

Implementação e avaliação de um aplicativo biométrico utilizando o método Fuzzy Vault e ferramentas open-source

Bruno Guedes Faria, Sandra Maria Dotto Stump

¹Departamento de Engenharia Elétrica – Universidade Presbiteriana Mackenzie (UPM)
01302-090 – São Paulo – SP – Brazil

brunoguedesfaria@gmail.com, sstump@mackenzie.br

Abstract. *Biometric Systems have been remarkably used in the past years, mainly those based on fingerprints. In terms of security, they need the same care which is given to traditional systems that uses cards and passwords. Fuzzy Vault comes in this scenario to provide security to biometric systems, specifically, protecting the stored biometric template. In this present study, the Fuzzy Vault scheme will be developed, and then used to hide a 128 bits secret; the scheme will be used into the context of a biometric application based on fingerprints. Evaluation of security and performance of the application will be shown, and experimental results, common to biometric systems (FRR, GAR, FAR), will also be presented.*

Resumo. *Sistemas biométricos vem sendo utilizados consideravelmente nos últimos anos, principalmente aqueles baseados em impressão digital. No que tange à segurança, necessitam da mesma preocupação que se tem com sistemas tradicionais de senhas e cartões. Fuzzy Vault aparece neste cenário para prover a segurança de sistemas biométricos, particularmente, protegendo o template biométrico armazenado. Neste trabalho será desenvolvido o método Fuzzy Vault, aplicando-o para ocultar um segredo de 128 bits; o método será utilizado dentro do contexto de um aplicativo biométrico de impressão digital. Serão expostas avaliações sobre o desempenho e segurança do aplicativo e também resultados experimentais comuns a sistemas biométricos (FRR, GAR, FAR).*

1. Introdução

O avanço tecnológico vem permitindo que a biometria se torne cada vez mais presente em sistemas que necessitam de identificação pessoal; o voto (Tanzânia e Brasil), a identificação criminal, o acesso lógico (terminais bancários, computadores e smartphones) e físico (instalações e áreas restritas) são alguns exemplos que podem ser citados. Esta crescente adoção de sistemas biométricos apresenta duas principais vantagens: não repudição e conveniência para o usuário [Uludag et al. 2005].

Dentre os tipos de sistemas biométricos, os que utilizam impressão digital são a maioria; dados do IBG (*International Biometric Group*) de 2009 [Maltoni et al. 2009] relatam que estes sistemas, baseados em impressão digital, possuem uma margem de 50% do mercado de sistemas biométricos. A identificação de um indivíduo pela sua impressão digital é a forma mais antiga de biometria [Liu et al. 2011], e mesmo já consolidada, no momento em que se traz esta forma de biometria para mundo computacional e a transforma em um sistema biométrico automatizado, este sistema se torna passível de

ataques como qualquer outro. Devido ao fato de existirem vulnerabilidades, o aspecto da segurança nos sistemas biométricos se torna uma preocupação primordial. Para Jain et al. 2011, um sistema biométrico de impressões digitais possui 8 pontos vulneráveis a ataques, sendo que, o ponto de vulnerabilidade mais crítico é o de armazenagem do *template* e, é o objeto desta pesquisa. Proposto por Juels and Sudan 2002, *Fuzzy Vault* é uma construção criptográfica que une biometria à criptografia com o objetivo de proteção do *template* biométrico de uma impressão digital; atualmente, de acordo com Jain et al. 2011, *Fuzzy Vault* é um dos métodos mais promissores.

Algumas implementações foram propostas para o método de *Fuzzy Vault*, entre elas, Nandakumar et al. 2007, Uludag et al. 2005, Nandakumar et al. 2007, Uludag et al. 2004 e Jeffers and Arakala 2006. A de Jeffers and Arakala 2006 propôs trabalhar com tipos de algoritmos de *matching* para o método *Fuzzy Vault* que, até então, ainda não tinham sido explorados. Entretanto, na implementação destes autores, foram avaliados apenas o *matching* entre as impressões digitais, e não uma implementação completa do método de *Fuzzy Vault*, codificando e decodificando uma chave. Diante dos resultados preliminares positivos destes algoritmos, e de na literatura esta implementação completa ainda não ter sido desenvolvida, constatou-se a possibilidade de realizá-la nesta pesquisa.

