# FUNCIONALIDADE DE SENHAS POR COMANDOS DE VOZ

Edio Roberto Mafio[1]

**RESUMO**
Alguns processadores de sinais da fala disponíveis no mercado e compatíveis com minicomputadores amplamente utilizados em Domótica e Mecatrônica têm significativa eficiência em termos de acurácia. Neste âmbito, este artigo tem como objetivo avaliar um desses processadores quanto à capacidade de operar simulando o recurso de biometria por voz – em Português do Brasil -, que normalmente requerem sistemas muito mais robustos. A relevância do estudo está em evidenciar possibilidades de utilização de senha por voz com uso de dispositivos mais acessíveis em termos de custo e que sejam aplicáveis a projetos e protótipos em cursos de graduação voltados a Desenvolvimento de Sistemas ou Mecatrônica. Estão envolvidas na pesquisa as áreas de Linguística, Processamento de Linguagem Natural, Programação, Eletrônica e outras diretamente relacionadas.
**PALAVRAS-CHAVE:** Senhas, Autenticação por voz, Biometria, Comandos por Voz.



**ABSTRACT**
Some speech signal processors available and compatible with minicomputers that are widely used in home automation and Mechatronics have significant efficiency in accuracy terms. In this context, this article aims to evaluate one of these processors according to its ability to operate by simulating voice biometrics capability, which typically require much more robust systems. The relevance of this study is to show possibilities of using password for voice with use of more affordable devices in terms of cost and applicability to projects and prototypes in undergraduate courses aimed at the development of systems or Mechatronics. It is involved in the research Linguistics, Natural Language Processing, Programming, Electronics and other areas directly related.
**KEYWORDS:** Passwords, Voice Authentication, Biometrics, Voice Commands.

## INTRODUÇÃO

Nas Idades Antiga e Média, a utilização de senhas entre os humanos era pouco comum e restrita a pequenos grupos organizados, normalmente compostos por pessoas capazes de ler e escrever. Na conjuntura atual, no entanto, sua criação e uso é algo bastante trivial e, quase sempre se trata de um procedimento que não está vinculado a pequenos grupos organizados, mas sim, à maior parte da população mundial (COUTO, 2008). De uma forma geral, elas permitem - ou não - acesso a um smartphone, a um computador pessoal,

[1] Doutorando em Linguística pela Universidade Estadual de Londrina (2013), Mestre em Linguística pela Universidade Estadual de Maringá (2006), Graduado em Letras pela Universidade Estadual Paulista Júlio de Mesquita Filho (1997). E-mail: prof.ediorobertomanfio@gmail.com

a uma casa, a um edifício, a um banco de dados, a uma conta bancária, ao controle da iluminação de uma cidade toda, entre outros.

As senhas podem ser compostas por sequências alfabéticas, numéricas ou alfanuméricas, situação em que o usuário, muitas vezes para atender ao quesito comodidade em detrimento da segurança, pode utilizar desde datas comemorativas até nomes de entes queridos como senhas. Essas palavras ou números secretos podem ainda ser associados à tecnologia biométrica, condição em que a segurança aumenta significativamente.



Há também sistemas em que apenas a biometria é utilizada. Especificamente naqueles que operam com identificação por impressões digitais, basta ao usuário posicionar o dedo no leitor para que o acesso seja permitido. Porém, a segurança oferecida em sistemas biométricos depende da sua robustez e isso inclui qualidade do banco de dados, acurácia da gravação/leitura, velocidade de processamento e modo de implementação (MALTONI, 2009).

Entretanto, embora as senhas por biometria não sejam novidade, ainda apresentam custos relativamente elevados para aplicações em protótipos para trabalhos ou pesquisas de graduação. Em se tratando de biometria por voz, especificamente, há no mercado alguns processadores de sinais da fala de relativa qualidade e que têm significativa eficiência em termos de acurácia. Além disso, são compatíveis com vários tipos de minicomputadores amplamente utilizados em Domótica e Mecatrônica.

Este artigo, portanto, tem como objetivo avaliar um desses processadores quanto à capacidade de operar simulando o recurso de biometria por voz - em Português do Brasil, especificamente -, que normalmente requer sistemas muito mais robustos. A relevância deste estudo está em evidenciar possibilidades de utilização de senha por voz com uso de dispositivos mais acessíveis em termos de custo e que sejam aplicáveis a projetos e protótipos em cursos de graduação voltados a Desenvolvimento de Sistemas ou Mecatrônica. Esta pesquisa é interdisciplinar e nela estão envolvidas as áreas de Linguística, Processamento de Linguagem Natural, Programação, Eletrônica e outras diretamente relacionadas.

