

**EMPREGO DE CÓDIGO DE BARRAS BIDIMENSIONAIS
PARA CONFERÊNCIA DA AUTENTICIDADE DE
CERTIFICADO DIGITAIS¹**

*EMPLOYING TWO-DIMENSIONAL BAR CODES TO ENSURE
AUTHENTICITY IN DIGITAL CERTIFICATES*

**Caroline F. Vicentini², Francisco T. M. Avelar², João Carlos D. Lima³
e Iara Augustin³**

RESUMO

Abordam-se, neste artigo, ferramentas de código de barras bidimensionais que possibilitam o acesso e a disponibilidade de informações virtuais em ambientes ubíquos pela utilização de telefones celulares. A partir dessa primeira abordagem, faz-se uma contextualização envolvendo o desenvolvimento de um aplicativo para conferência de autenticidade em certificados, por meio da utilização de códigos de barras bidimensionais, a fim de ilustrar sua tecnologia de tradução para conteúdo textual.

Palavras-chave: computação ubíqua, códigos de barras 2D, autenticidade, certificados.

ABSTRACT

This paper presents two-dimensional barcode tools that grant access to virtual informations in ubiquitous environments using cell phones. Hence, a contextualization is made covering the development of an application program to check for authenticity in certificates using two-dimensional barcodes, which is used to illustrate its translation technology for textual content.

Keywords: ubiquitous computation, 2D barcode, authenticity, certifications.

¹ Trabalho de Iniciação Científica - UFSM.

² Acadêmicos do Curso de Ciência da Computação - UFSM. carol@inf.ufsm.br; avelar@inf.ufsm.br

³ Orientadores - UFSM. caio@inf.ufsm.br; august@inf.ufsm.br

INTRODUÇÃO

A informática possibilitou, nos últimos anos, o armazenamento e a consulta de informações de forma bastante rápida e eficiente. Entretanto, o acesso aos dados e o manuseio de computadores nem sempre ocorre de maneira transparente ao usuário, sendo necessário, na maioria das vezes, conhecimento técnico e utilização de computadores pessoais para acessar as informações desejadas.

Segundo a concepção da computação ubíqua de Mark Weiser (1991), a computação deve ser transparente para o usuário, as informações precisam ser facilmente acessadas e estar disponíveis no ambiente, sem a necessidade de interação com computadores para acessá-las. Para obtenção de informações relacionadas a objetos ou a locais, o usuário realiza o mínimo de interações com sistemas, sendo desnecessário saber sobre seu funcionamento ou como as informações vêm até ele.

Uma forma de criar ambientes ubíquos consiste em agregar informações a objetos. A tecnologia de códigos de barras 2D frequentemente é utilizada para esse fim, pois permite a codificação de informações em imagens para que essas insiram-se no ambiente. Depois de adequadamente decodificada, o usuário visualiza a informação referente ao objeto. Dessa forma, a inserção de informações torna-se possível em objetos e locais tornando o acesso às informações mais fácil e instantâneo.

A partir dessa perspectiva, objetiva-se descrever o funcionamento de códigos de barras 2D, relatando as aplicações mais comuns para essa tecnologia atualmente. Como estudo de caso, apresentam-se o desenvolvimento e o funcionamento de um sistema que utiliza códigos de barras 2D para verificar a autenticidade de certificados emitidos.

Sendo assim, as etapas do texto definem-se conforme segue: primeiramente, explica-se a tecnologia de código de barras 2D, seguida de exemplos de aplicação; após, estuda-se o sistema de certificados, seu funcionamento e etapas do desenvolvimento; a outra etapa apresenta os resultados obtidos e, por fim, definem-se as considerações finais, seguidas de trabalhos futuros a serem desenvolvidos em relação ao sistema que o estudo apresenta.

CÓDIGOS DE BARRAS 2D

A partir da criação de códigos de barra e de sua utilização no comércio, possibilitou-se a codificação de informações e sua rápida recuperação. Esse sistema desenvolveu as transações comerciais e facilitou o controle e o cálculo do estoque

dos produtos e dos lucros obtidos. Para a codificação e decodificação de códigos de barras existem vários padrões, alguns destinados a aplicações específicas, outros utilizados para várias finalidades (ISO, 2007). Independentemente do padrão escolhido, o *scanner* que decodifica o código de barras deve configurar o padrão escolhido.

Existem três tipos de códigos de barras: o código de barras linear, que é o mais utilizado para catalogar produtos em mercados; o código de barras *stacked*, para cartões de identificação e o código de barras 2D, similar ao código de barras linear, mas com maior capacidade de armazenar informações (HIGH TECH AID, 2007). Exemplos dos três tipos de códigos de barras podem ser vistos na figura 1.

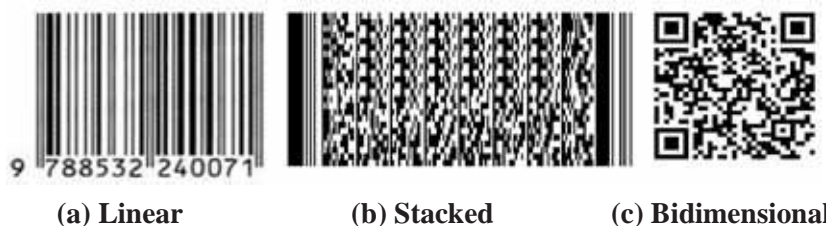


Figura 1 - Exemplos de tipos de barra de código: código de barras linear (a); código de barras stacked (b) e código de barras bidimensional (c).

Os códigos de barra 2D armazenam grande quantidade de dados em uma figura de tamanho pequeno, entretanto sua decodificação torna-se mais custosa em termos de *hardware* e de tempo e, desse modo, mais indicada e utilizada na área de computação. Assim como os códigos de barra lineares, existem diferentes padrões e aplicações para o código de barras 2D, no entanto, ambos possuem a mesma finalidade: codificar informações para serem posteriormente decodificadas e processadas por algum sistema.

Uma área de aplicação para os códigos de barras 2D é a computação ubíqua, como propõe o projeto semapedia.org. Nela, a utilização de barras 2D ocorre da seguinte forma: uma URL codifica-se, gerando uma imagem chamada TAG. A TAG gerada armazena-se em algum objeto ou local no qual se deseja a disponibilização de mais informações. As informações adicionais a respeito do objeto permanecem na página que a URL referencia. Para acessar as informações, utiliza-se um telefone celular com câmera e um *software* decodificador adequado. Depois de fotografar a TAG, o *software* instalado decodifica a URL e permite o acesso das informações na página pelo navegador do telefone celular.

A página gerada (TAG) representa uma espécie de *link* físico às informações, dessa maneira, os dados da página podem alterar-se sem a necessidade de troca da imagem colocada no local ou no objeto. Esse sistema permite que as informações permaneçam atualizadas e que o mundo físico ligue-se ao virtual por meio de *links*, como ocorre no projeto Semapedia (SEMAPEDIA.org., 2007).

Esse projeto tem, atualmente, um conjunto de informações catalogadas pelo mundo (SEMAPEDIA.org., 2007). Usuários de todo o planeta colocam TAGs tanto em pontos turísticos, como Machu Picchu e Torre de Pisa, quanto em mesas de bar. Isso possibilita o acesso das informações sem a necessidade de utilização de computadores pessoais e de saber onde buscar as informações.

Os códigos de barra 2D são também bastante utilizados no Japão e na Coreia do Sul desde 2003. Além de substituírem os códigos de barras tradicionais, usam esses sistemas como cartão de visitas, *links* de *sites*, comandos para telefones celulares, anúncios publicitários e nas embalagens de produtos alimentícios, para que o consumidor tenha mais informação sobre seu valor calórico e seus ingredientes.

APLICAÇÃO DOS CÓDIGOS DE BARRA PARA CONFERÊNCIA DE CERTIFICADOS

Eventos que geram certificados de participação *on-line* necessitam de algum meio para comprovar a validade dos certificados gerados, a fim de dificultar a confecção dos adulterados. Uma forma de fornecer esse serviço consiste na disponibilização de um sistema *on-line* para comprovação da validade.

Esse processo de verificação necessita da utilização de computadores pessoais e da interação do usuário com o sistema, fornecendo a ele alguma chave ou informação como entrada do sistema. Uma alternativa para automatizar a conferência dos certificados é a disponibilização de um sistema que utilize códigos de barras 2D.

Para verificar a validade de um certificado por um sistema que utilize esse código, necessita-se da instalação de um decodificador no telefone celular, da retirada de uma foto da TAG e da verificação de que se os dados retornados constam no certificado avaliado.

