UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC
CURSO DE CIÊNCIA DA COMPUTAÇÃO

FELIPE MADALENA

SISTEMA DE CONTROLE DE ACESSO FÍSICO UTILIZANDO RFID E BIOMETRIA

CRICIÚMA
2016

FELIPE MADALENA

SISTEMA DE CONTROLE DE ACESSO FÍSICO UTILIZANDO RFID E BIOMETRIA

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. Esp. Sérgio Coral

CRICIÚMA

2016

FELIPE MADALENA

SISTEMA DE CONTROLE DE ACESSO FÍSICO UTILIZANDO RFID E BIOMETRIA

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Automação

Criciúma, 20 de Junho de 2016.

BANCA EXAMINADORA

Prof. Sérgio Coral, Esp. - (UNESC) - Orientador

Prof. Paulo João Martins, MSc. - (UNESC)

Prof. Luciano Antunes, MSc. - (UNESC)

À Deus.

AGRADECIMENTOS

Primeiramente a Deus que permitiu que tudo isso acontecesse, ao longo de minha vida, e não somente nestes anos como universitário, mas que em todos os momentos é o maior mestre que alguém pode conhecer. A UNESC, seu corpo docente, direção e administração que oportunizaram a janela em que hoje vislumbro um horizonte superior. Agradeço a todos os professores por me proporcionar o conhecimento não apenas racional, mas a manifestação do caráter e afetividade da educação no processo de formação profissional, por tanto que se dedicaram a mim, não somente por terem me ensinado, mas por terem me feito aprender. A palavra mestre, nunca fará justiça aos professores dedicados aos quais sem nominar terão os meus eternos agradecimentos. Agradeço a minha mãe, heroína que me deu apoio, incentivo nas horas difíceis, de desânimo e cansaço. Ao meu querido pai que apesar de não estar ao meu lado nesse momento, me fortaleceu, me abençoou e que para mim foi muito importante. Meus agradecimentos aos amigos, companheiros de trabalho e irmãos na amizade que fizeram parte da minha formação e que vão continuar presentes em minha vida com certeza. A todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

“Seu trabalho vai preencher uma grande parte da sua vida, e a única maneira de ficar realmente satisfeito é fazer o que você acredita ser um ótimo trabalho. E a única maneira de fazer um excelente trabalho é amar o que você faz”

Steve Jobs

RESUMO

A segurança da informação é de grande valia para o funcionamento de uma organização, sendo necessário prover e manter dispositivos de segurança, tanto lógicos quanto físicos, para garantir que a informação não seja violada, alterada ou divulgada sem autorização. O objetivo do trabalho foi propor a elaboração de um sistema de controle de acesso, que serve como prova de conceito, baseado em Arduino, com dupla autenticação através da utilização de leitura biométrica da digital e da identificação por rádio frequência, além do armazenamento criptografado das informações dos usuários. Foi utilizada a linguagem de programação *Processing*, própria do Arduino e baseada em C/C++. Também foi utilizado o algoritmo de criptografia RC4. A leitura biométrica da digital e a identificação por rádio frequência se mostraram satisfatórias para garantir a segurança na identificação dos usuários ao liberar o acesso, e a criptografia RC4 pôde assegurar a confidencialidade das informações salvas no cartão SD. Através dos resultados alcançados pôde-se identificar vias para a evolução do projeto, como podem ser observadas na conclusão.

Palavras-chave: Arduino. RFID. Criptografia. Segurança da Informação.

ABSTRACT

Information security is of great value to the functioning of an organization, it is necessary to provide and maintain security devices, both logical and physical, to ensure that the information is not tampered with, altered or disclosed without authorization. The objective was to propose the development of an access control system, which serves as proof of concept, based on Arduino, double authentication with digital biometric scanning and radio frequency identification, in addition to the encrypted storage of user information. It used the Processing programming language, own Arduino-based C / C ++. It was also used the RC4 encryption algorithm. The biometric scanning of digital and radio frequency identification proved satisfactory to secure the identification of users to allow access, and RC4 encryption could ensure the confidentiality of information saved on the SD card. Through the achieved results, it was possible to identify avenues for the development of the project, as can be observed in conclusion

Keywords: Arduino. RFID. Cryptography. Information Security.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

a.C.	antes de Cristo
ABNT	Associação Brasileira de Normas Técnicas
AES	*Advanced Encryption Standard*
CA	Corrente Alternada
CC	Corrente Continua
CFTV	Circuito Fechado de Televisão
CIA	*Confidentiality, Integrity e Availability*
d.C.	depois de Cristo
DES	*Data Encryption Standard*
DMZ	*Demilitarized Zone*
DVD	*Digital Versatile Disc*
E/S	Entrada e Saída
EEPROM	*Electrically-Erasable Programmable Read-Only Memory*
EPC	*Electronic Product Code*
FAT	*File Allocation Table*
GB	Gigabyte
GND	*Ground*
GPRS	*General Packet Radio Service*
GSM	*Global System for Mobile Communications*
HD	*Hard Disk*
HF	*High Frequency*
HTTPS	*Hypertext Transfer Protocol Secure*
IDE	*Integrated Development Environment*
IFF	*Identify Friend or Foe*
IV	*Initialization Vector*
KB	Kilobyte
KSA	*Key Scheduling Algorithm*
LCD	*Liquid Crystal Display*
LED	*Light Emitting Diode*
LF	*Low Frequency*
LFSR	*Linear Feedback Shift Register*

mA	miliAmpère
MB	Megabyte
Mbits/s	Megabits por segundo
MHz	Mega-hertz
MISO	*Master In Slave Out*
MIT	Massachusetts Institute of Technology
MOSI	*Master Out Slave In*
NFC	*Near Field Communication*
PRGA	*Pseudo-Random Generation Algorithm*
PWM	*Pulse Width Modulation*
RC4	*Rivest Cipher Version 4*
RFID	*Radio Frequency Identification*
RISC	*Reduced Instruction Set Computer*
SCK	*Serial Clock*
SD	*Secure Digital*
SMS	*Short Message Service*
SPI	*Serial Peripheral Interface*
SRAM	*Static Random Access Memory*
SS	*Slave Select*
SSL	*Secure Socket Layer*
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security*
UDP	*User Datagram Protocol*
UHF	*Ultra-High Frequency*
UNESC	Universidade do Extremo Sul Catarinense
USB	*Universal Serial Bus*
V	Volts
WEP	*Wired Equivalent Privacy*
WIFI	*Wireless Fidelity*
WPA	*Wi-Fi Protected Access*

SUMÁRIO

1. INTRODUÇÃO

Na sociedade atual, a informação é o bem mais precioso que se possui. Um indivíduo ou uma empresa, destaca-se através do conhecimento adquirido com as informações à que estes têm acesso. Todavia, principalmente em empresas, se pensa somente em segurança da informação através de controles de acessos lógicos, esquecendo-se da proteção física dos equipamentos que armazenam as informações.

Com base nessa premissa, este trabalho irá abordar tecnologias empregadas em controles de acesso físico a um ambiente. Dentre essas tecnologias, será visto com maior ênfase, as tecnologias de identificação por rádio frequência, leitura biométrica da digital, algoritmos de criptografia, além da plataforma de prototipação Arduino.

1.1 OBJETIVO GERAL

Desenvolver o protótipo de um sistema de controle de acesso físico que ofereça segurança no acesso através de duas etapas de autenticação, utilizando as tecnologias de RFID e leitura biométrica da digital, baseado na plataforma Arduino.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste Trabalho de Conclusão de Curso são:

a) compreender a plataforma Arduino, hardware, linguagem e IDE, que foi a base do sistema de controle de acesso;
b) compreender os conceitos e técnicas de biometria relacionados ao reconhecimento de digital;
c) compreender os conceitos e técnicas envolvidas na utilização da tecnologia RFID;
d) integrar a plataforma Arduino com os leitores de biometria e RFID;
e) desenvolver um protótipo de um sistema de controle de acesso físico;
f) disponibilizar o projeto para a comunidade Arduino.

1.3 JUSTIFICATIVA

Atualmente o bem mais precioso de uma organização é a informação. Esta é gerada através da aquisição de dados de diferentes fontes que, após análise, é transformada em informação e conhecimento.

Com o avanço das tecnologias, essas informações são armazenadas em servidores, *Hard Disks* (HD), *Digital Versatile Disc* (DVD), entre outros meios, que acabam sendo alvos de ataques tantos virtuais quanto reais. É então de suma importância que a organização possua recursos para proteger a informação que possui. Atualmente se dispõe de diversos meios de proteção, tanto lógicos, como por exemplo, firewalls, *Demilitared Zone* (DMZ), Antivírus, entre outros; quanto físicos, como sistema de prevenção contra incêndio, inundação, riscos elétricos, controles de acesso físico, como trancas automatizadas, catracas, entre outros.

O Projeto 21:204.01-010:2001 da Comissão de Estudo de Segurança Física em Instalações de Informática da Associação Brasileira de Normas Técnicas (ABNT), dispõe sobre a segurança física e do ambiente

> Convém que os recursos e instalações de processamento de informações críticas ou sensíveis do negócio sejam mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso. Convém que estas áreas sejam fisicamente protegidas de acesso não autorizado, dano ou interferência. (ABNT, 2001, p 13).

Em uma estrutura de *Data Center* essa necessidade por segurança se torna ainda maior, nota-se que os atuais *Data Centers* comercias são verdadeiros *bunkers*. Porém, nas organizações de pequeno e médio porte, alguns desses sistemas são deixados de lado, seja por questões de orçamento ou mesmo por descuido e despreocupação. Percebeu-se então a necessidade de desenvolver um sistema de controle de acesso físico que pudesse garantir certa segurança no acesso à um *Data Center*.

Segundo Liu e Silverman (2001, tradução nossa), sistemas autenticação são baseados em três preceitos:

a) algo que você é, leitura da digital, da face, da íris, entre outros;

b) algo que você sabe, senhas;

c) e algo que você tem, cartões com identificação por rádio frequência, do

inglês *Radio-Frequency Identification* (RFID), código de barras, entre outros.

Os sistemas atuais são baseados em uma, ou outra, dessas tecnologias. Para controlar e monitorar esses acessos, este trabalho tem por objetivo desenvolver o protótipo de um sistema de controle de acesso utilizando-se de dois dos preceitos mencionados acima, algo que você tem, *tag* RFID e algo que você é, biometria da digital. Esse sistema será desenvolvido sobre a plataforma Arduino.

A plataforma Arduino é composta de um *hardware* para prototipação e também de uma IDE de desenvolvimento. Possui uma linguagem de programação de fácil aprendizagem, derivada da linguagem C/C++. Suas principais vantagens são a utilização de bibliotecas fornecidas por fabricantes e também pela grande comunidade de desenvolvedores que trabalham com essa plataforma no mundo.

A escolha dessas tecnologias se baseia, principalmente, na difusão e atualidade das tecnologias e, secundariamente, no baixo custo dos equipamentos utilizados.

1.4 ESTRUTURA DO TRABALHO

Este documento está dividido em 5 capítulos. O primeiro apresenta uma breve contextualização do projeto, apresentando o problema vislumbrado, a justificativa e os objetivos, geral e específicos.

No segundo capítulo é mostrada uma revisão sobre as áreas de estudo necessárias ao desenvolvimento do projeto, promovendo um maior conhecimento das técnicas, funcionalidades e equipamentos utilizados.

O terceiro capítulo faz uma breve análise de projetos correlatos ao trabalho proposto.

O quarto capítulo apresenta o desenvolvimento do trabalho, este capítulo está dividido em 2 partes principais, a montagem dos componentes e a programação do Arduino além das principais dificuldades encontradas.

Por fim, o quinto capítulo apresenta as considerações finais e os trabalhos futuros.

2. FUNDAMENTAÇÃO TEÓRICA

1.5 SEGURANÇA DA INFORMAÇÃO

Por informação entende-se todo conjunto de dados que possua valor para uma organização ou para um indivíduo, atualmente, é um recurso de grande valor para a sociedade. Com a utilização de sistemas informatizados cada vez mais integrados e conectados através das redes, as informações trafegadas e armazenadas estão vulneráveis e sujeitas a diversas ameaças que podem comprometer a sua integridade, prejudicando a organização ou o indivíduo que é mantenedor dessa informação. Nesse contexto a segurança da informação é essencial, sendo considerada crítica em alguns casos, pois ela deve garantir menores riscos de erros, fraudes, roubos e uso indevido das informações (FERREIRA, 2003).

A segurança da informação pode ser afetada de várias formas, por comportamentos dos usuários, por indivíduos mal-intencionados que visam destruir, furtar ou alterar a informação e por características de ambiente, fogo, água, eletricidade entre outros. Com uma política de segurança podem ser definidos níveis de acesso, juntamente com proteções lógicas e físicas para acesso ás informações contidas, por exemplo, em um *Data Center*. Todavia, alguns fatores necessitam serem observados quando se considera tal implementação, tais como riscos existentes, benefícios, esforços de implementação e custos gerados (FERREIRA, 2003).

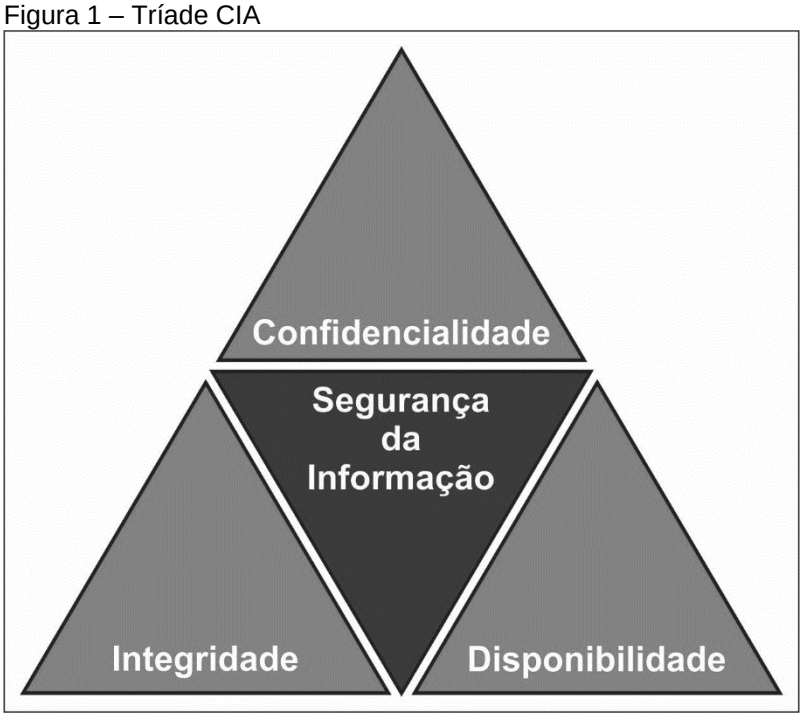
1.5.1 Histórico

Conforme Nakamura e Geus (2007), nas décadas de 70 e 80, o principal enfoque da segurança em organizações, era o sigilo dos dados. Após o surgimento das redes, nas décadas de 80 e 90, passou-se a dar importância para a integridade, tendo em vista a informação e não mais os dados. A partir da década de 90, a informática tornou-se algo essencial nos negócios, e, a partir do crescimento das redes, a disponibilidade passou a ter maior atenção.

1.5.2 Princípios básicos

A segurança da informação possui três princípios básicos que são representados pela tríade conhecida como Confidencialidade, Integridade e Disponibilidade, do inglês *Confidentiality, Integrity* e *Availability* (CIA).

Figura 1 – Tríade CIA



Fonte: Abreu (2011).

Esta tríade, vista na figura 1, representa os principais atributos do conceito de segurança da informação orientando a análise, o planejamento e a implementação de um sistema de segurança sobre um determinado conjunto de dados (informação), que deverá ser protegido, sendo definidos a seguir (BAUMANN; CAVIN; SCHMID, 2006, tradução nossa):

a) **confidencialidade (*confidentiality*)**: significa que estes dados devem estar disponíveis somente para os usuários apropriados, ou seja, somente pessoas previamente autorizadas podem ter acesso ao seu conteúdo, sendo vetada a visualização e manipulação por qualquer pessoa não autorizada. Aqui aplica-se tanto a segurança física quando lógica;
b) **integridade (*integrity*)**: refere-se à certeza de que os dados apresentados não foram alterados, por pessoas não autorizadas.

Existem basicamente dois momentos em que a informação pode ter sua integridade comprometida, no momento da transmissão e/ou durante a escrita ou leitura dos dados;

c) **disponibilidade (*availability*)**: assegura que a informação deverá estar disponível, sempre que for solicitada. Para garantir a disponibilidade, são usados sistemas de controle de falhas elétricas, de desastres naturais, de falhas de hardware, links de Internet, entre outros.

Além dos três atributos principais, pode-se citar ainda, o não-repúdio, a autenticidade e a privacidade – este último surgiu recentemente a partir da preocupação com a proteção dos dados disponibilizados na Internet. O não-repúdio pode ser entendido como a junção entre autenticidade e integridade da informação, é a garantia da origem da informação e de que ela não sofreu nenhuma alteração durante qualquer processo (STONEBURNER, 2001, tradução nossa).

Segundo Stoneburner (2001, tradução nossa), a segurança é obtida através da relação e da implementação de quatro princípios de segurança, os três mencionados anteriormente, confidencialidade, integridade e disponibilidade, com o acréscimo de sistemas de auditoria. A auditoria, é a análise sobre as formas com que os recursos são utilizados, por quem são utilizados, quando foram utilizados e que alterações foram realizadas.

Conforme Ferreira (2003), há ligação entre todos esses princípios, a confidencialidade depende da integridade, pois uma vez perdida, faz com que os mecanismos aplicados para controle da confidencialidade não sejam mais confiáveis; a integridade depende da confidencialidade, caso alguma informação confidencial seja perdida ou obtida de alguma forma, pode-se desativar os mecanismos que garantem a integridade, como a senha do administrador do sistema, por exemplo; por último há a dependência entre estes e a auditoria e disponibilidade, pois estes garantem a auditoria através dos registros históricos e a disponibilidade do sistema respectivamente. Para aplicar estes princípios, utilizam-se mecanismos de segurança, ou seja, recursos disponíveis para garantir que sejam oferecidos níveis de segurança corretos, às informações que se quer proteger.

1.5.3 Mecanismos de segurança

Para se aplicar e dar suporte aos princípios básicos de segurança da informação são utilizados recursos de controle lógicos e físicos:

a) **controles lógicos**: definem-se como barreiras que limitam ou impedem o acesso à informação através de recursos de software como assinatura digital, autenticação, firewall, criptografia entre outros;

b) **controles físicos**: são as barreiras que limitam o contato ou acesso direto à infraestrutura onde encontra-se a informação, além dos mecanismos que garantem a segurança do ambiente contra água, fogo, temperatura, entre outros, pode-se citar como exemplos desses controles portas reforçadas, trancas com controles biométricos, circuito fechado de televisão (CFTV), entre outros.