Pretende-se implementar e avaliar o método de *Fuzzy Vault* utilizando, para *matching*(combinação ou casamento) de impressões e extração de minúcias, respectivamente, os algoritmos de código aberto, *Bozorth3* e *MINDTCT* [NBIS-EC 2013]. Para *matching* de impressões, o algoritmo *Bozorth3* apresenta semelhanças com os propostos no artigo de [Jeffers and Arakala 2006], onde o algoritmo de *matching* é invariante à translação e rotação. Com o *MINDTCT* é possível realizar extração de minúcias, automaticamente, sem a ajuda de um *expert*(especialista).

2. Método Fuzzy Vault

Proposto por Juels and Sudan 2002, *Fuzzy Vault* esta incluída dentro dos criptosistemas por *key-binding* e, particularmente, consiste de uma construção criptográfica onde tanto o *template* biométrico armazenado quanto a impressão retirada do leitor são protegidas dentro de um cofre (*vault*). Estes autores ilustram o funcionamento de *Fuzzy Vault* da seguinte maneira: Alice possui uma lista de filmes e deseja encontrar alguém que compartilhe de seu gosto por estes; entretanto, ela não quer dividir informações com pessoas que não compartilham de sua preferência. Uma abordagem que poderia adotar é a de criptografar seu telefone utilizando este conjunto de filmes de seu gosto. Sendo assim, apenas uma pessoa que tivesse um gosto similar ao de Alice, poderia descriptografar seu telefone. Como exemplo, se Bob tivesse uma lista de filmes que fosse similar ao de Alice, ele poderia descriptografar o telefone dela e visualizar seu número.

O método *Fuzzy Vault* pode ser mais detalhado da seguinte maneira: suponha que Alice deseje ocultar um segredo k por meio de um conjunto A . Ela seleciona um polinômio p de uma única variável x , sendo que p codifica k de alguma forma, neste caso, atrelando o coeficiente k ao polinômio p . Por exemplo, se o segredo k fosse 1234, o polinômio p codificaria k da seguinte maneira: $1x^3 + 2x^2 + 3x + 4$. O conjunto A seria tratado como elementos de coordenadas x , que seriam substituídos, resultando assim em pontos em um plano e, estes pontos derivados de A seriam os pontos genuínos gerados pela função. Após estes pontos serem gerados, para garantir a segurança do esquema, seriam aplicados *chaff*

points, que são pontos randômicos projetados no mesmo plano dos pontos genuínos. A fusão destes pontos randômicos com pontos genuínos formam uma coleção de pontos R .

Se Bob deseja encontrar este conjunto para ter acesso ao segredo k , utilizando o seu conjunto B , então ele só terá sucesso se conseguir encontrar em R um número de pontos que coincidam em grande número com A , que são os pontos genuínos. Uma vez que no conjunto B não existam pontos que coincidam com os pontos em A , não será possível Bob obter o segredo k .

Embora proposto por Juels and Sudan 2002, não foi disponibilizada uma implementação, apenas a ideia por trás do método, apresentando os principais conceitos. Clancy 2003 apresentou a implementação do método baseando-se nas localidades das minúcias (características extraídas de uma impressão digital que a distingue das outras). Obteve com esta pesquisa uma alta taxa de FNMR (*False Non-Match Rate*) que ficou entre 20-30%. *False Non-Match Rate* refere-se à taxa de impressões digitais que não foram reconhecidas pelo sistema, mesmo sendo genuínas. Em um estudo feito por Uludag et al. 2004, foi apresentada uma implementação de *Fuzzy Vault* para impressões digitais, sendo que os autores assumiram que a captura da impressão pelo leitor biométrico era sempre a mesma, eliminando assim, questões de alinhamento de imagem. Para Maltoni et al. 2009 o problema de alinhamento de imagem no método *Fuzzy Vault* ainda continua em aberto.