## 1. CONCEITO BÁSICO DE SENHA

A palavra senha, embora bastante difundida e corriqueira no mundo moderno, encerra uma quantidade muito grande de significados. Os dicionários de língua portuguesa, por exemplo, trazem várias acepções para o verbete. Importante lembrar que, etimologicamente, essa palavra se origina do termo latino signa, plural de signum (FERREIRA, 2009). Dessa forma, é bem provável que tenha sido usada pelos homens da antiguidade na maior parte das vezes no plural, ou seja, 'sinais', utilizados para dar andamento a um procedimento com autorização restrita: gesto combinado entre crianças, entre civis, entre sentinelas, etc.



Devido à ampla variedade de aplicações discursivas mais atuais, a palavra senha, em diversas situações, confunde-se com criptografia, momento em que ambas podem figurar como sinônimos, ou seja, em alguns casos, a expressão 'gerar uma criptografia' pode ser equivalente a 'gerar uma senha'. A criptografia, no entanto, é mais complexa por se tratar de uma metodologia e/ou um conjunto de técnicas com as quais se pode criptografar grande quantidade dados (FERREIRA, 2009), algo cuja realização torna-se inviável apenas com a utilização de senhas. Ambas, porém, cada vez mais operam em conjunto. Os dados, após serem criptografados, precisam passar pelo processo inverso para que o destinatário possa a eles ter acesso. Para isso, cria-se uma senha que aciona o software capaz de decriptografar o conteúdo secreto (STALLINGS, 2008).

Nos meios digitais, a criptografia deixou de ser eventual e tornou-se práxis. Se outrora o uso de técnicas criptográficas era de uso exclusivo de alguns grupos, a partir do surgimento da era digital ela se faz presente desde práticas comuns de simples usuários até atividades de grandes corporações. O modo como ela será feita está diretamente relacionado ao resultado da avaliação de riscos e da classificação das informações a serem tratadas em cada caso (FERREIRA e ARAÚJO, 2008).

O processo de converter um texto claro em texto criptografado , de acordo com Stallings (2008) é denominado cifragem ou criptografia. Cifragem é, basicamente, a criação de cifras, termo que também tem vários significados. Note-se que já há a intersecção de vários termos até o momento: senha,

criptografia, cifra e cifragem. A maleabilidade e certo grau de equivalência dessas terminologias requerem sempre o cuidado de, quando do uso, verificar a área envolvida e os autores e profissionais vinculados à atividade em questão.

Cifragem por exemplo, em música, pode ser o processo pelo qual se converte notações musicais do pentagrama em letras que, eventualmente, associadas a números e outros símbolos, correspondem a acordes representados na partitura por notas musicais. Note-se que é algo um tanto diverso da criptografia utilizada em meios digitais.



Mas a criptografia não surgiu com o advento dos computadores no século XX e sua história é tão antiga quanto a das senhas. Criptografar é, basicamente, escrever em códigos ou cifras e, daí, sua relação muito estreita com a palavra senha. Uma senha relativamente longa, formada por versos, rimas ou frases inteiras pode, em alguns casos, por si só, ser um conjunto de dados criptografado cuja decifração depende de um conjunto de regras, uma chave ou conhecimento profundo sobre os significados alternativos de cada um dos elementos (COUTO, 2008).

Dessa forma, curiosamente, a expressão ‘senha secreta’ é um pleonasmo risível, pois a senha é criada para que haja um segredo inviolável, seja ele de qualquer magnitude. Código, cifra, segredo, chave, senha, criptografia, enigma são alguns termos cujas dimensões semânticas se sobrepõem em alguns pontos e que muitas vezes figuram no vocabulário de pessoas pertencentes a áreas de conhecimento diferentes.

Neste estudo, o termo senha será considerado em sua acepção mais simples: permissão de acesso. Note-se que isso vale para senhas das categorias oral, escrita, gestual, biométrica, considerando interações humano-humano ou humano-máquina.

## 2. SISTEMAS BIOMÉTRICOS

Biometria é uma palavra derivada dos termos gregos bíos (vida) e métron (medida) e diz respeito às medidas que podem ser feitas do corpo humano em vida (MALTONI et al., 2009). Essa definição, no entanto, abarca apenas a biometria que envolve os seres humanos. Se tomarmos o termo

grego bíos mais amplamente, a biometria pode incluir mensurações feitas a partir de qualquer organismo vivo existente ou conhecido. Há, por exemplo, modelos biométricos para mensurar o grau de abrangência relativo à transmissão da malária no Brasil (CORDEIRO, 2005). Neste trabalho serão considerados apenas aqueles que dizem respeito às medições feitas em humanos.

Os sistemas biométricos evoluíram muito após a era digital. Os mais comuns no início do século XXI como as medições de digitais, íris e voz são apenas alguns dos existentes. Há à disposição o reconhecimento facial, a geometria da mão, a identificação pela íris, o reconhecimento pela retina, o reconhecimento por voz (PINHEIRO, 2008; SILVA; SIQUEIRA FILHO, 2011) e mesmo o reconhecimento de odores, situação em que são utilizados os sensores de gases, mais conhecidos como 'narizes eletrônicos', dispositivos que, entre outros em franco desenvolvimento, fazem parte do futuro da biometria, uma vez que não apenas têm aplicações imediatas ao meio ambiente; à segurança em indústrias, mas também na medicina (LISBOA; PAGÉ; GUY, 2009).



A partir destes exemplos, pode-se projetar discussões sobre o modo como aquilo que conhecemos por senhas operam junto a sistemas biométricos e como podem proporcionar maior segurança de informações de uma modo geral.

A respeito da eficácia, Maltoni et al. (2009) comentam que as identificações biométricas não podem ser facilmente movidas, alteradas ou compartilhadas e por isso são consideradas mais confiáveis para identificação pessoal que as convencionais como cartões eletrônicos ou senhas memorizáveis. Assim, proporcionam melhor segurança, maior eficiência e aumenta o conforto do usuário e por esse motivo vem sendo utilizadas em maior escala por instâncias governamentais, institucionais e cidadãos.

No Brasil, por exemplo, o Tribunal Regional Eleitoral - TRE de São Paulo lançou em 2015 uma campanha de cadastramento biométrico que, de acordo com o próprio TRE "é o processo de atualização dos dados constantes do cadastro eleitoral, com o objetivo de implantar a identificação de cada eleitor através de impressão digital, fotografia e, desde que viabilizado, assinatura digitalizada" (TRIBUNAL Regional, online, 2015). Fácil notar que o sistema

adotado opera com a eficácia da redundância biométrica, uma vez que associa a nova mensuração a outras já presentes no documento do eleitor.

A propósito, muito antes da era da eletrônica, iniciada com a válvula termiônica no começo do século XX, as medições e verificações biométricas eram feitas em pessoas por pessoas – não máquinas automáticas, ou seja, a Biometria é um recurso conhecido e utilizado desde épocas mais remotas da história do ser humano. Embora fundamentadas em critérios bastante discutíveis, descrições fisionômicas, comportamentais e outras verificações simples como peso e estatura, além da extração de digitais por meio de carimbo e coleta de assinaturas era o que havia à disposição do governo e da polícia em termos de biometria.



Dentre os sistemas biométricos comentados até o momento, o mais comum é o que opera com leitura de impressões digitais dos dedos das mãos – papiloscopia: há vários softwares e leitores no mercado e eles se proliferam em consultórios, clubes e redes bancárias. Entre os mais incomuns está o leitor de íris, talvez pelo fato de a tecnologia empregada ainda não oferecer comodidade suficientes ao usuário durante a coleta e leitura dos dados – para citar apenas uma das dificuldades, as pessoas têm estaturas bem diferentes.

Tendo em vista esse panorama, as senhas em sistemas biométricos podem constituir-se do próprio resultado da biometria, ou seja, ela é o próprio indivíduo – afirmação contida no título na obra de Pinheiro (2008): “Biometria nos Sistemas Computacionais: você é a senha” (grifo nosso). Note-se que, com o avanço da tecnologia, há uma tendência de o indivíduo estar sendo mensurado biometricamente sem saber, como é o caso dos identificadores de face e/ou narizes eletrônicos, eventualmente instalados em locais estratégicos de alguns ambientes controlados – corporações ou instituições.

## 3. SISTEMA BIOMÉTRICO POR VOZ

O sistema biométrico mais amigável e talvez menos intrusivo, no entanto, é certamente aquele por voz, pois não há necessidade sequer de posicionar o dedo, a palma das mãos, a planta dos pés ou um dos olhos: basta falar. Ele, entretanto, não oferece um alto grau de precisão e funcionalidade na maioria dos casos, tendo em vista que a característica física da voz são as

vibrações sonoras que quase sempre estão acompanhadas de outras coexistentes. Em outras palavras, o som está em toda parte e é muito difícil conseguir isolar apenas a voz do usuário quando da mensuração. Por esse motivo o sistema biométrico por voz ainda se restringe a ambientes controlados como salas fechadas, microfones dedicados ou ligações telefônicas com qualidade mínima de áudio.

Também conhecido como *autenticação por voz*, o sistema biométrico por voz opera com princípios básicos do Processamento de Sinais da Fala (doravante PSF), que por sua vez pertence à grande área de Processamento de Linguagem Natural (doravante PLN), tal como ilustra a Figura 01.



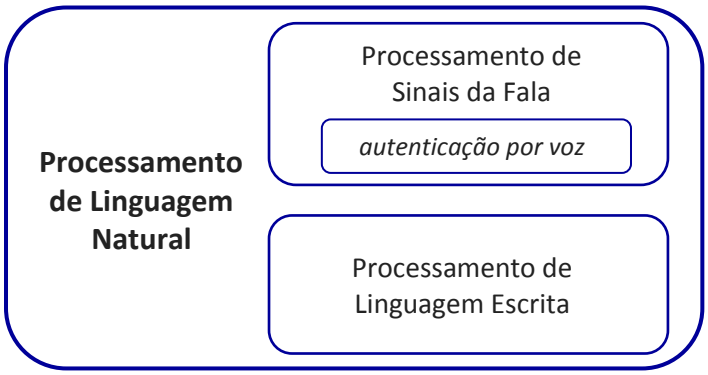



Figura 01 – Área de pertencimento da *autenticação de voz*
Fonte: o próprio autor, Rich (1993)

Normalmente, pesquisadores de diferentes áreas têm a impressão de que há mais pesquisas em PSF que em PLE (Processamento de Linguagem Escrita) um função de haver uma infinidade de equipamentos que operam com recursos baseados em voz no dia a dia. O PLE, no entanto, é imediatamente anterior ao PSF na linha do tempo. Os corretores ortográficos e de sintaxe dos editores de texto e os robôs de conversação são dois exemplos podem que economizam palavras (MANFIO, 2013; 2014; MANFIO; MORENO; BARBOSA, 2014)

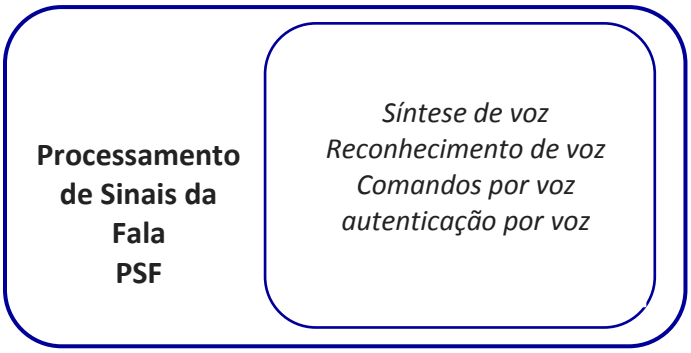



Figura 02 – Área de pertencimento da *autenticação de voz*
Fonte: o próprio autor, Rich (1993)



Importante deixar claro que, além da *autenticação de voz*, fazem parte da área PSF a *síntese de voz*, o *reconhecimento de voz*, o *comando por voz*, tal como representa a Figura 02. Outro detalhe é que a maioria dos equipamentos que operam com *reconhecimento* e *comandos por voz* não disponibilizam a função da autenticação por voz pelo fato já mencionado ao início: comparativamente, são necessárias máquinas com maior capacidade de processamento.

## 4. SENHA POR VOZ

A senha, por si só, como definido anteriormente, pode ser muito pouco eficiente em sistemas digitais. Uma senha como 'bolodecenoura' pode ser adivinhada pelos familiares do usuário, uma vez que se tratam de duas coisas relativamente óbvias: um elemento do cotidiano (comida), um prato apreciado (especificidade). No entanto, associada a métodos de criptografia, torna-se com esta um conjunto bastante eficiente quando da proteção de dados ou limitação de acesso. A mesma senha 'bolodecenoura' utilizada para acesso a um serviço e correio eletrônico certamente opera num sistema em que outros recursos de segurança agem simultaneamente.

Outra maneira de ampliar a capacidade de sigilo de dados ou acesso físico a determinados locais é associar a senha básica a um sistema biométrico, situação em que parte do conjunto de dados necessários para dar acesso são as próprias mensurações biológicas do usuário – voz, digitais, íris, retina entre outros. Então, após 'bolodecenoura' ser digitado no campo

destinado à senha, as digitais são solicitadas para leitura. Nesse contexto, a senha por voz pode então ser definida como a adição de uma senha memorizável - como 'bolodecenoura'- a um sistema biométrico por voz - ou *autenticação por voz*.

Para exemplificar o funcionamento de senha por voz foi criado um protótipo que dispõe do recurso de reconhecimento por voz[2]. O protótipo compreendeu a maquete de uma garagem para automóveis - Figura 03 - com portão de abertura horizontal - 'portão de correr' – cujo acionamento depende de três comandos por voz básicos: 'casa', 'abre' e 'fecha' – em Português do Brasil, considerando a variante linguística do próprio pesquisador.



Figura 03 – protótipo/maquete de uma garagem para automóveis
Fonte: o próprio autor

'Casa' foi definida como a senha memorizável, enquanto os comandos 'abre' e 'fecha' acionam os dois únicos movimentos do portão: abrir e fechar. Todos esses três comandos operam a partir do processador de sinais da fala comercial denominado *Voice Recognition Module V2* (doravante apenas *V2*), o equipamento utilizado para o experimento. O motivo de sua escolha se deve ao fato de que tem sido bastante utilizado em aplicações mais elementares das áreas de Robótica e Domótica. Embora a acurácia do *V2* – Figura 04 - seja bastante discutível, como verificado nos resultados mais adiante, ele tem as vantagens de oferecer soluções práticas e baratas para aplicações gerais, não depender de conexões de rede ou sistema operacional. Outro detalhe bastante

[2] O protótipo é parte integrante do Trabalho de Conclusão de Curso denominado "Acionamento eletrônico de portão via comando por voz" dos graduandos em Mecatrônica Industrial Danilo Servoni Lima e Jean Carlo de Figueiredo Mendes, e alunos da Faculdade de Tecnologia de Garça – SP.

atrativo é que oferecer suporte para voz humana em geral, ou seja, não depende de uma ou outra variante linguística, muito menos de idioma específico.

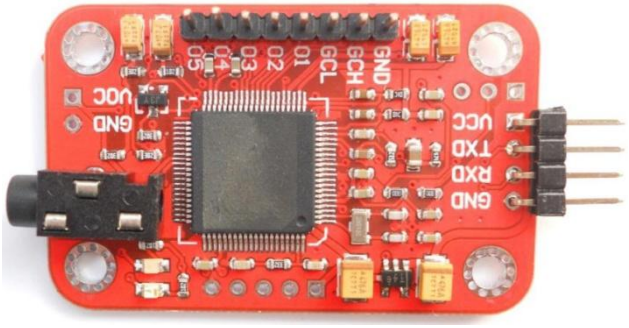



Figura 04 – Voice Recognition Module V2
Fonte: Voice Recognition (online, 2014)



Outro dispositivo, do mesmo fabricante e mais avançado que o *V2* é o *V3*. Porém, como ambos operam da mesma forma e a diferença do mais novo em relação ao antigo é apenas maior capacidade de gravação, não havia muitas razões para sua utilização em um protótipo com apenas três comandos. Há também no mercado um processador mais robusto que o *V2* denominado *Easy Voice Recognition*. Trata-se de um conjunto pronto para ser conectado a vários modelos de Arduino e com muito maior capacidade de gravação e implementação. Seu custo, porém é mais elevado e, por se tratar de um dispositivo de outra categoria, provavelmente será avaliado em outro estudo.

O *V2* operou em conjunto com uma plataforma de desenvolvimento *Arduino* UNO R3, a partir do qual foi possível implementar algumas linhas de código – baseadas em linguagem C – que permitiu, entre outras coisas, controlar a velocidade e o número de passos do motor que movimenta o portão, criar o acesso a partir de senha por voz e temporizá-la para que necessite ser acionada novamente caso o comando subsequente não seja dado. A Figura 05 exibe o modo como os dispositivos estão interconectados.