1.6 CRIPTOGRAFIA

Criptografia é a ciência ou o estudo de técnicas de escrita secreta e ocultação de mensagens. Sendo tão ampla quanto a linguística formal, ocultando o conteúdo daqueles que não possuem o conhecimento para decifrá-la (KAHN, 1967, tradução nossa).

Também especifica os algoritmos de criptografia moderna, utilizados para proteger as transações feitas através de redes digitais. Criptografia constitui qualquer método utilizado para esconder uma mensagem, ou o seu significado, em algum meio, seja físico ou digital (MCDONALD, [2010], tradução nossa).

1.6.1 Definições

Encriptação é um elemento especifico da criptografia, onde se ocultam os dados ou informações, transformando-o em um código indecifrável. Normalmente se utiliza um parâmetro ou uma chave especifica para executar a transformação dos dados. Alguns algoritmos exigem que a chave tenha o mesmo comprimento da mensagem, enquanto outros podem trabalhar com chaves bem menores em relação à mensagem (KAHN, 1967, tradução nossa).

Decriptação, ou decriptografia, é classificada como o oposto da encriptação. Decriptação de uma informação criptografada retornará o valor original da informação (MCDONALD, [2010], tradução nossa).

Segundo Churchhouse (2001, tradução nossa), cifras são métodos ou processos de criptografia que produzem a informação criptografa de acordo com regras definidas para criptografar ou decriptografar mensagens.

A operação de uma cifra depende, em grande parte, do uso de uma chave de encriptação. Esta pode ser qualquer informação auxiliar, adicionada a cifra, para produzir os resultados esperados (MCDONALD, [2010], tradução nossa).

O texto original de uma mensagem, antes de ter sido criptografado é referido como *plaintext*, ou texto simples, após ter sido criptografado é referido como *ciphertext*, ou texto cifrado (CHURCHHOUSE, 2001, tradução nossa).

Conforme McDonald ([2010], tradução nossa), muitos sistemas de encriptação, transportam várias camadas de criptografia, onde o *ciphertext* de uma camada se torna o *plaintext* da camada seguinte.

Criptoanálise são procedimentos, processos e métodos utilizados para traduzir ou interpretar mensagens ocultas, comunicação, códigos e cifras, onde a chave é desconhecida. Embora sempre com o mesmo objetivo os métodos e técnicas de análise criptográfica sofrem mudanças drásticas ao longo do tempo, com a tentativa de adequar-se à crescente complexidade da criptografia (MCDONALD, [2010], tradução nossa).

1.6.2 Histórico

1.6.2.1 Criptografia antiga

Segundo McDonald ([2010], tradução nossa), o texto mais antigo conhecido contendo componentes de criptografia é de cerca de 4.000 anos atrás, no antigo Egito. Por volta de 1900 antes de Cristo (a.C.), o escriba do nobre Khnumhotep II, usou um número de símbolos incomuns para ocultar o significado das inscrições em sua tumba. Este é um método de encriptação conhecido como cifra de substituição, que é qualquer sistema de criptografia que substitui um símbolo ou caractere por outro. À medida em que a cultura egípcia evolui, a substituição hieroglífica tornou-se mais

comum. Este método foi relativamente fácil de quebrar por aqueles que sabiam ler e escrever.

Por volta de 500 a.C. os espartanos desenvolveram um dispositivo para troca de mensagens secretas chamado *Scytale*, também conhecido como Bastão de Licurgo. Na figura 2 é possível ver um exemplo.

Figura 2 – *Scytale* ou Bastão de Licurgo

Fonte: McDonald ([2010]).

O *Scytale* consistia em um cilindro, de um diâmetro especifico, onde um pergaminho era enrolado e a mensagem escrita, ao desenrolar o pergaminho, este só poderia ser lido por alguém com um pergaminho idêntico ao original, dessa forma as letras estariam alinhadas corretamente resultando na mensagem original. Este é um exemplo de cifra de transposição, que é qualquer sistema de cifra em que se alteram a ordem dos caracteres em vez de alterar os próprios caracteres. Nos padrões atuais o *Scytale* poderia ser facilmente decifrado, no entanto a 2.500 anos o percentual de pessoas que sabiam ler e escrever era relativamente pequeno, assim, este era um método seguro de comunicação dos espartanos (MCDONALD, [2010], tradução nossa).

Segundo McDonald ([2010], tradução nossa), o mais antigo registro de uso militar de criptografia é de 2.000 anos atrás, quando o imperador Júlio César resolveu o problema de comunicação segura com suas tropas. À época, mensageiros de mensagens secretas eram frequentemente ultrapassados pelo inimigo. César desenvolveu um método de cifra de substituição, onde as letras eram substituídas por letras diferentes, seguindo algum número predeterminado. Na figura 3 pode-se

observar como funciona a substituição através de uma chave número 3, por exemplo. Dessa forma, apenas aqueles que conheciam a substituição poderiam decifrar as mensagens. Agora, quando as mensagens fossem interceptadas o inimigo não poderia ler o conteúdo oculto. Isso deu ao exército romano uma grande vantagem durante a guerra.

Figura 3 – Cifra de César (com chave 3)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fonte: Do autor.

Durante meados de 1400, Leon Battista Alberti inventou um sistema de criptografia utilizando um disco de cifras. Este dispositivo permitiria, que ao girar o disco, muitos métodos diferentes de substituição fossem aplicados. Este é o conceito base de uma cifra poli alfabética, que é um método de encriptação que passa por várias cifras de substituição. Alberti é considerado o pai da criptografia ocidental. Todavia, Alberti nunca desenvolveu seu conceito de disco de cifras (KAHN, 1967, tradução nossa).

Ainda conforme Kahn (1967, tradução nossa), em 1500 Blaise Vigenère, seguindo o estilo de codificação poli alfabética de Alberti, criou a cifra conhecida como Cifra de Vigenère. Seu funcionamento é exatamente como a Cifra de Cesar, a exceção de que ele altera a chave em todo o processo de criptografia. A Cifra Vigenère utiliza uma tabela de letras que fornece o método de substituição, chamada de Praça Vigenère, vista na figura 4. A tabela é formada por um alfabeto de 26 letras deslocado um do outro por uma letra. Na figura 5 pode-se ver um exemplo da aplicação dessa cifra.

Figura 4 – Praça de Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Donda ([2007]).

Figura 5 – Mensagem criptografada com a Cifra de Vigenère

Chave: SEGREDO															
Chave	S	E	G	R	E	D	O	S	E	G	R	E	D	O	S
Plaintext	M	E	N	S	A	G	E	M	S	E	C	R	E	T	A
Ciphertext	E	I	T	J	E	J	S	E	W	K	T	V	H	H	S

Fonte: Do autor.

No final da primeira guerra mundial, Arthur Scherbius inventou a Enigma, uma máquina eletromecânica utilizada para criptografia e decriptografia de mensagens secretas. Pode-se ver um exemplar na figura 6.

Figura 6 – Máquina de criptografia Enigma

Fonte: McDonald ([2010]).

Esta máquina, possuía, em sua configuração original, vários discos rotores e engrenagens que permitiam até 10114 configurações possíveis. Devido ao grande número de configurações, a Enigma era praticamente inquebrável com métodos de força bruta. Durante a segunda guerra mundial é que a máquina ficou realmente conhecida, devido a sua larga utilização pela Alemanha nazista. Contudo, em 1940 o matemático Allan Turing, criou uma máquina capaz de decriptografar as mensagens enviadas pela Enigma (MCDONALD, [2010], tradução nossa).

1.6.2.2 Criptografia moderna

O algoritmo de criptografia *one-time-pad* foi criado no início de 1900, e tem sido considerado inquebrável. Este algoritmo é derivado de uma cifra anterior chamada Cifra Vernan, criada por Gilbert Vernan. A Cifra Vernan era uma cifra que combinava uma mensagem com a chave lida, em uma fita de papel. Não era considerada inquebrável, até que Joseph Mauborgne reconheceu que, se a chave for

completamente aleatória, a dificuldade da criptoanálise seria igual a tentar cada chave possível (KAHN, 1967, tradução nossa).

Mesmo tentando cada chave possível, ainda seria necessário analisar cada tentativa de decriptação para verificar se foi utilizada a chave adequada. O aspecto inquebrável do *one-time-pad*, vem de duas hipóteses: A chave utilizada é completamente aleatória; e a chave só pode ser utilizada uma única vez (MCDONALD, [2010], tradução nossa).

A grande parte dos algoritmos e métodos de criptografia citados até o momento utilizam o princípio de chave simétrica, chamada também de chave privada, é qualquer cifra em que a chave para encriptação é a mesma para decriptação. O grande problema desse tipo de cifra é que a chave precisa manter-se sempre secreta. Muitos algoritmos modernos implementam o sistema de chave simétrica.

Um método de chave simétrica é a cifra de fluxo, em que um fluxo de números aleatórios, são combinados com a mensagem original. Como exemplo pode-se citar: *One-time-pad*, *Linear-Feedback Shift Register*, (LFSR) e *Rivest Cipher Version 4* (RC4). Sendo o RC4, a cifra de fluxo mais amplamente utilizada, é utilizada nos protocolos *Secure Sockets Layer* (SSL) e *Transport Layer Security* (TLS), para proteger o tráfico de Internet, e na proteção de redes sem fio, nos protocolos *Wired Equivalent Privacy* (WEP) e *Wi-Fi Protected Access* (WPA) (MCDONALD, [2010], tradução nossa).

Outro método de criptografia de chave simétrica é a cifra de bloco, que opera em um grupo fixo de bits. Na encriptação, pega-se um bloco de 128 bits de *plaintext* e gera-se um bloco de *ciphertext* de tamanho correspondente, ou seja, 128 bits. O controle exato de transformação é controlado pela chave de encriptação/decriptação. Exemplos de cifras de bloco incluem: *Blo*wfish, *Data Encryption Standard* (DES) e *Advanced Encryption Standard* (AES). Este último é um padrão de criptografia adotado pelo governo dos Estados Unidos, e aprovado pela Agência de Segurança Nacional, do inglês *National Security Agency* (NSA) para encriptação de documentos considerados *top secret*. Alguns métodos atuais de criptografia de chave simétrica implementam ambos os métodos de cifras de bloco e fluxo (MCDONALD, [2010], tradução nossa).

Segundo McDonald ([2010], tradução nossa), a era digital da década de 1970 provocou a necessidade de um método de criptografia que contaria com uma

chave predeterminada. Criptógrafos dessa época, perceberam a necessidade de que, para enviar uma mensagem sem uma reunião prévia com o destinatário, seria necessário um sistema que utilizasse uma chave para encriptação e outra diferente para a decriptação.

Em 1977, Ron Rivest, Adi Shamir e Leonard Adleman, desenvolveram o método que viria a ser conhecido como criptografia RSA, nomeada com base em seus sobrenomes. A criptografia RSA baseia-se na multiplicação e exponenciação. Este protocolo é construído a partir de dois números primos grandes, que são manipulados para gerar uma chave pública e uma chave privada. Uma vez geradas, estas chaves podem ser utilizadas várias vezes. Enquanto a chave privada deve ser mantida em segredo, a chave pública pode ser divulgada livremente. Dessa forma, qualquer pessoa pode criptografar uma mensagem através da chave pública e enviá-la ao portador da chave privada, que a usa para decriptar a mensagem. Um dos números especiais e utilizados na criptografia RSA é o módulo, que é o produto de dois números primos. A força do RSA depende da dificuldade em produzir esses cálculos. O RSA é o algoritmo de chave assimétrica mais utilizado em protocolos de comércio eletrônico (MCDONALD, [2010], tradução nossa).

1.6.3 Algoritmo RC4

Segundo Salas e Pereira (2011), o RC4, originalmente desenvolvido por Ron Rivest, para a empresa RSA Security em 1987, é um algoritmo de chave simétrica, é uma cifra de fluxo com tamanho de chave variável orientada a byte. Se tornou bastante utilizada em várias aplicações como Internet Explorer, Adobe Acrobat, entre outros. Tornou-se pública em 1994 através de um vazamento em uma lista de discussão sobre criptografia, a Cipherpunks.

1.6.3.1 Funcionamento

Dentre as utilizações atuais do RC4 pode-se citar os protocolos WEP e WPA, que são protocolos de segurança para redes *Wireless Fidelity* (WIFI) e SSL e TLS, que são protocolos de segurança na Internet utilizados em conexões *Hyper Text*

Transfer Protocol Secure (HTTPS). O algoritmo RC4 é extremamente rápido quando implementado em software (ALFARDAN et al, 2013, tradução nossa).

Em um algoritmo de fluxo, os bits do *plaintext* são combinados através de operação de Xor, bit a bit ou unidades maiores, conforme definido na programação, contra uma cadeia de bits pseudoaleatórios, também chamados *keystream*. Numa operação Xor, os bits ativos em A (chave) ou em B (*plaintext*), porém, não em ambos, são ativados, gerando C (*ciphertext*). Como pode-se observar no exemplo abaixo.

A	^	B	=	C
01000	^	10111	=	11111
11111	^	01000	=	10111
10111	^	01010	=	11101
00010	^	00000	=	00010
00011	^	11111	=	11101

Segundo Salas e Pereira (2011), o RC4 se divide em dois algoritmos: um algoritmo de agendamento de chaves, do inglês *Key Scheduling Algorithm* (KSA) e um algoritmo de geração pseudoaleatória, do inglês *Pseudo-Random Generation Algorithm* (PRGA). O KSA consiste em iniciar um vetor V de 256 Bytes como uma substituição de todos os números de 8 bits. Essa substituição é condicionada a chave C utilizada no algoritmo. Na figura 7 tem-se um pseudocódigo do KSA.

Figura 7 – Algoritmo KSA

```
Para (i = 0 e i <256; i ++)
V[i] = i
T [i] = C[i Módulo do tamanho da chave C]
Fim do para
j = 0
Para (i = 0 e i <256; i ++)
j = (j + V[i] + T[i]) Módulo de 256
Swap {V[i], V[j])
Fim do para
```

Fonte: Salas e Pereira (2011).

Já a segunda etapa do algoritmo, o PRGA, visto da figura 8, consiste em gerar um fluxo de bytes contendo números pseudoaleatórios, que são números imprevisíveis sem o conhecimento da chave, que serão utilizados para fazer a operação Xor com o fluxo de bytes do *plaintext* produzindo assim o *ciphertext*.

Normalmente utilizam-se chaves diferentes a cada seção, dessa forma uma mesma chave não será utilizada para uma sequência muito longa de bytes. Nos protocolos de rede, por exemplo, é possível utilizar uma chave diferente para cada pacote transmitido (ALFARDAN et al, 2013, tradução nossa).

Figura 8 – Algoritmo PRGA

```
i=0
j=0
Enquanto for verdade faça
i = (i + 1) módulo de 256
j = (j + V[i]) módulo de 256
swap(V[i], V[j])
t = (V[i] + V[j]) módulo de 256
c = V[t]
Fim do enquanto
```

Fonte: Salas e Pereira (2011).

1.6.3.2 Segurança

Os primeiros ataques de criptoanálise ao RC4, começaram a surgir logo após a publicação na lista Cipherpunks, em 1994. Mas somente em 2001 surgiu um ataque significativo, quando Scott Fluhrer, Itsik Martin e Adi Shamir, demonstraram que o RC4 possuía vulnerabilidades no KSA, sendo possíveis ataques práticos aos protocolos que utilizassem esse algoritmo, todavia sem realizar os ataques. Em 2002 foram realizados alguns ataques seguindo o modelo proposto por Shamir, mostrando as vulnerabilidades de segurança do protocolo WEP (SALAS; PEREIRA, 2011).

Nos anos seguintes, seguidos ataques sobre o RC4 foram praticados. Em 2006, Andreas Klein, publicou dois ataques, o primeiro demonstrava uma correlação entre os primeiros bytes do *keystream* com os primeiros bytes da chave, permitindo uma grande diminuição na quantidade de vetores de inicialização, do inglês *initialization vector* (IV), necessários em um ataque, o segundo ataque não necessitava dos primeiros bytes do fluxo do *keystream*. Este segundo ataque possui uma complexidade computacional maior do que os ataques realizados até então (KLEIN, 2007, tradução nossa).

Apesar das vulnerabilidades apresentadas acima, o RC4 pode ser considerado seguro se for utilizado através de uma implementação segura. Um exemplo dessa possibilidade é o protocolo TLS. Sua segurança é devido ao seu pré-

processo da chave e do IV através do uso de funções de *hash* seguras, como o *Message-Digest Algorithm 5* (MD5), *Secure Hash Algorithm* (SHA), entre outras, isso resulta em chaves completamente diferentes não relacionadas entre as seções de comunicação (SALAS; PEREIRA, 2011).

Uma recomendação de segurança para a utilização do RC4, feita pela criadora do protocolo, a empresa RSA Security, diz que para um uso seguro do RC4, os primeiros 256 bytes do fluxo do *keystream* gerados, devem ser ignorados, evitando assim as fraquezas do algoritmo KSA. Os ataques apresentados contra a cifra RC4 atuam apenas sobre o KSA. Todavia, o centro da criptografia RC4 que é o PRGA, ainda pode ser considerado seguro, desde que seguidas essas recomendações (RSA SECURITY, [2001], tradução nossa).

1.7 BIOMETRIA

Entende-se por biometria, a medida de características únicas encontradas em um indivíduo, que podem ser utilizados para reconhecê-lo e confirmar sua identidade (LIU; SILVERMAN, 2001, tradução nossa).

Biometria é um ramo da ciência que estuda formas de mensurar os seres vivos. Tecnologicamente, é a identificação automatizada de um indivíduo através de características físicas ou comportamentais especificas (GUMZ, 2002).

Ainda segundo Gumz (2002), as características comportamentais, podem ser influenciadas por fatores químicos ou biológicos, visto que são reflexos de atitudes psicológicas do indivíduo. Exemplos destas características são o reconhecimento de voz, a assinatura manuscrita, a maneira de digitar em um teclado, entre outras. As características físicas, entretanto, são basicamente imutáveis e estão presentes no próprio corpo do indivíduo. Entre estas, pode-se citar o reconhecimento de digitais, da íris, da face, da palma da mão, entre outras. Nota-se que as características físicas são mais seguras na identificação, com exceção de algum ferimento no dedo, por exemplo, as digitais são iguais durante toda a vida. Ao contrário de uma assinatura, que é influenciada por fatores emocionais ou fisicamente controláveis. Os sistemas de identificação baseados em características comportamentais, deverão ser reajustados com frequência para se adequar as variações ocorridas ao longo dos anos.

Entre os principais usos de sistemas de identificação biométrica, pode-se citar o utilizado no âmbito policial para identificar suspeitos de um crime. Entretanto a biometria está inserida também em outras atividades. Atualmente é grande a preocupação em evitar fraudes através da correta identificação de um indivíduo. Os computadores têm se tornado um item essencial desses sistemas, agilizando e garantindo precisão no processo de identificação. Pode-se classificar os sistemas automáticos de identificação biométrica de acordo com o seu funcionamento, em um para um ou um para muitos (SUCUPIRA JÚNIOR, 2004).

Ainda conforme Sucupira Júnior (2004), em um sistema um para um compara-se a informação apresentada pelo usuário à uma informação pré-existente no sistema vinculada à esse usuário, dessa forma, o sistema irá verificar se existe uma igualdade entre os dados encontrados, ou seja, o usuário apresenta, por exemplo, um código para se identificar ao sistema, posteriormente o sistema irá solicitar a informação biométrica para compará-la com a informação anexada ao código de identificação desse usuário, em caso de igualdade entre todas as informações apresentadas ocorre a liberação do acesso à esse usuário. Dá-se o nome de sistema de verificação aos sistemas construídos dessa forma.

Já um sistema um para muitos, por outro lado, realiza uma busca em sua base de dados a procura de algum registro que seja igual a informação biométrica informada. Estes sistemas tem um custo maior de processamento, pois o sistema deverá comparar a informação de entrada com basicamente todos os registros do banco de dados. Um exemplo dessa aplicação são os relógios ponto, onde o usuário informa a sua digital e o sistema percorre a base de dados para identificar à qual individuo pertence à digital apresentada. Estes sistemas são chamados de sistema de identificação (SUCUPIRA JÚNIOR, 2004).

1.7.1 Tipos de sistemas biométricos

Abaixo serão apresentados os tipos mais comuns de sistemas baseados em características biométricas utilizados na identificação pessoal (LIU; SILVERMAN, 2001, tradução nossa):

a) **voz**: este sistema realiza a conversão da voz em texto. Há um grande potencial de crescimento na utilização dessa técnica, não sendo

necessário nenhum hardware específico além de um microfone. Porém, ruídos externos influenciam no desempenho desse sistema;

b) **assinatura manuscrita**: analisa a maneira que um indivíduo escreve seu nome, levando em consideração características como a pressão, velocidade e formato da assinatura. Neste sistema não é necessário que o usuário entre diretamente em contato com o sistema;
c) **face**: esse tipo de sistema é utilizado com o intuito de identificar um indivíduo em meio à uma multidão. Para realizar a identificação considera-se as curvas do rosto, entre outros aspectos geométricos como a distância entre a boca e o queixo e entre os dois olhos, por exemplo;
d) **retina**: realiza a análise dos vasos sanguíneos localizados atrás dos olhos. É altamente precisa, porém, por necessitar de contato direto com o sistema de escaneamento da retina, não é muito popular entre os usuários;
e) **íris**: nesse sistema são analisadas as características do anel de tecido colorido encontrado ao redor da pupila. Encontram-se aproximadamente 250 pontos de diferenciação em cada íris;
f) **impressão digital**: também chamado de datiloscopia, é baseado nas características encontradas nos desenhos papilares que estão presentes nas pontas dos dedos. Atualmente é o sistema mais utilizado.

A tabela 1 mostra um comparativo entre os tipos de biometria citados.

Tabela 1 – Comparativo entre os tipos de biometria

Características	Digital	Retina	Iris	Face	Assinatura	Voz
Facilidade de uso	Alta	Baixa	Média	Média	Alta	Alta
Incidência de erros	Sujeira, idade	Óculos	Má iluminação	Idade, óculos, cabelo	Alteração na assinatura	Ruído, resfriado
Precisão	Alta	Muito alta	Muito alta	Alta	Alta	Alta
Aceitação do usuário	Médio	Médio	Médio	Médio	Muito alta	Alta
Nível de segurança necessário	Alta	Alta	Muito alta	Média	Média	Média
Estabilidade a longo prazo	Alta	Alta	Alta	Media	Media	Media

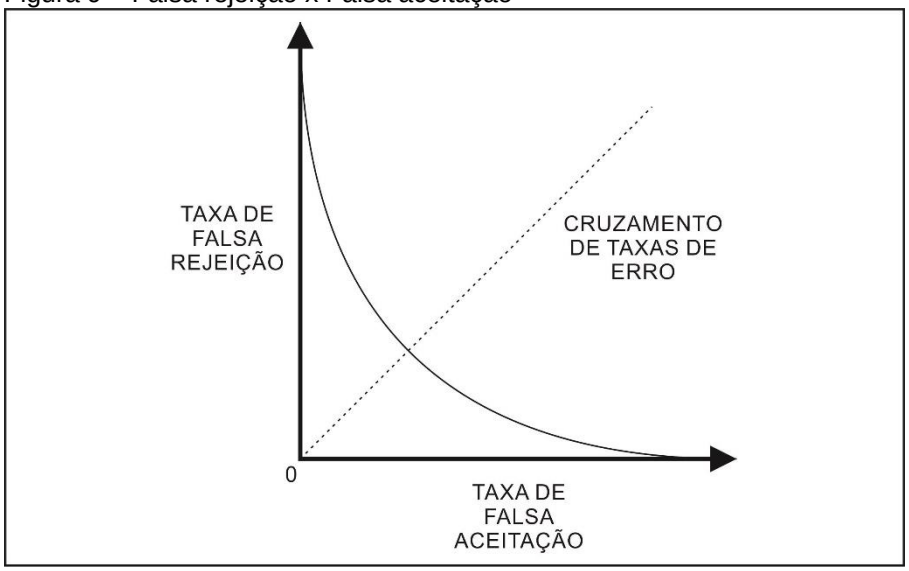
Fonte: Liu e Silverman (2001, tradução nossa).

1.7.2 Eficiência de um sistema biométrico

A leitura de informações biométricas não é perfeitamente exata. Existem vários fatores que podem influenciar a captura dessas informações, estado emocional ou físico do indivíduo, se tratando de características comportamentais, e fatores externos como a temperatura ou umidade quando analisadas características físicas.

Segundo Liu e Silverman (2001, tradução nossa), existem duas estimativas de erros na autenticação de sistemas biométricos, erros do tipo I e tipo II. Erros do tipo I, também chamados de erro de falsa aceitação, acontecem quando o sistema aceita uma informação biométrica que deveria ser rejeitada, liberando o acesso à um indivíduo não autorizado. Erros do tipo II, também chamados de erro de falsa rejeição, acontecem quando o sistema rejeita uma informação que deveria ser aceita, bloqueando o acesso à um indivíduo autorizado. Quanto menor a probabilidade de ocorrerem esses erros mais confiável é o sistema. Percebeu-se, todavia, que a medida em que os erros de tipo I são reduzidos, os erros de tipo II são proporcionalmente aumentados, conforme mostrado na figura 9. Não sendo possível, portanto, eliminar qualquer um deles.

Figura 9 – Falsa rejeição x Falsa aceitação



Fonte: Liu e Silverman (2001, tradução nossa).

Conforme Liu e Silverman (2001, tradução nossa), ajusta-se essas taxas com base no nível de segurança pretendido no sistema. Caso queira-se um sistema mais seguro quanto ao acesso de pessoas não autorizadas, baixa-se a taxa de falsa aceitação à 0. Porém, os usuários do sistema terão maior dificuldade em sua utilização, pois a taxa de falsa rejeição irá aumentar e poderá ser necessário um maior número de tentativas de acesso para que ele seja aceito.

1.8 DATILOSCOPIA

Segundo Kehdy (1968), datiloscopia é a ciência baseada na comparação entre as impressões digitais, sejam elas impressas ou armazenadas em um banco de dados, com a intenção de identificar um indivíduo. Para realizar essas comparações, é realizada a verificação de pontos específicos, conhecidos como minúcias.

1.8.1 História da datiloscopia

As primeiras utilizações de impressão digital datam de 782 depois de Cristo (d.C.), quando estas, eram utilizadas para firmar acordos. Em 1300 esse sistema já era empregado na identificação de criminosos pelos chineses. No ano de 1664 o médico italiano Marcelo Malpighi, publicou um estudo sobre os desenhos da digital e da palma da mão chamado Epístola sobre o órgão do tato. Já em 1900 na Inglaterra,

Edward Richard Henry publicou o livro *Classification and Uses of Fingerprints*, onde expõe um novo sistema de identificação datiloscópico através da adoção de 4 tipos fundamentais de minúcias: arcos, presilhas, verticilos e compostos. Sistema que foi adotado oficialmente pela *Scotland Yard* em 1901. Em 1963 é inaugurado em Brasília, o Instituto Nacional de Identificação, com o objetivo de centralizar a identificação criminal no Brasil. O instituto de Identificação de São Paulo, possuía em 1998, aproximadamente 40 milhões de prontuários e expedia diariamente, uma média de 15 mil cédulas de identidade e 300 atestados de antecedentes criminais. Desde 2008 a biometria vem sendo utilizada pela Justiça Eleitoral como forma de garantir mais segurança às eleições brasileiras, nas eleições de 2014 cerca de 21 milhões de pessoas foram identificadas utilizando o sistema de impressão digital.

Pode-se verificar, assim, a evolução no processo de identificação utilizando o sistema de impressão digital. Percebe-se ainda, visto os vários estudos realizados por importantes e respeitáveis entidades, a importância dada a esse método, além da confiança no mesmo.

1.8.2 Princípios da datiloscopia

Segundo Gumz (2002), pode-se dividir a datiloscopia em clínica, criminal e civil, utiliza-se a clínica para estudar perturbações causadas por doenças, em impressões digitais. Na criminal, analisam-se as marcas de impressões digitais deixadas em uma cena de crime, para identificar um possível suspeito. Já a civil, é usada na autenticação de um indivíduo para que este tenha acesso à recursos protegidos, como por exemplo, carteira profissional, identidade, entre outros.

Para Hong (1998, tradução nossa), para que as características físicas como face, íris, retina, digitais e outras, possam ser utilizadas para identificação biométrica, elas devem respeitar as seguintes condições:

a) **universalidade**: é necessário que todos os indivíduos possuam as características escolhidas;
b) **unicidade**: não podem haver dois indivíduos com as mesmas características. Todavia, a unicidade na Datiloscopia depende da quantidade de pontos verificados, conforme será visto na tabela 2;

c) **imutabilidade**: as características escolhidas não podem sofrer alteração no decorrer do tempo;

d) **critério quantitativo**: deve-se poder medir quantitativamente as características escolhidas, ou seja, é necessário que se possa analisar, individualizar e medir os diferentes detalhes presentes, para comparação futura.

Conforme Xiao e Raafat (1991, tradução nossa), ao se analisar a datiloscopia, vê-se que a grande parte dos indivíduos possui impressões digitais, sendo assim uma característica universal. Sabe-se que estas impressões são únicas, havendo diferenciação até mesmo entre os dedos de uma mesma pessoa, não havendo, assim, dois indivíduos com digitais iguais. O desenho característico das digitais é formado aproximadamente no sexto mês de gestação permanecendo inalterado mesmo após a morte e antes do estado de putrefação do corpo. Atendendo ao critério quantitativo, pode-se medir todas essas características e ao encontrar 12 pontos iguais, independentemente da minúcia utilizada, é possível fazer a identificação do indivíduo. Valendo-se desse conceito, verifica-se que as impressões digitais atendem às quatros condições citados acima, podem assim, serem utilizadas em sistemas de identificação biométrica. Salvo em casos raros, onde há uma alteração física por fatores externos, como a perda de um dedo ou uma doença genética, por exemplo.

1.8.3 Classificação dos componentes de uma impressão digital

Com base nos estudos que foram realizados em 1982, por Francis Galton, que classificou em quatro grupos as impressões digitais, Vucetich, em 1904, criou um sistema de identificação através de impressões digitais, com maior atenção no arquivamento e classificação das digitais dos dez dedos das mãos.

Galton classificou as digitais baseando-se nos seguintes tipos de desenhos (RABELLO, 1996):

a) ***arch*** **(arco)**: são desenhos formados por linhas arqueadas e paralelas entre si;

b) ***loop*** **(presilha)**: desenhos que, em sua parte central, apresentam linhas dobradas sobre elas mesmas na forma de presilha ou alça. Estas,

divididas em dois tipos: radial e cubital, conforme as extremidades livres das alças consideradas apontassem, respectivamente, para o rádio ou o cúbito do antebraço;

c) ***whorl* (verticilo)**: estes desenhos são constituídos por linhas em círculos concêntricos ou espiral.

Segundo Rabello (1996), Vucetich, partindo da classificação de Galton, simplesmente realizou a tradução de *arch* para arco, *loop* para presilha e *whorl* para verticilo. Percebeu então que existia um pequeno acidente nas digitais, com o formato de um triangulo, que o chamou de *delta* e foi incluído na classificação, considerando-se a ausência ou presença do mesmo. Os conceitos dos tipos fundamentais de Juan Vucetich ficaram os seguintes:

a) **arco**: imagem da digital que não possui *delta*. Suas linhas atravessam a digital de um lado ao outro, com uma forma abaulada;

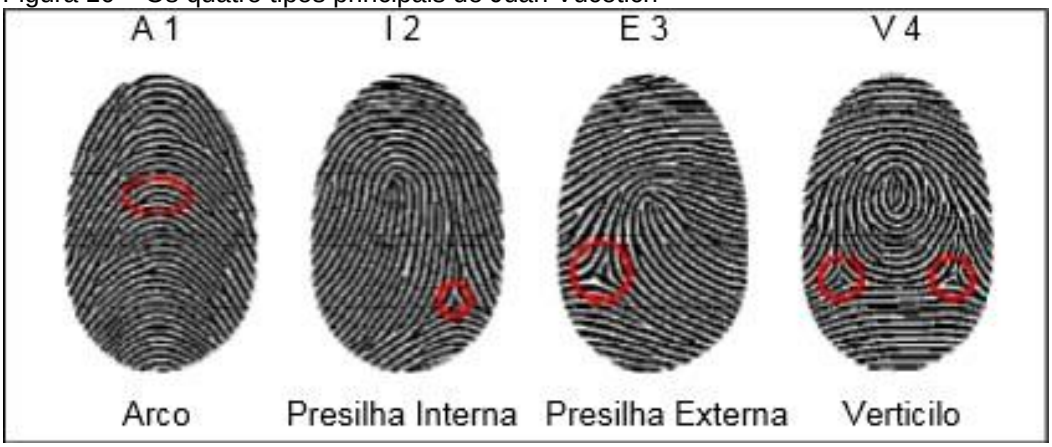
b) **presilha interna**: mostra um *delta* à direita do observador, com as linhas da região do núcleo dirigindo-se à esquerda;

c) **presilha externa**: mostra o *delta* à esquerda do observador, com as linhas do núcleo dirigindo-se à direita;

d) **verticilo**: normalmente apresenta dois *deltas*, uma à esquerda e um à direita do observador. Outra característica são as linhas da região nuclear que se encerram entre as linhas que prolongam dos *deltas*.

Foi também definido por Vucetich, os símbolos característicos dos tipos de impressões digitais, que auxiliam no armazenamento. Estes são representados de forma literal ou numérica representando os tipos arco (A ou 1), presilha interna (I ou 2), presilha externa (E ou 3) e verticilo (V ou 4). Utilizados, respectivamente, para representar as digitais dos polegares e dos dedos restantes. Os desenhos de digitais que seguem esta classificação, são representados na figura 10.

Figura 10 – Os quatro tipos principais de Juan Vucetich



Fonte: Gumz (2002).

As impressões digitais adquiridas devem ser classificadas conforme os grupos citados anteriormente. Todavia, existe a possibilidade de que o sistema não consiga classificar a digital em uma dessas classes, nesses casos a imagem será classificada em uma classe X. Caso a digital verificada for classificada em um grupo diferente da que se encontra no banco de dados, a identidade do indivíduo pode ser negada, pois a igualdade de tipos, não significa que as digitais sejam de um mesmo indivíduo.

Sabendo-se que as impressões digitais adquiridas podem ser classificadas em um mesmo grupo, são levados em consideração outras características para melhor identificar as digitais. Estas chamam-se minúcias e serão abordadas a seguir.

1.8.4 Segurança de um sistema datiloscópico – Regra dos 12 pontos

Segundo Martins e Nascimento (2011), a regra nos diz que são necessários no mínimo 12 pontos de análise para se confirmar uma identidade. Mesmo após muitos estudos, ninguém sabe ao certo a origem dessa determinação. Foi somente em 1914 que o francês Edmond Locard, publicou o artigo *La Preuve Judiciaire par les Empreintes Digitales*, em Lyon, onde apresentou a teoria que ficaria conhecida como Teoria Tripartite:

a) se mais de 12 pontos característicos estão presentes e a digital está clara, então a certeza de identidade é indubitável;
b) se 8 ou 12 pontos estão envolvidos, então o caso está no limite e a certeza de identidade dependerá: da qualidade da impressão digital; da

raridade do tipo em questão; da presença do núcleo e\ou do *delta* da impressão; da presença de poros; da perfeita e clara identidade em relação aos sulcos e cristas; da direção das linhas e do valor do ângulo nas bifurcações. Nestes casos, a certeza é obtida somente após uma discussão por um ou mais especialistas competentes e experientes;

c) se um número limitado de pontos característicos está presente, o fragmento de impressão digital não pode fornecer certeza para a identificação, mas apenas presunção proporcional ao número de pontos característicos disponíveis e deles identificados.

Nota-se que a primeira parte do texto, que ficou mais conhecida, fala em mais de 12 pontos, ou seja, no mínimo 13 pontos de coincidência, porém, a tabela 2, a seguir, nos mostra que 12 pontos são suficientes para uma identificação positiva. A segunda parte mostra exatamente o que se utiliza atualmente, a análise completa das minúcias contidas na digital. A terceira parte acabou sendo abandonada. No âmbito da prática criminalística, opiniões qualificadas, também chamadas de opinião de probabilidade, são dadas como evidência.

A datiloscopista da Polícia Federal, Clemil José de Araújo, do Instituto Nacional de Identificação do Distrito Federal, publicou em 2003 um artigo, onde apresenta um interessante exercício de probabilidade. Usando a teoria matemática das probabilidades, pode-se definir que se um evento pode ocorrer de “a” formas e falhar de “b” formas, sendo cada hipótese igualmente provável, a probabilidade de ocorrência é de $\frac{a}{a} + b$ e de não ocorrer é de $\frac{a}{a} + b$. Pode-se aplicar essa fórmula para a ocorrência de pontos característicos nas cristas papilares. Uma impressão pousada apresenta, em média, 50 linhas, sendo cada uma delas, em média, com 35 pontos característicos.

Assim, a probabilidade de ocorrência de um ponto característico numa correspondência exata de local na impressão digital de outro dedo é de $\frac{1}{1} + 49$ ou $\frac{1}{50}$ e de não ocorrer é de $\frac{49}{1} + 49$ ou de $\frac{49}{50}$. Levando em consideração 35 pontos característicos por linha, a probabilidade de uma impressão apresentar coincidência de todos os pontos característicos será de $\frac{1}{50}35$. Assim, 1 em cada 5.035 dedos tem a chance de ter todos os pontos característicos coincidentes.

Sob o mesmo raciocínio, a probabilidade da ocorrência de um único ponto característico em impressões de diferentes dedos, em exata correspondência, é de $\frac{1}{50}1$, de dois pontos característicos é de $\frac{1}{50}2$, que é igual a 1 a cada 2.500, de três pontos será de $\frac{1}{50}3$, ou 1 a cada 125.000 dedos tem a chance de apresentar três pontos característicos coincidentes, o que é equivalente a 6.250 pessoas, assumindo que cada uma possua 20 dedos, incluindo os das mãos e o dos pés. A continuação do raciocínio nos leva aos números da tabela 2 (MARTINS; NASCIMENTO, 2011).

Tabela 2 – Probabilidade de pontos coincidentes em impressões de diferentes dedos

Pontos Coincidentes	Chances de Dedos	Chances de Pessoas
1	50	2
2	2.500	125
3	125.000	6.250
4	6.250.000	312.500
5	312.500.000	15.625.000
6	15.625.000.000	781.250.000
7	781.250.000.000	39.062.500.000
8	39.062.500.000.000	1.953.125.000.000
9	1.953.125.000.000.000	97.656.250.000.000
10	97.656.250.000.000.000	4.882.812.500.000.000
11	4.882.812.500.000.000.000	244.140.625.000.000.000
12	244.140.625.000.000.000.000	12.207.031.250.000.000.000

Fonte: Martins e Nascimento (2011).

Conforme Martins e Nascimento (2011) para se encontrar 12 pontos em comum, seriam necessárias mais de 12 quintilhões de pessoas, número muito maior que a população mundial atual. Nesse exercício não foi considerado o fato de que alguns pontos são mais raros do que outros, e nem a variação de sentido e direção de alguns pontos. Também não foi mencionado que nenhuma das linhas papilares é igual à outra, pois nossos poros sudoríparos, tem formato e posição diferentes, constituindo elementos individualizadores, sendo objetos de estudos da poroscopia.

1.9 RFID

RFID é o acrônico em inglês de *Radio Frequency Identification* – identificação por radiofrequência. É uma tecnologia de identificação que utiliza frequências de rádio para comunicação entre seus componentes. Seu objetivo é melhorar a eficiência na localização e rastreamento de produtos e também oferecer benefícios no registro de bens físicos (GLOVER; BHATT, 2007).

Segundo Igoe (2012, tradução nossa), RFID ou identificação por radiofrequência é uma tecnologia *wireless* que tem como objetivo a coleta automática de dados.

Conforme Ramos e Nascimento (2007), RFID é um método de identificação automática que através de sinais de rádio possibilita a recuperação e o armazenamento remoto através de *tags* RFID.

1.9.1 Histórico

Segundo Santini (2008), a tecnologia RFID, tem suas origens nos sistemas de radares utilizados na Segunda Guerra Mundial. Os ingleses, americanos japoneses e alemães utilizavam radares para poderem identificar com antecedência a aproximação de aviões, porém havia um problema, como distinguir os aviões inimigos dos aviões aliados? Os alemães descobriram então que se girassem seus aviões quando estivessem se aproximando de sua base, o sinal de rádio refletido seria diferente, dessa forma os técnicos responsáveis pelo radar saberiam que esses eram aviões alemães.

De acordo com Ramos e Nascimento (2007), os ingleses, sob o comando de Watson-Watt, desenvolveram o primeiro identificador ativo de amigo ou inimigo do inglês Identify Friend or Foe (IFF). Um transmissor era colocado em cada avião inglês e ao receber sinais dos radares em solo transmitiam um sinal de resposta, que o identificava como amigo.

Porém, a história do RFID começa realmente em 1973, quando Mario W. Cardullo, solicitou a primeira patente americana de um sistema ativo de RFID com memória regravável. Também em 1973, Charles Walton, recebeu a patente de um sistema passivo, utilizado para destrancar uma porta sem precisar das chaves. Ainda

na década de 1970, o governo norte americano trabalhava no desenvolvimento de sistemas de RFID para um sistema de rastreamento de material radioativo para o departamento de energia e outro para rastreamento de gado para o departamento de agricultura (RAMOS; NASCIMENTO, 2007).

Conforme Santini (2008), nessa época utilizavam-se identificadores de baixa frequência, em inglês *Low Frequency* (LF), de 125 kHz, após algum tempo as empresas mudaram para sistema de alta frequência, em inglês *High Frequency* (HF), de 13,56 MHz. Atualmente estes sistemas são utilizados em sistemas de controle de acesso e de pagamento.

No início da década de 1980, a IBM patenteou os sistemas de frequência ultra alta, em inglês *Ultra-High Frequency* (UHF), possibilitando leituras com distâncias superiores aos dez metros. Atualmente a detentora desta patente é a Intermec, empresa provedora de códigos de barra, que comprou os direitos de uso da IBM na década de 1990. A grande expansão do RFID UHF aconteceu em 1999, quando as empresas Uniform Code Concil, EAN International, Procter & Gamble e Gillete fundaram o Auto-id Center, no MIT. Sua intenção era mudar a essência do RFID de um pequeno banco de dados móvel para um número de série, baixando consideravelmente os custos e transformando o RFID em uma tecnologia de rede, interligando objetos à Internet através dos identificadores (SANTINI, 2008).

Entre 1999 e 2003 o Auto-id Center ganhou o apoio do departamento de defesa dos Estados Unidos e de mais 100 companhias. Nesta mesma época diversos laboratórios foram abertos em outros países, iniciando o desenvolvimento de dois protocolos:

a) de interferência aérea (classes 1 e 0);
b) o código eletrônico de produto, do inglês *Electronic Product Code* (EPC), que indica a arquitetura e o esquema de rede para associação de RFID na Internet.

O Auto-id Center fechou suas portas em 2003, passando suas responsabilidades aos Auto-id Labs. Em 2004 a EPC aprovou a segunda geração de padrões, melhorando o caminho para outras adoções (RAMOS; NASCIMENTO, 2007).

1.9.2 Tecnologia

A tecnologia RFID, assim como o sistema de códigos de barra, é utilizada para várias formas de identificação, desde objetos até seres vivos. Diferentemente de sua antecessora, a tecnologia RFID não precisa de contato visual para realização da leitura. Dependendo da sensibilidade e do tamanho da antena leitora e da força da antena transmissora, a etiqueta pode ser lida a distâncias razoáveis, permitindo a utilização dessa tecnologia em várias situações (IGOE, 2012, tradução nossa).

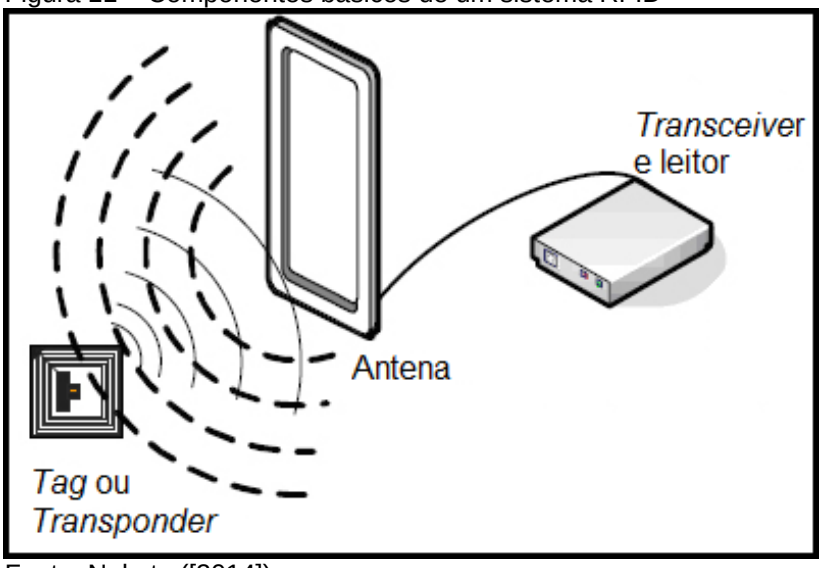
O *hardware* dos dispositivos RFID é composto por três elementos descritos a seguir e demonstrados na figura 11 (IGOE, 2012, tradução nossa):

a) **antena**: fabricadas em diversos tamanhos e formatos, de acordo com as necessidades específicas de uso, são responsáveis por ativar a etiqueta para a troca de informações. Existem casos em que a antena, o *transceiver* e o decodificador estão no mesmo equipamento, nesse caso, denomina-se leitor;

b) ***transceiver* e leitor**: sua função é alimentar o *transponder* (*tag*), para que ele responda ao leitor com o conteúdo armazenado em sua memória. O campo emitido pela etiqueta é detectado quando essa, passa pela área de cobertura da antena. Desta forma, o leitor decodifica a informação repassada e envia à um computador para processamento;

c) ***transponder* (*tag*)**: etiqueta, propriamente dita, é responsável por guardar as informações, assim como as antenas, são encontradas em diversos formatos, dependendo da aplicação, performance e ambiente de uso. Podem ser ativas, que possuem bateria interna e, ou passivas, em que a alimentação é fornecida pelo leitor.

Figura 11 – Componentes básicos de um sistema RFID



Fonte: Nakata ([2014]).

Além dos componentes citados acima, é necessária uma infraestrutura de rede, composta por um software capaz de gerenciar o hardware, repassar os dados obtidos e integrar o sistema RFID com outros sistemas. Essas atividades são realizadas por um *middleware* que deve possuir requisitos capazes de filtrar, agregar e disseminar os dados; leitura e escrita em *tags* e elementos de privacidade (BHUPTANI; MORADPOUR, 2005).

Os sistemas de RFID são diferenciados também pela faixa de frequência que operam, podendo ser sistemas de baixa ou alta frequência. O primeiro é utilizado, normalmente, para controle de acesso, identificação e rastreabilidade, enquanto o segundo é utilizado em leituras de média e longa distância e em alta velocidade, um exemplo dessa utilização é o sistema SEM PARAR utilizado em pedágios (PINHEIRO, 2004).

Segundo Stanford (2003, tradução nossa), a utilização da tecnologia RFID tem várias vantagens em relação a outros métodos de identificação, como por exemplo, não há necessidade de contato direto para leitura, é capaz de ler objetos simultaneamente, armazena uma maior quantidade de dados, entre outros. No entanto, alguns pontos negativos da adoção dessa tecnologia são: o bloqueio de sinais por elementos como metais, líquidos ou o corpo humano; o custo significativo de implementação; e a falta de padronização das frequências utilizadas.

1.10 ARDUINO

A plataforma Arduino surgiu na cidade italiana de Ivrea, em 2005, desenvolvido por Massimo Banzi, David Cuartielles, Tom Igoe, Gianluca Martino e David Mellis. Tinha o intuito de interagir com projetos escolares de forma a reduzir o custo dos projetos quando comparados com outros sistemas disponíveis à época.

Conforme Banzi (2012, tradução nossa), a plataforma Arduino busca atingir um grande grupo composto por entusiastas de eletrônica, programadores e *hobbystas*, proporcionando um ambiente de desenvolvimento fácil e acessível financeiramente. O Arduino beneficia aqueles que possuem conhecimentos em programação, mas pouco conhecimento em eletrônica, que podem realizar, desde pequenos projetos até experimentos de grande nível, como por exemplo o ArduSat, um satélite totalmente desenvolvido em Arduino (ARDUSAT, 2015, tradução nossa).

Ainda segundo Banzi (2012, tradução nossa), existem outras plataformas criadas com o mesmo objetivo, porém, não possuem a mesma facilidade de uso e preço acessível como o Arduino.

Arduino é uma plataforma de prototipagem eletrônica open-source, formada por uma placa de circuito impresso composta de um microprocessador ATMEL, entradas e saídas digitais e analógicas e de uma IDE multiplataforma que implementa a linguagem *Processing*. Sua linguagem de programação pode ser considerada uma versão simplificada de C++ (ARDUINO, 2015, tradução nossa).

Basicamente um programa típico é constituído de duas funções, *void setup* que é executada somente uma vez quando se liga ou reinicia o Arduino, e *void loop* uma rotina de *loop* que é executada repetidamente no microcontrolador. Todavia, existem outras funções que fazem a leitura/escrita dos pinos digitais e analógicos (PURDUM, 2015, tradução nossa).

Pode-se utilizar a plataforma Arduino tanto para projetos autônomos quanto em projetos interativos, como o controle de acesso que será desenvolvido, interpretando as variáveis de entrada através de sensores ou *switches* e controlando atuadores como LEDs, servomotores, relés entre outras saídas (PURDUM, 2015).

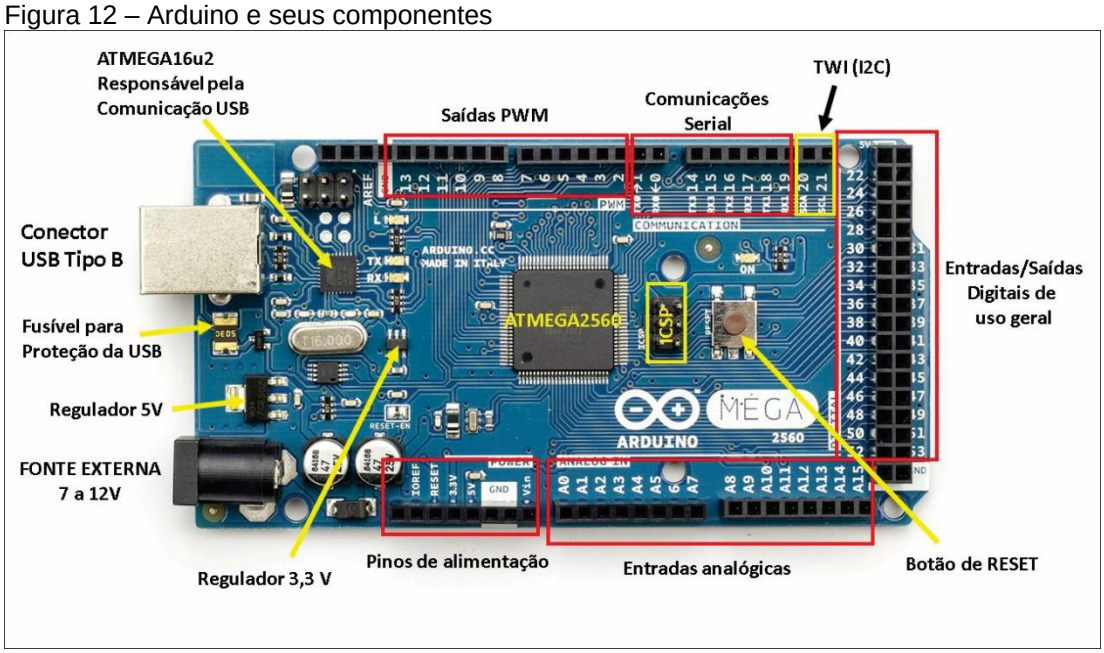
Sendo uma plataforma de Hardware e Software *open-source,* todos os esquemas eletrônicos estão disponíveis para que, alguém com noções de eletrônica, possa construir sua própria placa, reduzindo ainda mais o custo do projeto. De

qualquer forma, existem diversos tipos de placas prontas disponíveis no mercado, entre as mais comuns estão o Arduino Uno, Mega 2560, Duemilanove entre outras. Cada uma com suas características especificas e servindo a diferentes propósitos (ARDUINO, 2015, tradução nossa).

1.10.1 Arduino Mega 2560

Na figura 12 é apresentada a placa Arduino Mega que será utilizada no desenvolvimento deste sistema de controle de acesso. Os detalhes sobre a placa em questão serão apresentados nas próximas seções.

Figura 12 – Arduino e seus componentes



Fonte: Do autor.

1.10.1.1 Alimentação

Segundo Arduino (2015, tradução nossa), a placa Mega 2560 possui duas formas de alimentação, que pode ser tanto a porta USB quanto por uma fonte externa, a seleção de alimentação é feita automaticamente pela placa. A alimentação externa, pode ser feita de duas formas, através de uma bateria ou de um adaptador CA-CC. A voltagem recomendada para a alimentação é de 7-12V.

1.10.1.2 Memória

O microcontrolador ATmega2560 utilizado pelo Arduino Mega 2560 possui 256 KB de memória, desse total 8 KB são reservados para o *bootloader*, que é o gerenciador de *boot* responsável por gerenciar a execução dos programas em determinados ciclos de tempo, ele possui ainda, 8 KB de memória estática de acesso aleatório (tradução nossa), do inglês *Static Random Access Memory* (SRAM) e 4 KB de memória volátil somente de leitura (tradução nossa), do inglês *Electrically-Erasable Programmable Read-Only Memory* (EEPROM). Apesar dos baixos valores de memória disponíveis para gravar os *sketches*, pode-se utilizar uma *Shield* de Cartão SD para estender essa capacidade (ARDUINO, 2015, tradução nossa).

1.10.1.3 Entrada e Saída

O modelo Mega 2560 possui 54 pinos digitais que podem assumir valores de entrada ou saída, essa atribuição é realizada dentro da função *void setup*. Possui ainda outros 16 pinos analógicos, além de pinos com funções específicas pré-definidas. Essa quantidade de pinos permite um número considerável de possibilidades de controle de sensores e atuadores que podem ser utilizados. Deste total de 60 pinos, 15 podem ser utilizados como saídas PWM (ARDUINO, 2015, tradução nossa).

De acordo com Arduino (2015, tradução nossa), PWM ou modulação de largura de pulso (tradução nossa), é uma técnica para se obter resultados com significado digital através de respostas analógicos. Utiliza-se o controle digital para variar um sinal entre o ligado e desligado, podendo assim, simular voltagens completas entre 0 e 5 volts. Através da variável de tempo gasta com o sinal ligado vezes o tempo gasto com o sinal desligado, tem-se uma duração de tempo que é chamada de largura de pulso. Manipulando esse valor pode-se, por exemplo, controlar o brilho de um diodo emissor de luz, do inglês *Light Emitting Diode* (LED).

1.10.2 *Shields*

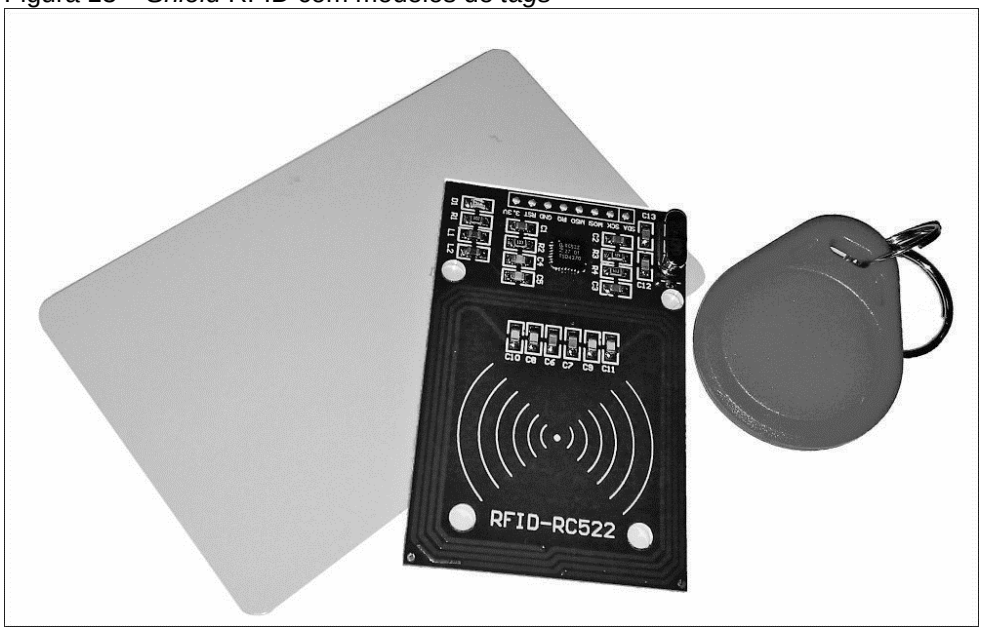
Existe uma comunidade ativa que trabalha constantemente na evolução da plataforma, agregando novas funcionalidades e recursos ao projeto. Facilmente encontram-se dispositivos que podem ser agregados a placa principal permitindo assim, novas possibilidades na criação de protótipos. Dá-se a esses dispositivos o nome de *Shields*. Existem inúmeros *Shields* criados para se utilizar em conjunto com o Arduino, os mais comuns são (ARDUINO, 2015, tradução nossa):

a) ***ethernet***: agrega uma placa de rede, onde utilizando-se uma biblioteca especifica que suporta os protocolos TCP e UDP, para conexão com a Internet;
b) **cartão SD**: permite aplicar a capacidade de memória disponível para os *Sketches* ou como registrador de *logs*;
c) **WIFI**: possui as mesmas funções do *Ethernet*, porém para conexões sem fio usando o protocolo 802.11 b/g;
d) **Global System for Mobile Communications (GSM)**: permite ao Arduino a comunicação via rede de dados GPRS, comumente utilizadas por celulares, podendo dessa forma enviar comando ao Arduino via SMS por exemplo;
e) ***shields* de visores**: Telas LCD que permitem mostrar mensagens de interações com usuários;
f) **RFID**: *shield* que agrega uma antena RFID ao Arduino;
g) **leitor biométrico (digital)**: realiza a coleta, processamento e comparação entre as impressões digitais armazenadas e aquela apresentada.

1.10.2.1 *Shield* RFID

Pode ser visto na figura 13, este *shield* possui integrada a antena e o transceiver, dessa forma pode-se fazer com que a placa Arduino possa trabalhar com a leitura das *tags* RFID.

Figura 13 – *Shield* RFID com modelos de *tags*



Fonte: Do autor.

1.10.2.2 *Shield* Leitor Biométrico

O *shield* de leitor biométrico, figura 14, realiza toda a manipulação das digitais. Os processos de coleta, armazenamento e comparação entre digitais, é todo realizado pelo módulo que somente fornece uma resposta de verdadeiro ou falso ao Arduino, que dessa forma irá realizar os devidos tratamentos com essa informação.

Figura 14 – Leitor Biométrico

Fonte: Do autor.

3. TRABALHOS CORRELATOS

Para a realização deste trabalho foram pesquisados alguns trabalhos semelhantes, adquirindo assim um maior embasamento do que já foi realizado.

1.11 SEM PARAR - CONTROLE DE ACESSO CONDOMINIAL VIA RFID

Trabalho de Conclusão de Curso desenvolvido por Adriel Kendrick de Mello, apresentado no Centro Universitário de Brasília e defendido no primeiro semestre de 2013. O projeto consiste no desenvolvimento de um sistema de controle e automação de acesso condominial através da tecnologia RFID. Foi desenvolvido tendo em base o Arduino UNO R3, um motor de passo e da antena e *tag* RFID. Foi criada uma maquete para simular um condomínio, onde foi instalada uma antena na área de acesso dos veículos e utilizando um carrinho de controle remoto simulando um veículo real dando entrada no condomínio (MELLO, 2013).

1.12 PROPOSTA PARA CONTROLE DE ACESSO FÍSICO SEGURO BASEADA EM *NEAR FIELD COMMUNICATION* (NFC) E ANDROID

Desenvolvido por Danilo Souza Lima e apresentando na Universidade de São Paulo (USP) em novembro de 2013. O trabalho propõe o desenvolvimento de um sistema para controle de acesso físico seguro e intuitivo através da utilização de um telefone celular através da tecnologia NFC, que é uma tecnologia de comunicação de Rádio Frequência de baixo alcance. Foi utilizado o microcontrolador Arduino com uma s*hield* NFC, além do desenvolvimento de um aplicativo em Android (LIMA, 2013).

1.13 DATABASE DESIGN FOR PHYSICAL ACCESS CONTROL SYSTEM FOR NUCLEAR FACILITIES

Artigo escrito por Sathishkumar, Rao e Arumugam, para o *Nuclear Engineering and Design Journal* no primeiro semestre de 2016. O artigo dispõe sobre a criação de um sistema de controle de acesso físico, baseado em dois níveis de autenticação, RFID e Biometria, para instalações nucleares. Foram desenvolvidos o

hardware para controle de acesso e os softwares necessários, Banco de Dados e um software cliente web. O Projeto do Banco de Dados visa organizar a hierarquia de acesso, agrupando os empregados e as portas com base em zonas de acesso. O artigo visa descrever uma nova abordagem no projeto de Banco de Dados para controles de acesso (SATHISHKUMAR; RAO; ARUMUGAM, 2016, tradução nossa).

1.14 DESENVOLVIMENTO DE SISTEMA PARA CONTROLE DE HORÁRIOS DE FUNCIONÁRIOS DOMÉSTICOS COM IDENTIFICAÇÃO POR RÁDIOFREQUÊNCIA.

Trabalho de conclusão de curso desenvolvido por Igor Carvalho e apresentando na Universidade do Extremo Sul Catarinense (UNESC), em 2013. O trabalho consiste no desenvolvimento de um sistema de controle de horário para empregados domésticos. Devido ao alto valor de um sistema de registro eletrônico, este sistema tem como objetivo facilitar o controle do empregador sobre os horários de entrada e saída dos funcionários. A tecnologia utilizada para identificação foi a identificação por rádio frequência. Usou-se o Arduino como plataforma do sistema (CARVALHO, 2013).

1.15 BIOMETRIA APLICADA A SEGURANÇA RESIDENCIAL

Trabalho de Conclusão de Curso desenvolvido por Rodrigo Rohling Cruz e Sandro Dutra do Nascimento Junior, apresentado na Faculdades Integradas do Vale do Ivaí, e defendido no segundo semestre de 2013. Devido ao crescente número de furtos em residências, o projeto consiste no desenvolvimento de um sistema de controle de acesso residência similar aos existentes, porém de baixo custo para que uma parcela maior da população possa ter acesso à esse tipo de sistema. No projeto foi utilizada a leitura biométrica da digital (CRUZ; NASCIMENTO JUNIOR, 2013).

4. CONTROLE DE ACESSO FÍSICO COM DUPLA AUTENTICAÇÃO

1.16 METODOLOGIA

Após a aprovação da proposta no segundo semestre de 2014, foi iniciado o projeto de pesquisa, constituído do levantamento bibliográfico e elaboração do referencial teórico, utilizando os recursos disponibilizados pela UNESC e/ou adquiridos pelo acadêmico.

Com o levantamento bibliográfico inicial pode-se aprimorar o tema proposto enfatizando seus principais aspectos, entre eles, pode-se citar o funcionamento das tecnologias de RFID, de Biometria, da criptografia, o Arduino e os *shields* necessários para o desenvolvimento do sistema proposto.

Para conclusão deste trabalho foi desenvolvido um protótipo de controle de acesso físico utilizando-se de leitura biométrica da digital e de *tags* RFID para identificação e confirmação de um determinado usuário.

1.17 APRESENTAÇÃO

Através das pesquisas e levantamentos bibliográficos gerados em torno do projeto de pesquisa realizado, o conhecimento adquirido resultou no propósito de desenvolver um protótipo de sistema de controle de acesso físico, utilizando duas tecnologias de identificação que são o RFID e a biometria da digital, e que possa proporcionar maior segurança, prevenindo o acesso de pessoas não autorizadas em um determinado ambiente. O desenvolvimento foi dividido em duas partes principais, a montagem dos componentes eletrônicos e a programação do Arduino.

O Arduino permite que se integrem a sua estrutura principal diversos *shields* que agregam funções especificas. Nesse projeto foram utilizados os seguintes *shields*, que serão abordados com mais detalhes a seguir:

a) - leitor de cartão SD, modelo YL-30;

b) - leitor de digitais, modelo ZFM-20 Series;

c) - display 16x2, modelo 1602A;

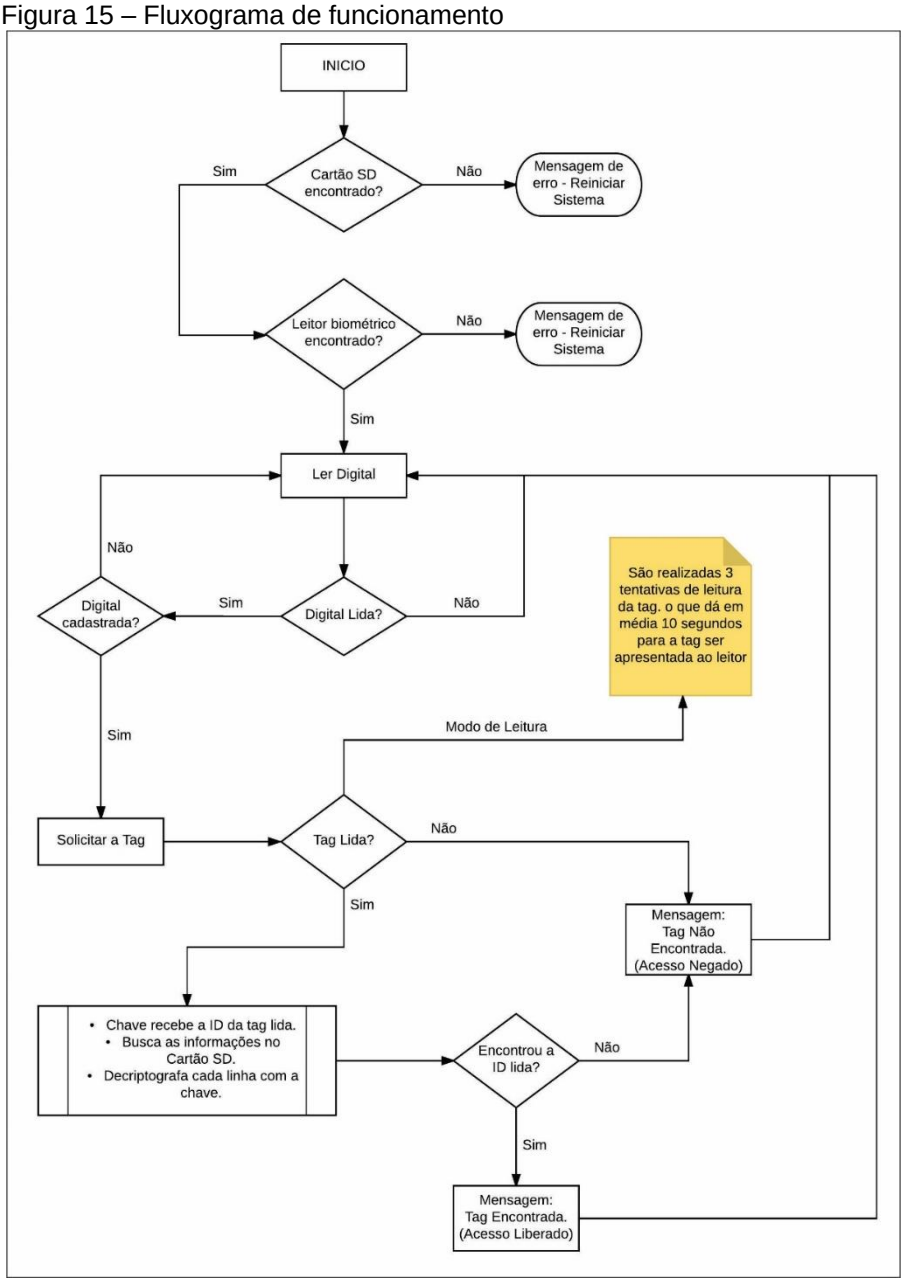
d) - leitor RFID, modelo mfrc522 Mifare.

1.17.1 Fluxograma de funcionamento

Fluxograma designa a representação gráfica do fluxo de trabalho de um processo, através dessa representação gráfica fica mais rápida a compreensão do funcionamento do sistema de controle de acesso.

Para início do projeto foi desenvolvido o fluxograma de operação que o protótipo deveria executar, na figura 15, pode-se verificar o fluxograma de operação do sistema.

Figura 15 – Fluxograma de funcionamento

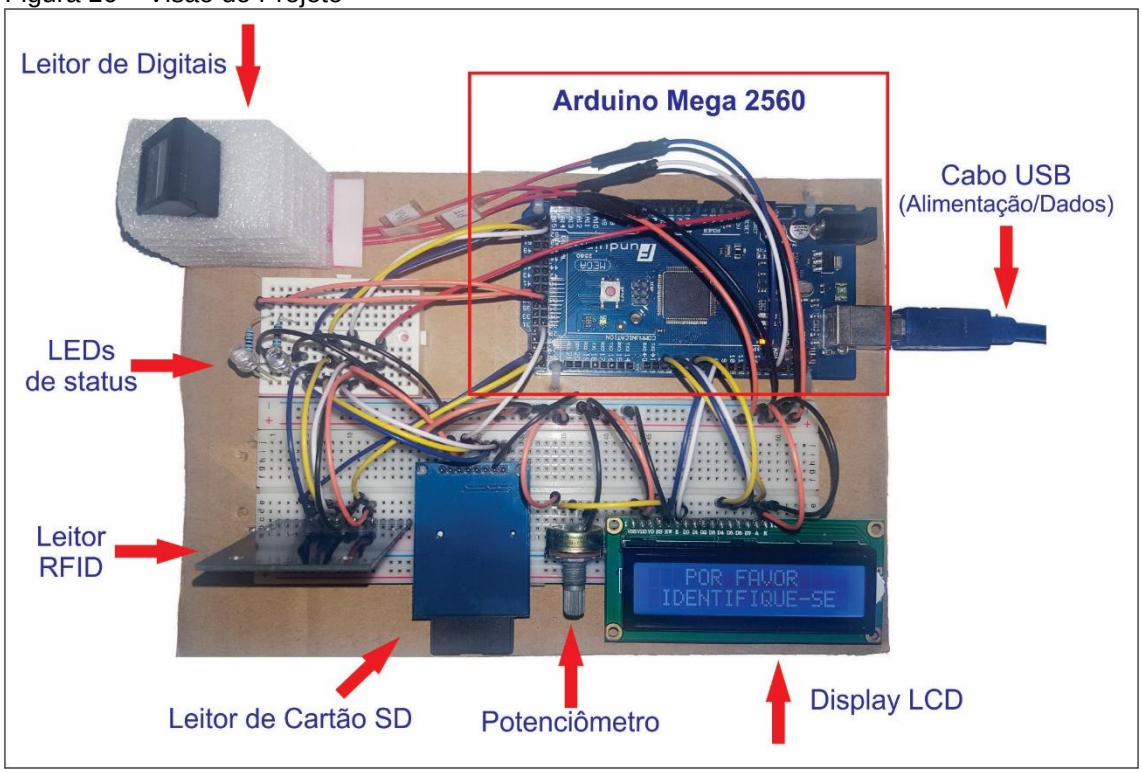


Fonte: Do autor.

1.17.2 Visão do Projeto

Na figura 16 pode-se observar o protótipo do projeto montado, com a identificação de cada componente utilizado.

Figura 16 – Visão do Projeto



Fonte: Do autor.

1.18 MONTAGEM DOS COMPONENTES

1.18.1 Arduino

O Arduino é o centro do projeto, responsável por executar todas as ações necessárias ao funcionamento do sistema. Ele captura, analisa e compara todas as informações fornecidas entre os *shields* e os elementos externos, *display*, leitor de Cartão SD, leitor de digitais e *tags* RFID. Devido à complexidade do código e ao número de *shields* necessários ao projeto, optou-se, por utilizar o Arduino Mega 2560 para o desenvolvimento do projeto. Essa versão do Arduino possui 54 pinos digitais, dos quais dezesseis foram utilizados, e maior capacidade de memória, necessária para armazenar e executar o código, quando comparado ao Arduino UNO, versão

comumente utilizada. Todavia, durante o desenvolvimento, foi utilizado um Arduino UNO de apoio para os testes e conexões individual de cada *shield* para posteriormente unir os códigos individuais ao programa principal. Na tabela 3, pode-se verificar um comparativo entre as duas versões.

Tabela 3 – Comparativo entre os Arduino UNO e MEGA

	Arduino UNO	Arduino Mega
Microcontrolador	ATMega 328	ATMega 2560
Portas digitais	14	54
Portas PWM	6	15
Portas analógicas	6	16
Memória	32Kb (0,5Kb *bootloader*)	256Kb (8Kb *bootloader*)
Clock	16 Mhz	16 Mhz
Conexão	USB	USB
Conector para alimentação externa	Sim	Sim
Tensão de operação	5V	5V
Corrente máxima portas E/S	40 mA	40 mA
Alimentação	7 – 12V	7 – 12V

Fonte: ARDUINO (2015, tradução nossa).

O microcontrolador utilizado no Arduino Mega 2560 é o ATMega 2560 da Atmel, possui 8 bits e arquitetura RISC avançada, possui 256KB de memória *flash*, dos quais 8KB são utilizados pelo *bootloader*, 4KB de EEPROM, 8KB de SRAM. Seu *Clock* opera em 16 MHz. Sua tensão de operação é de 5V, a alimentação deve ser entre 7 e 12V. Possui 54 pinos digitais, 15 são saída PWM, 16 saídas analógicas. Possui multiplicador por hardware além de diversos periféricos para aumentar as possibilidades da plataforma, dentre as quais pode-se destacar 4 canais de comunicação serial, 16 entradas analógicas e 15 saídas PWM. Possui ainda comunicação SPI, I2C e 6 pinos de interrupções externas.

1.18.2 Leitor de Cartão SD

O modelo escolhido foi o YL-30. Este *shield* é necessário para o armazenamento das informações referentes aos usuários cadastrados. Utiliza cartões no formato MicroSD. Faz as vezes de banco de dados um arquivo de caracteres, com

as informações criptografadas. Neste arquivo estão armazenados os nomes dos usuários, a *tag* RFID associada a este e a ID da digital cadastrada no leitor de biométrico. Essas informações são utilizadas pelo Arduino para comparação e validação do usuário que está sendo apresentado ao sistema. No quadro 1, pode-se verificar as ligações feitas entre o *Shield* e o Arduino.