Não só na biometria por impressão digital que *Fuzzy Vault* é um assunto relevante de pesquisa; outros sistemas biométricos também já foram implementados utilizando este método, como é o caso de Wu and Yuan 2010, que implementaram o método no reconhecimento de face; Reddy and Babu 2008 aplicaram no reconhecimento de íris. Sowkarthika and Radha 2013 propuseram a utilização de *Fuzzy Vault* em um sistema biométrico multimodal (possuem mais de uma característica biométrica, por exemplo: íris e impressão digital), onde ocorreria a fusão entre as características da íris e da impressão digital, resultando em uma só característica, e então todo o processo pertinente ao método seria aplicado.

3. Método Implementado

3.1. Codificação

A primeira etapa implementada foi a extração de minúcias da impressão digital, utilizando o algoritmo *MINDTCT*, seguida da codificação do segredo. A implementação da codificação foi baseada no trabalho de Uludag et al. 2005, e por sua vez foi realizada da seguinte forma: selecionam-se 8 minúcias, no formato de coordenadas (x,y) e o polinômio $p(u) = c_8u^8 + c_7u^7 + \dots + c_1u + c_0$, que apresenta grau 8. Uma chave de 128 bits, gerada por um algoritmo de AES no formato de um conjunto de *short*, também é utilizada, e ela será o segredo que se pretende ocultar; a chave gerada é ligada ao polinômio, atrelando cada um dos valores do conjunto no formato *short* como um coeficiente do polinômio. Um exemplo de uma chave e seus coeficientes atrelados seria: 12432, 12989, 31111, 32122, 23111, 21980, 21876, 19990; atrelando cada um destes valores da chave ao polinômio de grau 8 tem-se o seguinte polinômio: $p(u) = 12432u^8 + 12989u^7 + 31111u^6 + 32122u^5 + 23111u^4 + 21980u^3 + 21876u^2 + 19990u + 25876$; neste polinômio é possível observar que cada um dos 8 valores da chave foi agregado como um coeficiente. Observa-se que o último valor "25876" não aparece na chave, porque ele corresponde a um código verificador CRC (*Cyclic Redundancy Check*, utilizado para identificar ruídos em canais de

transmissão), que é necessário para certificar que mais tarde o segredo (chave) foi decodificado corretamente. São realizadas avaliações sobre o polinômio de grau 8 com as coordenadas X e Y (concatenadas) das minúcias e, os pontos gerados decorrentes das avaliações são considerados pontos genuínos. Geram-se pontos aleatórios no plano cartesiano justamente para ocultar os pontos genuínos que, se descobertos, podem revelar o segredo. Estes pontos aleatórios ou falsos são adicionados no mesmo plano dos pontos genuínos e, quanto mais pontos "chaff" (falsos) são adicionados, mais seguro fica o cofre (*vault*). Assim sendo, um grande número destes pontos falsos farão os pontos genuínos serem dificilmente identificados, sem que se tenha uma impressão digital de consulta genuína do indivíduo.

3.2. Decodificação

Na etapa de decodificação, tenta-se encontrar os pontos genuínos que estão ocultados no plano cartesiano juntamente com os pontos falsos; na literatura, este plano cartesiano, onde se encontram os pontos, é referido como *vault*(cofre). Nesta etapa, seleciona-se uma impressão digital de consulta (*query*) para encontrar os pontos genuínos no plano. Compara-se primeiramente a impressão que codificou o segredo com a impressão de consulta, utilizando para isso, o algoritmo *bozorth3*; caso esta comparação indique que ambas impressões pertencem ao mesmo indivíduo, então as coordenadas de minúcias utilizadas para codificar o segredo são identificadas dentro do cofre (*vault*). Uma vez que os pontos (x,y) , que representam os pontos genuínos, são encontrados dentro do cofre, suas coordenadas são submetidas à interpolação polinomial de Lagrange. Com a aplicação da interpolação polinomial consegue-se a chave no formato *short* de 16 bits; para se ter certeza que a chave encontrada representa a que codificou o segredo, é realizada uma verificação *CRC* nos 8 primeiros valores do segredo (lembrando que o segredo é composto por um conjunto de 9 valores no formato *short*, como mostrado nas etapas anteriores) e, caso o código desta verificação apresente o mesmo valor do último número do conjunto, ou seja, o valor na posição 9, tem-se a chave *short* de 128 bits AES decodificada.

