Why quantum steganography can be stronger than classical steganography

NATORI Shin*

Quantum Computation and Information Project, ERATO, JST
Daini Hongo White Bldg. 201, 5-28-3, Hongo, Bunkyo-ku,
Tokyo 113-0033, Japan

Steganography is the art and science of hiding data into innocently looking cover-data so that no eavesdropper can detect the existence of the hidden data. It is similar to cryptography, but steganography hides not only the content of a message but also the existence of a message itself. In order to hide the message, steganography needs preexistence of cover message. The encoder of a steganography system (embedder) computes a stego message, which is similar to the cover message, from a secret message, a key, and environmental inputs (such as the original cover message). This stego message retains the secret message in it and the recipient of the stego message can compute the original secret message using a key. If the cover message and stego message is indistinguishable to any eavesdropper, the steganography system is called secure.

In this paper, we first define a quantum steganography model by extending the classical one. We do this by adding key generation step and replacing random variables with quantum registers. Next we introduce a cover message model of unknown distribution and unknown environmental input distribution. In general, it is impossible to construct a perfectly secure classical steganography system over this type of cover message, since any embedding process can introduce distortion into the original cover distribution. Then we present a perfectly secure quantum steganography system over this type of cover message. This system is a modified version of the dense coding system, and can hide information into the entanglement between the cover message and the decoding key. Since no eavesdropper can retrieve the information in this entanglement part, this quantum steganography system is secure against any eavesdropper. In this sense, quantum steganography system can be stronger than classical steganography system.

*natori@qci.jst.go.jp