Quadro 1 – Conexões do leitor de cartão SD

Sinal *shield* leitor cartão SD	Conexão no Arduino
GND	GND
MISO	50
SCK	52
MOSI	51
CS	26
3.3V	3.3V
GND	GND
+5V	+5V

Fonte: Do autor.

A principais características do modelo de leitor utilizado são:

a) tensão de entrada: +5V e 3.3V.

b) interface SPI: MOSI, SCK, MISO e CS.

c) formatação do cartão: FAT16 ou FAT32.

1.18.3 Leitor de Digitais

Devido à dificuldade de encontrar modelos nacionais para leitores de digital, optou-se por comprar na Internet o modelo importado, ZFM-20 Series. Este modelo de leitor possui internamente todas as funções necessárias ao projeto, captura, armazenamento, leitura, comparação e validação das digitais. Podendo-se programar no Arduino, para que ele solicite ao leitor que forneça a ID da digital lida. Este leitor permite um total de 162 digitais, que são armazenadas em sua memória interna. Por esse leitor pagou-se a soma de R$ 370,00, sendo esse o item mais caro do projeto.

Esse modelo de leitor possui uma pinagem bastante simples, são utilizados somente quatro cabos de conexão, como pode ser visto no quadro 2.

Quadro 2 – Pinagem do leitor biométrico

Sinal leitor de digitais	Pinagem no Arduino
Serial IN	12
Serial OUT	13
+5V	+5V
GND	GND

Fonte: Do autor.

1.18.4 Display LCD 16x2

O modelo de display LCD utilizado é o 1602A v2.0, este display possui 16 colunas e 2 linhas, com luz de fundo azul e letras na cor branca. Para a conexão com o Arduino existem 16 pinos, dos quais 12 são suficientes para uma conexão básica e foram utilizados nesse projeto, já incluindo as conexões de alimentação, pinos 1 e 2, luz de fundo, pinos 15 e 16, e contraste, pino 3, este último ligado a um potenciômetro para poder realizar o ajuste. No quadro 3 é possível observar as conexões desse *shield*. Este visor fica responsável pela exibição das informações e orientações ao usuário na operação do sistema.

Quadro 3 – Pinagem do display 16x2

Sinal Display 16x2	Pinagem no Arduino
VSS	GND
VDD	+5V
V0	Potenciômetro
RS	6
RW	GND
E	7
D0 à D3	Não conectado
D4	5
D5	4
D6	3
D7	2
A	+5V
K	GND

Fonte: Do autor.

1.18.5 Leitor RFID

Outro *Shield* responsável pela captura de dados. O leitor de RFID utilizado neste projeto foi o modelo mfrc522 Mifare, este modelo de leitor RFID utiliza o protocolo ISO/IEC 14443, utilizado em identificação de cartões – cartões com circuitos integrados sem contato – cartões de vizinhança. Nesse projeto foram utilizadas *tags* passivos, com a frequência de 13,56 Mhz. Esse leitor é responsável por capturar a ID das *tags* apresentadas ao mesmo, para que o Arduino possa posteriormente fazer as comparações com os outros dados fornecidos.

O leitor RFID tem 8 pinos que seguem a sequência de ligação apresentada no quadro 4. Diferente dos demais *shields*, a alimentação deste módulo é somente de 3.3 V.

Quadro 4 – Conexões do leitor RFID

Sinal Leitor RFID	Pinagem no Arduino
DAS	23
SCK	52
MOSI	51
MISO	50
IRQ	Não conectado
GND	GND
RST	22
3.3V	3.3V

Fonte: Do autor.

As principais características do modelo de leitor utilizado são:

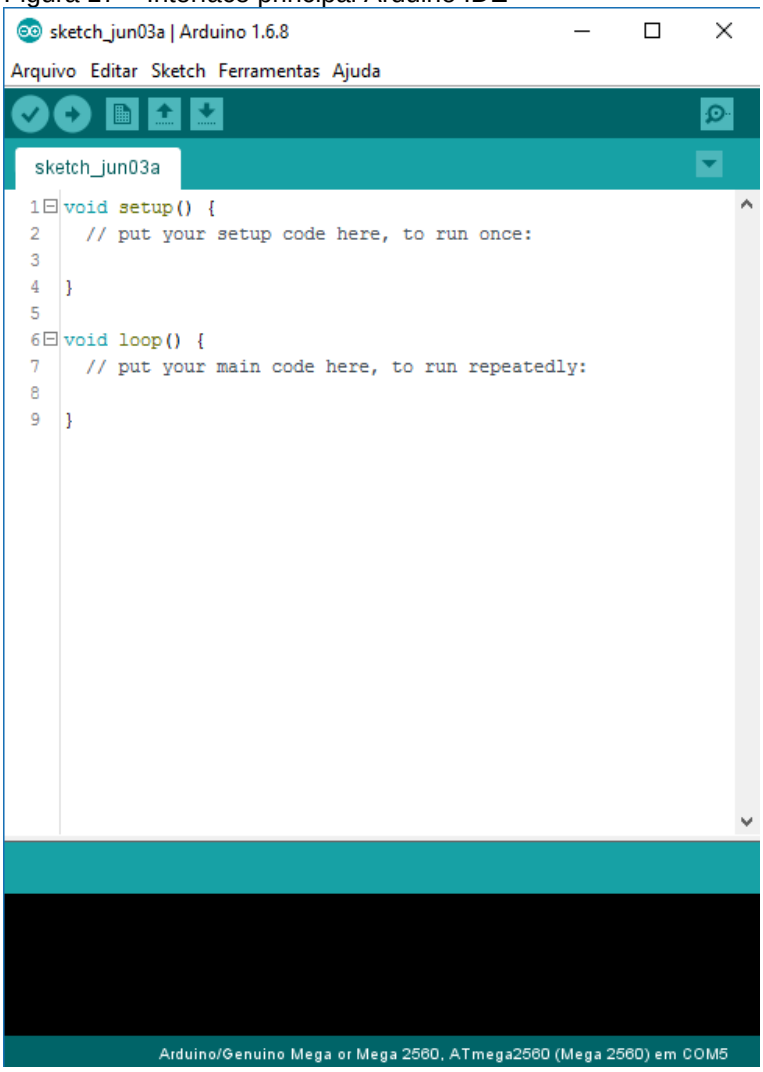
a) corrente de trabalho: 13-26mA / CC 3.3V;
b) frequência de operação: 13,56MHz;
c) tipos de cartões suportados: Mifare1 S50, S70 Mifare1, Mifare Ultra Light, Mifare, Pro Mifare, Desfire;
d) parâmetro de Interface SPI: MOSI, SCK, MISO e SDA;
e) taxa de transferência: 10 Mbit/s.

1.19 PROGRAMAÇÃO

1.19.1 Arduino IDE

O software que controla as funcionalidades do Arduino, pode ser desenvolvido na própria IDE fornecida pelos criadores, chamada Arduino IDE. Conta com uma interface gráfica bastante intuitiva, como pode-se observar na figura 17. Sua linguagem de programação é a Processing, que é baseada em C/C++. O programa deve sempre contar com as seguintes chamadas de procedimento: *setup*, que ajusta as configurações das portas de entrada e saída, a comunicação serial e é executada somente uma vez na inicialização do Arduino, e *loop*, que é um laço infinito onde o usuário cria a rotina do seu programa, este fica rodando infinitamente.

Figura 17 – Interface principal Arduino IDE

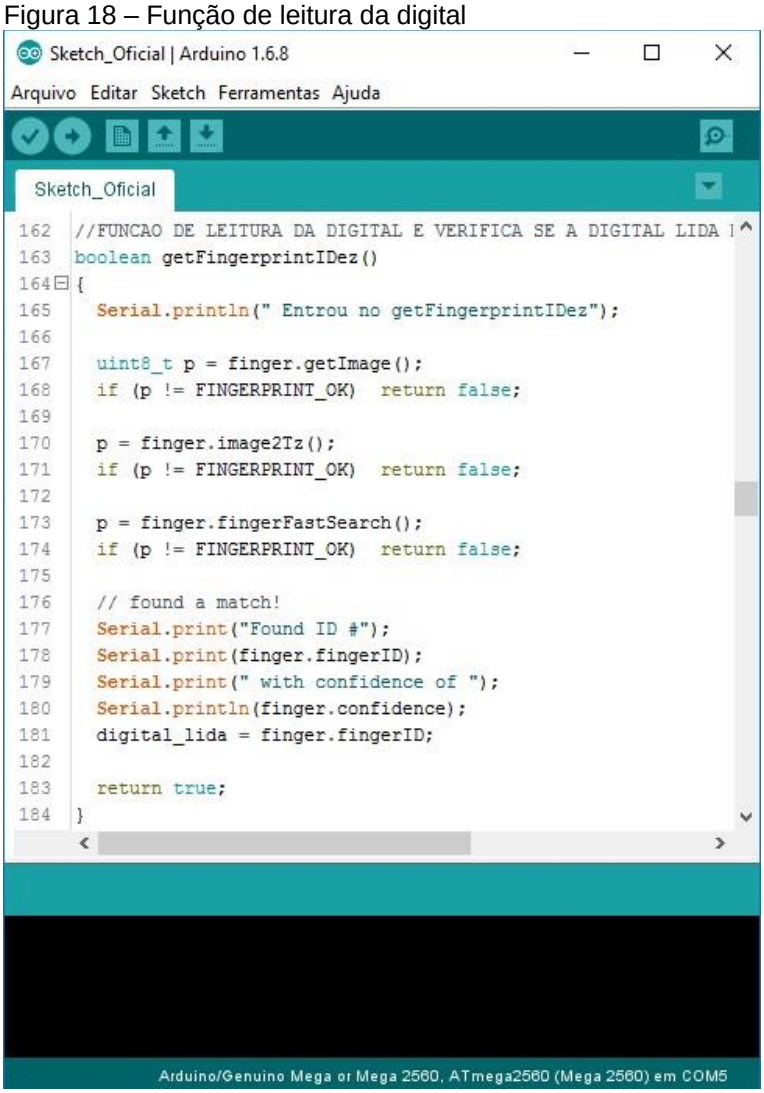


Fonte: Do autor.

A versão utilizada da IDE foi a 1.6.8. Durante o desenvolvimento do código foi utilizado como apoio um Arduino UNO, para testar o funcionamento de cada componente, nesse processo foram gerados códigos individuais que originaram funções no programa principal, estas responsáveis por executar funções especificas em cada *shield*.

Na figura 18 é possível ver um exemplo de função, a qual foi utilizada para leitura das digitais.

Figura 18 – Função de leitura da digital



Fonte: Do autor.

Toda a programação foi realizada utilizando a própria IDE do Arduino. O envio do código para o Arduino é extremamente fácil. Ao conectá-lo ao computador o mesmo é reconhecido como uma porta serial. Quando este processo está terminado

basta selecionar na IDE à porta de comunicação e o modelo do Arduino e fazer o *upload* do código para o Arduino.

Após carregar o programa para o Arduino, pode-se ligar o mesmo á uma fonte externa e operá-lo sem a necessidade de conexão com o computador.

1.19.2 Bibliotecas

Dentre outras, uma das principais vantagens da plataforma Arduino é a possibilidade de utilização de bibliotecas, que são fornecidas pelos fabricantes dos *shields* ou pela comunidade, para execução de funções especificas, especialmente na utilização de *shields*, nesse projeto foram utilizadas as seguintes bibliotecas:

a) ***adafruit_fingerprint***: Biblioteca utilizada para controle do *shield* de leitura da digital;
b) ***mfrc522***: Biblioteca que possui os controles do leitor de *tag* RFID;
c) ***RC4***: biblioteca responsável por criptografar e decriptografar as informações;
d) ***SD***: biblioteca para controle do *shield* do leitor de cartão SD;
e) ***SPI***: controla a comunicação serial dos *shields*;
f) ***liquidcrystal***: controla o display para exibição das informações;
g) ***softwareserial***: cria uma comunicação serial baseada em software.

1.19.3 Criptografia

No início do projeto optou-se por desenvolver o algoritmo de criptografia utilizando a Cifra de César, porém esse algoritmo pode ser facilmente quebrado. Com a familiaridade adquirida com a utilização de bibliotecas durante o desenvolvimento das outras funções, buscou-se a utilização de uma biblioteca para realizar a criptografia dos dados. Nessa análise optou-se por trabalhar com dois algoritmos de criptografia que dispunham de bibliotecas na comunidade do Arduino, o DES e o RC4.

A aplicação da biblioteca do algoritmo DES, correspondeu aos testes realizados com o Arduino, porém a utilização no projeto foi desmotivada por questões referentes a segurança desse algoritmo, que possui uma pequena chave de 56-bit, e que já havia sido quebrada em 1999 em cerca de 22 horas.

Após essa decisão, definiu-se por utilizar a biblioteca do algoritmo RC4. Este é um algoritmo simétrico ainda muito utilizado. Atualmente ele está presente nos protocolos SSL, para proteção do tráfego de Internet, e WEP e WAP, para proteção de redes sem fio. Mesmo não sendo considerado um dos melhores sistemas criptográficos disponíveis atualmente, dentro de determinadas situações práticas ele se mostra ainda, bastante eficiente.

Para tornar o algoritmo ainda mais eficiente para esse projeto, cada linha de informação do arquivo de dados é criptografada utilizando como chave a ID da *tag* RFID correspondente.

1.19.4 Gravação de dados no cartão SD

Ao criar o arquivo com as informações dos usuários do sistema, foram encontradas dificuldades, referentes a leitura dos dados armazenados. Inicialmente para testes foram criptogradas manualmente as informações e copiadas para o arquivo de caracteres presente no cartão. Notou-se, porém, que o Arduino não realizava corretamente a decriptografia das informações. Após uma pesquisa sobre o assunto, verificou-se que a codificação ANSI da arquitetura do Arduino é diferente da utilizada por computadores.

Outro problema encontrado foi a formatação do cartão SD que deveria ser formatado com os seguintes formatos de arquivo: FAT16 ou FAT32.

Validando essas pesquisas foi realizado o teste formatando o cartão SD com FAT16, como esse formato só suporta partições até 2GB e visto o baixo volume ocupado pelo arquivo utilizado, limitou-se a partição utilizada em 500MB, e foi utilizado o Arduino UNO de apoio para realizar a criptografia e gravação dos dados no cartão SD.

As informações salvas no arquivo de caractere armazenado no cartão SD, tem o seguinte formato: [Nome do Usuário];[ID da Digital];[ID da *TAG*];.

1.19.5 Comunicação SPI

Dos quatro *shields* utilizados nesse projeto, dois utilizam a comunicação SPI, o leitor RFID e o leitor de cartão SD. Para que não houvesse conflito na comunicação, visto que os dois utilizam o mesmo canal de comunicação, foram

criadas duas variáveis de controle para selecionar qual dispositivo deveria estar ligado.

A variável SS_RFID_PIN, definida no pino 23, serve para selecionar quando o leitor de RFID deve estar ativo, enquanto a variável SS_SD_PIN, definida no pino 26, seleciona o leitor do cartão SD. Essa seleção é ativada enviando um sinal *HIGH* ao pino do *Select Slave* que deve estar ativo no momento da comunicação.

1.20 DIFICULDADES ENCONTRADAS

Apesar de o Arduino ser uma excelente plataforma, também foi o responsável pelas maiores dificuldades encontradas nesse desenvolvimento.

Dentre as principais dificuldades encontradas, pode-se citar as que seguem:

a) adaptação de códigos ao Arduino MEGA, é possível encontrar diversos tutoriais na Internet com exemplos de códigos para o Arduino UNO, porém poucos para o MEGA. Durante o desenvolvimento do projeto foram necessários vários testes e pesquisas afim de entender as diferenças entre os mesmos, para saber quais pinos devem ser utilizados, no quadro 5, por exemplo, é possível ver a diferença de pinagem, entre o Arduino UNO e MEGA, dos pinos de comunicação SPI;

Quadro 5 – Diferença pinagem SPI Arduino UNO x MEGA

ARDUINO	MOSI	MISO	SCK	SS (Select Slave)
UNO	11	12	13	10
MEGA 2560	51	50	52	53

Fonte: Arduino (2015).

b) para a criptografia do texto no cartão SD também foram necessários vários testes e simulações, na utilização de bibliotecas, para que se chegasse ao pleno e correto funcionamento do sistema. Após algumas análises e testes verificou-se que o cartão SD deveria ser formatado em FAT16, limitou-se o cartão de 4 GB em 500 MB. Inicialmente a criptografia havia sido gerada manualmente e copiada pelo computador para o arquivo de caractere, porém foi verificado posteriormente que a

melhor solução seria fazer o Arduino gerar a criptografia e gravar diretamente as informações no cartão SD. Analisando os erros e a bibliografia, verificou-se que os caracteres ANSI do computador são diferentes do assembly do Arduino;

c) inicialmente optou-se por utilizar a primeira verificação do sistema através da *tag* RFID e após essa leitura confirmar a identidade do usuário com a leitura da digital, porém durante o desenvolvimento do projeto observou-se uma maior velocidade na utilização do leitor de digitais no início do código, dessa forma, após cada leitura o leitor é desativado, liberando recursos para o sistema. Optou-se, então, por colocar a primeira verificação como sendo a leitura da digital e posteriormente confirmando a identidade com a leitura da *tag* RFID;
d) dois shields utilizam a comunicação SPI nesse projeto, o leitor RFID e o leitor de cartão SD, para que não houvessem conflitos no sistema, criou-se posteriormente duas variáveis para selecionar o módulo que deveria comunicar em cada momento da execução do programa.

1.21 RESULTADOS OBTIDOS

Os resultados obtidos com o desenvolvimento deste projeto foram:

a) implementação de Criptografia no arquivo de caracteres do cartão SD, através do algoritmo RC4;
b) integração de todos os componentes necessários, destaque aos que utilizam comunicação SPI;
c) desenvolvimento do Protótipo.

5. CONCLUSÃO

Atualmente a informação é o bem mais valioso que se possui. Na sociedade moderna o poder da informação, para transformá-lo em conhecimento, pode construir e destruir uma pessoa, uma empresa ou até mesmo um país inteiro. Por isso, é de suma importância que as organizações estejam preocupadas com a segurança dos dados em sua posse. É necessário que elas se protejam tanto com controles lógicos, como *firewall*, antivírus, entre outros, quanto controles que impeçam o acesso físico ao meio onde a informação está armazenada.

O objetivo principal deste trabalho foi desenvolver um sistema de controle de acesso físico com dupla identificação, para esse trabalho foram utilizadas duas tecnologias muito utilizadas no momento que são a comunicação RFID e a leitura biométrica da digital, unidas pela plataforma de prototipação Arduino. Para que esse desenvolvimento fosse possível, foi necessário estudar e compreender o funcionamento e técnicas relacionadas à criptografia, Arduino, RFID e biometria, em especial a leitura da digital.

No estudo da plataforma Arduino foi possível conhecer diversas aplicações possíveis, desde um simples sensor para controlar a luminosidade de uma sala, até o desenvolvimento de um satélite, passando por projetos de impressoras 3D. Através do desenvolvimento do algoritmo que foi inserido no Arduino, os conhecimentos sobre programação também foram aprimorados. Na plataforma Arduino pode-se destacar como benefício suas comunidades de desenvolvedores, que possibilitam a troca de experiências e conhecimentos sobre desenvolvimento, em especial de automação.

O levantamento bibliográfico acerca dos conceitos e técnicas de biometria foi fundamental para a compreensão do funcionamento dessa tecnologia, em especial a datiloscopia. Através deste projeto pôde-se conhecer as minucias que são comparadas e analisados para identificar uma pessoa com base na leitura de sua impressão digital. Também foi possível ter uma leve compreensão sobre os demais tipos de biometria existentes, como leitura da íris, face, escrita, entre outras.

Durante o levantamento da fundamentação teórica, foi possível compreender com maior profundidade o funcionamento da tecnologia de rádio frequência, dentre as aplicações mais comuns estão o controle de mercadorias, a identificação de pessoas e o registro de acesso. Pôde-se observar a forma de leitura

das *tags* juntamente com os componentes necessários à operação de sistemas baseados em RFID.

Adquiridas as bases de conhecimento necessárias, foi possível integrar os *shields* de leitura de digital e *tags* RFID, juntamente com o visor LCD e leitor de cartão SD, com a plataforma Arduino como proposto. Concluiu-se que as tecnologias de identificação por leitura da digital e de identificação por rádio frequência unidas, dão ao sistema de controle de acesso a segurança necessária, garantindo que somente as pessoas autorizadas tenham acesso ao ambiente definido. A garantia de segurança das informações armazenadas na memória do sistema, foi conseguida através da implementação do algoritmo de criptografia RC4, atualmente utilizado em protocolos de comunicação SSL e TLS, que fornece a segurança necessária para operação do sistema.

Futuramente, para continuação deste trabalho, poderá ser integrado um *shield* de comunicação *ethernet*, com isso, será possível criar um gerenciador centralizado, através de comunicação via rede, para administração dos diversos pontos de controle que são implementados em um ambiente. A implementação de uma *touchscreen* poderá também melhorar a interação com o sistema em uma instalação *standalone*. Faz-se também necessária a implementação de sistema de auditoria dos acessos, atendendo dessa forma os quatro princípios de segurança da informação citados por Stoneburner (2001, tradução nossa).

6. REFERÊNCIAS

ALFARDAN, Nadhem J.; BERNSTEIN, Daniel J.; PATERSON, Kenneth G.; POETTERING, Bertram; SCHULDT, Jacob C. N. **On the Security of RC4 in TLS and WPA.** [s. L.]: [s.n.], 2013. 31 p.

ABNT (Associação Brasileira de Normas Técnicas). **NBR 27001**: Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001. 52 p.

ARDUINO. **Site Oficial**. Disponível em: <http://www.arduino.cc/>. Acesso em: 14 abr. 2015.

ARDUSAT. **Site Oficial**. Disponível em: <http://www.ardusat.com/>. Acesso em: 12 abr. 2015.

BANZI, Massimo. **Arduino:** La guida ufficiale. Gorgonzola: Tecniche Nuove, 2012. 117 p.

BAUMANN, Rainer; CAVIN, Stephane; SCHMID, Stefan. **Voice Over IP:** Security and SPIT. Berna: [s.n.], 2006. 34 p.

BHUPTANI, Manish; MORADPOUR, Shahram. **RFID:** Implementando o Sistema de Identificação por Radiofrequência. [s. L.]: Imam, 2005. 250 p.

CARVALHO, Igor. **Desenvolvimento de Sistema para Controle de Horários de Funcionários Domésticos com Identificação por Radiofrequência**. 2013. 66 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense, Criciúma, 2013.

CHURCHHOUSE, Robert. **Codes and Ciphers:** Julius Cesar, the Enigma and the Internet. Cambridge: Cambridge University Press, 2001. 252 p.

CRUZ, Rodrigo Rohling; NASCIMENTO JUNIOR, Sandro Dutra do. **Biometria Aplicada a Segurança Residencial**. 2013. 71 f. TCC (Graduação) - Curso de Tecnologia em Análise e Desenvolvimento de Sistemas, Faculdades Integradas do Vale do Ivaí, Ivaipora, 2013.

DONDA, Daniel. **CIFRA DE VIGENÈRE:** LE CHIFFRE INDÉCHIFFRABLE. [2007]. Disponível em: <https://danieldonda.wordpress.com/2007/10/31/cifra-de-vigenere-le-chiffre-indechiffrable/>. Acesso em: 01 jun. 2016.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação.** [s. L.]: Ciência Moderna, 2003. 176 p.

FLUHRER, Scott; MARTIN, Itsik; SHAMIR, Adi. **Weaknesses in the key scheduling algorithm of RC4.** Israel: [s.n.], [2001]. 23 p.

GALTON, Francis. **Fingerprints.** Londres e Nova Iorque: Mcmillian & Co., 1892. 246 p.

GLOVER, Bill; BATH, Himanshu. **Fundamentos do RFID.** Rio de Janeiro: Alta Books, 2007. 228 p.

GUMZ, Rafael Araújo. **Protótipo de um Sistema de Identificação de Minúcias em Impressões Digitais Utilizando Redes Neurais**. 2002. 134 f. TCC (Graduação) - Curso de Ciência da Computação, Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau, 2002.

HONG, Lin. **Automatic Personal Identification Using Fingerprints.** 1998. 242 f. Tese (Doutorado) - Curso de Filosifia, Department of Computer Science, Michigan State University, Ann Arbor, 1998.

IGOE, Tom. **Getting Start with RFID:** Identify Objects in the Physical World with Arduino. Sebastopol: O'reilly Media, 2012. 30 p.

KAHN, David. **The Codebreakers:** The Story of Secret Writing. Nova Iorque: Mcmillian & Co., 1967. 1164 p.

KEHDY, Carlos. **Elementos de Criminalística.** São Paulo: Luzes, 1968. 267 p.

KLEIN, Andreas. **Attacks on the RC4 stream cipher.** [s. L.]: [s.n.], 2007. 22 p.

LIMA, Danilo Souza. **Proposta para Controle de Acesso Físico Seguro Baseada em Near Field Communication (NFC) E Android.** 2013. 99 f. TCC (Graduação) - Curso de Engenharia Elétrica, Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2013.

LIU, Simon; SILVERMAN, Mark. A Practical Guide to Biometric Security Technology. **IT Professional,** [s.l.], v. 3, n. 1, p.27-32, 2001. Institute of Electrical & Electronics Engineers (IEEE).

MARTINS, Darian Becker; NASCIMENTO, Rafael Silva. **Critérios Quantitativos e Qualitativos acerca de Pontos Característicos do Fragmento Papilar no Confronto Papiloscópico.** [s. L.]: [s.n.], 2011. 6 p.

MCDONALD, Nicholas G. **Past, Present, and Future Methods of Cryptography and Data Encryption**: A Research Review. Salt Lake City: [s.n.], [2010]. 22 p.

MELLO, Adriel Kendrick de. **SEM PARAR - Controle de Acesso Condominial via RFID**. 2013. 70 f. TCC (Graduação) - Curso de Engenharia da Computação, Faculdade de Tecnologia e Ciências Sociais Aplicadas, Centro Universitário de Brasília, Brasília, 2013.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de Redes:** em Ambientes Corporativos. São Paulo: Novatec, 2007. 488 p.

NAKATA, Gabriel. **[Hands On] – Arduino + LCD + Leitor RFID.** [2014]. Disponível em: <http://www2.joinville.udesc.br/~i9/2014/08/15/hands-on-arduino-lcd-leitor-rfid/>. Acesso em: 01 jun. 2016.

PINHEIRO, José Mauricio Santos. **RFID:** Identificação por Radiofrequência. 2004. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_identificacao_por_radiofrequencia.php>. Acesso em: 04 ago. 2015.

PURDUM, Jack. **Beginning C for Arduino, Second Edition:** Learn C Programming for the Arduino. 2. ed. Cincinnati: Ecosoft, Inc., 2015. 388 p.

RABELLO, Eraldo. **Curso de Criminalística.** Porto Alegre: Sagra Luzzato, 1996. 208 p.

RAMOS, Larissa de Fátima; NASCIMENTO, Rodrigo Grotti. **Redes RFID.** 2007. 78 f. Monografia (Especialização) - Curso de Ciência da Computação, Pós-Graduação, Centro Federal de Educação Tecnológica de Mato Grosso, Cuiabá, 2007.

ABREU, Leandro Farias dos Santos. **A Segurança da Informação nas Redes Sociais São Paulo 2011.** 2011. 56 f. TCC (Graduação) - Curso de Tecnologia em Processamento de Dados, Faculdade de Tecnologia de São Paulo, São Paulo, 2011.

SALAS, Marcelo Invert Palma; PEREIRA, André Augusto da Silva. **Análise Crítica da Implementação da Cifra RC4 no Protocolo WEP.** [s. L.]: [s.n.], 2011. 7 p.

SANTINI, Arthur Gambi. **RFID:** Conceitos, Aplicabilidades e Impactos. Rio de Janeiro: Ciencia Moderna, 2008. 96 p.

SATHISHKUMAR, T.; RAO, G. Prabhakara; ARUMUGAM, P.. Database design for Physical Access Control System for nuclear facilities. **Nuclear Engineering And Design,** [s.l.], v. 305, p.68-72, ago. 2016. Elsevier BV.

RSA SECURITY. **RSA SECURITY Response to Weaknesses in Key Scheduling Algorithm of Rc4**. [2001]. Disponível em: <http://brazil.emc.com/emc-plus/rsa-labs/historical/rsa-security-response-weaknesses-algorithm-rc4.htm>. Acesso em: 26 maio 2016.

STANFORD, Vince. Pervasive Computing Goes the Last Hundred Feet with RFID Systems. **Ieee Pervasive Computing,** [s.l.], p.9-14, abr. 2003.

STONEBURNER, Gary. **Underlying Technical Models for Information Technology Security:**Recommendations of the National Institute of Standards and Technology. Gaithersburg: [s.n.], 2001. 28 p.

SUCUPIRA JÚNIOR, Luiz Humberto Rabelo. **Uma Metodologia para Avaliação de Pacotes de Software Biométricos.** 2004. 176 f. Dissertação (Mestrado) - Curso de Engenharia Elétrica e de Computação, Departamento de Comunicações, Universidade Estadual de Campinas, Campinas, 2004.

XIAO, Qinghan; RAAFAT, Hazem. Fingerprint Image Postprocessing: a Combined Statistical and Structural Approach. **Pattern Recognition,** [s.l.], v. 24, n. 10, p.985-992, jan. 1991.

APÊNDICES

7. APÊNDICE A - SISTEMA DE CONTROLE DE ACESSO FÍSICO UTILIZANDO RFID E BIOMETRIA

Madalena, Felipe

Departamento de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC)
Criciúma – SC – Brasil

{felipemadalena@gmail.com

Abstract. *The security in the physic access to the ways maintainers of the information is indispensable to the security information. The main people or organizations thinking only in logic security in detriment of systems of physic security. Are necessary procedures and systems that can guarantee of the information will be secure.*

Resumo. *A segurança no acesso físico aos meios mantenedores de informações é imprescindível para a segurança da informação. A maioria dos indivíduos ou organizações pensam somente em segurança lógica em detrimento de sistemas de segurança física. São necessários procedimentos e sistemas que garantam o controle no acesso aos ambientes onde as informações são armazenadas. A instalação desse tipo de sistema pode aumentar a garantia de que as informações estejam seguras.*

1. Introdução

Atualmente a informação é o bem mais precioso que se possui. Porém quando se pensa em segurança da informação, pensa-se somente nos meios de segurança lógicos. Para garantir a segurança física dos ambientes e equipamentos onde a informação está armazenada é necessário que se utilizem políticas e sistemas que controlem esse acesso .

As tecnologias de identificação mais utilizadas atualmente para sistemas de controle de acesso são a leitura biométrica da digital e a identificação por rádio frequência (RFID). Além disso também é necessário garantir a segurança do próprio sistema de controle de acesso, como por exemplo, a utilização de tecnologias de criptografia nas informações do banco de dados do sistema.

Este artigo visa mostrar as tecnologias utilizadas no desenvolvimento de um protótipo de controle de acesso com a utilização da identificação por rádio frequência e leitura da digital, além da criptografia das informações dos usuários.

1.1. Segurança da Informação

Por informação entende-se todo conjunto de dados que possua valor para um indivíduo ou uma organização. Com a utilização de sistemas informatizados cada vez mais integrados e conectados através das redes se torna essencial que se garanta o controle no acesso a essas informações (FERREIRA, 2003).

Segundo Baumann; Cavin e Schmid (2006, tradução nossa) A segurança da informação possui três princípios básicos que são seus pilares:

a) confidencialidade: significa que os dados devem estar disponíveis somente aos usuários com direito de acesso;

b) integridade: refere-se a certeza de que os dados apresentados não foram alterados;

c) disponibilidade: assegura que a informação deverá estar disponível, sempre que for solicitada.

Segundo Stoneburner (2001, tradução nossa), a segurança é obtida através da relação e da implementação de quatro princípios de segurança, os três mencionados anteriormente, confidencialidade, integridade e disponibilidade, com o acréscimo de sistemas de auditoria. A auditoria, é a análise sobre as formas com que os recursos são utilizados, por quem são utilizados, quando foram utilizados e que alterações foram realizadas.

Ainda segundo Stoneburner (2001, tradução nossa), para se aplicar e dar suporte aos princípios básicos de segurança da informação são utilizados recursos de controle lógicos e físicos:

a) controles lógicos: definem-se como barreiras que limitam ou impedem o acesso à informação através de recursos de software como assinatura digital, autenticação, firewall, criptografia entre outros;

b) controles físicos: são as barreiras que limitam o contato ou acesso direto à infraestrutura onde encontra-se a informação, além dos mecanismos que garantem a segurança do ambiente contra água, fogo, temperatura, entre outros, pode-se citar como exemplos desses controles portas reforçadas, trancas com controles biométricos, circuito fechado de televisão (CFTV), entre outros.

1.2. Criptografia

Criptografia é a ciência ou o estudo de técnicas de escrita secreta e ocultação de mensagens. Sendo tão ampla quanto a linguística formal, ocultando o conteúdo daqueles que não possuem o conhecimento para decifrá-la (KAHN, 1967, tradução nossa).

Também especifica os algoritmos de criptografia moderna, utilizados para proteger as transações feitas através de redes digitais. Criptografia constitui qualquer método utilizado para esconder uma mensagem, ou o seu significado, em algum meio, seja físico ou digital (MCDONALD, [2010], tradução nossa).

Teve sua origem no antigo Egito, onde foram utilizadas as primeiras formas de ocultação de mensagem através de substituição hieroglífica. Todavia foi facilmente quebrada por aqueles que sabiam ler e escrever. Por volta de 500 a.C. os espartanos desenvolveram um método de criptografia que ficou conhecido como Bastão de Licurgo, este mecanismo consistia em uma fita de papel enrolada em um bastão, a mensagem era então escrita e para decifrá-la era necessário utilizar um bastão com as mesmas dimensões do primeiro. Já o mais antigo registro de criptografia utilizada no âmbito militar, data de 2000 a.C. quando o imperador Júlio César desenvolveu a Cifra de César, que também era uma cifra de substituição, onde escolhia-se um número aleatório para ser a chave e avançavam-se as letras do alfabeto conforme essa chave, na figura 1 pode-se ver um exemplo dessa cifra com chave 3(MCDONALD, [2010], tradução nossa).

2Figura 1 – Cifra de César (com chave 3)

Ainda segundo Mcdonald, ([2010], tradução nossa), atualmente, as criptografias mais utilizadas são as baseadas em chaves assimétricas, também conhecidas como chaves publicas, nesses métodos a chave utilizada para criptografia é diferente da chave utilizada na decriptografia,

podemos citar, por exemplo, o *one-time-pad*, o (AES), o *Data Encryption Standard* (DES), o RSA, entre outros.

Segundo Salas e Pereira (2011), o RC4, originalmente desenvolvido por Ron Rivest, para a empresa RSA Security em 1987, é um algoritmo de chave simétrica. É uma cifra de fluxo com tamanho de chave variável orientada a byte. Se tornou bastante utilizada em várias aplicações como Internet Explorer, Adobe Acrobat, entre outros. Tornou-se pública em 1994 através de um vazamento em uma lista de discussão sobre criptografia, a Cipherpunks.

1.3. Biometria

Entende-se por biometria, a medida de características únicas encontradas em um indivíduo, que podem ser utilizados para reconhecê-lo e confirmar sua identidade (LIU; SILVERMAN, 2001, tradução nossa).

Biometria é um ramo da ciência que estuda formas de mensurar os seres vivos. Tecnologicamente, é a identificação automatizada de um indivíduo através de características físicas ou comportamentais especificas. Dentre as características físicas, pode-se citar a digital, a íris, a face, entre outras, já as características comportamentais, pode-se citar a escrita, a voz, entre outras. Nota-se que as características físicas são mais seguras para a identificação, pois permanecem as mesmas durante toda a vida, enquanto as comportamentais podem mudar com o tempo (GUMZ, 2002).

Na tabela 1 é possível visualizar um comparativo entre os tipos mais comuns de biometria (LIU E SILVERMAN, 2001, tradução nossa).

Tabela 1 – Comparativo entre os tipos de biometria

Características	Digital	Retina	Iris	Face	Assinatura	Voz
Facilidade de uso	Alta	Baixa	Média	Média	Alta	Alta
Incidência de erros	Sujeira, idade	Óculos	Má iluminação	Idade, óculos, cabelo	Alteração na assinatura	Ruído, resfriado
Precisão	Alta	Muito alta	Muito alta	Alta	Alta	Alta
Aceitação do usuário	Médio	Médio	Médio	Médio	Muito alta	Alta
Nível de segurança necessário	Alta	Alta	Muito alta	Média	Média	Média
Estabilidade a longo prazo	Alta	Alta	Alta	Media	Media	Media

1.4. Datiloscopia

Segundo Kehdy (1968), datiloscopia é a ciência baseada na comparação entre as impressões digitais, sejam elas impressas ou armazenadas em um banco de dados, com a intenção de identificar um indivíduo. Para realizar essas comparações, é realizada a verificação de pontos específicos, conhecidos como minúcias.

