

Aplicativo de Troca de Mensagens Utilizando Criptografia Baseada em Imagens

Marcus Antonio Grécia Brandt¹, Mikhail Yasha Ramalho¹

¹ Centro de Ensino Superior FUCAPI (CESF)
Av. Gov. Danilo de Mattos Areosa, 381 – Distrito Industrial – Manaus – AM – Brasil

{marcusbrandt, mikhailramalho}@gmail.com

Abstract. *This meta-paper describes the style to be used in articles and short papers for SBC conferences. For papers in English, you should add just an abstract while for the papers in Portuguese, we also ask for an abstract in Portuguese (“resumo”). In both cases, abstracts should not have more than 10 lines and must be in the first page of the paper.*

Resumo. *Aplicações de troca de mensagens possuem naturalmente um forte apelo popular e figuram como aplicações de destaque nas lojas de aplicativos. Porém levantam questões relativas a segurança e confiabilidade das informações que por eles trafegam. Este artigo descreve a implementação de um aplicativo de comunicação por meio do bluetooth que utiliza um algoritmo de criptografia baseado em imagens como chave de acesso.*

1. Introdução

2. Fundamentação Teórica

2.1. ASCII

O ASCII *American Standard Code for Information Interchange* (Código Padrão Americano Para o Intercâmbio de Informação) é um esquema de codificação inicialmente baseado no alfabeto americano, posteriormente se tornou um esforço para padronização da representação de caracteres pelos fabricantes de computadores.

Cada caracter (pontuação, valores alfanuméricos e valores de controle) é representado por um valor numérico divididos em uma tabela. Originalmente como eram representados apenas caracteres americanos, acentuações e letras com essa característica não podiam ser representados, posteriormente a tabela passou por uma revisão e foram criadas 12 novas partes pra suprir essa necessidade.

2.2. Imagem

Quando digitalizadas as imagens são representadas por bits e bytes que são convertidos para números pra representar cada cor de um pixel específico, podendo ser representada por uma matriz de pixels(Figura 1) .

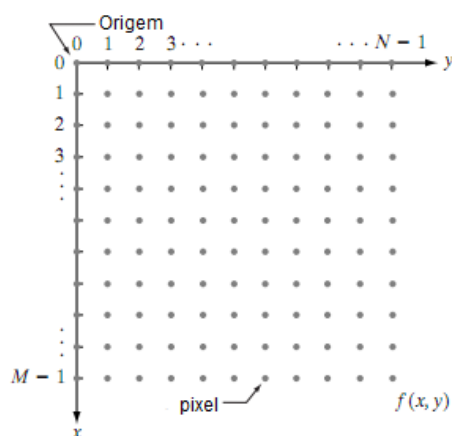


Figura 1. Representação de uma imagem digital

2.3. Criptografia

2.3.1. Chave Simétrica

2.3.2. Chave Assimétrica

2.4. Bluetooth

Bluetooth é uma tecnologia sem fio para troca de informação em pequenas distâncias baseada em ondas curtas e é padronizada pelo IEEE 802.15.1, foi originalmente concebida para ser alternativa ao RS-232.

Ele opera em uma faixa de freqüência de 2400–2483.5 MHz, utiliza a tecnologia de rádio chamada de salto de frêquencia em espalhamento espectral (*frequency-hopping spread spectrum*). Baseado em um protocolo de troca de pacotes com estrutura de *master-slave*.

Um servidor Bluetooth pode se comunicar com até 7 devices em uma rede piconet(uma ad-hoc baseada na tecnologia Bluetooth).

3. Sistema

3.1. Android

O protótipo apresentado neste trabalho foi desenvolvido em Android, por ser uma plataforma popular para desenvolvimento de aplicativos móveis. O Android possui interfaces de programação de aplicativo (APIs), que vêm com o seu Software Development Kit (SDK) e possui recursos completos de interface[Developers 2014].

Para este protótipo utilizamos a versão 4.4.2 do Android conhecida como Jelly Beans, por ser a versão mais recente disponível, quando do desenvolvimento deste trabalho.

3.2. OpenCV

O OpenCV é um conjunto de bibliotecas desenvolvidas com o objetivo de provêr visão computacional em tempo real. Desenvolvida originalmente em C mudou sua plataforma

para C++ com o objetivo de se tornar mais fácil o desenvolvimento de novas funcionalidades, melhor implementação e aplicação de padrões, com suporte em Python e Java (Android), com suporte em Windows, Linux, iOS, Mac OS e Android.

3.3. Java & JNI

Java é uma linguagem de programação adotada como padrão no desenvolvimento de aplicativos em Android, é baseada em classes, orientada a objeto e existem várias APIs (biblioteca) [qual o melhor?] prontas, oferecendo uma sintaxe muito parecida com C e C++ é atualmente a linguagem mais popular do mundo utilizada principalmente em sistemas web cliente-servidor, foi originalmente desenvolvida por James Gosling na Sun Microsystems posteriormente adquirida pela Oracle.

Para comunicações mais baixo nível o Java utiliza um artifício de comunicação via callbacks através da sua API de comunicação nativa a JNI (*Java Native Interface*)

3.4. Processo de Criptografia

?????

3.5. Sistema de Criptografia Utilizando Imagens

Nossa proposta é composta primeiramente por um algoritmo de chave simétrica, pois haverá uma troca de cada caractere por uma correspondente da imagem escolhida. O algoritmo se baseia na seguinte ideia:

*.Uma imagem é representada por pixels que tem valores de 0 até 255 assim como a tabela ASCII que tem valores de 0 à 255 incluindo dígitos de controle.

4. Resultados

5. Conclusão

Referências

Developers, A. (2014). Develop. android developers.