy of Sciences, Tashkent*, pp. 83-86, 1967.

[11] M. E. Haroutunian, S. A. Tonoyan, "Random coding bound of information hiding E-capacity", *Proc. of IEEE International Symposium on Information Theory*, p. 536, USA, Chicago, 2004.

[12] M. E. Haroutunian and S. A. Tonoyan, "On estimates of rate-reliability-distortion function for information hiding system", *Transactions of the Institute for Informatics and Automation Problems of the NAS of RA. Mathematical Problems of Computer Scence 23*, pp. 20-31, 2004.

[13] M. E. Haroutunian, "New bounds for E-capacities of arbitrarily varying channel and channel with random parameter", *Trans. IIAP NAS RA, Mathematical Problems of Computer sciences*, vol. 22, p. 44-59, 2001. Available at http://ipia.sci.am/itas.

[14] M. E. Haroutunian, "Estimates of E-capacity and capacity regions for multiple-access channel with random parameter", *Electronic Notes in Discrete Mathematics*, v.21, General Theory of Information Transfer and Combinatorics, pp. 303-308, 2005. Available at http://www.sciencedirect.com/science.

[15] I. Csiszár and J. Körner, *Information Theory: Coding theorems for discrete memoryless systems*, Academic Press, New York, 1981.

[16] I. Csiszár, "The method of types", *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2505–2523, 1998.

[17] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding", *IEEE Trans. Inform. Theory*, vol. 49, no. 3, pp. 563-593, Mar. 2003.

[18] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley, New York, 1991.

[19] E. A. Haroutunian and H. Belbashir, "Lower bound of the optimal transmission rate depending on given error probability exponent for discret memoryless channel and for

asymmetric broadcast channel", (in Russian), *Abstracts of papers of Sixth International Symposium on Information Theory, Tashkent, USSR*, vol. 1, pp. 19-21, 1984.

Տեղեկություններ թաքցնող շրջելի համակարգի E-ունակության պատահական կոդավորման գնահատականը

Մ. Հարությունյան, Ս. Տոնոյան, Օ. Կովալ, Ս. Վոլոշինովսկի

Ամփոփում

Աշխատանքում հետազոտված է տեղեկությունների շրջելի թաքցման ինֆորմացիոն-տեսական խնդիրը: Դիտարկված համակարգի համար հետազոտվել է E-ունակություն ֆունկցիան: Այն իրենից ներկայացնում է տեղեկությունների թաքցման արագության կախվածությունը հուսալիությունից, տեղեկություններ թաքցնողի ու հարձակվողի համար թույլատրելի շեղման մակարդակներից և նախնական տվյալների վերականգնման համար թույլատրելի շեղման մակարդակից: E-ունակության համար կառուցվել է պատահական կոդավորման գնահատական: Համապատասխան գնահատական է ստացվել համակարգի ունակության համար:

Ուսումնասիրվել են նաև երկու մասնավոր դեպքեր՝ մաքուր շրջելիության և հաղորդագրությունների մաքուր հաղորդման դեպքերը: