

Universidade Federal do Triângulo Mineiro

Jonas Bruno da Silva Morais

Desenvolvimento de um software para verificação de autenticidade de documentos
por meio de dispositivos móveis

Uberaba

2018

**Catálogo na fonte: Biblioteca da Universidade Federal do
Triângulo Mineiro**

M825d Morais, Jonas Bruno da Silva
 Desenvolvimento de um software para verificação de autenticidade
de documentos por meio de dispositivos móveis / Jonas Bruno da Silva
Morais. -- 2018.
60 f. : il., fig., tab.

Dissertação (Mestrado Profissional em Inovação Tecnológica) --
Universidade Federal do Triângulo Mineiro, Uberaba, MG, 2018
Orientador: Prof. Dr. David Calhau Jorge

1. Criptografia. 2. Documentos. 3. Autenticação. 4. Sistemas ima-
geadores de documentos. 5. Utilitários (Programas de computador). 6.
Aplicativos móveis. I. Jorge, David Calhau. II. Universidade Federal do
Triângulo Mineiro. III. Título.

CDU 004.056.55

Jonas Bruno da Silva Morais

Desenvolvimento de um software para verificação de autenticidade de documentos
por meio de dispositivos móveis

Dissertação apresentada ao Programa de
Mestrado Profissional em Inovação
Tecnológica, da Universidade Federal do
Triângulo Mineiro, como requisito para a
obtenção do título de mestre.

Orientador: Prof. Dr. David Calhau Jorge.

Uberaba

2018

JONAS BRUNO DA SILVA MORAIS

DESENVOLVIMENTO DE UM SOFTWARE PARA VERIFICAÇÃO DE
AUTENTICIDADE DE DOCUMENTOS POR MEIO DE DISPOSITIVOS
MÓVEIS

Trabalho de conclusão apresentado ao
Programa de Mestrado Profissional em
Inovação Tecnológica da Universidade Federal
do Triângulo Mineiro, como requisito para
obtenção do título de mestre.

Uberaba, 04 de dezembro de 2018

Banca Examinadora:



Prof. Dr. David Calhau Jorge
Orientador – PMPIT – UFTM



Prof. Dr. Marcelo Bacci da Silva
Membro Titular – UFTM



Prof. Dr. Marcelo Ponciano da Silva
Membro titular – IFTM

Dedico este trabalho à Deus, a meu amigo Reginaldo (em memória) e aos anjos guardiões que sempre cuidaram de mim.

AGRADECIMENTOS

Agradeço a minha família, a minha companheira, aos meus amigos que sempre me apoiam e ao meu Orientador David Calhau Jorge por sua imensa contribuição e dedicação sem os quais não haveria este projeto.

À Universidade Federal do Triângulo Mineiro e a Fapemig pela oportunidade e grande apoio ao desenvolvimento desta pesquisa.

À coordenação do PMPIT - Programa de Mestrado Profissional em Inovação Tecnológica pelos conhecimentos obtidos.

Ao Instituto Federal do Triangulo Mineiro, pelo apoio as minhas necessidades enquanto mestrando e por fazer parte dos objetivos desta dissertação.

RESUMO

A crescente popularização dos computadores e muitos outros dispositivos eletrônicos aumenta a emissão de documentos na forma impressa e principalmente na forma digital. Há preocupação por parte do Instituto Federal do Triângulo Mineiro (IFTM) de criar um mecanismo seguro e que possa coibir a falsificação e alteração indevida de documentos. Buscando a criação de uma ferramenta off-line que seja capaz de validar os documentos emitidos, com o objetivo de melhorar o processo de validação de documentos, foi desenvolvido um software capaz de colocar o conteúdo textual do documento. Utilizando uma tabela reduzida de caracteres é possível gerar uma economia de alguns bits por caractere resultando em uma forma de compressão e também de criptografia. Após tratar o texto e gerar um QR Code (quick response code) para inserção no documento, sendo um QR Code a cada 1200 caracteres, será possível através da aplicação que o usuário possa fazer a leitura e comparar os dados textuais contidos no QR Code e verificar se o documento não sofreu alteração, realizando deste modo uma validação quanto a sua autenticidade.

Palavras-chave: qrcode, criptografia, validação de documentos

ABSTRACT

The increasing computers popularization and many other electronic devices increases the emission of printed documents and mainly in the digital documents. There is concern of the Instituto Federal do Triangulo Mineiro (IFTM) to create a secure mechanism that can prevent falsification and improper alteration of documents. Looking the creation of an offline tool that is able to validate the documents issued, with the aim of improving the document validation process, a software was developed capable of placing the textual content of the document. Using a reduced character table it is possible to generate a saving of a few bits per character resulting in a form of compression and also of encryption. After treating the text and generating a QR Code (quick response code) for insertion in the document, being a QR Code every 1200 characters, it will be possible through the application that the user can read and compare the textual data contained in the QR Code and verify that the document has not changed, thereby performing a validation as to its authenticity.

Keywords: qr code, encryption, document validation

LISTA DE ILUSTRAÇÕES

Figura 1 - Processo de validação	13
Figura 2 - Modelos de Selo de Autenticação de Minas Gerais.....	15
Figura 3 - Consulta numeração de selo de autenticidade	16
Figura 4 - Criptografia simétrica	18
Figura 5 - Autenticação com chave assimétrica	19
Figura 6 - Confidencialidade com chave assimétrica	20
Figura 7 - Uso das versões do Android.....	21
Figura 8 - Exemplo de um QR Code.	24
Figura 9 - Comparativo entre versões do QR Code.	24
Figura 10 - Itens da metodologia.....	33
Figura 11 - Exemplo página com 1200 caracteres.....	34
Figura 12 - Exemplo QR Code Versão 21.....	38
Figura 13 - Mensagem de advertência do Gerador QR Code.....	40
Figura 14 - Tela principal do gerador de QR Code.....	41
Figura 15 - Tela gerador com texto preenchido.....	42
Figura 16 - Exemplo de código gerado.	43
Figura 17 - Documento com QR Code inserido.....	44
Figura 18 - Diagramas de classe.....	45
Figura 19 - Tela inicial aplicativo de leitura.	47
Figura 20 - Tela de leitura do código.....	47
Figura 21 - Aplicativo visualizando o texto.	48
Figura 22 - Comportamento com QR Code não esperado.....	49
Figura 23 - Documento exemplo para a geração.	50
Figura 24 - Gerador QR Code com o documento exemplo.	51
Figura 25 - QR Code gerado contendo o documento.....	51
Figura 26 - Aplicativo Android exibindo o texto do documento.....	52
Figura 27 - Exemplo documento com mais elementos textuais.	53
Figura 28 - Exemplo gerador texto mais complexo.	53
Figura 29 - QR Code gerado com mais conteúdo.....	54
Figura 30 - Texto com mais conteúdo lido pelo aplicativo.....	54

LISTA DE TABELAS

Tabela 1 – Tabela proposta de caracteres 6 bits	35
Tabela 2 – Exemplo de outra configuração da tabela	36
Tabela 3 – Alfabeto Coreano.....	37

LISTA DE SIGLAS

API – Interface de Programação de Aplicativos (*Application Programming Interface*)

ASCII – Código Padrão Americano para o Intercâmbio de Informação (*American Standard Code for Information Interchange*)

CERT.Br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança

IFTM – Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro

MP – Megapixel. Valor equivalente a um milhão de pixels

MATLAB – Laboratório de matrizes (*matrix laboratory*)

OCR – Reconhecimento ótico de caracteres (*Optical Character Recognition*)

PNG – Formato de imagem de alta qualidade (*Portable Network Graphics*)

QRCODE – Código de Resposta Rápida (*Quick Response Code*)

SMS – Serviço de mensagens curtas (*Short Message Service*)

TTS – Texto para fala (*text to speech*)

URL – Localizador uniforme de recursos (*Uniform Resource Locator*)

XOR – Ou Exclusivo (*Exclusive Or*)

SUMÁRIO

1. INTRODUÇÃO	11
2. OBJETIVO.....	14
2.1 OBJETIVOS GERAIS.....	14
2.2 OBJETIVOS ESPECIFICOS	14
3. FUNDAMENTAÇÃO TEÓRICA	15
3.1 VALIDAÇÃO DE DOCUMENTOS	15
3.2 CRIPTOGRAFIA	17
3.3 ANDROID.....	20
3.4 QR CODE	22
4. REVISÃO BIBLIOGRÁFICA	25
4.1 CÓDIGOS QR E SOLUÇÕES DE SEGURANÇA	25
4.2 MÉTODO DE CRIPTOGRAFAR MENSAGEM USANDO QR CODE	26
4.3 O CONCEITO QR CODE E SEUS BENEFÍCIOS PARA EMPRESAS.....	27
4.4 TEXTO BASEADO EM QR CODE PARA CONVERSÃO DE VOZ	28
4.5 GERAÇÃO E RECONHECIMENTO DE QR CODES.....	29
4.6 AUTENTICAÇÃO USANDO ASSINATURA DIGITAL E QR CODE	30
4.7 CRIPTOGRAFIA NO QR CODE USANDO ESTEGANOGRAFIA.....	32
5. MÉTODOS.....	33
5.1 COMPRESSÃO DO TEXTO	35
5.2 CRIPTOGRAFIA	38
5.3 APLICATIVO GERADOR DO QR CODE	39
5.4 APLICATIVO LEITOR DO QRCODE (DECODER).....	45
5.5 EXEMPLOS DE USO DO APLICATIVO	50
CONCLUSÃO	56
6. SUGESTÕES DE FUTURAS IMPLEMENTAÇÕES.....	58
7. REFERÊNCIAS	59

1. INTRODUÇÃO

Com a popularização crescente dos computadores, celulares e outros dispositivos eletrônicos, há uma utilização crescente na emissão de documentos na forma digital segundo Pasa (2001), o papel não é o único suporte possível para se confeccionar um documento. Uma vez que um documento possa ter um suporte material eletrônico passando a oferecer rapidez e agilidade no transporte da informação, e seu armazenamento em meio digital configura uma economia no seu armazenamento. A tecnologia de documentação eletrônica tem um recurso que se propõe a assegurar a consistência do conteúdo original e a identificação da procedência ao mesmo tempo. Este recurso é conhecido como firma digital ou assinatura digital (PASA, 2001). Segundo o CERT.Br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança) (2017) para um serviço eletrônico ser considerado seguro ele deverá possuir os requisitos básicos:

- Identificação (permitir que os usuários do serviço se identifiquem),
- Autenticação (verificar se a entidade é realmente quem diz ser),
- Autorização (determinar as ações que a entidade pode executar),
- Integridade (proteger a informação contra alteração não autorizada),
- Confidencialidade ou Sigilo (proteger uma informação contra acesso não autorizado),
- Não repúdio (evitar que uma entidade possa negar que foi ela que executou uma ação),
- Disponibilidade (garantir que um recurso esteja disponível sempre que necessário).

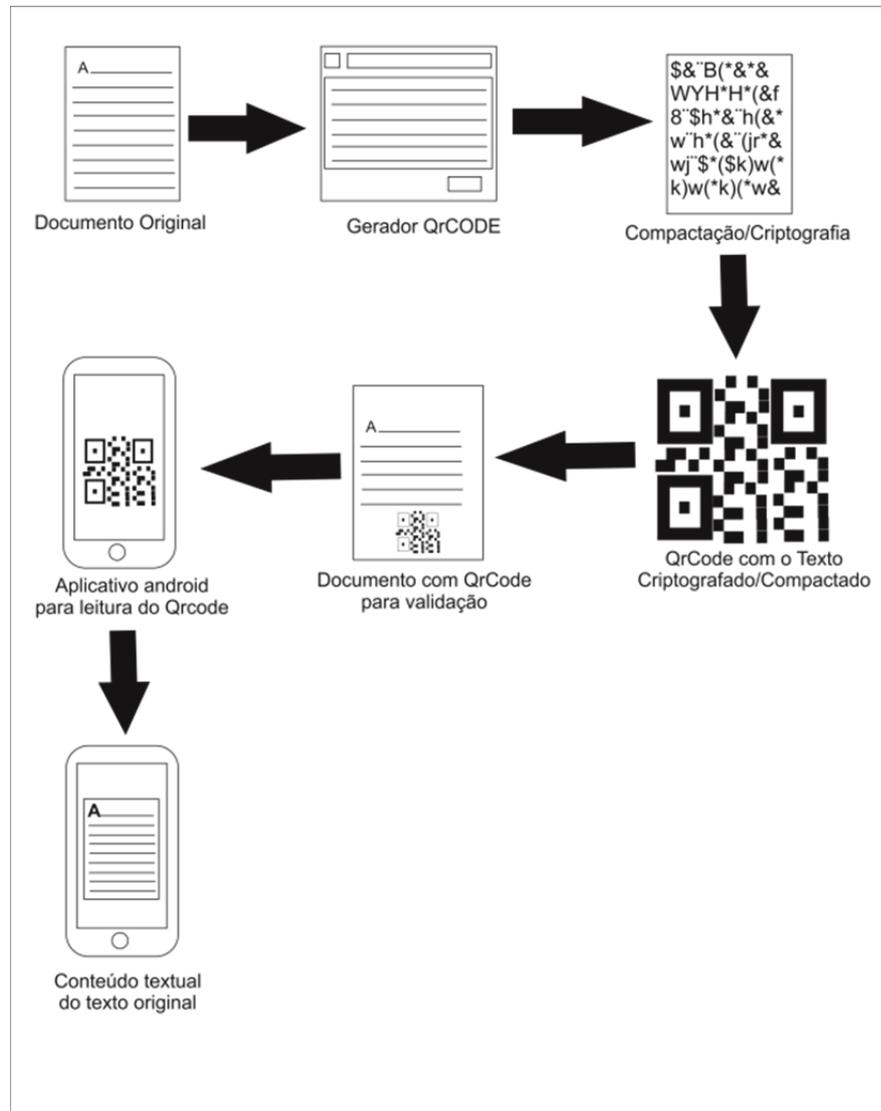
A secretaria de controle e Registro Acadêmico do Instituto Federal do Triângulo Mineiro (IFTM), emite alguns documentos para os alunos, como por exemplo, a declaração de matrícula. É importante ressaltar a preocupação por parte da instituição de criar um mecanismo seguro e que possa coibir a falsificação e alteração indevida dos documentos.

A criação de uma ferramenta que possa operar off-line (sem acesso a internet), podendo ser utilizada de maneira rápida e prática pelas entidades que

recebem esses documentos e que ao mesmo tempo seja capaz de validar os documentos emitidos, considerando que para a grande maioria dos documentos emitidos pelo IFTM também não existe uma forma de verificação on-line e apesar desta modalidade on-line ser consideravelmente mais fácil de implementar, possui a dependência de recursos (acesso a internet, servidores, máquinas dedicadas, softwares) que nem sempre se tem disponíveis, criando uma barreira a ser transposta pelos interessados em fazer a validação do documento.

Com o objetivo de melhorar o processo de validação de documentos, este projeto se destina ao desenvolvimento de um software capaz de colocar todo o conteúdo textual da página, utilizando algum método de criptografia e compressão, e logo após inserindo em um QR Code que estará disposto a cada 1200 caracteres, podendo ser agrupados um por página ou vários por página, conforme a necessidade, e permitirá que através da aplicação o usuário possa comparar os dados textuais inseridos por meio do QR Code e verificar se o documento não sofreu alteração, realizando deste modo uma validação quanto a sua autenticidade.

A figura 1 ilustra o processo de validação do documento. Dada a utilização do aplicativo na tentativa de validar o teor de documentos, a sua utilização pode se estender a demais instituições e entidades que tenham essa preocupação de criar uma forma off-line de validação de documentos.

Figura 1 - Processo de validação

Fonte: Autor (2018)

2. OBJETIVO

2.1 OBJETIVOS GERAIS

Desenvolver uma aplicação prática para dispositivos móveis para auxiliar o usuário no processo de validação de documentos, que seja capaz de gerar um QR CODE criptografado/compactado, para que possa ser inserido como método de controle no documento, decriptografar/descompactar e apresentar o conteúdo textual original do documento.

2.2 OBJETIVOS ESPECIFICOS

- Conhecer sobre o funcionamento do QR Code
- Estudar as aplicações para dispositivos móveis
- Criar protótipo para leitura do QR Code
- Estabelecer uma ou mais 'Tabelas de compressão' da informação e a forma de armazenamento.
- Eleger uma criptografia para inserir os dados no QR Code
- Apresentar o conteúdo textual original na geração do documento para comparação com capacidade de até 1200 caracteres por página.
- Criar uma aplicação para ler o QR Code e apresentá-lo em forma de texto para comparação com a folha impressa por meio de um dispositivo móvel.

3. FUNDAMENTAÇÃO TEÓRICA

Segundo Santos e Flores (2015) um grande fluxo de dados está circulando por meio de computadores e algumas tecnologias evoluíram tão rapidamente que se tornaram práticas comuns, causando reformulações na forma antiga de trafegar e armazenar os dados, e por esta razão se questiona se este avanço não estaria se tornando uma dependência.

3.1 VALIDAÇÃO DE DOCUMENTOS

A validação de documentos serve para comprovar a autoria e a veracidade da informação. A forma mais utilizada para validar um documento não eletrônico é feita através dos cartórios. Através deste método o cartório verifica o teor do documento e se for considerado um documento autêntico ele recebe um selo e uma numeração e é assinado por um responsável pela sua validação. A Figura 2 ilustra os selos utilizados no estado de Minas Gerais.

Figura 2 - Modelos de Selo de Autenticação de Minas Gerais



Fonte: Autor (2018)

O Tribunal de Justiça do Estado de Minas Gerais disponibiliza um serviço de consulta de selos de fiscalização que pode ser acessado através do endereço de

website de internet: <https://clientes.thomasgreg.com.br/MG/TJ/Telas/Principal.aspx>. Na figura 3 tem-se um exemplo de uma consulta, que mostra que a situação do selo é válida e também informações de qual cartório ele foi utilizado.

Figura 3 - Consulta numeração de selo de autenticidade

Consulta de Selos Cartorários

Número Selo:	CRG088203	Tipo Selo:	Autenticação
CNPJ:	20025698000107	Serventia:	Ofício do 1º Tabelionato de Notas
Endereço:	Rua Segismundo Mendes , 100 Centro		
Município:	Uberaba	Comarca:	Uberaba
Telefone:	3332-1303	Fax:	
Situação:	Selo Válido		
Data Entrega:	10/10/2016		
Observação:			

Fonte: Tribunal de Justiça de Minas Gerais

Para validar um documento eletrônico é preciso que ele seja assinado digitalmente ou que ele possua um código de controle e um mecanismo de acesso a esse código, a exemplo dos códigos dos selos dos cartórios de Minas Gerais.

Quando um documento é validado por código de controle, é preciso que o emissor do documento crie um serviço de acesso para consulta desses códigos, e através das informações dispostas por este serviço, o consultante do código deverá averiguar a validade do documento.

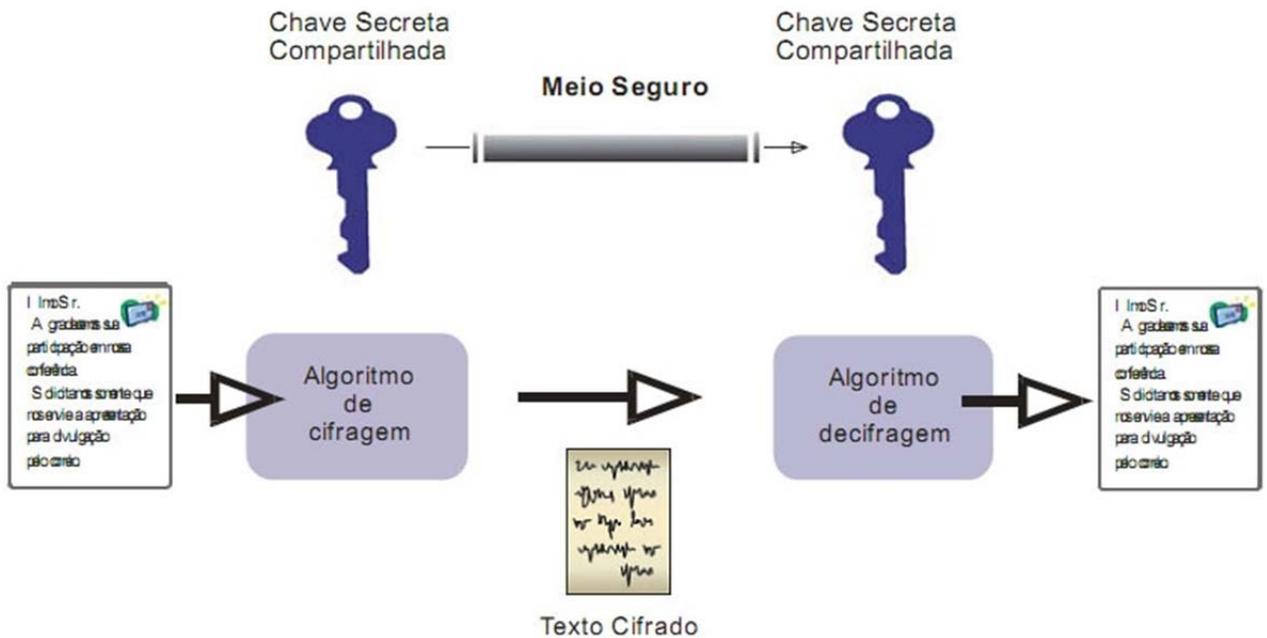
Os cartórios, também conhecidos como tabelionatos de notas, fornecem serviços de autenticação de documentos, reconhecimentos de firmas, e execução da lavratura de testamentos públicos, atas notariais e de procurações públicas. Para um cartório entrar em funcionamento ele deve estar devidamente autorizado, participar de processo licitatório por concurso público e cumprir com todas as legislações vigentes, que podem variar de acordo com o estado onde será o seu local de funcionamento. Estes estabelecimentos possuem um número limitado, a depender do município em que funcionam, oferecem seus serviços apenas no horário comercial, que muitas vezes é reduzido em uma hora a menos que o comércio local,

operando em locais de difícil acesso nos horários de tráfego intenso de veículos, e cobrando taxas, em espécie, por todos os serviços cobrados.

3.2 CRIPTOGRAFIA

Criptografia, segundo Portnoi (2014), é a ciência que trata de cifrar a escrita, de modo a torná-la ininteligível para os que não tenham os métodos convencionados para ter acesso a ela. Em Tecnologia da Informação, esta definição é ampliada a fim de englobar não só a escrita, mas qualquer tipo de documento ou dados que devam ser tratados secretamente. Seu uso na tecnologia da informação geralmente se resume em dois tipos: criptografia com chave simétrica e com chaves assimétricas. Na criptografia com chaves simétricas tanto o emissor da mensagem, quanto o receptor possuem chaves iguais. O que foi criptografado por esta chave só pode ser decifrado por uma cópia idêntica da mesma chave. A criptografia assimétrica possui um par de chaves ao invés de uma única chave, e o que foi criptografado por uma chave só pode ser decifrado pela outra chave. Uma das duas chaves é selecionada para ser a chave pública, e a outra para ser a chave privada. Quando uma mensagem é enviada ela é criptografada pela chave pública, somente o portador da chave privada poderá ver o conteúdo da mensagem enviada.

Figura 4 – Criptografia simétrica



Fonte: Nunes (2007)

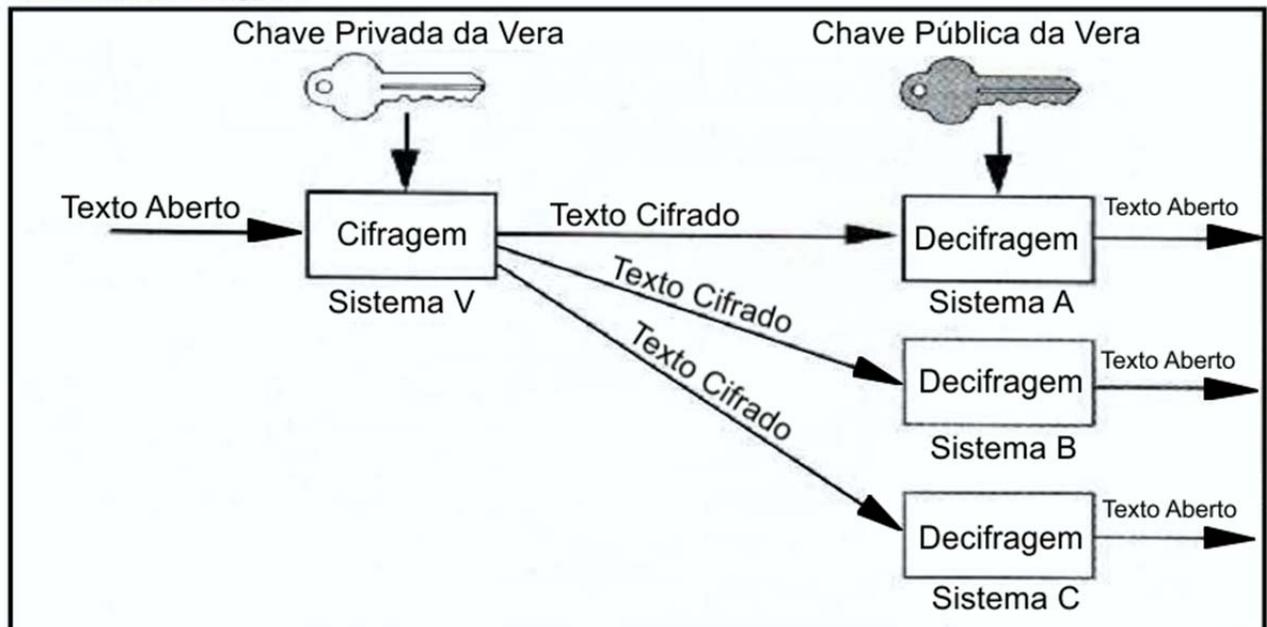
A criptografia simétrica é baseada em uma única chave, com cópias idênticas entre as partes, nesse tipo de criptografia, a chave é considerada sempre secreta e deve permanecer sempre muito bem guardada. Somente as pessoas que possuem uma cópia da chave podem entender a mensagem. Conforme podemos ver na figura 4, a mensagem é cifrada pela chave, enviada e decifrada pela mesma chave. Caso a mensagem seja interceptada no meio, ela não será inteligível por nenhuma parte que não possua a mesma chave.

Em se tratando da criptografia assimétrica, de acordo com Nunes (2007) também conhecida como criptografia de 'chave pública', possuindo duas chaves distintas, uma pública e a outra que é mantida em segredo denominada de chave privada. O que uma dessas duas chaves cifra, somente a outra decifra e vice versa. Muito comumente a tecnologia de chaves simétricas (par de chaves iguais) e assimétricas (par de chaves diferentes, pública e privada) são usadas em conjunto. O método de chaves assimétricas frequentemente é utilizado para criptografar uma chave simétrica e enviá-la ao destinatário desejado (o que chamamos de chave de sessão), desta forma as duas tecnologias de criptografia de chaves trabalham em conjunto. O uso da criptografia assimétrica permite fornecer confidencialidade e autenticação.

Na autenticação, conforme demonstra a figura 5, o ‘texto plano’ é cifrado através da chave privada, gerando assim um ‘texto cifrado’. No exemplo dessa figura esse texto cifrado é enviado ao ‘Sistema A’, ‘Sistema B’ e ‘Sistema C’, e através da chave pública do mesmo par o texto cifrado se torna novamente igual ao texto plano utilizado anteriormente. A chave pública fornece acesso a qualquer sistema ou processo que necessite checar se a informação realmente foi cifrada pelo usuário que diz ser, e por isso sabe-se que a mensagem é autêntica.

Figura 5 – Autenticação com chave assimétrica

Autenticação

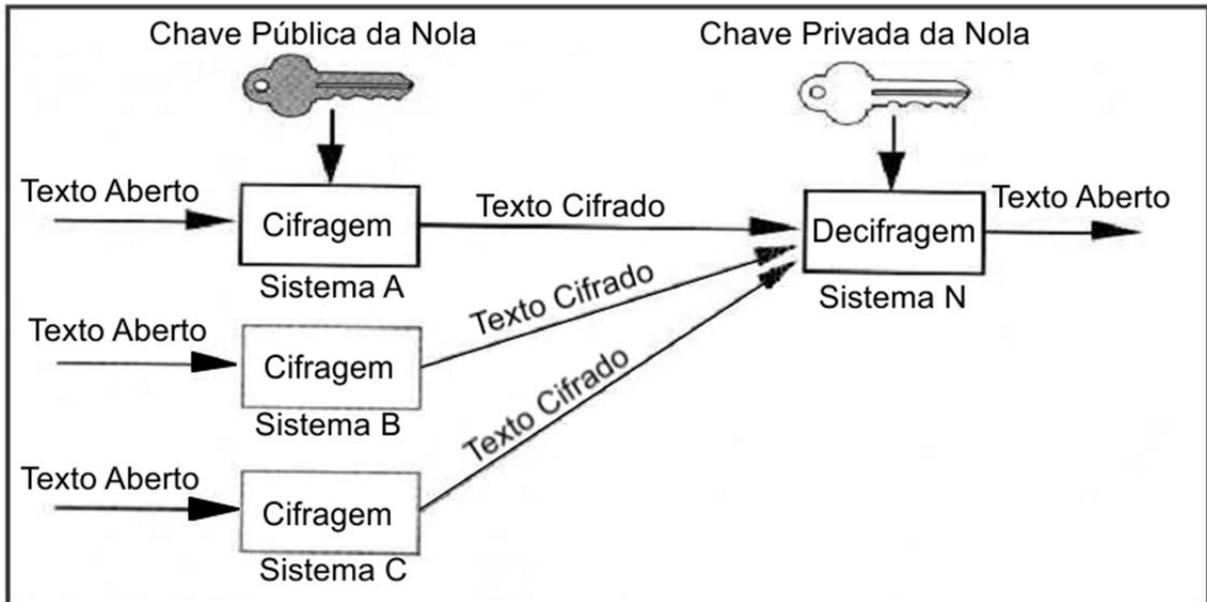


Fonte: Adaptado de Nunes (2007)

Para assegurar a confidencialidade, conforme a figura 6, o ‘texto plano’ dessa vez é cifrado pela chave pública do usuário, e tanto o ‘Sistema A’, ‘Sistema B’ e ‘Sistema C’ tem acesso a essa chave. Neste processo a mensagem é enviada cifrada ao usuário portador da chave privada, e somente esta chave é capaz de decifrar o texto, garantindo desta maneira que a mensagem é ‘confidencial’, uma vez que mesmo que a mensagem se extravie, ela só será decifrável pelo portador da chave privada do mesmo par que a chave pública utilizada para cifrar a mensagem.

Figura 6 – Confidencialidade com chave assimétrica

Confidencialidade



Fonte: Adaptado de Nunes (2007)

3.3 ANDROID

O sistema operacional Android, segundo Lecheta (2015) é baseado no sistema operacional Linux e vários de seus recursos nativos são baseados no kernel do Linux, como a capacidade de controle de processos e threads (processo simplificado, utilizado para que um processo possa se subdividir em mais de uma tarefa) e suas implementações de segurança.

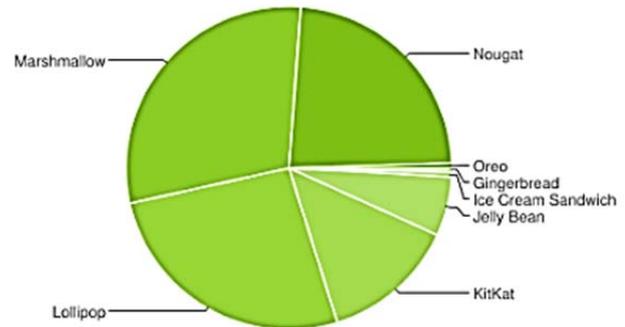
De acordo com Ekong et al. (2017), em 2014, os smartphones com o sistema operacional Android representaram um terço das conexões móveis em todo o mundo, a ainda há a previsão que aumentem para dois terços até 2020.

Conforme descrição do Android Open Source Project (2018), o Android foi originado por um grupo de empresas conhecido como Open Handset Alliance, liderado pelo Google e pode ser definido como um conjunto de software de código aberto, criado para uma ampla gama de dispositivos (como celulares, aparelhos

GPS, relógios, tablets, televisores, carros e outros) no intuito de ofertar aos fabricantes de hardware, vendedores de serviços e desenvolvedores, uma plataforma aberta e bem sucedida para melhorar a experiência do usuário. O sistema nativamente já oferece um conjunto básico de aplicativos como alarme, navegador, calculadora, calendário, câmera, relógio, gerenciador de contatos, gerenciamento de telefone, email, execução de mídias, álbuns de fotos, mensagens sms e outros. Esses aplicativos podem ser atualizados ou até mesmo substituídos conforme o fabricante do aparelho. O usuário também pode optar por baixar novos aplicativos conforme sua necessidade, utilizando para isso alguma plataforma de aplicativos, como por exemplo, a Google Play.

Figura 7 - Uso das versões do Android.

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.4%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.5%
4.1.x	Jelly Bean	16	2.0%
4.2.x		17	3.0%
4.3		18	0.9%
4.4	KitKat	19	13.4%
5.0	Lollipop	21	6.1%
5.1		22	20.2%
6.0	Marshmallow	23	29.7%
7.0	Nougat	24	19.3%
7.1		25	4.0%
8.0	Oreo	26	0.5%



Fonte: Android Developers (2018)

O sistema operacional android possui várias versões, conforme figura 7, e 93,2 % usam a versão 4.4 (kit kat) ou superior. Suas APIs (Interface de Programação de Aplicativos) são retrocompatíveis, permitindo que aplicativos construídos para versões alvo anteriores continuem rodando nas versões mais atuais, mas os aplicativos desenvolvidos para as versões mais recentes não executam corretamente nas versões anteriores.

3.4 QR CODE

O sistema de QR Code (quick response code, em português, código de resposta rápida) foi primeiramente desenvolvido para a indústria automobilística japonesa, uma evolução do código de barras tradicional que funciona como um rótulo que pode ser lido por máquinas e pode conter informações sobre os objetos que estão junto a ele (Thamer; Ameen, 2016).

Ao contrário do código de barras convencional que é escaneado por um feixe de luz, o QR Code é escaneado por um sensor de imagem bi-dimensional e analisado por um processador de imagem que procura os marcadores de posição e transforma os pequenos pontos em informações binárias que são validadas por um algoritmo de validação de erros (Thamer; Ameen, 2016).

Atualmente, os smartphones são muito presentes nas vidas das pessoas, e são muitas as atividades que as pessoas podem desenvolver através deles, e o QR Code se torna uma ferramenta muito útil para auxiliar nessas tarefas, guardando um endereço de website, um código, uma especificação de produto, um conjunto de informações pessoais, tudo isso pronto para ser usado de forma ágil por outros sistemas. O QR Code é frequentemente usado em jornais e revistas, sites, propagandas, e para endereços de sites além de informações e dados diversos, além disso o QR Code se tornou a ferramenta oficial utilizada pela maioria dos governos e empresas. As principais vantagens do uso do QR Code ao invés dos outros códigos é o fato dele ter uma alta capacidade de armazenamento de dados, ter um tamanho de impressão relativamente pequeno pela sua capacidade de armazenamento, suportar caracteres orientais (Kanji e Kana), ter um controle de erro e redundância em quatro níveis, permitindo que um código seja lido mesmo que ele esteja ligeiramente rasurado ou faltando, possibilidade de leitura em qualquer posição. (JI, 2014)

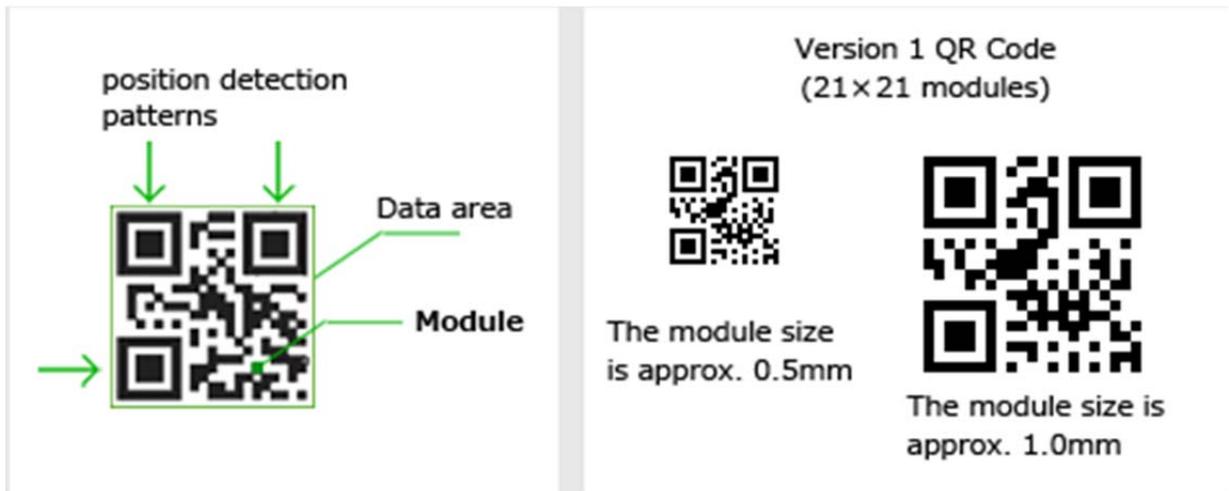
O QR Code foi criado e patenteado pela empresa DENSO-WAVE e é semelhante a um código de barras tradicional. Segundo a DENSO WAVE INCORPORATED (2017), enquanto o código de barras convencional consegue armazenar no máximo 20 dígitos aproximadamente, o código QR é capaz de armazenar qualquer tipo de dados e tem uma capacidade de até 7.089 caracteres em um único código QR. O

termo QR é oriundo de “Quick Response” que em português significa “resposta rápida”. O QR Code, além da sua maior capacidade de armazenamento, também apresenta alguns recursos extras em comparação com o código de barras convencional, como poder ser lido em qualquer posição 360°, e por conseguir ser lido mesmo caso parte dele esteja danificado, sujo ou parcialmente obstruído.

Existem 4 níveis de redundância que devem ser escolhidos no momento da geração do QR Code. No nível baixo, ele oferece redundância de 7%, no médio 15%, no quartil (nível que faz referencia a $\frac{1}{4}$ da informação) 25% e no alto 30%.

A figura 8 mostra um exemplo de um QR Code e suas especificações conforme a versão 1. Os QR Codes podem possuir até 40 versões e cada versão gera uma imagem maior e com mais capacidade de armazenamento. Quanto maior a versão, maior a dificuldade de leitura por câmeras e dispositivos computacionais, por isso deve-se utilizar sempre a menor versão possível, mas não existe nada que impeça de se criar um código na versão 40 com apenas poucos caracteres. Existem três quadrados maiores, também conhecidos como marcadores, que formam um triângulo e é usado pra detectar o padrão de posição ‘detection position patterns’, é por causa deles que o QR Code pode ser lido em qualquer posição. A parte interna do marcador é delimitada por uma distância que é utilizada para descobrir o tamanho do módulo (cada pontinho preto ou branco é denominado módulo), e por essa razão o QR Code não tem necessidade de padronizar seu tamanho, pois ele é pré-configurado através de seus marcadores. Pode-se observar a alteração de tamanho nos módulos através da parte direita da figura 8. A área que não pertence aos marcadores é chamada ‘área de dados’ (data area), onde toda a informação é armazenada.

Figura 8 - Exemplo de um QR Code.



Fonte: Qrcode.com (2017)

Através da figura 9 tem-se um comparativo das diferentes versões, todas as imagens foram geradas com o mesmo texto de exemplo 'ABC 123456789' para facilitar a comparação.

Figura 9 - Comparativo entre versões do QR Code.



Fonte: Autor (2018)

4. REVISÃO BIBLIOGRÁFICA

4.1 CÓDIGOS QR E SOLUÇÕES DE SEGURANÇA

Narayanan (2012), aborda a importância de ter uma ferramenta que permita identificar objetos e lugares e compartilhar pequenas informações úteis e destacando que o QR Code tem se mostrado uma excelente ferramenta para tais ações.

Um QR Code é mais comumente usado para auxiliar em:

- Informações de contato
- Evento de calendário
- Endereço de email
- Número de telefone
- Posicionamento GPS (Geo localização)
- SMS (mensagem telefônica)
- Texto ou parágrafo
- Conectar a uma rede Wi-fi
- URL (endereço web)

Após mapear os usos mais comuns do QR Code, Narayanan (2012) listou como isso pode ser usado de forma maliciosa. Em setembro de 2011 a KasperskyLab, uma empresa especializada em segurança, detectou um código malicioso em um código QR, que quando era escaneado um arquivo malicioso era baixado no telefone do usuário sem que ele soubesse. Basicamente a única forma de fazer um ataque malicioso com um QR Code é alterando seu conteúdo para que o usuário acesse sem saber.

A vulnerabilidade presente no QR Code, segundo Narayanan (2012) é causada pela próprio design do código que é ilegível para os seres humanos, e uma pessoa não consegue saber se o que ele vai fazer é bom ou ruim simplesmente olhando para o código, então ele listou uma série de ações a serem tomadas para que o QR Code possa oferecer mais segurança:

- Informar ao usuário qual a finalidade do QR Code, permitindo que ele verifique se ele está fazendo exatamente isto.
- Se for uma URL, deixar ela impressa próxima ao código.
- Tentar usar sempre a URL com https.
- Tentar usar encurtadores de URL (para facilitar a verificação por parte do usuário).
- Se o QR Code estiver em uma área pública ou movimentada, evite fazer com que o usuário tenha que pegar documentos e informações pessoais ou de pagamento.

Com estas ações, os QR Codes bastante presentes nas mídias sociais, para identificar e compartilhar informações podem se tornar mais seguros e dar meios para que o usuário possa se proteger de possíveis ataques.

4.2 UM NOVO MÉTODO DE CRIPTOGRAFAR UMA MENSAGEM USANDO QR CODE

Nesta técnica descrita por Thamer e Ameen (2016), são gerados dois códigos QR, um para a mensagem e um para a chave que vai criptografar a mensagem. Quando a mensagem é criptografada um terceiro QR Code é gerado, contendo a chave e a mensagem criptografada.

Processo de criptografia é baseado nos seguintes passos:

- Gerar o QR Code para a mensagem (M)
- Gerar o QR Code para a chave (C)
- Gerar QR Code resultado de XOR entre M e C (R)
- Colocar o valor da chave em (R)
- Salvar o QR Code final

E o processo de decifragem:

- Ler o QR Code criptografado
- Extrair a chave

- Gerar QR Code para a chave
- XOR com o QR Code gerado pela chave
- Ler mensagem

Com esta técnica um leitor comum de QR Code não consegue decifrar a mensagem porque ele não está apto a retirar a chave e decifrar a mensagem. Devido a manipulação binária ocasionada pelo XOR, o QR Code final gerado sequer é legível por um leitor QR Code comum.

4.3 EXPLORANDO O CONCEITO DE QR CODE E SEUS BENEFÍCIOS PARA EMPRESAS

Em sua pesquisa, Ji (2014) visa analisar e elencar as vantagens do uso do QR Code em empresas, mostrando o QR Code em detalhes e estudando suas informações mais gerais para que as pessoas possam entender como ele funciona. Além de explorar e analisar as tecnologias mais essenciais e viáveis relacionadas ao uso do QR Code. Adicionalmente a pesquisa citada também tenta trazer as melhores práticas e tenta explorar as melhores vantagens de cada uma e enfatiza as capacidades do QR Code na integração com o aplicativo WeChat (um 'super' aplicativo muito comum na china, de propósito geral, que pode ser usado pra trocar mensagens, chamar taxis, fazer compras, enviar ou cobrar dinheiro a amigos, comprar passagens de trem, agendar uma consulta ao médico, entre outros), e por meio do WeChat, permitir uma empresa utilizar-se de todas as funcionalidades que ele fornece.

O WeChat possui um gerador e um leitor de QR Code, que pode ser utilizado para que o usuário gera seus próprios códigos, o que faz do QR Code não só o coração desse aplicativo de mídia, mas também um recurso especial do WeChat. Ele é utilizado para fazer compartilhamento de informações entre os usuários, eles podem se adicionar através dele, onde cada usuário possui um QR Code individual, e o mesmo acontece com as contas empresariais. Os QR Codes não necessariamente precisam ser lidos pela câmera do telefone, mas podem ser lidos através de arquivos de imagem salvos na memória do dispositivo.

Os benefícios do uso do QR Code aqui listados são discutidos do ponto de vista de um usuário empresarial. O QR Code facilita muito a criação de propagandas e campanhas, reduzindo os custos, principalmente se a empresa produzir o próprio aplicativo. Existem muitos casos do QR Code aumentando vendas e produzindo receita. Quando utilizado para fazer integrações com outros aplicativos como o WeChat, a gama de opções aumentam ainda mais Ji (2014).

4.4 TEXTO BASEADO EM QR CODE PARA CONVERSÃO DE VOZ

Moorty et al. (2017) elucida que os QR Codes foram desenvolvidos há mais de quinze anos, mas somente a popularização dos dispositivos móveis de maior desempenho passamos a testemunhar um crescimento constante de aplicativos comerciais usando esta tecnologia. Esta pesquisa tem como objetivo fornecer as pessoas uma tecnologia que permita a elas obter informação sobre qualquer coisa simplesmente digitalizando um QR Code. E o resultado dessa obtenção de informação textual é posteriormente convertida em fala usando um software especializado.

Em situações em que uma pessoa viaja a um ponto turístico, por exemplo algum patrimônio cultural, a pessoa precisa de ajuda de um guia turístico para conhecer os aspectos culturais do lugar. Isso muitas vezes resulta em um passeio com uma multidão de pessoas, fazendo que a visita fique conturbada. Além disso, se a pessoa desejar explorar o local por conta própria, ela precisará comprar um guia impresso e ficar consultando-o para obter as informações contidas nele, o que será demorado. Por isso acreditamos que a informação textual poderia ser transmitida de forma mais eficiente oralmente.

O principal objetivo deste projeto é proporcionar a independência para poder explorar coisas (e locais), fornecendo uma maneira de acessar informações a palma da mão. O projeto basicamente lida com a leitura de um texto contido em QR Code e o converte em fala. Então supondo que num determinado ponto turístico haja um QR Code com informações sobre este local, o turista usando seu telefone, o aponta para o QR Code fazendo sua leitura, e por meio de um software especializado este texto

é convertido em fala, e ele pode então ouvir as informações sobre o local usando fones de ouvidos plugados ao seu telefone móvel e continuar explorando outros lugares do local histórico como bem quiser. Desta maneira, num curto intervalo de tempo o usuário possui toda a informação que ele precisa ao seu dispor, e se ele julgar necessário, ele também poderá ler a informação ao invés de ouvi-la.

A metodologia é baseada em dois estágios, sendo o primeiro composto pela geração do QR Code, que é feito através de endereços da web que oferecem esse serviço de geração gratuitamente e colocando as informações sobre o local desejado. O segundo passo consiste na leitura do QR Code e na conversão do texto para fala.

A conversão do texto para fala ocorre em várias etapas. Os sistemas TTS (text to speech, texto para fala) obtém um texto como entrada, que é primeiramente analisado e depois transformado em uma descrição fonética. Então na próxima etapa é gerada a prosódia (parte da linguística que estuda a entonação, o ritmo, o acento da linguagem falada e demais atributos correlatos na fala) e dessa informação produz o sinal de voz.

Como resultado tem-se muitas formas de utilizar este aplicativo que conta com a vantagem de ser um processo rápido e livre de erros, o usuário pode facilmente salvar os dados no seu telefone para se lembrar depois, e ressaltando que os QR Codes podem armazenar muito mais informação comparados aos códigos de barras convencionais e podem ser lidos em qualquer posição, por isso se tornam uma questão estratégica nesta aplicação.

4.5 GERAÇÃO E RECONHECIMENTO DE QR CODES

Bhargav, Kumar e Bhondekar (2015), afirmam que os QR Codes são ilegíveis aos humanos, e são códigos em duas dimensões, focados na alta velocidade de leitura e grande capacidade de armazenamento quando comparados aos códigos de barra tradicionais. Visando aumentar a sua capacidade foram desenvolvidos três QR Codes usando Zxing (Biblioteca usada para trabalhar com códigos de barra no desenvolvimento de aplicativos Android) e MATLAB. Os QR Codes resultantes foram

processados através do MATLAB por um algoritmo que utiliza as propriedades como a área e usa para alterar a cor dos 'marcadores' e da sua cor de fundo criando uma terceira dimensão, fazendo que haja três códigos com mensagens separadas ao invés de um.

A metodologia é dividida em alguns passos, primeiro usa-se a Zxing para criar os QR Codes e salvar os arquivos para que possam ser abertos pelo MATLAB, logo após a mensagem é inserida e a imagem é salva novamente, repetindo esse processo por mais três vezes, até a geração de Códigos QR com cores distintas. Nesse ponto as três imagens serão mescladas num único QR Code, possuindo em cada camada colorida uma mensagem distinta. Desta maneira a capacidade do QR Code é aumentada três vezes.

A leitura deste QR Code aprimorado é feita através do tratamento da imagem, separando a imagem de acordo com os canais de cores, e restaurando as imagens que geraram o código mesclado. A imagem é processada pelo MATLAB, e através das funções de reconhecimento de padrão e separação de canais das cores, as três mensagens guardadas no código podem ser corretamente lidas e exibidas.

4.6 AUTENTICAÇÃO DE DOCUMENTOS EM PAPEL USANDO ASSINATURA DIGITAL E QR CODE

Warasart e Kuacharoen (2018) afirma-se que há situações em que documentos eletrônicos ainda não podem substituir de forma eficiente o documento baseado em papel. Como por exemplo, os documentos emitidos pelo governo, certidões de nascimento, carteiras de motorista, passaportes ainda são baseados em papel (mesmo com versões digitais). Com acesso a algumas tecnologias avançadas, esses documentos podem ser facilmente fraudados. Baseando-se nisto apresenta-se a autenticação de documentos em papel onde a integridade do texto, mensagem e o autor do documento podem ser verificados com o uso de uma assinatura digital e um QR Code. O método proposto pode ser automático ou semiautomático. Será considerado semiautomático quando não houver uso de OCR (reconhecimento ótico de caracteres), e a comparação for feita visualmente pelo próprio usuário,

comparando a mensagem do texto e a mensagem obtida pelo QR Code, no entanto, esse método fornece conveniência para o usuário ao lidar com uma grande quantidade de documentos.