Segundo Gumz (2002), pode-se dividir a datiloscopia em clínica, criminal e civil, utiliza-se a clínica para estudar perturbações causadas por doenças, em impressões digitais. Na criminal, analisam-se as marcas de impressões digitais deixadas em uma cena de crime, para identificar um possível suspeito. Já a civil, é usada na autenticação de um indivíduo para que este tenha acesso à recursos protegidos, como por exemplo, carteira profissional, identidade, entre outros.

Segundo Rabello (1996), com base nos estudos que foram realizados em 1982, por Francis Galton, que classificou em quatro grupos as impressões digitais, Vucetich, em 1904, criou um sistema de identificação através de impressões digitais, com maior atenção no arquivamento e classificação das digitais dos dez dedos das mãos. Partindo da classificação de Galton, ele simplesmente realizou a tradução de arch para arco, loop para presilha e whorl para verticilo. Percebeu então que existia um pequeno acidente nas digitais, com o formato de um triangulo, que o chamou de delta e foi incluído na classificação, considerando-se a ausência ou presença do mesmo. Os conceitos dos tipos fundamentais de Juan Vucetich ficaram os seguintes:

a) arco: imagem da digital que não possui delta. Suas linhas atravessam a digital de um lado ao outro, com uma forma abaulada;

b) presilha interna: mostra um delta à direita do observador, com as linhas da região do núcleo dirigindo-se à esquerda;

c) presilha externa: mostra o delta à esquerda do observador, com as linhas do núcleo dirigindo-se à direita;

d) verticilo: normalmente apresenta dois deltas, uma à esquerda e um à direita do observador. Outra característica são as linhas da região nuclear que se encerram entre as linhas que prolongam dos deltas

1.5. RFID

RFID é o acrônico em inglês de *Radio Frequency Identification* – identificação por radiofrequência. É uma tecnologia de identificação que utiliza frequências de rádio para comunicação entre seus componentes. Seu objetivo é melhorar a eficiência na localização e rastreamento de produtos e também oferecer benefícios no registro de bens físicos (GLOVER; BHATT, 2007).

Segundo Igoe (2012, tradução nossa), RFID ou identificação por radiofrequência é uma tecnologia wireless que tem como objetivo a coleta automática de dados.

O hardware dos dispositivos RFID é composto por três elementos descritos a seguir e demonstrados na figura 11 (IGOE, 2012, tradução nossa):

a) antena: possuem diferentes formatos, são responsáveis por ativar a etiqueta para a troca de informações. Existem casos em que a antena, o transceiver e o decodificador estão no mesmo equipamento, nesse caso, denomina-se leitor;

b) transceiver e leitor: sua função é alimentar o transponder (tag), para que ele responda ao leitor com o conteúdo armazenado em sua memória. O campo emitido pela etiqueta é detectado quando essa, passa pela área de cobertura da antena.

c) transponder (tag): é responsável por guardar as informações, assim como as antenas, são encontradas em diversos formatos, dependendo da aplicação, performance e ambiente de uso. Podem ser ativas, que possuem bateria interna, ou passivas, em que a alimentação é fornecida pelo leitor.

1.6. Arduino

Conforme Banzi (2012, tradução nossa), a plataforma Arduino surgiu na cidade italiana de Ivrea, em 2005, desenvolvido por Massimo Banzi, David Cuartielles, Tom Igoe, Gianluca Martino e David Mellis. Tinha o intuito de interagir com projetos escolares de forma a reduzir o custo dos projetos quando comparados com outros sistemas disponíveis à época.

Arduino é uma plataforma de prototipagem eletrônica open-source, formada por uma placa de circuito impresso composta de um microprocessador ATMEL, entradas e saídas digitais e analógicas e de uma IDE multiplataforma que implementa a linguagem Processing. Sua linguagem de programação pode ser considerada uma versão simplificada de C++ (ARDUINO, 2015, tradução nossa).

2. Controle de Acesso Físico com Dupla Autenticação

Através das pesquisas e levantamentos bibliográficos gerados em torno do projeto de pesquisa realizado, o conhecimento adquirido resultou no propósito de desenvolver um protótipo de sistema de controle de acesso físico, utilizando duas tecnologias de identificação que são o RFID e a biometria da digital, e que possa proporcionar maior segurança, prevenindo o acesso de pessoas não autorizadas em um determinado ambiente. O desenvolvimento foi dividido em duas partes principais, a montagem dos componentes eletrônicos e a programação do Arduino.

O Arduino permite que se integrem a sua estrutura principal diversos shields que agregam funções especificas. Nesse projeto foram utilizados os seguintes shields, que serão abordados com mais detalhes a seguir:

a) - leitor de cartão SD, modelo YL-30;

b) - leitor de digitais, modelo ZFM-20 Series;

c) - display 16x2, modelo 1602A;

d) - leitor RFID, modelo mfrc522 Mifare.

2.1. Montagem dos componentes

2.1.1. Arduino

O Arduino é o centro do projeto, responsável por executar todas as ações necessárias ao funcionamento do sistema. Ele captura, analisa e compara todas as informações fornecidas entre os *shields* e os elementos externos, *display*, leitor de Cartão SD, leitor de digitais e tags RFID. Devido à complexidade do código e ao número de shields necessários ao projeto, definiu-se, por utilizar o Arduino Mega 2560 para o desenvolvimento do projeto. Essa versão do Arduino possui 54 pinos digitais, dos quais dezesseis foram utilizados, e maior capacidade de memória, necessária para armazenar e executar o código, quando comparado ao Arduino UNO, versão comumente utilizada. O microcontrolador utilizado no Arduino Mega 2560 é o ATMega 2560 da Atmel, possui 8 bits e arquitetura RISC avançada, possui 256KB de memória flash, dos quais 8KB são utilizados pelo bootloader, 4KB de EEPROM, 8KB de SRAM. Seu Clock opera em 16 MHz. Sua tensão de operação é de 5V, a alimentação deve ser entre 7 e 12V. Possui 54 pinos digitais, 15 são saída PWM, 16 saídas analógicas. Possui multiplicador por hardware além de diversos periféricos para aumentar as possibilidades da plataforma, dentre as quais pode-se destacar 4 canais de comunicação serial, 16 entradas analógicas e 15 saídas PWM. Possui ainda comunicação SPI, I2C e 6 pinos de interrupções externas.

2.1.2. Leitor de cartão SD

O modelo de leitor de cartão de memória escolhido foi o YL-30. Este shield é necessário para o armazenamento das informações referentes aos usuários cadastrados. Utiliza cartões no formato MicroSD. O cartão SD foi formatado em FAT16 e criada uma partição de 500MB para o armazenado do banco de dados, para isso foi utilizado um arquivo de caracteres, com as informações criptografadas. Neste arquivo estão armazenados os nomes dos usuários, a tag RFID associada a este e a ID da digital cadastrada no leitor de biométrico. Essas informações são utilizadas pelo Arduino para comparação e validação do usuário que está sendo apresentado ao sistema.

2.1.3. Leitor biométrico

Para a leitura das digitais, optou-se por utilizar o modelo importado, ZFM-20 Series. Este modelo de leitor possui internamente todas as funções necessárias ao projeto, a captura, o armazenamento, a leitura, a comparação e a validação das digitais. Podendo-se programar no Arduino, para que ele solicite ao leitor que forneça a ID da digital lida. Este leitor permite um total de 162 digitais, que são armazenadas em sua memória interna. Esse modelo de leitor possui uma pinagem bastante simples, são utilizados somente quatro cabos de conexão a alimentação 5V, o terra e as portas seriais de entrada e saída dos dados.

2.1.4. Display LCD

O modelo de *display* LCD utilizado é o 1602A v2.0, este, possui 16 colunas e 2 linhas, com luz de fundo azul e letras na cor branca. Para a conexão com o Arduino existem 16 pinos, dos quais 12 são suficientes para uma conexão básica e foram utilizados nesse projeto, já incluindo as conexões de alimentação 5V, pinos 1 e 2, luz de fundo, pinos 15 e 16, e contraste, pino 3, este último ligado a um potenciômetro para poder realizar o ajuste. Este visor fica responsável pela exibição das informações e orientações ao usuário na operação do sistema.

2.1.5. Leitor RFID

Outro Shield responsável pela captura de dados. O leitor de RFID utilizado neste projeto foi o modelo mfrc522 Mifare, este modelo de leitor RFID utiliza o protocolo ISO/IEC 14443, utilizado em identificação de cartões – cartões com circuitos integrados sem contato. Nesse projeto foram utilizadas tags passivos, com a frequência de 13,56 Mhz. Esse leitor é responsável por capturar a ID das tags apresentadas ao mesmo, para que o Arduino possa posteriormente fazer as comparações com os outros dados fornecidos.

O leitor RFID tem 8 pinos que são ligados ao Arduino. Diferente dos demais shields, a alimentação deste módulo é somente de 3.3 V,

2.2. Programação

O software que controla as funcionalidades do Arduino, pode ser desenvolvido na própria IDE fornecida pelos criadores, chamada Arduino IDE. Conta com uma interface gráfica bastante intuitiva. Sua linguagem de programação é a Processing, que é baseada em C/C++. O programa deve sempre contar com as seguintes chamadas de procedimento: setup, que ajusta as configurações das portas de entrada e saída, a comunicação serial e é executada somente uma vez na inicialização do Arduino, e loop, que é um laço infinito onde o usuário cria a rotina do seu programa, este fica rodando infinitamente.

2.2.1. Bibliotecas

Dentre outras, uma das principais vantagens da plataforma Arduino é a possibilidade de utilização de bibliotecas, que são fornecidas pelos fabricantes dos shields ou pela comunidade, para execução de funções especificas, especialmente na utilização de shields, nesse projeto foram utilizadas as seguintes bibliotecas:

a) adafruit_fingerprint: Biblioteca utilizada para controle do shield de leitura da digital;

b) mfrc522: Biblioteca que possui os controles do leitor de tag RFID;

c) RC4: biblioteca responsável por criptografar e decriptografar as informações;

d) SD: biblioteca para controle do shield do leitor de cartão SD;

e) SPI: controla a comunicação serial dos shields;

2.2.2. Criptografia

No início do projeto optou-se por desenvolver o algoritmo de criptografia utilizando a Cifra de César, porém esse algoritmo pode ser facilmente quebrado. Com a familiaridade adquirida com a utilização de bibliotecas durante o desenvolvimento das outras funções, buscou-se a utilização de uma biblioteca para realizar a criptografia dos dados. Nessa análise optou-se por trabalhar com dois algoritmos de criptografia que dispunham de bibliotecas na comunidade do Arduino, o DES e o RC4.

A aplicação da biblioteca do algoritmo DES, correspondeu aos testes realizados com o Arduino, porém a utilização no projeto foi desmotivada por questões referentes a segurança desse algoritmo, que possui uma pequena chave de 56-bit, e que já havia sido quebrada em 1999 em cerca de 22 horas.

Após essa decisão, definiu-se por utilizar a biblioteca do algoritmo RC4. Este é um algoritmo simétrico ainda muito utilizado. Atualmente ele está presente nos protocolos SSL, para proteção do tráfego de Internet, e WEP e WAP, para proteção de redes sem fio. Mesmo não sendo considerado um dos melhores sistemas criptográficos disponíveis atualmente, dentro de determinadas situações práticas ele ainda se mostra bastante eficiente.

Para tornar o algoritmo ainda mais eficiente para esse projeto, cada linha de informação do arquivo de dados é criptografada utilizando como chave a ID da tag RFID correspondente

2.2.3. Gravação de dados no cartão SD

Ao criar o arquivo com as informações dos usuários do sistema, foram encontradas dificuldades, referentes a leitura dos dados armazenados. Inicialmente para testes foram criptogradas manualmente as informações e copiadas para o arquivo de caracteres presente no cartão. Notou-se, porém, que o Arduino não realizava corretamente a decriptografia das informações. Após uma pesquisa sobre o assunto, verificou-se que a codificação ANSI da arquitetura do Arduino é diferente da utilizada por computadores.

Outro problema encontrado foi a formatação do cartão SD que deveria ser formatado com os seguintes formatos de arquivo: FAT16 ou FAT32. Validando essas pesquisas foi realizado o teste formatando o cartão SD com FAT16, como esse formato só suporta partições até 2GB e visto o baixo volume ocupado pelo arquivo utilizado, limitou-se a partição utilizada em 500MB. As informações salvas no arquivo de caractere armazenado no cartão SD, tem o seguinte formato: [Nome do Usuário];[ID da Digital];[ID da TAG];.

2.2.4. Comunicação SPI

Dos quatro shields utilizados nesse projeto, dois utilizam a comunicação SPI, o leitor RFID e o leitor de cartão SD. Para que não houvesse conflito na comunicação, visto que os dois utilizam o mesmo canal de comunicação, foram criadas duas variáveis de controle para selecionar qual dispositivo deveria estar ligado.

A variável SS_RFID_PIN, definida no pino 23, serve para selecionar quando o leitor de RFID deve estar ativo, enquanto a variável SS_SD_PIN, definida no pino 26, seleciona o leitor do cartão SD. Essa seleção é ativada enviando um sinal HIGH ao pino do Select Slave que deve estar ativo no momento da comunicação.

3. Resultados Obtidos

Os resultados obtidos com o desenvolvimento deste projeto foram:

a) implementação de Criptografia no arquivo de caracteres do cartão SD, através do algoritmo RC4;

b) integração de todos os componentes necessários, destaque aos que utilizam comunicação SPI;

c) desenvolvimento do Protótipo.

4. Conclusão

Atualmente a informação é o bem mais valioso que se possui. Na sociedade moderna o poder da informação, para transformá-lo em conhecimento, pode construir e destruir uma pessoa, uma empresa ou até mesmo um país inteiro. Por isso, é de suma importância que as organizações estejam preocupadas com a segurança dos dados em sua posse. É necessário que elas se protejam tanto com controles lógicos, como firewall, antivírus, entre outros, quanto controles que impeçam o acesso físico ao meio onde a informação está armazenada.

O objetivo principal deste trabalho foi desenvolver um sistema de controle de acesso físico com dupla identificação, para esse trabalho foram utilizadas duas tecnologias muito utilizadas no momento que são a comunicação RFID e a leitura biométrica da digital, unidas pela plataforma de prototipação Arduino. Para que esse desenvolvimento fosse possível, foi necessário estudar e compreender o funcionamento e técnicas relacionadas à criptografia, Arduino, RFID e biometria, em especial a leitura da digital.

No estudo da plataforma Arduino foi possível conhecer diversas aplicações possíveis, desde um simples sensor para controlar a luminosidade de uma sala, até o desenvolvimento de um satélite, passando por projetos de impressoras 3D. Através do desenvolvimento do algoritmo que foi inserido no Arduino, os conhecimentos sobre programação também foram aprimorados. Na plataforma Arduino pode-se destacar como benefício suas comunidades de desenvolvedores, que possibilitam a troca de experiências e conhecimentos sobre desenvolvimento, em especial de automação.

O levantamento bibliográfico acerca dos conceitos e técnicas de biometria foi fundamental para a compreensão do funcionamento dessa tecnologia, em especial a datiloscopia. Através deste projeto pôde-se conhecer as minucias que são comparadas e analisados para identificar uma pessoa com base na leitura de sua impressão digital. Também foi possível ter uma leve compreensão sobre os demais tipos de biometria existentes, como leitura da íris, face, escrita, entre outras.

Durante o levantamento da fundamentação teórica, foi possível compreender com maior profundidade o funcionamento da tecnologia de rádio frequência, dentre as aplicações mais comuns estão o controle de mercadorias, a identificação de pessoas e o registro de acesso. Pôde-se observar a forma de leitura das tags juntamente com os componentes necessários à operação de sistemas baseados em RFID.

Adquiridas as bases de conhecimento necessárias, foi possível integrar os shields de leitura de digital e tags RFID, juntamente com o visor LCD e leitor de cartão SD, com a plataforma Arduino como proposto. Concluiu-se que as tecnologias de identificação por leitura da digital e de identificação por rádio frequência unidas, dão ao sistema de controle de acesso a segurança necessária, garantindo que somente as pessoas autorizadas tenham acesso ao ambiente definido. A garantia de segurança das informações armazenadas na memória do sistema, foi conseguida através da implementação do algoritmo de criptografia RC4, atualmente utilizado em protocolos de comunicação SSL e TLS, que fornece a segurança necessária para operação do sistema.

Futuramente, para continuação deste trabalho, poderá ser integrado um shield de comunicação ethernet, com isso, será possível criar um gerenciador centralizado, através de comunicação via rede, para administração dos diversos pontos de controle que são implementados em um ambiente. A implementação de uma touchscreen poderá também melhorar a interação com o sistema em uma instalação standalone. Faz-se também necessária a implementação de sistema de auditoria dos acessos, atendendo dessa forma os quatro princípios de segurança da informação citados por Stoneburner (2001, tradução nossa).

5. Referências

FERREIRA, Fernando Nicolau Freitas. (2003). Segurança da Informação. [s. L.]: Ciência Moderna. 176 p.

BAUMANN, Rainer; CAVIN, Stephane; SCHMID, Stefan. (2006). Voice Over IP: Security and SPIT. Berna: [s.n.]. 34 p.

STONEBURNER, Gary. (2001). Underlying Technical Models for Information Technology Security:Recommendations of the National Institute of Standards and Technology. Gaithersburg: [s.n.]. 28 p.

KAHN, David. (1967). The Codebreakers: The Story of Secret Writing. Nova Iorque: Mcmillian & Co.. 1164 p.

MCDONALD, Nicholas G. ([2010]). Past, Present, and Future Methods of Cryptography and Data Encryption: A Research Review. Salt Lake City: [s.n.]. 22 p.

SALAS, Marcelo Invert Palma; PEREIRA, André Augusto da Silva. (2011). Análise Crítica da Implementação da Cifra RC4 no Protocolo WEP. [s. L.]: [s.n.]. 7 p.

LIU, Simon; SILVERMAN, Mark. (2001). A Practical Guide to Biometric Security Technology. IT Professional, [s.l.], v. 3, n. 1, p.27-32. Institute of Electrical & Electronics Engineers (IEEE).

GUMZ, Rafael Araújo. (2002). Protótipo de um Sistema de Identificação de Minúcias em Impressões Digitais Utilizando Redes Neurais. 134 f. TCC (Graduação) - Curso de Ciência da Computação, Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau.

KEHDY, (1968). Carlos. Elementos de Criminalística. São Paulo: Luzes . 267 p.

RABELLO, Eraldo. (1996). Curso de Criminalística. Porto Alegre: Sagra Luzzato. 208 p.

GLOVER, Bill; BATH, Himanshu. (2007). Fundamentos do RFID. Rio de Janeiro: Alta Books. 228 p.

IGOE, Tom. (2012). Getting Start with RFID: Identify Objects in the Physical World with Arduino. Sebastopol: O'reilly Media. 30 p.

BANZI, Massimo. (2012). Arduino: La guida ufficiale. Gorgonzola: Tecniche Nuove. 117 p.

ARDUINO. (2015). Site Oficial. Disponível em: <http://www.arduino.cc/>. Acesso em: 14 abr.