Para a construção de um sistema que verifique a validade dos certificados, precisa-se definir uma maneira para analisar as informações referentes aos certificados. Para isso, deve levar-se em conta, que as TAGs de cada certificado são diferentes. Existem duas possíveis abordagens para geração das TAGs e para a verificação do sistema. Uma delas consiste na criação de um endereço estático para

cada certificado, gerando, assim, uma TAG diferente para cada um deles. Dessa forma, cada URL torna-se o identificador cujo conteúdo reúne informações válidas de um certificado em particular. Entretanto, ela apresenta grande complexidade de gerência e manutenção do sistema.

A outra abordagem eficaz vale-se de um sistema on-line que processa informações passadas como parâmetro para validar os certificados. Isso facilita a administração do sistema, pois, em vez de gerenciar diversas páginas, apenas comanda uma base de dados. Entretanto, a URL utilizada para a verificação é igual para todos os certificados, gerando, dessa forma, a mesma TAG. Esse problema resolve-se com a passagem de parâmetros junto com a URL.

Caso as informações referentes ao certificado, evento ou pessoa sejam alteradas na base de dados, o certificado será impresso novamente. Apesar da TAG não se alterar com a mudança dos dados do certificado, as informações nele impressas se diferenciarão das contidas no sistema, criando, assim, dúvidas em relação à sua autenticidade. Existe, portanto, nesse sistema em específico, a necessidade de não haver trocas constantes nos valores referentes aos eventos realizados, mas essa não é uma característica preocupante, pois os dados do evento geralmente não necessitam de alteração.

No desenvolvimento, uma preocupação que se deve considerar é a interface com o usuário, pois, pela limitação do tamanho da tela do dispositivo, a quantidade de informações fornecidas não deve ser demasiada, para não dificultar a visualização e tornar difícil a utilização do sistema.

O cuidado com certificados adulterados consiste em outra questão importante, pois caso a mensagem de confirmação não contenha nenhuma informação sobre os dados do evento ou do participante, pessoas mal intencionadas podem alterar um desses dados e utilizar a mesma TAG de um certificado válido. Dessa forma, o retorno da consulta de verificação informa que o certificado encontra-se na base de dados sem que se perceba a fraude realizada.

Uma alternativa que possibilita essa verificação ocorre por meio de barras de códigos 2D, acontecendo independentemente de dispositivos. A partir da funcionalidade do sistema proposto, iniciou-se o desenvolvimento de um protótipo para realizar a verificação dos certificados por meio de códigos de barras 2D.

CONSTRUÇÃO DO APLICATIVO

Na construção do aplicativo, utilizou-se um servidor *web* para o processamento das requisições, em conjunto com uma base de dados centralizada para a

manutenção das informações dos certificados. O código de barras 2D escolhido foi o SEMACODE. Instalou-se um sistema para gerar e decodificar as TAGs em computadores pessoais, a fim de testar o funcionamento delas e do aplicativo a ser desenvolvido. Aplicou-se, também, um decodificador em um telefone celular com câmera e acesso à *internet* para verificar o comportamento do aplicativo.

A modelagem da base de dados fez-se levando em consideração apenas informações que ajudam na conferência da validade de um certificado: nome da pessoa que participou do evento, nome do evento, se participou como ouvinte ou como palestrante, a carga horária e a data de realização. As informações referiam-se às pessoas, aos eventos e à participação, desse modo, a base de dados gerada ficou com um relacionamento *n-n* entre pessoas e evento, tendo certificados como tabela resultante para armazenar informações referentes à participação. Visualiza-se a modelagem da base de dados na figura 2.



Figura 2 - Modelagem da base de dados.

A base de dados para testes ficou no computador belluno, na pasta “Certificados”, o formato da URL a ser codificada teria a estrutura mostrada na figura 3, na qual o idCertificado consiste no valor do identificador do certificado na base de dados. Assim, cada certificado tem uma TAG diferente, fornecendo ao sistema meios de encontrar o certificado relacionado à TAG e apresentar as informações referentes a eles.



Figura 3 - URL e TAG para acesso à página de validação.