A autenticidade de documentos impressos em papel geralmente requer um especialista, geralmente essa atividade é realizada por um perito. Este tipo de trabalho utiliza equipamentos especiais, como lâmpadas UV, lupas, detectores infravermelhos. Na prática a inspeção para uma organização de uma grande quantidade de documentos é muito difícil, pois muitas vezes há a necessidade que o documento seja inspecionado rapidamente.

A metodologia deste projeto se baseia no uso de chaves assíncronas. Tão logo o documento é criado uma chave privada é usada para assinar o documento criando um hash (código alfanumérico calculado, utilizado para gerar uma identificação única). A mensagem é compactada juntamente com a assinatura, o resultado dessa compactação é enviado a um gerador de Código QR e o código QR é impresso no documento. Para a validação do documento o usuário que recebeu o documento fará a leitura do QR Code, a mensagem será descompactada, resultando na mensagem juntamente com a assinatura (hash), a assinatura é decriptada com a chave publica da pessoa que assinou o documento e após comparada com a mensagem original, se elas forem iguais o documento será sinalizado como autentico, caso não sejam ele será sinalizado para verificação manual.

A autenticidade dos documentos em papel pode ser obtida usando assinatuitas digitais e QR Codes, sem necessidade de acesso a banco de dados, e se a impressão estiver dentro de condições adequadas, pode ser usado OCR para fazer a comparação automaticamente, caso contrário deverá ser feito por inspeção humana, ressaltando as possíveis diferenças. Este projeto tem a vantagem de não precisar de um perito especialista para verificar o documento.

4.7 CRIPTOGRAFIA NO QR CODE USANDO ESTEGANOGRAFIA

A esteganografia é o estudo de diversas técnicas com o objetivo de esconder uma imagem em outra. Possui muitas aplicações práticas, e é muito utilizada para fins de segurança e privacidade.

Os QR Codes, segundo Sahu (2013) são usados principalmente para transmitir ou armazenar mensagens porque eles têm maior, ou melhor, capacidade de armazenamento do que um código de barras convencional e por isso podem ser usados perfeitamente para enviar dados criptografados. Este método visa adequar-se a empresas, setores do governo e redes de comunicações poderem enviar suas mensagens criptografadas rapidamente para o seu destino, protegendo-a de vazamentos externos (acessos não autorizados).

Neste contexto o objetivo principal é esconder imagens no QR Code, para que possa ser usada por exemplo pra comprar a imagem impressa no passaporte, com a imagem escondida e possivelmente, até mesmo acessar uma base de dados de acesso restrito para comparação.

Na fase de incorporação é gerado um QR Code de forma convencional, essa imagem será usada como capa. Nesta imagem podem ser inseridas quaisquer informações que se julguem relevantes, com exceção de informações q se deseja esconder. O próximo passo é escolher uma imagem de capa e escolher o arquivo ou dados que serão incorporados na imagem QR que será usada como capa (imagem visível a todos). Usando esta imagem de capa e com esteganografia os dados ocultos serão incorporados na imagem capa do QR Code.

Na fase de desincorporação, será usada a stegno descriptografia. O remetente da mensagem conseguirá ler a mensagem somente pelo software desenvolvido nesse projeto. Ao salvar a imagem do QR Code o software realizará todos os processos necessários para retirar da imagem os dados incorporados e para ler o QR Code utilizado como capa e apresentar os dados ao remetente.

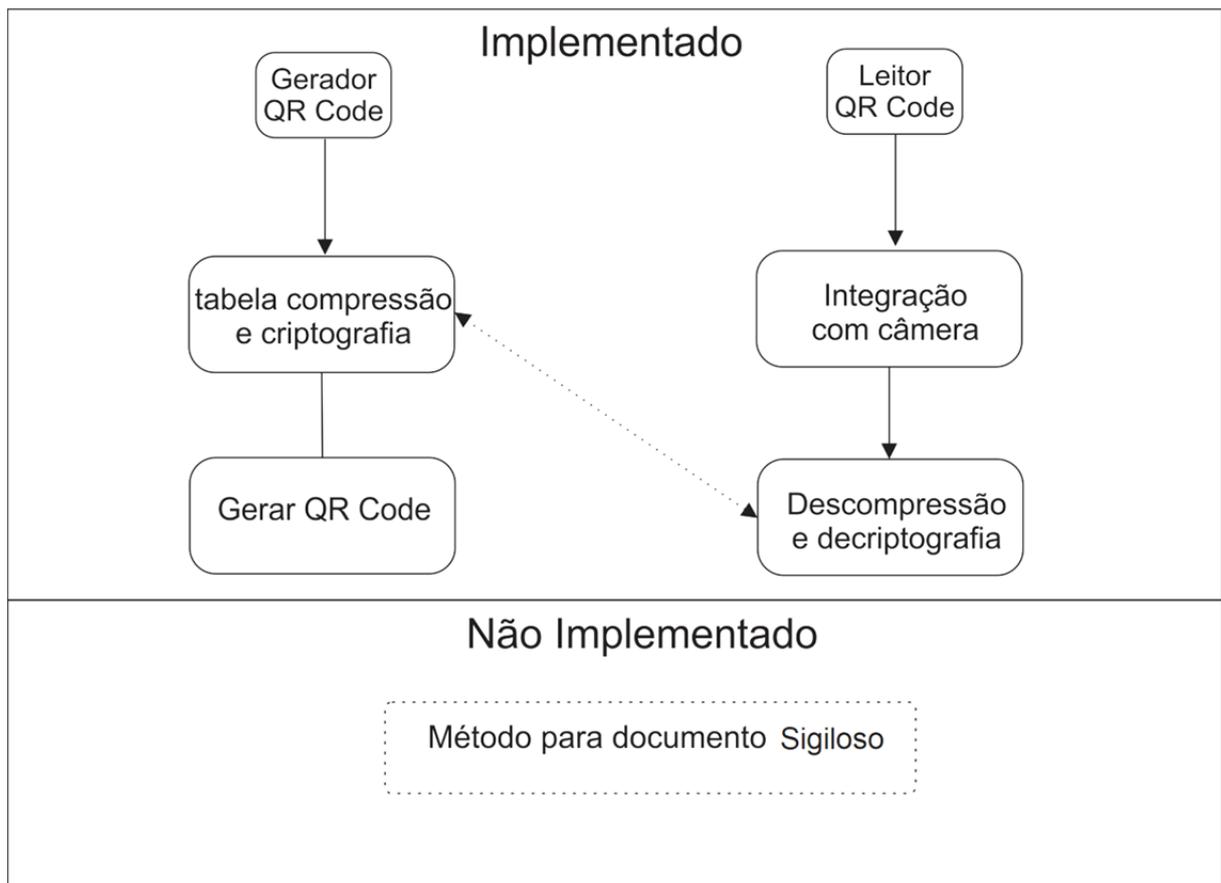
QR Codes criptografados são códigos que nem todos podem ler ou acessar, eles não são muito comuns, já que a maioria dos QR Codes são utilizados por marketing e outros usos que desejam que eles sejam acessíveis por todos.

5. MÉTODOS

Foi desenvolvido um aplicativo para dispositivo móvel em ANDROID (4.4 kit kat), com a função de ler através da câmera do dispositivo e mostrar o conteúdo dos QR Codes permitindo que seja feita a comparação com o documento original e também foi desenvolvida uma ferramenta para a geração dos QR Codes, com a função de gerar um QR Code a cada 1200 caracteres.

Conforme podemos observar através da figura 10, o ultimo item, que cria uma nova funcionalidade para tratar de arquivos com um nível de sigilo não foi implementado. Este passo será apenas citado na metodologia e sugerido como uma futura implementação. Também através da figura 10, temos os itens que foram implementados, e que descrevem passo a passo as etapas necessárias, mesmo que se tratem de duas aplicações distintas.

Figura 10 - Itens da metodologia.

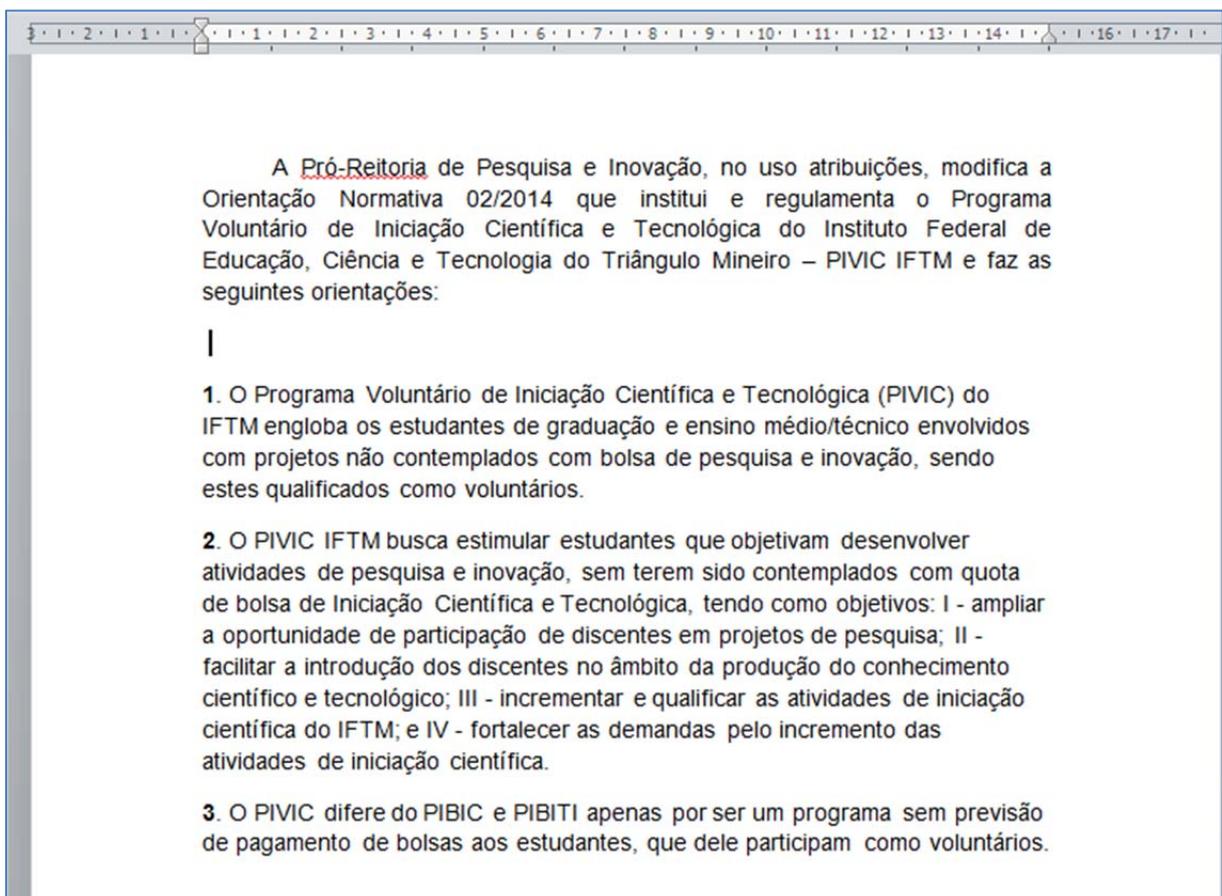


Fonte: Autor (2018)

A opção por 1200 caracteres se baseia em tentar utilizar versões menores do QR Code, sendo um QR Code menos denso e mais fácil de ler.

