ASEGURAMIENTO DE DATOS DIGITALES EN ARQUEOASTRONOMÍA

José Isaac Zablah Avila
Facultad de Ciencias Espaciales
Universidad Nacional Autónoma de Honduras
Email: mrzablah@yahoo.com

RESUMEN

Este trabajo se centra en la necesidad inherente de proteger datos inéditos de origen arqueoastronómico, resultantes de investigaciones. Estos datos son clasificados y la mayoría de ellos se encuentran digitalizados, usualmente están almacenados en un ordenador para su procesamiento y manipulación posterior. La finalidad de este trabajo es proponer un método efectivo para el manejo seguro de los datos digitales, recabados en distintas actividades arqueoastronómicas, todo ello mediante el empleo de técnicas de cifrado.

Palabras Clave: Seguridad de la Información, Arqueoastronomía, Cifrado.

ABSTRACT

This work focuses on the inherent need to protect archaeoastronomical unpublished data, resulting from research. These data are classified and most of them are digitized, they are usually stored in a computer for processing and subsequent handling. The purpose of this paper is to propose an effective method for the safe handling of digital data, collected in different archaeoastronomical activities, all secured by using encryption techniques.

Key Words: Information Security, Archaeoastronomy, Encryption.

INTRODUCCIÓN

Vivimos en la era de la información, lo cual ha llegado con el aumento del número de computadoras personales y el crecimiento acelerado de los usuarios de las mismas, creando así una sociedad centrada y basada en la información (Redha Mani, Radha Krishna; 2007). A esto hay que agregar el incremento de la cobertura de la red Internet, proveyendo así acceso a servicios y aplicaciones que permiten manejar una gran cantidad de datos; en estos tiempos es posible compartir datos a velocidades nunca antes alcanzadas por la humanidad (Redha Mani, Radha Krishna; 2007 & Stalling, 2005).

Desafortunadamente, estos avances han abierto nuevas amenazas a la seguridad de las personas y de las redes de información a todos los niveles, siendo esto una vía para amenazar computadoras y los datos almacenados en ellas, a partir de ataques que pueden destruir, modificar e inutilizar los sistemas computacionales. Actualmente, las amenazas a la privacidad han permitido a extraños tener accesos no autorizado a datos, que posteriormente se utilizan para controlar otros servicios y ordenadores (Stallings, 2005 & Huth, 2001).

Al momento que un investigador colecta muchos datos, se incurre en la necesidad de compartir éstos con los miembros de los equipos de trabajo o colegas en distintas localidades geográficas. Estos datos usualmente viajan por redes públicas o por medios digitales, los cuales no siempre

resultan seguros. Es posible que alguien tenga acceso a esos datos y pueda emplearlos con distintos fines, sin previo consentimiento; y más grave aún, antes que sean publicados. En esta situación, los autores no tienen ninguna administración de sus derechos digitales, con lo cual pierden control del uso y manejo de su información.

Para minimizar las amenazas existentes y asociadas al mundo digital, se han desarrollado a través del tiempo técnicas para la protección de datos, muchos de estos métodos se han elaborado con el fin de proteger aspectos específicos o situaciones definidas. Dado a lo anterior, nace la importancia de poder determinar si alguna de esas técnicas (o varias de ellas) pueden ser empleadas en conjunto para asegurar datos resultantes de investigaciones y sobre todo si entre todas pueden conformar un método efectivo y eficaz para emplearse en arqueoastronomía con la finalidad primordial de proteger los derechos digitales de sus autores.

En esta investigación, se ha desarrollado una serie de lineamientos confiables y prácticos, para lograr asegurar la integridad de datos digitales usados en investigaciones arqueoastronómicas, en lo que refiere a la forma cómo sus usuarios comparten y manipulan información.

PROTEGIENDO LOS DATOS

En arqueoastronomía, los datos que se generan se pueden clasificar en dos tipos básicos: los primeros, como *documentos ofimáticos* que son aquellos generados a partir del empleo de aplicaciones orientadas al procesamiento de textos, elaboración de hojas de cálculo y elaboración de diapositivas. Los segundos son los de *tipo gráfico o imágenes*. En cualquiera de los casos, se colocan datos valiosos para los investigadores.