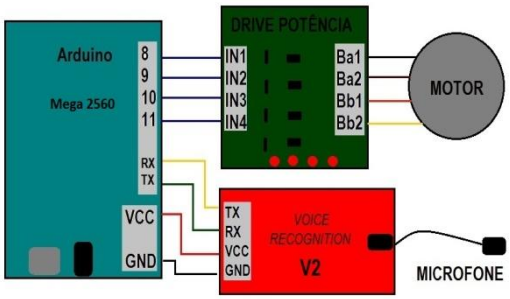



Figura 05 – Diagrama em blocos dos dispositivos
Fonte: Lima e Mendes (2016)



Sequencialmente, o protótipo comporta-se da seguinte maneira: (a) o usuário pronuncia a senha, aqui representada pela palavra ‘casa’; (b) o sistema emite um sinal luminoso - aciona um led - quando dos dados são idênticos; (c) o usuário pode pronunciar, respectivamente, os outros dois comandos ‘abre’ e ‘fecha’ para proceder com o ato simbólico de guardar o carro. Caso o usuário pronuncie a senha mas demore mais que dez segundos para dar o comando, o sistema reinicia e retorna à posição em que é necessária novamente a senha. Uma vez fechado o portão - terminado o último passo do portão - o sistema também reinicia e retorna à posição em que é necessária novamente a senha. Veja-se que as execuções dependem grandemente da senha por voz.

Mesmo que, em princípio o funcionamento do protótipo pareça simples - e de fato é -, o conjunto de elementos envolvidos já abarcam uma série de cuidados que devem ser adotados quando do desenvolvimento de um protótipo que tem o mínimo de potencial para se tornar algo fabricável ou comercializável.

Importante lembrar, novamente, que a escolha por este dispositivo - o *V2* – não foi fortuita. Além das vantagens elencadas há pouco, seus defeitos também foram requeridos. Um deles, salientado pelo próprio fabricante no manual do dispositivo (VOICE Recognition, *online*, 2014), diz respeito ao fato de que possivelmente ele não atende aos comandos de outra pessoa - amigo, parente, cônjuge - mesmo considerando a pronúncia da mesma palavra.

Isso significa que, embora o fabricante deixe claro que o *V2* foi desenvolvido para operar bem apenas com a voz do usuário que fornece os padrões – que grava os comandos com sua própria voz – ele não garante que o processador reconhecerá tão somente a voz do usuário: pode eventualmente

e aleatoriamente ser acionado por outro indivíduo – Gráfico 02. Esses detalhes funcionais, que não podem ser considerados falhas ou erros do dispositivo, uma vez que o fabricante alerta previamente sobre sua existência, é uma *deficiência* que foi amplamente explorada por esse estudo. Dito de outro modo, como o próprio título do trabalho evidencia, trata-se de verificar em primeiro plano a 'funcionalidade de senhas por comandos de voz' considerando alguns critérios de sistemas biométricos. Essa é a razão pela qual enfatiza-se a palavra simulação neste estudo.



Outro detalhe sobre o qual o manual é pouco claro é que, os ruídos de ambiência devem ser minimizados ao máximo durante a gravação. O mesmo deve ser adotado quando da pronúncia dos comandos/palavras. Quando esses quesitos não são ou não podem ser atendidos, o processamento de áudio fica claramente comprometido: o sistema biométrico não responde adequadamente.

De qualquer forma, é válido salientar que um protótipo como esse ou similar a esse, utilizando os mesmos componentes, pode oferecer reais possibilidades de utilização de senha por voz com custos acessíveis e é amplamente aplicável a projetos de cursos de graduação voltados a Computação, Desenvolvimento de Sistemas ou Mecatrônica. Para tanto, basta adquirir os dispositivos, consultar seus manuais e/ou *datasheets* e construir linhas de programação em C para atender às características dos hardwares escolhidos.

## 5. RESULTADOS GERAIS

A metodologia básica aplicada para os testes com o protótipo consistiu em organizar 10 usuários do sexo masculino. Essa exigência de pertencerem ao mesmo sexo se deu em função das características de reconhecimento de voz do processador – as amplitudes e pressões sonoras das vozes masculinas e femininas são muito diversas. Feito isso, cada um deles testou 10 vezes cada um dos comandos, ou seja, 10 vezes a palavra 'casa', 10 vezes a palavra 'abre' e 10 vezes a palavra 'fecha'.

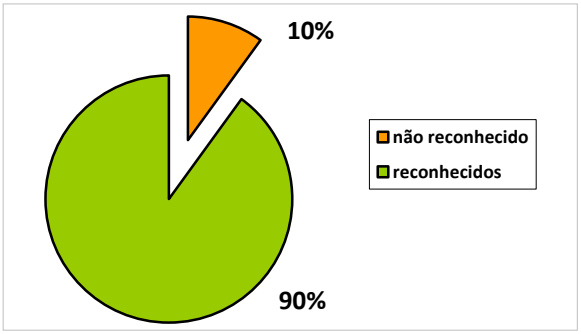
Então, primeiramente, considerando apenas os recursos de reconhecimento e comandos por voz, o protótipo apresentou bons resultados.