4. Resultados Preliminares

4.1. Avaliações de FRR, FAR e GAR

Com intuito de avaliar o método aqui proposto, foram realizados alguns experimentos comuns à sistemas biométricos, como: Falsa Rejeição ou FRR (*False Rejection Rate*), Falso Aceite ou FAR(*False Acceptance Rate*) e Aceite Genuíno GAR(*Genuine Accept Rate*); estes serão tratados a partir de agora, respectivamente, apenas como FRR, FAR e GAR. A base de dados utilizada nesta pesquisa foi o DB1 da FVC2004, que possui 800 imagens pertencentes a 100 pessoas diferentes, onde de cada indivíduo foram capturadas 8 imagens distintas (100x8).

Para a realização do teste de FAR, que verifica a taxa de impressões não genuínas, e que são identificadas como genuínas, obteve-se 0%, o que significa que nenhuma impressão não genuína foi identificada pelo algoritmo como genuína. No total, foram realizadas 316800 comparações e a FAR resultou em 0%. Para o cálculo de FRR, que verifica a taxa de impressões pertencentes a um indivíduo e que são identificadas como não genuínas, foram realizadas 2800 comparações ao todo. Obteve-se uma taxa de 37,25% para FRR e uma taxa de GAR, que verifica a taxa de impressões genuínas identificadas

corretamente, de 62,75%. É importante observar que, caso fossem utilizadas apenas impressões de qualidade média e alta, seria possível obter maiores taxas de GAR e menores taxas de FRR.

4.2. Avaliação de segurança e desempenho do aplicativo de encriptação e decriptação de arquivos

A etapa subsequente foi o desenvolvimento de um encriptador/decriptador de arquivos com o algoritmo AES para avaliar o desempenho e a segurança do método de *Fuzzy Vault*, onde o tamanho da chave AES definida foi de 128 bits. Para avaliação do aplicativo de encriptação/decriptação foram utilizadas 4 impressões digitais de indivíduos distintos e 3 arquivos randômicos de 16 Bytes, 46.8 MB e 86.6 MB. Um total de 12 avaliações foram realizadas encriptando os 3 arquivos, onde foram utilizadas duas impressões de cada indivíduo, sendo que, uma delas para codificar o segredo e a outra para decodificá-lo.

Neste experimento foram utilizados 306 *chaff points* e 9 pontos genuínos, totalizando 315 pontos. Seriam inviáveis tentativas de ataque ao aplicativo biométrico para descobrir os 9 pontos genuínos; um exemplo seria a utilização de critérios aleatórios (Força Bruta), onde sem uma impressão genuína teriam de ser feitas milhões de comparações e a probabilidade de acerto seria praticamente nula. Uma vez que cada tentativa de descobrir os pontos genuínos leva em média de 0.005 a 10 segundos, dependendo da chave ocultada e dos "chaff points" gerados, o tempo para uma máquina decodificar a chave seria de anos a décadas, devido ao alto número de comparações a serem feitas.