Los datos usualmente carecen de protección; éstos se almacenan en ordenadores, en medios transportables o se transmiten por redes públicas. A los ordenadores puede accederse mediante uso personal o a través de una red. Los medios de almacenamiento pueden colocarse en otros ordenadores y los datos contenidos allí pueden duplicarse sin ningún tipo de restricción. Los que se transmiten mediante una red pueden capturarse en su transmisión o manipularse de formas, a veces hasta inimaginables, en su destino.

Dado esto, se propone un flujo como método de protección, éste se puede visualizar en la figura 1, que se muestra a continuación:

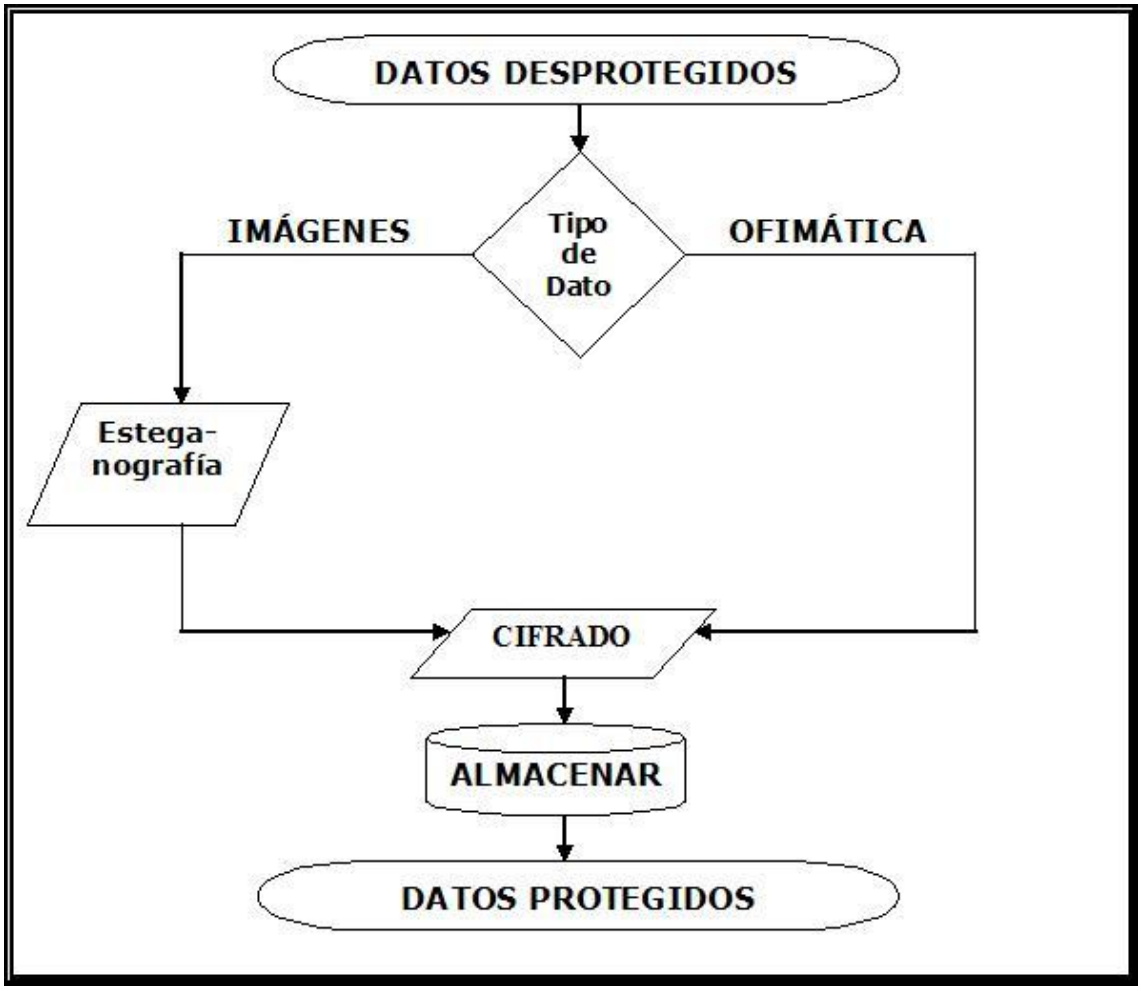

Figura 1. Flujo propuesto para el Aseguramiento de Datos.