Válido lembrar que reconhecimento e comandos por voz são recursos que ocorrem quase concomitantemente pois não há, em princípio, muito sentido em reconhecer um comando e não executá-lo. Logo, quando há autenticação por voz, pode-se dizer que ocorreram também ao quase ao mesmo tempo reconhecimento e comando: estão inter-relacionados.

Do ponto de vista da Biometria básica, o protótipo também funcionou bem. Se a função de um sistema biométrico é comparar um sinal fornecido com outro existente em seu banco de dados e emitir parecer positivo se os dados forem quase idênticos, então protótipo comportou-se como biometricamente eficiente. A cada 10 comandos pronunciados pelo usuário que forneceu a voz à gravação, ocorreu em média uma falha – para a mesma palavra, evidentemente. Isso significa que o comando ‘casa’ foi reconhecido 09 vezes - Gráfico 01. O mesmo ocorreu com os comandos ‘abre’ e ‘fecha’. Importante lembrar que essa falha ocorreu provavelmente em função de um ruído ambiente extra, variação na distância em que se fala ao microfone ou diferença significativa no modo da pronúncia – ritmo ou prosódia.



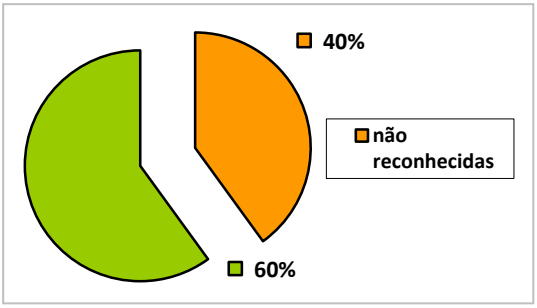
Gráfico 01 – Índice de reconhecimento, por comando, da voz padrão gravada.




Fonte: o próprio autor

Sob a perspectiva da Biometria de precisão, ou seja, da *autenticação de voz*, no entanto, o sistema deixou quase que totalmente a desejar. Embora tenha falhado muito pouco com a voz do usuário que forneceu-lhe o padrão - gravação - funcionou também com outras vozes masculinas. Superando as perspectivas e preceitos do fabricante citadas há pouco, 06 de 10 outras pessoas que testaram conseguiram acionar o recurso do protótipo - Gráfico 02. Para uma aplicação profissional, porém, fica clara sua inviabilidade.

Gráfico 02 – Paralelo entre reconhecimento e não reconhecimento de vozes masculinas em termos biométricos




Fonte: o próprio autor



Tal como comentado na Introdução, as senhas de um modo geral podem ser compostas por sequências alfabéticas, numéricas ou alfanuméricas. Neste protótipo, essa situação pode ser reproduzida sem problemas: o usuário pode optar pelo quesito comodidade em detrimento da segurança utilizando datas comemorativas ou mesmo nomes de entes queridos como senhas. Para esse caso, o processador de sinais da fala envolvido no sistema oferece pouca segurança pelo fato da voz do intruso ter cerca de 60 por cento de probabilidade (Gráfico 2) de ser minimamente similar ao padrão registrado, caso saiba ou descubra a senha.

Entretanto, se a senha escolhida for pouco trivial e resistente a um massivo ataque do método de tentativa e erro – adotado inclusive por alguns crackers – o sistema ganha muito em eficiência. Para determiná-la, é necessário um estudo criterioso à parte, considerando que as características de áudio como amplitude e/ou pressão sonora de cada um dos fonemas que compõem palavras em Português - como em muitos idiomas - são bastante diversas entre si e a composição pode gerar centenas de combinações no formato final da amostra de áudio.

## CONSIDERAÇÕES FINAIS

Alguns processadores de sinais da fala disponíveis no mercado realmente têm significativa eficiência em termos de acurácia e o objetivo deste estudo foi justamente avaliar um desses processadores quanto à capacidade de operar simulando o recurso de biometria por voz. Note-se que a palavra ‘simulando’ deve ser plenamente considerada uma vez que sistemas de

biometria por voz, principalmente aqueles que têm por especificidade a autenticação por voz normalmente requerem sistemas muito mais robustos.

