REZUMATUL TEZEI DE DOCTORAT

SECURITATEA INFORMAȚIEI FOLOSIND TEHNICI DE BIOCRIPTOGRAFIE

Autor: Ing. Marius-Alexandru VELCIU
E-mail: alexandruvelciu@gmail.com , Tel: 0745037750
Conducător de doctorat: Prof. Dr. Ing. Victor-Valeriu PATRICIU

Teza de doctorat vizează analiza și evidențierea principalelor beneficii puse la dispoziție de sistemele biocriptografice, prin comparație cu sistemele biometrice clasice. Sunt vizate, în primul rând, aspectele de țin de nivelul de securitate, precum și cele referitoare la modalitățile de reducere a complexității computaționale a unui astfel de sistem.

În *primul capitol* este realizată o prezentare a cadrului general al sistemelor biocriptografice, urmată de o trecere în revistă a principalelor obiective ale lucrării și de rezumatul lucrării pe capitole.

Capitolul 2 prezintă tematica sistemelor biometrice, pornind de la rolul acestora, ce poate fi de identificare sau autentificare a utilizatorilor înrolați, continuând cu arhitectura generală a unui astfel de sistem și metodele de evaluare asociate, dintre care cele mai importante sunt ratele de eroare. Capitolul se încheie cu descrierea importanței sistemelor biometrice, expusă în contrast cu principalele vulnerabilități întâlnite la nivelul unui astfel de sistem.

Cel de-al treilea capitol introduce domeniul Biocriptografiei și principalele moduri de operare ale sistemelor biocriptografice, ce permit generarea, blocarea / recuperarea de chei, precum și îmbinarea de chei (criptarea biometrică). În continuare, este detaliat procesul de criptare biometrică și sunt evidențiate principalele beneficii ale utilizării acestuia.

În cadrul *celui de-al patrulea capitol*, sunt prezentate principiile celui mai cunoscut algoritm de criptare biometrică, schema biocriptografică Fuzzy Vault. De asemenea, este descrisă și evaluată implementarea schemei Fuzzy Vault propusă pentru biometrica voce, bazată pe metoda analizei cepstrale pentru parametrizarea vorbirii.

Capitolul 5 prezintă o serie de modalități de evaluare a algoritmilor biocriptografici. În prima parte a acestuia, sunt descriși principalii parametri specifici schemei Fuzzy Vault, dintre care face parte și ordinul de mărime a puntelor de difuzie, urmând a fi descrisă o modalitate de evaluare a tăriei biocriptogramelor, trecând în revistă și rezultatele experimentale obținute. Cea de-a doua secțiune a capitolului descrie principalele rate de eroare asociate lucrului cu date biometrice, ce pot fi aplicate, cu succes, și în domeniul biocriptografiei.

În cadrul *capitolului 6*, sunt propuse două metode de reducere a complexității computaționale a schemei de criptare biometrică Fuzzy Vault, una axată pe utilizarea codurilor corectoare de erori Reed-Solomon, menită să reducă nivelului computațional din etapa de reconstrucție polinomială, iar cealaltă bazată pe utilizarea biocriptogramelor partajate, în scopul eliminării necesității utilizării punctelor de difuzie.

Capitolul 7 prezintă o modalitate de sporire a nivelului de securitate conferit de schema de criptare biometrică analizată. Este descrisă vulnerabilitatea schemei biocriptografice Fuzzy Vault în fața atacurilor prin corelare, propunându-se o metodă eficientă de reducere a acestui risc, utilizarea hash-urilor biometrice cu „salt".

Capitolul 8 descrie, în început, principalele tipuri de infrastructuri biocriptografice, atât pentru utilizări la scară medie, cât și extinsă. Ulterior, este exemplificat și implementat un astfel de model de infrastructură biocriptografică, menită să faciliteze și securizeze accesul la un mediu de stocare partajat. În cea de-a doua parte a capitolului, este prezentat un protocol biocriptografic de schimbare de mesaje securizate, precum și posibilitatea aplicării acestuia în mediul de mobile computing, fie pentru securizarea accesului la fișierele de pe un dispoztiv mobil, fie pentru criptarea convorbirilor dintre doi interlocutori.

În cadrul *capitolului 9*, este construit un framework biocriptografic pentru securizarea conținutului de pe un dispozitiv mobil ce rulează sistemul de operare Android, folosind senzorul integrat pentru amprentă al acestuia și criptarea simetrică. Acesta propune, practic, un sistem biocriptografic de blocare / deblocare a cheilor, privind accesul la depozitul de chei criptografice al sistemului de operare, precum și posibilitatea prelucrării datelor biometrice într-o zonă securizată a memoriei, dacă se folosește tehnologia Trustzone. Arhitectura generală a framework-ului propus s-a concretizat prin dezvoltarea unei aplicații pentru criptarea fișierelor și a directoarelor de pe un dispozitiv mobil.

Lucrarea se încheie cu trecerea în revistă a concluziilor finale, ce sumarizează întreaga tematică abordată în cadrul lucrării de față, enumerarea contribuțiilor originale ce au fost aduse la aceasta, lista publicațiilor de pe perioada doctoratului, precum și cu bibliografia consultată pe durata întregului proces de cercetare științifică.