Al realizar sus actividades, los investigadores manejan datos que no están protegidos. Es necesario clasificar los datos, ya que si son del tipo de imágenes digitales, es posible almacenar en éstas, datos descriptivos de ellas mismas, o en su defecto, otro documento. A esta técnica se le conoce como esteganografía. Tanto los datos gráficos como los ofimáticos deben cifrarse para ser almacenados y/o transmitidos (Churchhouse, 2001). Para ello se sugiere emplear lo que se conoce como cifrado. Las técnicas más útiles para fines arqueoastronómicos son el cifrado simétrico y el asimétrico.

Para comprender la utilidad del cifrado es necesario partir de que hay un emisor y un receptor (sobre todo en el caso que los datos se transmitan a otra persona) (Stallings, 2005 & Churchhouse, 2001). En el cifrado simétrico existe una clave (contraseña) que se utilizará tanto para cifrar como para descifrar los datos (Konheim, 2007 & Huth, 2001 & Burnett, Pain; 2001). Este proceso incrementa y basa su seguridad en la complejidad de la clave y en la forma como ésta sea manipulada. En la figura 2, se describe el flujo de los datos y su cifrado partiendo del emisor (sin cifrar) al receptor (cifrado).

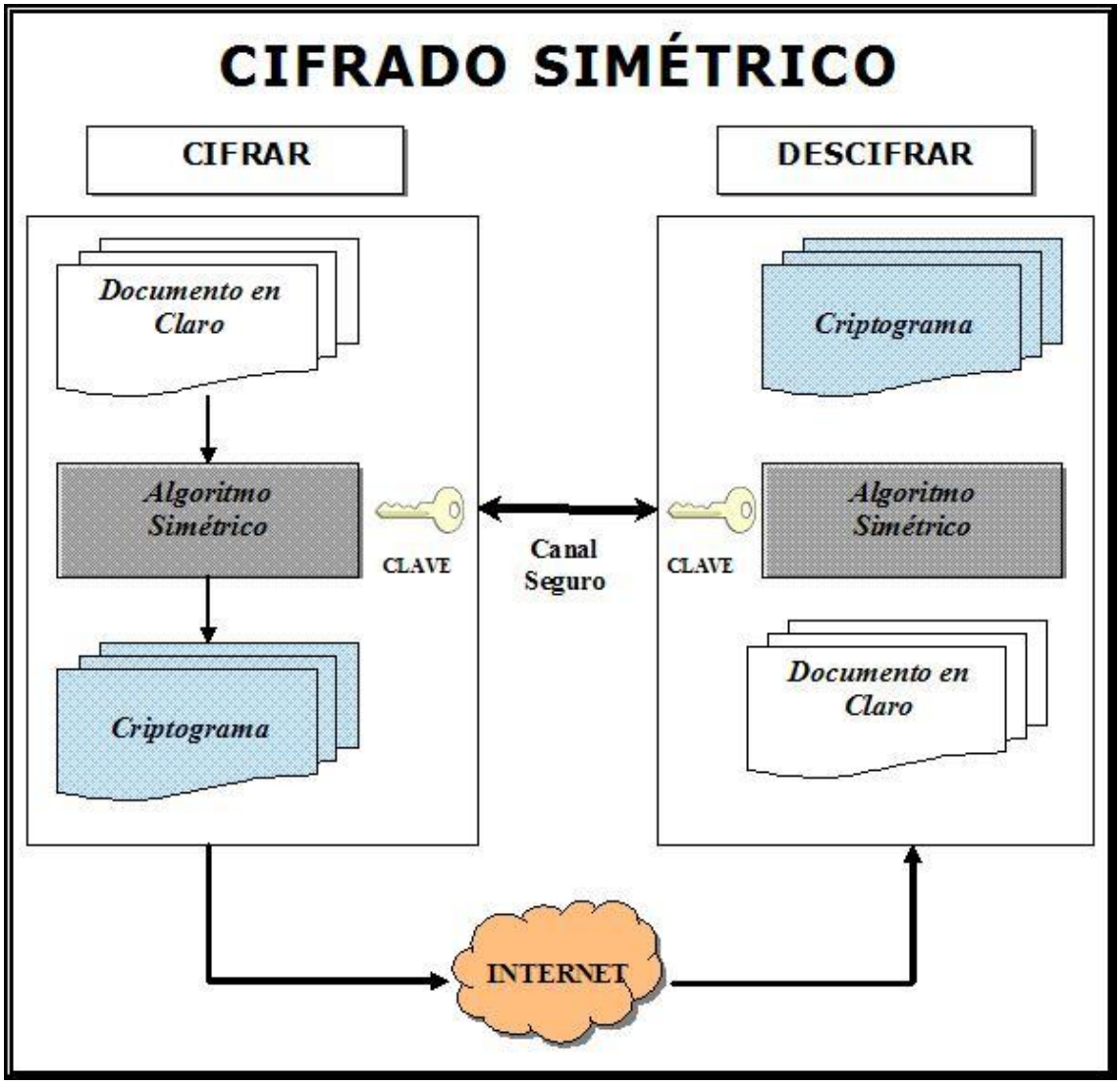

Figura 2. Cifrado Simétrico

Tal como se muestra en la figura 2, los datos están inicialmente sin cifrar. Al utilizar una herramienta de software, se emplea un algoritmo simétrico y se proporciona una clave. El resultado es el documento cifrado, el cual recibe el nombre de criptograma. Estos datos pueden almacenarse y transmitirse sin la posibilidad de que alguien pueda manipularlos. Para descifrar los datos, se emplea el mismo proceso, sólo que a la inversa.