Um *script PHP* (CONVERSE; PARK, 2003) de consulta na base de dados *MySQL* (SUEHRING, 2002) e retorno da informação foi necessário para a realização do processamento. Desse modo, em virtude de o sistema decodificador ficar no telefone celular e de as TAGs serem criadas separadamente ao sistema, qualquer linguagem de programação e sistemas gerenciadores de banco de dados podem ser adotados para a implementação no servidor. Existe somente a necessidade de a linguagem retornar o resultado do processamento da requisição para o navegador do telefone celular.

Projetou-se o comportamento do sistema a partir das recomendações descritas na seção anterior. Entretanto, com a adoção de uma base de dados centralizada com informações referentes aos certificados e com utilização de um servidor *web* para o processamento das requisições de validação, foi possível ter um endereço único, mas com uma URL diferente para cada certificado por meio da passagem de parâmetros pelo método GET. O parâmetro passado como argumento, em cada URL gerada, identifica a tabela participação, pois possibilita a recuperação de todas as informações do certificado, a partir da consulta SQL montada. Se os dados retornados da consulta apresentam-se iguais aos presentes no certificado, então ele é válido, caso contrário, foi adulterado.

RESULTADOS OBTIDOS

Após a implementação do *script* para responder às requisições feitas por telefone celular, geraram-se TAGs a partir do padrão definido com identificadores existentes e não existentes na base de dados. O resultado obtido com o simulador *Java Wireless Toolkit* (SUN, 2007), por meio do exemplo disponibilizado com o código de barras 2D, foi o esperado: caso o certificado não se presentificasse na base de dados, mostrava-se um aviso na tela, caso o identificado fosse válido, os dados referentes ao certificado apareciam, conforme mostra a figura 4.

Testou-se o aplicativo também em um telefone celular com câmera e acesso à *internet*. Para isso, a base de dados e o *script* hospedaram-se em um servidor acessível na *web*. Aplicou-se, ainda, um decodificador de TAGs 2D e os resultados obtidos foram os mesmos do simulador.

O desenvolvimento do aplicativo demonstrou a possibilidade de disponibilizar um sistema de conferência de informações utilizando códigos de barras 2D. O sistema adapta-se facilmente a sistemas de gerenciamento de eventos com emissão de certificados já existentes. A parte mais trabalhosa da integração dos sistemas

fundamenta-se na impressão das TAGs nos certificados gerados, pois um script para geração de TAGs em computadores pessoais deve ser adicionado ao sistema.



Figura 4 - Retorno dos dados no simulador de celular.

CONSIDERAÇÕES FINAIS

Este trabalho relatou o emprego dos códigos de barras utilizados para facilitar o acesso às informações por meio de símbolos, em especial o código de barras 2D, o qual permite a codificação de maior quantidade de informações e também sua utilização em ambientes computacionais ubíquos, a partir do desenvolvimento de um protótipo de sistema de verificação de validade de certificados. A partir dessa amostragem, buscou-se fornecer a verificação dessas validades de certificados emitidos de forma *on-line*, por meio da utilização de telefone celular com câmera e decodificador instalado. Testou-se o aplicativo final da pesquisa com a utilização de simuladores e, posteriormente, com o telefone

celular, obtendo-se, dessa forma, os resultados esperados. Ainda, como trabalho futuro, pretende-se implementar um sistema para geração e impressão das TAGs nos certificados gerados pelo sistema.

REFERÊNCIAS

ISO, **Standards and/or guides of JTC 1/SC 31**. Disponível em: <http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeStandardsListPage.TechnicalCommitteeStandardsList?COMMID=156>. Acesso em: julho de 2007.

HIGH TECH AID, **Bar Code Standards**. Disponível em: http://www.hightechaid.com/standards/bar_code_standards.htm. Acesso em: julho de 2007.

SEMAPEDIA.org. Disponível em: <http://semapedia.org>. Acesso em: julho de 2007.

SEMACODE. Disponível em: <http://semacode.org>. Acesso em: julho de 2007.

CONVERSE, T.; PARK, J. **PHP A Bíblia**; 2. ed., Editora Campus/Elsevier, 2003.

SUEHRING, S. **MySQL – A Bíblia**, Editora Campus/Elsevier, 2002

SUN, **Sun Java Wireless Toolkit for CLDC**. Disponível em: <http://java.sun.com/products/sjwtoolkit/>. Acesso em: julho de 2007.

WEISER, M. **The Computer for the 21st Century** - Scientific American Special Issue on Communications, Computers, and Networks, September, 1991.