Entretanto caso seja necessário, o usuário poderá optar em colocar mais de um QR Code por página, desta maneira cada código conterá até 1200 caracteres. O gerador já se encarrega de fazer essa separação e gerar quantos códigos forem necessários. A figura 11 é um exemplo de um documento com essa quantidade de caracteres.

Figura 11 - Exemplo página com 1200 caracteres.



Fonte: Autor (2017)

5.1 COMPRESSÃO DO TEXTO

A compressão será necessária para redução do tamanho do QR Code, neste método de compressão foi utilizada uma tabela de caracteres simplificada com apenas 6 bits, ao contrário da tabela ASCII que possui 8 bits.

Tabela 1 – Tabela proposta de caracteres 6 bits

COD	CHAR	COD	CHAR	COD	CHAR	COD	CHAR	COD	CHAR
1	A	14	N	27	0	40	?	53	=
2	B	15	O	28	1	41	!	54	:
3	C	16	P	29	2	42	@	55	
4	D	17	Q	30	3	43	#	56	;
5	E	18	R	31	4	44	°	57	
6	F	19	S	32	5	45	+	58	
7	G	20	T	33	6	46	-	59	
8	H	21	U	34	7	47	(60	
9	I	22	V	35	8	48)	61	
10	J	23	X	36	9	49	%	62	
11	K	24	Z	37	(SPC)	50	C	63	
12	L	25	W	38	,	51	/	64	
13	M	26	Y	39	.	52	*	--	--

Fonte: Autor (2018)

A tabela ASCII, utiliza 8 bits ou 1 byte por caractere, com esta nova tabela haverá uma economia de 2 bits por caractere, permitindo assim uma compressão ($1200 \cdot 6/8 = 900$) com uma economia de 300 bytes em relação com a tabela ascii normal. Para esse máximo de 900 caracteres estima-se que será utilizada no máximo a versão 21 do QR Code. Entretanto, há a possibilidade da utilização de versões com maiores capacidades de armazenamento, esta escolha se deu somente pelo fato de uma maior legibilidade com a câmera dos dispositivos.

Neste método a tabela de caracteres poderá ser ajustada conforme as necessidades, na versão inicial deste gerador ele trabalha apenas com uma tabela muito semelhante a tabela 1. A troca de tabela pode ser facilmente implementada no método proposto por este projeto, a tabela 2 exemplifica como os caracteres podem ser trocados, e por possuir uma troca mnemônica (de equivalência 1 para 1 e de

troca simples) os caracteres utilizados também podem ser ajustados. Por ser uma tabela reduzida, no tamanho atual pode se usar um limite máximo de 64 caracteres que poderão ser selecionados. Por este motivo preferiu-se não utilizar acentos (agudo, circunflexo, trema) por que a tabela de caracteres precisa de posições distintas para os mesmos caracteres com e sem acento, gastando assim o dobro de posições (para cada acento) e limitando muito a tabela nas posições destinadas aos numerais e pontuação. O gerador está programado para efetuar a troca dos caracteres com esse tipo de acentuação para seu caractere correspondente sem acento automaticamente.

Tabela 2 – Exemplo de outra configuração da tabela

COD	CHAR	COD	CHAR	COD	CHAR	COD	CHAR	COD	CHAR
1	M	14	D	27	8	40		53	=
2	N	15	S	28	5	41		54	°
3	B	16	A	29	2	42	*	55	
4	V	17	P	30	7	43	&	56	:
5	C	18	O	31	4	44	/	57	@
6	X	19	I	32	1	45	+	58	#
7	Z	20	U	33	9	46	-	59	?
8	L	21	Y	34	6	47	(60	“
9	K	22	T	35	3	48)	61	
10	J	23	R	36	,	49	%	62	
11	H	24	E	37	.	50	(spc)	63	
12	G	25	W	38	:	51	/	64	
13	F	26	Q	39	:	52	*	--	--

Fonte: **Autor (2018)**

Na tabela 2, além de um embaralhamento da posição dos caracteres convencionais, houve adição e remoção de alguns poucos caracteres em relação a tabela 1, mostrando um exemplo da personalização do uso dos aplicativos para casos mais específicos.

Outro uso para este sistema de tabelas, seria a utilização deste sistema de validação de documentos em outros idiomas. A tabela 3 demonstra a inserção do alfabeto coreano, em tabela de mesmo tamanho, mantendo sua compressão,

adaptando dessa maneira o aplicativo gerador para que possa validar documentos que sejam elaborados através do alfabeto coreano.

Tabela 3 – Alfabeto Coreano

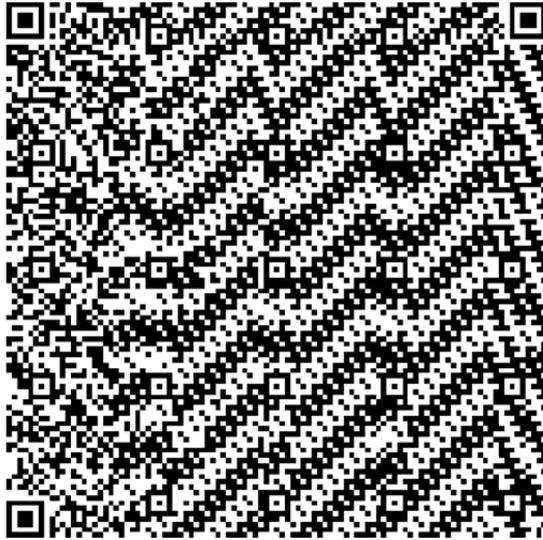
COD	CHAR	COD	CHAR	COD	CHAR	COD	CHAR	COD	CHAR
1	ㄱ	14	ㅇ	27	ㅈ	40	8	53	=
2	ㄴ	15	ㅅ	28	ㅊ	41	9	54	:
3	ㄷ	16	ㅇ	29	ㅋ	42	0	55	_
4	ㄹ	17	ㅈ	30	ㅌ	43	@	56	;
5	ㅁ	18	ㅊ	31	ㅍ	44	?	57	'
6	ㅂ	19	ㅍ	32	ㅑ	45	+	58	
7	ㅅ	20	ㅑ	33	1	46	-	59	
8	ㅇ	21	ㅑ	34	2	47	(60	
9	ㅈ	22	ㅑ	35	3	48)	61	
10	ㅊ	23	ㅑ	36	4	49	%	62	
11	ㅋ	24	ㅑ	37	5	50	(spc)	63	
12	ㅌ	25	ㅑ	38	6	51	/	64	
13	ㅍ	26	ㅑ	39	7	52	*	--	--

Fonte: **Autor (2018)**

Outra questão importante e que não poderia deixar de ser citada, é que poderia se abrir mão da compressão atual, por uma compressão menor (utilizando uma tabela superior a 6 bits), ou até mesmo não ter compressão alguma utilizando uma tabela de 8 bits ou mais, bem como utilizando versões superiores do QR Code para realizar seu armazenamento. Quanto maior a quantidade de caracteres na tabela menor será a compressão. Por isso podemos dizer que o tamanho da tabela de caracteres é inversamente proporcional a taxa de compressão.

Podemos observar na figura 12 um exemplo de como um QR Code na versão pretendida, e como ele pode ser denso (com muitos pontos), se comparado as versões com menor capacidade de armazenamento.

Figura 12- Exemplo QR Code Versão 21.



Fonte: Autor (2018)

5.2 CRIPTOGRAFIA

A utilização de uma tabela alternativa a ASCII cria uma sequência de caracteres aparentemente não legíveis, e para que a informação possa ser lida será necessário conhecer a tabela de caracteres e converter o texto de uma tabela para a outra. Esse processo por si só apesar de ser bem simples já pode ser considerado um nível bem básico de criptografia.

Para reforçar a segurança, há a possibilidade de serem aplicadas várias versões da tabela (conforme as tabelas aqui apresentadas), cada uma contendo um código identificador, onde a ordem dos caracteres seria embaralhada em cada versão. Desta maneira além de realizar a conversão, o usuário deveria saber também o código da tabela de caracteres utilizada, aumentando assim a segurança da criptografia.

As tabelas de caracteres poderão ter uma data de validade, forçando sua expiração e obrigando o cadastramento de uma nova tabela, gerando desta forma um retrabalho constante para qualquer interessado em burlar sua segurança. A data de validade poderia estar na própria tabela ou ser inserido no QR Code uma sessão para trazer essa informação separada da mensagem.

Este método tem a vantagem de poder ser feito off-line, sem conexão com a internet, ao contrário dos métodos de chaves que é necessário que haja uma conexão para que possa se obter a chave pública. O método atual permite que com os meios ajustados em ambos os aplicativos eles possam trabalhar em conjunto sem dependência de conexão ou de chaves. Caso o sistema trabalhe com mais de uma tabela, ou com tabelas com validade de data é possível criar rotinas de atualização apenas das tabelas, não necessitando de conexão com a internet para a realização do processo, mas somente para atualização das tabelas. Mesmo no método com chaves simétricas, que não é necessário uma conexão com a internet, ao dar-se a criptografia não existe a preocupação com relação a compactação, causando o efeito contrário e quando necessário compactar, isso se dá em etapas distintas, sendo necessário primeiramente cifrar e só depois compactar.