En el caso de necesitar una mayor seguridad, sobre todo si los datos necesitan ser transmitidos electrónicamente, el método de cifrado asimétrico brinda un mayor nivel de seguridad (Burnett, Pain; 2001 & Smith, Marchesini; 2007 & Huth. 2001 & Goldreich, 2005). Esta técnica se basa en utilizar un sistema de llave privada y llave pública. Su empleo se basa en generar dos llaves, una pública que se le da a conocer a todo aquel que desea enviar un mensaje o documento, que cifra los datos con esa clave; y otra que es la llave privada, la cual sólo el destinatario conoce y la emplea para descifrar el mensaje que se le ha enviado, cifrando con llave pública. Es oportuno aclarar que en esta técnica, el receptor deberá haber generado previamente el juego de llaves para poderle enviar mensajes cifrados. El empleo de esta técnica se muestra en la figura 3, que se presenta a continuación:

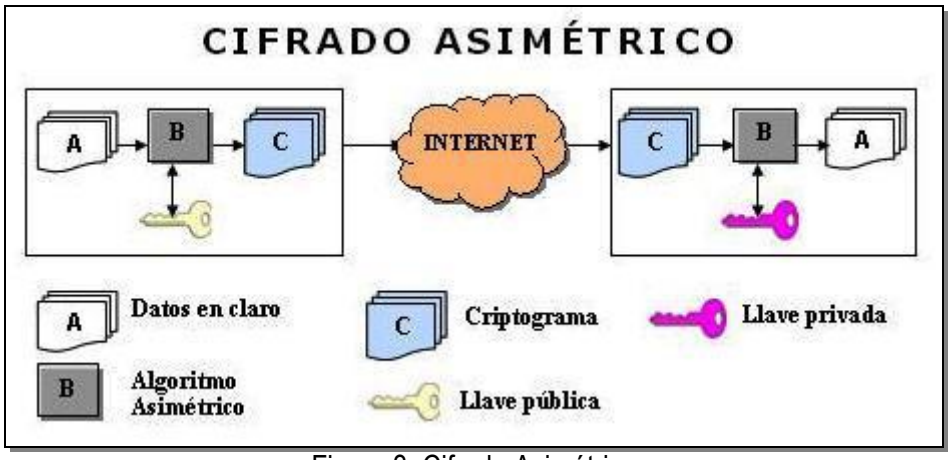

Figura 3. Cifrado Asimétrico

APLICACIÓN DE LOS MÉTODOS

Para las demostraciones, he preferido hacer uso de una plataforma del tipo IBM PC y compatible basado en arquitectura Intel x86 de 32bit y utilizar el sistema operativo Microsoft Windows XP, debido a que es la configuración de recursos de TI (Tecnologías de la Información) más popular entre los arqueoastrónomos al momento de elaborar este escrito. En caso de emplease otra plataforma, tenga la plena seguridad que existen herramientas similares para implementar y utilizar estas técnicas.

Esteganografía

Para hacer uso de esta técnica se puede emplear una serie de herramientas existentes (algunas de ellas ya se encuentran incorporadas en los sistemas operativos); para esta demostración he decido emplear la herramienta Xiao Stenography 2.6.1.