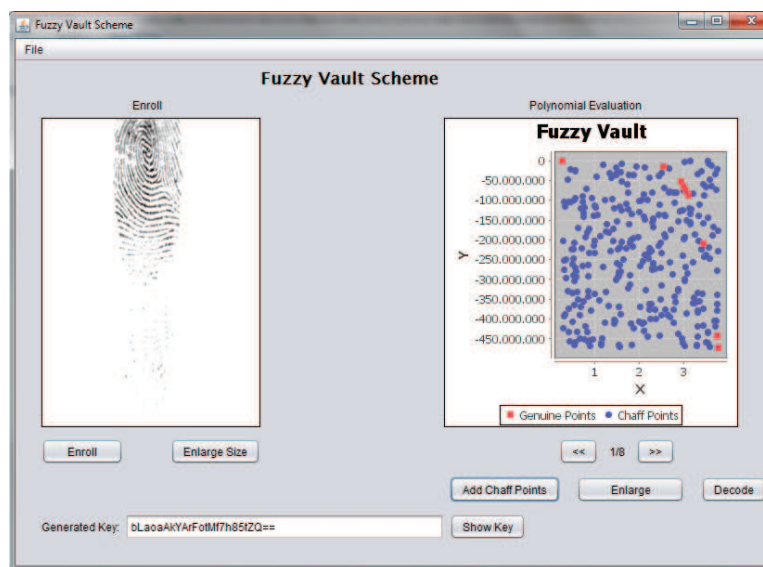


Figure 1. Tela de codificação com os campos preenchidos (acervo próprio).

5. Conclusão

A proposta do trabalho foi a apresentação do método *Fuzzy Vault* e, sua utilização na implementação de um aplicativo biométrico de impressão digital. Foram detalhadas as fases de codificação e decodificação tendo como segredo uma chave de 128 bits de um algoritmo AES, ocultada utilizando um polinômio de grau 8 e minúcias pertinentes a uma

impressão digital. Avaliações de FAR, GAR e FRR foram realizadas onde se mostrou resultados eficazes como o caso da FAR de 0%. Foi realizada também uma análise de segurança do método ao encriptar e decriptar arquivos, onde se mostrou a inviabilidade de descobrir a chave de 128 bits sem uma impressão digital genuína, o que comprova a eficácia do método aqui apresentado.

References

- Clancy, T. C. (2003). Secure smartcard-based fingerprint authentication. In *ACM Workshop on Biometrics: Methods and Applications*, pages 45–52.
- Jain, A. K., Ross, A. A., and Nandakumar, K. (2011). *Introduction to Biometrics*. Springer Publishing Company, Incorporated.
- Jeffers, J. and Arakala, A. (2006). Minutiae-based structures for a fuzzy vault. In *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the*, pages 1–6.
- Juels, A. and Sudan, M. (2002). A fuzzy vault scheme. In *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, pages 408–.
- Liu, H., Sun, D., Xiong, K., and Qiu, Z. (2011). Is fuzzy vault scheme very effective for key binding in biometric cryptosystems? In *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2011 International Conference on*, pages 279–284.
- Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S. (2009). *Handbook of Fingerprint Recognition*. Springer Publishing Company, Incorporated, 2nd edition.
- Nandakumar, K., Jain, A., and Pankanti, S. (2007). Fingerprint-based fuzzy vault: Implementation and performance. *Information Forensics and Security, IEEE Transactions on*, 2(4):744–757.
- NBIS-EC, N. (2013). The nbis-ec software is subject to u.s. export control laws - user's guide to export controlled distribution of nist biometric image software(nbis-ec).
- Reddy, E. S. and Babu, I. R. (2008). Performance of iris based hard fuzzy vault.
- Sowkarthika, S. and Radha, N. (2013). Securing iris and fingerprint templates using fuzzy vault and symmetric algorithm. In *Intelligent Systems and Control (ISCO), 2013 7th International Conference on*, pages 189–193.
- Uludag, U., , Uludag, U., and Jain, A. K. (2004). Fuzzy fingerprint vault.
- Uludag, U., Pankanti, S., and Jain, A. K. (2005). Fuzzy vault for fingerprints. In *in Proc. AVBPA, Lecture Notes in Computer Science 3546*, pages 310–319. Springer.
- Wu, L. and Yuan, S. (2010). A face based fuzzy vault scheme for secure online authentication. In *Data, Privacy and E-Commerce (ISDPE), 2010 Second International Symposium on*, pages 45–49.