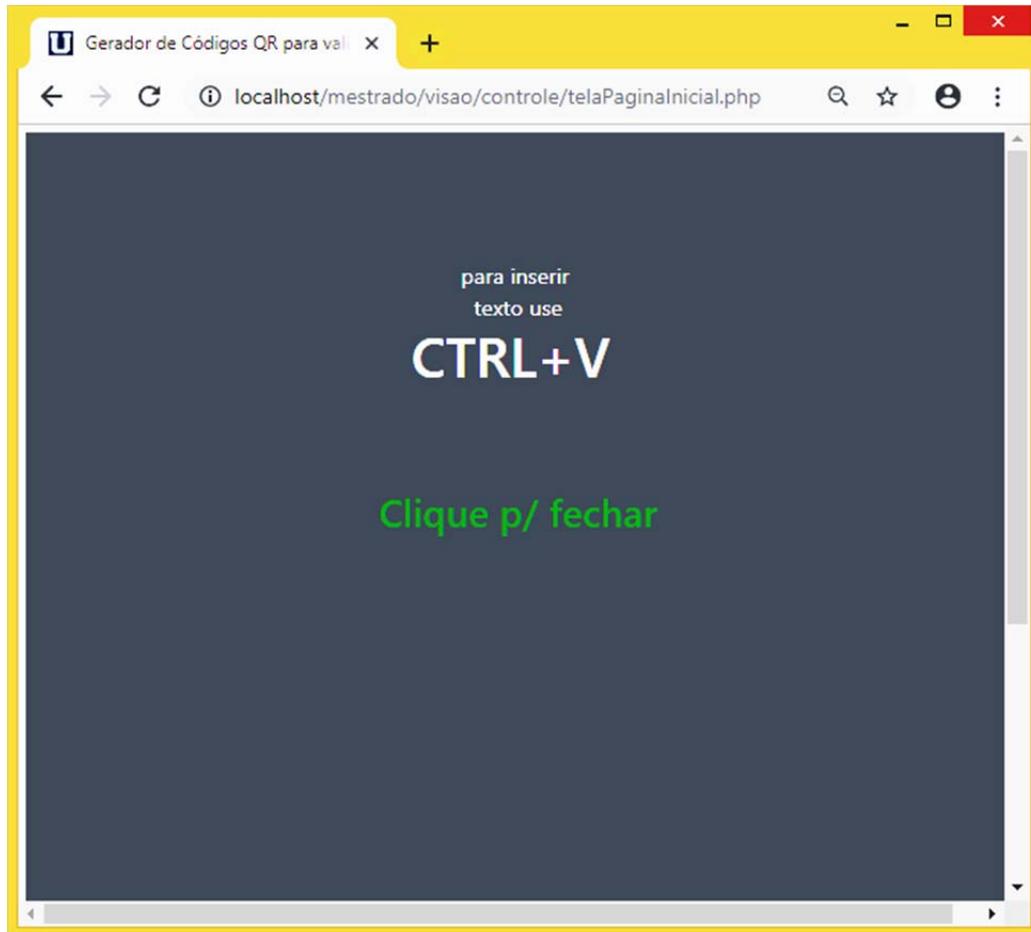
A técnica de criptografia utilizada ainda pode contemplar outros métodos de criptografia, podendo ser adaptada, ou até mesmo substituída, mas sem mudar os fins e os objetivos das ideias propostas por esse projeto.

5.3 APLICATIVO GERADOR DO QR CODE

Por meio deste aplicativo, o usuário poderá gerar os QR Codes para serem inseridos nos documentos. Ele será utilizado apenas para receber o conteúdo textual do documento e a partir dele gerar o QR Code correspondente.

Na figura 13, podemos observar que a tela inicial do aplicativo gerador é na verdade apenas uma advertência que será exibida até que seja dado um clique com o botão esquerdo do mouse, em seguida, a advertência é removida, mostrando a tela inicial. Esta tela inicial foi elaborada como uma advertência para elucidar que o gerador apenas receberá textos contidos na área de transferência do usuário e não permitirá que ele possa digitar o texto diretamente no gerador. Esta decisão foi tomada para tentar evitar que o usuário se confunda e nunca se esqueça de alterar a versão original do documento antes de gerar o QR Code.

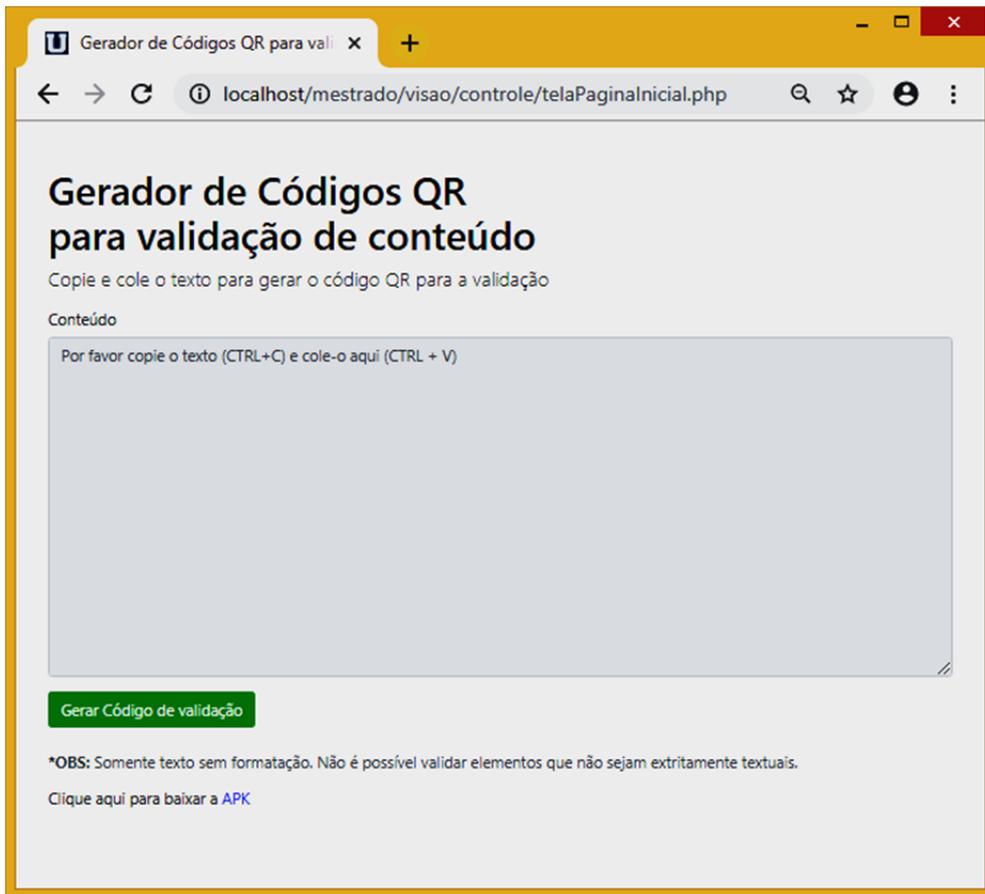
Figura 13 – Mensagem de advertência do Gerador QR Code.



Fonte: Autor(2018)

Logo após clicar com o botão esquerdo do mouse, a tela inicial disposta na figura 14 é apresentada, mostrando uma breve descrição do aplicativo gerador, observações e instruções de como utilizá-lo.

Figura 14 – Tela principal do gerador de QR Code.



Fonte: Autor (2018)

Inicialmente seria desenvolvido um botão com a funcionalidade de copiar a área de transferência do usuário diretamente para a caixa de texto, mas no processo de implementação desta funcionalidade, algumas barreiras para o seu funcionamento foram encontradas. Ao pesquisar brevemente sobre o assunto, foram encontradas advertências feitas pelos navegadores mozilla, e chrome para que não se utilizassem dessas funções, por que isso faria a página poder ser listada como página insegura e que rouba informações dos usuários. Esta funcionalidade de 'monitorar a área de transferência' do usuário poderia ser usada para coletar informações pessoais e por isso os navegadores citados nas versões mais recentes, desativaram o mecanismo que possibilitava o função 'colar' ser chamada pela página, agora ela só pode ser acionada pelo próprio usuário. Por isso a necessidade explícita de que ele aperte as teclas 'control + v'.

Todo o seu desenvolvimento foi feito em php, html e java script, por serem ferramentas livres, gratuitas e que rodam através de browsers (navegadores), facilitando assim o acesso dos setores da instituição interessados em usar este controle de validação de documentos. A instituição já possui servidores com essa tecnologia, desta maneira ela se encontra pronta para entrar em execução sem nenhuma preparação de ambiente exclusivo ou específico. Esta aplicação não utiliza banco de dados e seu controle de acesso poder se integrado a outros sistemas ou mesmo desenvolvido a parte e de forma independente.

Após colar o texto, usando as teclas (control + v) o texto aparece na caixa de texto do aplicativo gerador, conforme figura 15, e então o usuário pode proceder com a geração do QR Code, clicando no botão para tal finalidade e aguardando que ele apareça na tela logo abaixo do botão de geração.

Figura 15 – Tela gerador com texto preenchido.

Gerador de Códigos QR para validação de conteúdo

Copie e cole o texto para gerar o código QR para a validação

Conteúdo

PROGRAMA DE ASSISTÊNCIA ESTUDANTIL
DECLARAÇÃO DE PROFISSIONAL INFORMAL

Nome do estudante: ESTUDANTE DO IFTM
(candidato ao benefício)

Eu, ESTUDANTE DA SILVA, pai do candidato acima mencionado, portador do RG 99999 e do CPF111.222.333.444-55, nos termos do Regulamento do Programa de Assistência Estudantil do Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro, declaro que sou autônomo, exercendo atividade MESTRANDO, perfazendo uma renda mensal bruta, aproximadamente, de R\$ 1000,00 (hum mil reais).

Declaro estar ciente que poderão ser realizadas entrevistas ou visitas domiciliares para dirimir qualquer dúvida pertinente a documentação apresentada e que, persistindo a dúvida, poderão ser exigidos novos documentos comprobatórios que

Gerar Código de validação

*OBS: Somente texto sem formatação. Não é possível validar elementos que não sejam extritamente textuais.

Clique aqui para baixar a [APK](#)

Fonte: Autor (2018)