Uso de Técnicas Cuánticas en Esteganografía

Marcos Curty y David J. Santos

Abstract—**Information Hiding is an emerging research area which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography. Using some fundamental ideas from Quantum Information Processing, such as incompatible quantum measurements and quantum dense coding, we show how to increase the security and the capacity of classical steganographic methods based on the substitution of the redundant parts of a data set. First we address the simple case of pure steganography, that can be quantum-mechanically enhanced without the use of entanglement. Later on we consider secret-key steganography. In this case, physically-based security can be accomplished only if entanglement is used.**

Keywords— **Steganography, information hiding, quantum information processing, quantum cryptography, quantum dense coding.**

I. Introducción

Por esteganografía [1] se entiende el conjunto de técnicas cuyo objetivo es ocultar la existencia de una comunicación secreta, empleando para ello canales subliminales. La información secreta se inserta en un mensaje inocuo, denominado "cover message", para formar el "stego object" que es transmitido. Se pueden distinguir tres clases de protocolos esteganográficos [2]: Esteganografía pura, esteganografía de clave secreta y esteganografía de clave pública. En el primer caso es necesario que el algoritmo de inserción y extracción del mensaje secreto sólo sea conocido por los usuarios legítimos de la comunicación. En esteganografía de clave secreta una clave controla el acceso a la información. Por último, en esteganografía de clave pública se requiere el empleo de dos claves, una privada y otra pública.

En la última década se ha constatado que la información es una entidad física y, como tal, puede ser estudiada empleando una teoría de naturaleza física como la Teoría Cuántica. La disciplina resultante, denominada Teoría Cuántica de la Información, estudia el procesado y transmisión de información codificada en estados cuánticos (para una revisión de esta teoría, veáse [3]). El primer campo en el que se ha aplicado esta nueva disciplina ha sido la criptografía [4], [5]. La criptografía cuántica basa su seguridad en las leyes de la naturaleza reveladas por la Teoría Cuántica, en lugar de en suposiciones no probadas sobre complejidad computacional, como es el caso de la criptografía clásica.

En este artículo se mostrará cómo, empleando conceptos sencillos de Teoría Cuántica de la Información, también es posible incrementar la seguridad y capacidad de los métodos esteganográficos clásicos (puros y de clave secreta) basados en técnicas de substitución [2].

Marcos Curty (mcurty@com.uvigo.es) y David J. Santos (dsantos@com.uvigo.es) pertenecen al Departamento de Tecnologías de las Comunicaciones, Universidad de Vigo, Campus Universitario s/n. E-36200 Vigo.

II. Esteganografía Pura

En el caso de esteganografía pura, la idea es emplear, para codificar la información secreta y la perteneciente al "cover message", estados cuánticos correspondientes a medidas cuánticas incompatibles. En Mecánica Cuántica dos medidas se denominan incompatibles si sus respectivos observables no conmutan [6].

Considérese el siguiente escenario esteganográfico: Alice codifica un determinado mensaje de N bits mediante N qubits [7], y lo envía a Bob y Charlie. En la codificación se emplea la base natural $\{|0\rangle, |1\rangle\}$ ($|0\rangle$ representa el bit clásico '0' y $|1\rangle$ el bit clásico '1'). En recepción Bob y Charlie simplemente realizan la medida cuántica $\hat{A} = a_0|0\rangle\langle 0| + a_1|1\rangle\langle 1|$ y extraen la información enviada. Supóngase ahora que previamente Alice y Bob acuerdan establecer una comunicación secreta a través de un canal subliminal. Para ello, deciden codificar un mensaje secreto, que se supondrá de M bits, en una base cuántica diferente. En lugar de enviar la secuencia de N qubits anterior, codifican el "cover message" en la base natural y, empleando algún método de substitución clásico, introducen el mensaje secreto codificado en una base compuesta por los autovectores de un observable $\hat{B}$ incompatible con $\hat{A}$. Evidentemente, para extraer la información, Bob debe emplear el observable $\hat{B}$. Sin embargo, Charlie, desconocedor de la existencia del canal subliminal, medirá todo el "stego object" con el observable $\hat{A}$. Cabe destacar que debido al carácter incompatible de ambos observables, Charlie producirá, con su medida, la destrucción del mensaje secreto, introduciendo en promedio, como máximo, $M/2$ bits de ruido. Este hecho constituye una clara ventaja respecto a los métodos esteganográficos clásicos, ya que cualquier conocimiento a posteriori, por parte de Charlie, de la existencia de un canal subliminal y del algoritmo de inserción y extracción de la información (el método clásico de substitución empleado y la base utilizada para codificar el mensaje secreto) no permite acceder a la información oculta. Sin embargo, en los métodos clásicos el conocimiento del algoritmo empleado compromete la seguridad de todos los mensajes previamente enviados.

III. Esteganografía de Clave Secreta

El "entanglement" es posiblemente uno de los conceptos más intrigantes e interesantes de la Teoría Cuántica. Un sistema cuántico compuesto se dice "entangled" cuando su estado no puede verse como la yuxtaposición de los estados de los subsistemas que lo componen. En esta sección se mostrará que esta propiedad, junto con el concepto de códigos densos cuánticos [8], puede ser empleada para ocultar información de forma completamente segura, e introduciendo menos ruido en el "stego object".