Luego de instalar la herramienta siguiendo las instrucciones proporcionadas por el fabricante, he seleccionado una imagen de origen arqueoastronómico y un archivo de datos que deseamos ocultar; el detalle de estos archivos se muestra a continuación en la figura 4:

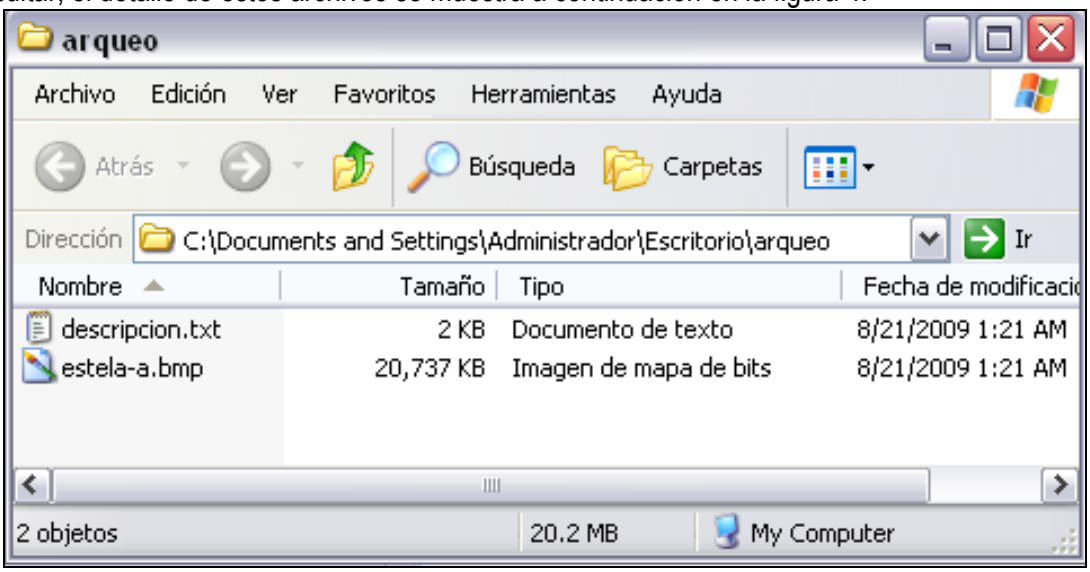

Figura 4. Archivos a utilizar en la demostración, se detalla su tipo y tamaño en kilobytes.

Para ocultar la información en la imagen “estela-a.bmp”, procedemos de la forma siguiente: *primero*, abrimos la Xiao Stenography y seleccionamos la opción “Agregar Archivos”; *segundo* seleccionamos la imagen a utilizar; *tercero* seleccionamos el archivo a ocultar; *cuarto* seleccionamos el algoritmo de cifrado junto con la contraseña a utilizar y finalmente salvamos el archivo resultante que contiene el archivo oculto. La secuencia de estos pasos se muestra en la figura 5.