Os testes preliminares com o protótipo que foi desenvolvido para esse fim teve o potencial de salientar a relevância do estudo, que está em evidenciar possibilidades de utilização de senha por voz com uso de dispositivos mais acessíveis em termos de custo. O preço final elevado de um protótipo pode, algumas vezes, inviabilizar sua construção, condição em recursos tecnológicos alternativos que sejam aplicáveis a projetos em cursos de graduação voltados a Desenvolvimento de Sistemas ou Mecatrônica não saem do papel.



A montagem de protótipos minimamente funcionais com esses processadores de sinais, plenamente compatíveis com os minicomputadores amplamente utilizados em Domótica e Mecatrônica, acrescentam muito a estudantes e pesquisadores uma vez que, não apenas abrem a dimensão da possibilidade, como também fomentam novas ideias que podem ser incrementadas a partir das maquetes previamente apresentadas.

## REFERÊNCIAS BIBLIOGRÁFICAS

CORDEIRO, Hérbetes de Hollanda. **Modelo Probabilístico Aplicado à Biometria**. Dissertação (Mestrado) Departamento de Estatística e Informática. Universidade Federal Rural de Pernambuco. Recife, dezembro de 2005.

COUTO, Sergio Pereira. **Códigos e Cifras: da antiguidade à era moderna**. São Paulo: Novaterra, 2008.

FERREIRA, Aurélio Buarque de Holanda**. Novo dicionário Aurélio da língua portuguesa**. 4. ed. Curitiba: Editora Positivo, 2009.

FERREIRA, Fernado Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação: guia prático para elaboração e implementação**. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

LIMA, Danilo Servoni; MENDES, Jean Carlo de Figueiredo. **Acionamento Eletrônico De Portão Via Comando Por Voz**. Monografia (Mecatrônica Industrial). Faculdade de Tecnologia de Garça – Fatec. Garça –SP, 2016.

LISBOA, Henrique de Melo; PAGÉ, Thierry; GUY, Christophe. **Aplicações do nariz eletrônico nas indústrias e na gestão de odores.** Revista Estudos Tecnológicos, vol. 5, n° 2, pp. 195-211, mai-ago. 2009.

MALTONI, Davide et al. Handbook of Fingerprint Recognition Second Edition. Londres: Springer: 2009.

MANFIO, Edio Roberto. **Processamento de linguagem natural, processamento de sinais da fala, geolinguística e um naco de humor.** In: X SEMINÁRIO DE INICIAÇÃO CIENTÍFICA SÓLETRAS - Estudos Linguísticos e Literários. 2013. Anais... UENP – Universidade Estadual do Norte do Paraná – Centro de Letras, Comunicação e Artes. Jacarezinho, 2013. ISSN – 1808-9216. p. 472- 478.

MANFIO, Edio Roberto. **Processamento de Linguagem Natural, robôs de conversação e Linguística**. In Revista e-f@tec. Disponível em: <http://www.fatecgarca.edu.br/revista/rev/Page335.htm>. Acesso em: 03 out. 2014. ISSN: 2317- 451X ,vol. 4. n. 1, 2014. Garça, 2014.



MANFIO, Edio Roberto; MORENO, Fabio Carlos; BARBOSA, Cinthyan Renata Sachs Camerlengo de. **Professor Tical e ALiB: Interação Humano Computador em Diferente Campo.** In: XIX TISE – Conferência Internacional sobre Informática na Educação. Anais... ISBN: 978-956-19-0836-9. Fortaleza, 2014, p. 782.

PINHEIRO, José Mauricio. Biometria **nos Sistemas Computacionais: você é a senha**. Rio de Janeiro: Editora Ciência Moderna, 2008.

RICH, Elaine. **Inteligência Artificial**. Tradução Maria Cláudia Santos Ribeiro Ratto. São Paulo: Makron Books, 1993.

SILVA, Márcia Santos da; SIQUEIRA FILHO, Venicio. **Biometria através de Impressão Digital**. Cadernos Unifoa. Edição no. 14, abril de 2011.

STALLINGS, William. **Criptografia e segurança de redes**. Tradução: Daniel Vieira. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

TRIBUNAL Regional Eleitoral. **Identificação Biométrica**. Disponível em: <http://www.tre-sp.jus.br/eleitor/recadastramento-biometrico-1/recadastramento-biometrico>. Acesso em 05 dez. 2015.

VOICE Recognition Module V2 Manual. Disponível em: <http://www.elechouse.com/elechouse/images/product/Voice%20Recognition%20Module/Manual.pdf>. Acesso em: 02 jul. 2014.