Supóngase que Alice y Bob disponen, como clave este-

ganográfica, de $M/2$ pares de qubits en un estado cuántico máximamente "entangled"; esto es, cada uno posee un qubit de cada pareja. En particular, se considerará que el estado cuántico de cada par, $|\psi\rangle_{A_i,B_i}$ con $i = 1 \ldots M/2$, es uno de los elementos de la base de Bell: $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$, donde

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)\,, \tag{1}$$

y

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)\,. \tag{2}$$

Resulta inmediato comprobar que si Alice o Bob realizan, sobre cada uno de sus qubits de la clave, una de las siguientes cuatro operaciones unitarias: (i) no se efectúa ningún cambio en el estado cuántico, (ii) se transforma localmente $|0\rangle$ en $|1\rangle$ y viceversa, (iii) se convierte localmente $|0\rangle$ en $-|0\rangle$ sin modificar $|1\rangle$, (iv) se aplican las dos últimas operaciones; se consigue transformar un estado de Bell en otro estado de Bell.

Con estos conceptos en mente, supóngase que Alice y Bob desean establecer un canal subliminal. Siguiendo la notación introducida en la Sección II, para codificar cada bit del "cover message", Alice emplea un qubit en un estado $|0\rangle$, si el bit original es '0', y en un estado $|1\rangle$, si el bit es '1'. En cuanto a los M bits del mensaje secreto, Alice realiza sobre cada uno de sus qubits de la clave, una de las cuatro transformaciones unitarias anteriores y los inserta, empleando cualquier método de substitución clásico, en el "cover message". Cuando Bob recibe el "stego object", realiza una medida ortogonal (proyectando sobre la base de Bell) en cada uno de los pares "entangled" que constituyen la clave, determinando así las operaciones efectuadas por Alice. Como hay cuatro posibles transformaciones por cada par, es posible transmitir dos bits secretos en cada qubit. Este aumento de la capacidad del canal subliminal, en comparación con los métodos clásicos, se puede considerar como una disminución del 50% en el ruido introducido en el "stego object". Esto implica que la detección del canal subliminal resulta mucho más difícil. Además, este protocolo cuántico también se diferencia de sus equivalentes clásicos en otra cuestión sumamente importante. Como ya se ha mencionado, las técnicas esteganográficas de clave secreta basan su seguridad en la clave compartida por Alice y Bob. Esta información sirve de filtro para restringir la extracción del mensaje secreto oculto en el "stego object" a aquellas partes que la conocen. Sin embargo, cuando se emplea una clave clásica no se tiene garantizado en absoluto que ésta sólo es conocida por los usuarios legítimos. Este problema siempre está presente en la criptografía clásica. En principio, Charlie podría acceder a la clave y copiarla sin dejar ninguna evidencia de ello. Empleando "entanglement", y teniendo en cuenta la imposibilidad de copiar estados cuánticos desconocidos, esto resulta imposible.

IV. Robustez de las Técnicas Cuánticas

Un sistema esteganográfico se denomina robusto si resulta díficil modificar el contenido del mensaje secreto sin realizar excesivos cambios en el "stego object". Se trata de un requisito bastante deseable, y quizás la gran desventaja de los métodos expuestos, en los que la mera presencia de un intruso pasivo destruye la información insertada. En el protocolo propuesto para esteganografía pura, ya se ha visto que una medida no deseada (con un observable incompatible con los datos secretos) produce la destrucción de la información oculta. Por otra parte, cuando se emplea "entanglement" como clave, debe tenerse en cuenta que cualquier medida local efectuada sobre el "stego object" conlleva la destrucción del entanglement, y con él también la posibilidad de recuperar el mensaje secreto.

Estos resultados refuerzan la hipótesis [2] sobre el carácter antagónico de los sistemas esteganográficos seguros y los sistemas robustos; lo que,, en la práctica, conlleva que estas técnicas cuánticas deban ser complementadas con métodos de autentificación de mensajes.

V. Conclusiones

En este artículo se ha mostrado cómo combinando conceptos fundamentales en esteganografía clásica, como las técnicas de substitución, con otros de procesado cuántico de la información, como medidas cuánticas incompatibles, "entanglement", y códigos densos cuánticos, es posible establecer canales subliminales seguros y de mayor capacidad. En el caso de esteganografía pura, las medidas cuánticas incompatibles proporcionan un buen mecanismo para ocultar información, aunque la seguridad obtenida en esta clase de protocolos no es física, sino que depende del conocimiento o no del algoritmo concreto utilizado (el método clásico de substitución y la base que codifica el mensaje secreto). La utilización, como clave, de estados cuánticos "entangled" resulta fundamental para lograr métodos esteganográficos de clave secreta absolutamente seguros. A su vez, se ha mostrado cómo simultáneamente se puede duplicar la capacidad de un canal subliminal.

References

[1] D. Kahn, *The codebreakers—The story of secret writing*, Scribner, New York, 1996.

[2] S. Katzenbeisser y F.A.P. Petitcolas, *Information hiding techniques for steganography and digital watermarking*, Computer Security. Artech House, Boston, 2000.

[3] C.H. Bennett y P.W. Shor, "Quantum information theory," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2724–2742, october 1998.

[4] C.H. Bennett y G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, New York, december 1984, pp. 175–179, IEEE Press.

[5] C.H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, pp. 3121–3124, may 1992.

[6] C. Cohen-Tannoudji, B. Diu, y F. Laloë, *Quantum Mechanics*, Wiley, New York, 1977.

[7] J. Mullins, "The topsy turvy world of quantum computing," *IEEE Spectrum*, pp. 42–49, february 2001.

[8] A. Barenco y A.K. Ekert, "Dense coding based on quantum entanglement," *Journal of Modern Optics*, vol. 42, pp. 1253–1259, 1995.