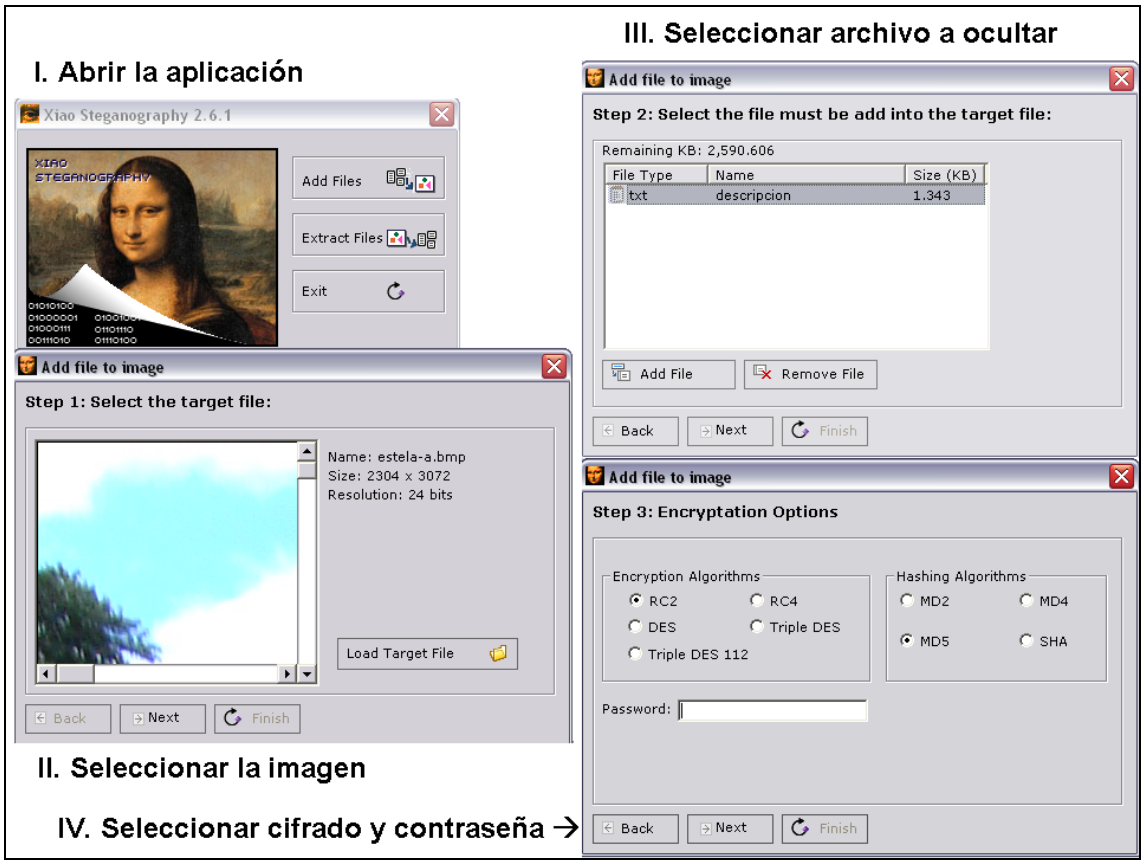

Figura 5. Secuencia para ocultar un archivo, empleado Xiao Stenography.

Al obtener la imagen con el archivo oculto (que he nombrado como “estela-a (encriptado).bmp” y compararla con la imagen original observamos que el tamaño del archivo y su visualización no ha sido alterado en lo más mínimo, tal como se muestra en la figura 6.

Figura 6. Comparación de archivos de imagen, antes y después de utilizar técnicas estenográficas.

Si se desea extraer el documento oculto de la imagen, se siguen los pasos siguientes: *primero,* abrir la herramienta Xiao Stenography y pulsar sobre la opción “Extraer Archivos”; *segundo*, seleccionamos la imagen que contiene el archivo oculto; *tercero*, seleccionamos el archivo oculto a extraer, colocando la contraseña y salvando en una carpeta el archivo resultante. En la figura 7, se muestran las interfaces de los dos últimos pasos.

Figura 7. Secuencia para extraer el archivo oculto, empleado Xiao Stenography. Aquí se muestran el segundo y tercer paso a seguir.

El archivo resultante se muestra a continuación en la figura 8; este es igual al original que fue almacenado en la imagen.

