Abstract

The extraordinary increase of new information technologies, the development of Internet of Things, the electronic commerce, the social networks, mobile or smart telephony and cloud computing and storage, have provided great benefits in all areas of society. Besides this fact, there are new challenges for the protection and privacy of information and its content, such as the loss of confidentiality and integrity of electronic documents and communications. This is exarcebated by the lack of a clear boundary between the personal world and the business world as their differences are becoming narrower.

In both worlds, i.e the personal and the business one, Cryptography has played a key role by providing the necessary tools to ensure the confidentiality, integrity and availability both of the privacy of the personal data and information. On the other hand, Biometrics has offered and proposed different techniques with the aim to assure the authentication of individuals through their biometric traits, such as fingerprints, iris, hand geometry, voice, gait, etc.

Each of these sciences, Cryptography and Biometrics, provides tools to specific problems of the data protection and user authentication, which would be widely strengthen if determined characteristics of both sciences would be combined in order to achieve common objectives. Therefore, it is imperative to intensify the research in this area by combining the basics mathematical algorithms and primitives of Cryptography with Biometrics to meet the growing demand for more secure and usability techniques which would improve the data protection and the user authentication. In this combination, the use of cancelable biometrics makes a cornerstone in the user authentication and identification process since it provides revocable or cancelation properties to the biometric traits.

The contributions in this thesis involve the main aspect of Biometrics, i.e. the secure and efficient authentication of users through their biometric templates, considered from three different approaches. The first one is designing a fuzzy crypto-biometric scheme using the cancelable biometric principles to take advantage of the fuzziness of the biometric templates at the same time that it deals with the intra- and inter-user variability among users without compromising the biometric templates extracted from the legitimate users.

The second one is designing a new Similarity Preserving Hash Function (SPHF), currently widely used in the Digital Forensics field to find similarities among different files to calculate their similarity level.

The function designed in this research work, besides the fact of improving the results of the two main functions of this field currently in place, it tries to expand its use to the iris template comparison.

Finally, the last approach of this thesis is developing a new mechanism of handling the iris templates, considering them as signals, to use the Walsh-Hadamard transform (complemented with three other algorithms) to compare them. The results obtained are excellent taking into account the security and privacy requirements mentioned previously.

Every one of the three schemes designed have been implemented to test their operational efficacy in situations that simulate real scenarios: The fuzzy crypto-biometric scheme and the SPHF have been implemented in Java language, while the process based on the Walsh-Hadamard transform in Matlab.

The experiments have been performed using a database of iris templates (CASIA-IrisV2) to simulate a user population. The case of the new SPHF designed is special since previous to be applied i to the Biometrics field, it has been also tested to determine its applicability in the Digital Forensic field comparing similar and dissimilar files and images.

The ratios of efficiency and effectiveness regarding user authentication, i.e. False Non Match and False Match Rate, for the schemes designed have been calculated with different parameters and cases to analyse their behaviour.

Resumen

El extraordinario auge de las nuevas tecnologías de la información, el desarrollo de la Internet de las Cosas, el comercio electrónico, las redes sociales, la telefonía móvil y la computación y almacenamiento en la nube, han proporcionado grandes beneficios en todos los ámbitos de la sociedad. Junto a éstos, se presentan nuevos retos para la protección y privacidad de la información y su contenido, como la suplantación de personalidad y la pérdida de la confidencialidad e integridad de los documentos o las comunicaciones electrónicas. Este hecho puede verse agravado por la falta de una frontera clara que delimite el mundo personal del mundo laboral en cuanto al acceso de la información.

En todos estos campos de la actividad personal y laboral, la Criptografía ha jugado un papel fundamental aportando las herramientas necesarias para garantizar la confidencialidad, integridad y disponibilidad tanto de la privacidad de los datos personales como de la información. Por otro lado, la Biometría ha propuesto y ofrecido diferentes técnicas con el fin de garantizar la autentificación de individuos a través del uso de determinadas características personales como las huellas dáctilares, el iris, la geometría de la mano, la voz, la forma de caminar, etc.

Cada una de estas dos ciencias, Criptografía y Biometría, aportan soluciones a campos específicos de la protección de datos y autentificación de usuarios, que se verían enormemente potenciados si determinadas características de ambas ciencias se unieran con vistas a objetivos comunes. Por ello es imperativo intensificar la investigación en estos ámbitos combinando los algoritmos y primitivas matemáticas de la Criptografía con la Biometría para dar respuesta a la demanda creciente de nuevas soluciones más técnicas, seguras y fáciles de usar que potencien de modo simultáneo la protección de datos y la identificacíón de usuarios. En esta combinación el concepto de biometría cancelable ha supuesto una piedra angular en el proceso de autentificación e identificación de usuarios al proporcionar propiedades de revocación y cancelación a los ragos biométricos.

La contribución de esta tesis se basa en el principal aspecto de la Biometría, es decir, la autentificación segura y eficiente de usuarios a través de sus rasgos biométricos, utilizando tres aproximaciones distintas:

1. Diseño de un esquema criptobiométrico borroso que implemente los principios de la biometría cancelable para identificar usuarios lidiando con los problemas acaecidos de la variabilidad intra e inter-usuarios.

2. Diseño de una nueva función hash que preserva la similitud (SPHF por sus siglas en inglés). Actualmente estas funciones se usan en el campo del análisis forense digital con el objetivo de buscar similitudes

en el contenido de archivos distintos pero similares de modo que se pueda precisar hasta qué punto estos archivos pudieran ser considerados iguales. La función definida en este trabajo de investigación, además de mejorar los resultados de las principales funciones desarrolladas hasta el momento, intenta extender su uso a la comparación entre patrones de iris.

3. Desarrollando un nuevo mecanismo de comparación de patrones de iris que considera tales patrones como si fueran señales para compararlos posteriormente utilizando la transformada de Walsh-Hadarmard. Los resultados obtenidos son excelentes teniendo en cuenta los requerimientos de seguridad y privacidad mencionados anteriormente.

Cada uno de los tres esquemas diseñados han sido implementados para poder realizar experimentos y probar su eficacia operativa en escenarios que simulan situaciones reales: El esquema criptobiométrico borroso y la función SPHF han sido implementados en lenguaje Java mientras que el proceso basado en la transformada de Walsh-Hadamard en Matlab.

En los experimentos se ha utilizado una base de datos de imágenes de iris (CASIA) para simular una población de usuarios del sistema. En el caso particular de la función de SPHF, además se han realizado experimentos para comprobar su utilidad en el campo de análisis forense comparando archivos e imágenes con contenido similar y distinto. En este sentido, para cada uno de los esquemas se han calculado los ratios de falso negativo y falso positivo.