
AGROPECUÁRIA
CIÊNCIAS BIOLÓGICAS
EXATAS E ENGENHARIAS
HUMANAS E HUMANIDADES
USP
CNPq
FAPESP
2006 SIMPÓSIO INTERNACIONAL DE INICIAÇÃO CIENTÍFICA
14º SIICUSP
SIICUSP


14 Siicusp - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
file:///E:/index01.htm
Google
Mais visitados
Primeiros passos
Últimas notícias
LEGENDAS.TV
isoHunt
14 Siicusp
SIIC
14º Simpósio Internacional de Iniciação Científica
Subarea/Autor
Subarea/Título
Autor
Orientador
Título
Voltar
Home
Resumo
Título
Método para utilização de impressão digital na geração de chaves criptográficas
Title
A method for the utilization of fingerprint in the generation of criptography key
Autor / Colaborador
Francisco de Souza Junior
Bolsista Agência
PIC-BM
Instituição (Sigla)
Centro Universitário Barão de Mauá / CBM
Unidade
Centro Universitário Barão de Mauá
Departamento
Computacao
Laboratório / Setor
Orientador
Thiago Pirola Ribeiro
Agência Financiadora
Centro Universitário Barão de Mauá
Ver Resumo do Trabalho
Área Pesquisa
ENGENHARIAS E EXATAS / Ciência da Computação
Done

Método para utilização de impressão digital na geração de chaves criptográficas

Francisco de Souza Junior[1] e Thiago Pirola Ribeiro[1]
[1]Centro Universitário Barão de Mauá, Ribeirão Preto-SP

1. Objetivos

A utilização da criptografia na segurança da informação está cada vez mais evidente, principalmente com o uso da Internet.
Para cifrar um texto é necessário a utilização de chaves criptográficas. Essas chaves, para uma melhor segurança, devem ser compostas de uma grande quantidade de caracteres, porém normalmente as pessoas não conseguem guardar tais senhas[1].
Os métodos atuais de biometria baseiam-se em métodos de cadastros e consultas para a autenticação. Dentre esses métodos um dos mais utilizados é a impressão digital.
O método propõe uma técnica para utilizar a impressão digital e torná-la uma chave forte para utilização em algoritmos criptográficos utilizando-se não mais de chaves difíceis de lembrar, mas utilizar a própria impressão digital como chave.

2. Material e Métodos

Para os testes iniciais utilizou-se impressões digitais do banco de imagens do conjunto de softwares NFIS (*NIST FingerPrint Image Software*)[2].
As análises das imagens para a detecção das minúcias, primeiramente, foram feitas com o software MINDTCT (*Minutae Detection*)[2] e posteriormente com algoritmos desenvolvidos. Todas as implementações foram feitas utilizando o GCC. Os algoritmos de criptografia e *hash* utilizados foram retirados da biblioteca *Nettle*[3].
O método consiste na obtenção de uma imagem de impressão digital e realização de análise da imagem e detecção de minúcias.
Com as minúcias detectadas gera-se uma saída numérica com o posicionamento das minúcias. Essa saída é então analisada e convertida, utilizando-se de expressões matemáticas, em uma chave criptográfica para ser utilizada como entrada do algoritmo de criptografia.

3. Resultados e Discussão

A Figura 1(a) apresenta a imagem da impressão digital original para os testes. A Figura 1(b) apresenta a imagem obtida como resultado dessa análise e destaca em um plano ampliado, algumas das minúcias encontradas.

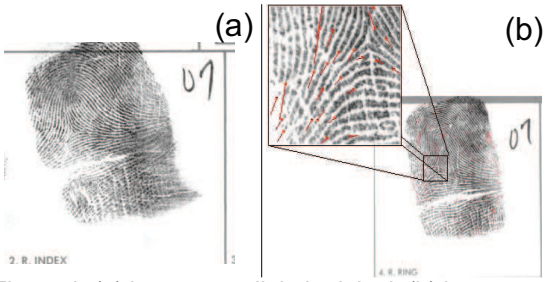

Figura 1: (a) impressão digital original; (b) imagem obtida como resultado das análises, destacando algumas das minúcias detectadas.

Os resultados obtidos foram satisfatórios para uma utilização rudimentar do método, porém em um segundo momento, o método será aperfeiçoado e automatizado.
O método proposto limitou-se a realizar pequenas otimizações apenas em impressões digitais transladadas, supondo um reconhecimento imutável de duas capturas diferentes de impressões digitais.

4. Conclusões

O método mostrou a viabilidade na utilização das técnicas, porém necessita de um melhor aperfeiçoamento das técnicas de extração e análise das minúcias para utilização do método em ambientes adversos como imagens de impressões digitais mal adquiridas ou mesmo rotacionadas entre a cifragem e decifragem.

5. Referências Bibliográficas

[1]MENEZES, A., OORSCHOT, P., VANSTONE, S.: Handbook of Applied Cryptography. CRC, Press, 1996.
[2] NIST. National Institute of Standards and Technology. Disponível em: <http://fingerprint.nist.gov/NFIS/> Acesso em: Mar. 2006.
[3] NETTLE. A low-level cryptographic library. Disponível em: <http://www.lysator.liu.se/~nisse/nettle/>. Acesso em: Mai. 2006.