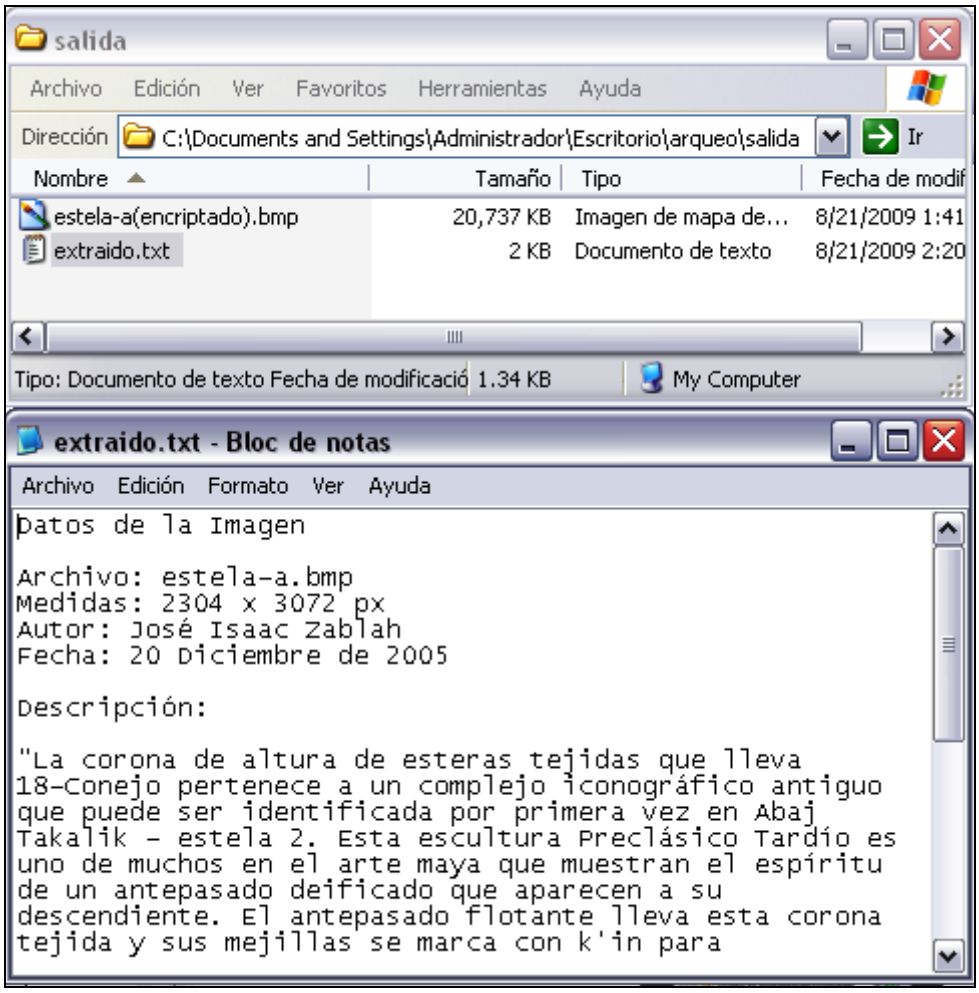

Figura 8. Archivo que se ocultó en la imagen después de su extracción.

Cifrado Simétrico

Para realizar esta demostración, he seleccionado la herramienta AxCrypt 1.6.1. Una vez que se ha instalado la aplicación, se colocará un menú contextual en el puntero del ratón (este es el menú que aparece usualmente al presionar el botón derecho del ratón). Para hacer uso de esta herramienta, se deberá ubicar sobre el archivo a cifrar, y hacer click derecho con el ratón; luego deberá seleccionar la opción en el menú contextual que dice “AxCrypt” y la sub opción “Cifrar”; observar estos pasos detallados en la figura 9.

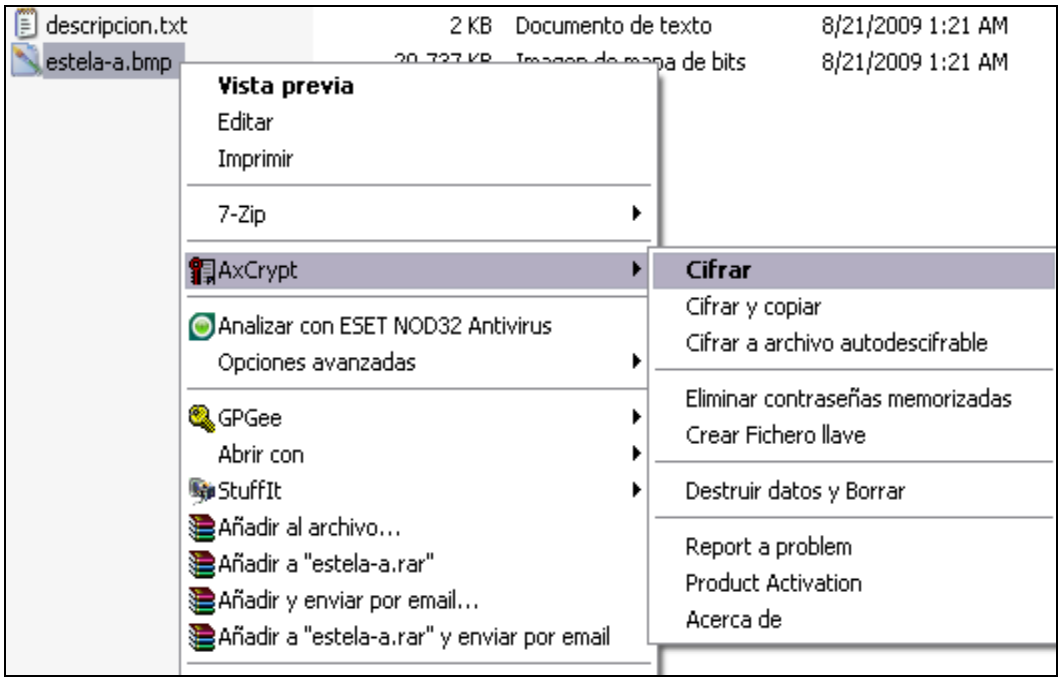

Figura 9. Menú contextual de AxCrypt, y su opción de cifrar. .

Al hacer lo anterior, aparecerá una ventana que pide introducir una contraseña y que ésta se verifique en la misma ventana (Ver figura 10). Finalmente se confirmará la operación y AxCrypt cifrará el archivo.

Figura 10. Parámetros para el cifrado usando AxCrypt.

El archivo cifrado, cambia de extensión y de formato de manera que no es posible visualizar su contenido debido a que ha sido protegido, lo anterior se evidencia en la figura 11.

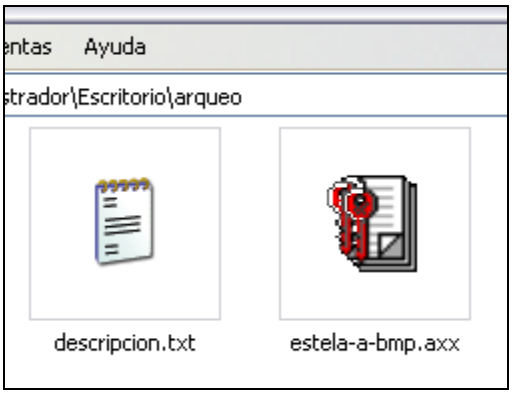

Figura 11. El archivo seleccionado una vez cifrado ha cambiado por completo sus propiedades y ha quedado protegido.

Para recuperar el archivo, se procede eligiendo la opción descifrar en el menú contextual de AxCrypt, luego se le solicitará la contraseña con la cual se cifró el archivo; finalmente se obtendrá el archivo original; el detalle de esta operación se muestra en la figura 12.

Figura 12. Proceso de descifrado empleando AxCrypt de un archivo.

CONCLUSIÓN

La combinación de las técnicas de seguridad, descritas aquí e implementadas en conjunto, protegen de manera efectiva los datos de origen arqueoastronómico. La utilización de estas técnicas permitirá a los investigadores proteger datos inéditos de cualquier plagio o manipulación, asegurando de esta manera todos los derechos digitales de sus autores.

Si bien es cierto que existe una diversidad de técnicas para proteger datos, los aquí expuestos, seleccionados y adaptados han sido el resultado de la realización de variadas pruebas de diversas técnicas, siendo las aquí propuestas las más prácticas de implementar, partiendo de que los arqueoastrónomos necesitan un método práctico para asegurar sus datos.

Con el advenimiento de la revolución en los derechos digitales, es probable que en algún momento todas estas técnicas se vean reemplazadas por firmas digitales basadas en biometría, o en su defecto, a través de certificados digitales, provenientes de autoridades emisoras de certificados de confianza, todo ello como parte de una autoridad de gobierno digital.

BIBLIOGRAFÍA

1. Churchhouse, Robert. *Codes and Ciphers: Julius Ceasar, the Enigma and the Internet.* Cambridge, Inglaterra: Cambrige University Press; 2001.

2. Delfs, Hans y Knebl Helmut. *Introduction to Cryptography.* 2da.ed. Nuremberg, Alemania: Springer; 2007.

3. Goldreich, Oded. *Foundations and Trends in Theoretical Computer Science*. Massachusetts, EEUU: Now Publishers Inc; 2005.

4. Huth, Michael. *Secure Communicating Systems: Design, Analysis, and Implementation.* Cambridge, Inglaterra: Cambridge University Press; 2001.

5. Konheim, Alan G. *Computer Security and Cryptography.* New Jersey, EEUU: Wiley-Interscience; 2007.

6. Radha Mani, G. and Radha Krishna Rao G.S.V. *Web Services Security and E-Bussines*. EEUU: Idea Group Publishing. 2007.

7. Smith, Sean and Marchesini, John. *The Craft of System Security.* Massachusetts, EEUU: Addison Wesley Professional – Pearson Education; 2007.

8. Stallings, William. *Cryptography and Network Security Principles and Practices.* 4.ed. New Jersey, EEUU: Prentice Hall; 2005.