Universidade Federal de Pernambuco

Centro de Informática

Implementação do Esquema de Identificação Visual de Naor & Pinkas

Paulo Henrique Padovan

Trabalho de Graduação

Recife

10 de junho de 2009

Universidade Federal de Pernambuco

Centro de Informática

Paulo Henrique Padovan

Implementação do Esquema de Identificação Visual de Naor & Pinkas

Monografia apresentada ao Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do Grau de Bacharel em Ciência da Computação.

Orientador: Ruy José Guerra Barretto de Queiroz

Recife

10 de junho de 2009

PAULO HENRIQUE PADOVAN

Implementação do Esquema de Identificação Visual de Naor & Pinkas

Monografia apresentada ao curso de Ciências da Computação da Universidade Federal de Pernambuco – UFPE – aprovada pela banca examinadora.

_____

Ruy José Guerra Barretto de Queiroz

PhD em Ciências da Computação

Universidade Federal de Pernambuco - UFPE

_____

Sílvio de Barros Melo

Doutor em Ciências da Computação

Universidade Federal de Pernambuco - UFPE

Recife

10 de junho de 2009

A meus pais pelos caminhos que me indicaram e incentivaram.

A minha família pela compreensão nas horas de ausência.

Agradecimentos

A Deus,

ao meu orientador Ruy José Guerra Barreto de Queiroz,

a todos que direta ou indiretamente colaboraram na elaboração deste trabalho.

"Nil sine magno

vita labore dedit mortalibus"

Quintus Horatius Flaccus

Livro I, sátira ix, linha 59

Resumo

Num protocolo de identificação, o usuário deve provar sua identidade ao verificador e, qualquer adversário que tente se passar pelo usuário não deve conseguir, a exceção de uma pequena probabilidade, convencer o verificador de que ele é o usuário.

Naor & Pinkas estabelecem um modelo de Identificação Visual que serve de base para este trabalho. Nele os autores descrevem um protocolo baseado em "resposta a desafio".

Visando a implementação do protocolo proposto, iniciou-se um estudo que analisou questões de acessibilidade, viabilidade, usabilidade além de manter as características de segurança do modelo com o intuito de prover uma melhor implantação do mesmo.

Como resultado, obtivemos não só em uma implementação do referido modelo como à proposição de um novo modelo denominado Naor, Pinkas & Padovan.

O novo modelo consiste na utilização de transparências monocromáticas com dez símbolos diferentes, que são de fácil distinção entre si. Um conjunto de símbolos diferentes pode ser usado, residindo assim à segurança no número de símbolos distintos do conjunto.

Ao eliminar as cores do modelo, não só beneficiamos os daltônicos, bem como barateamos os custos de implantação, visto que, não há mais a necessidade de uma impressora colorida para a impressão das transparências.

Palavras-chave: identificação, identificação visual.

Abstract

In an identification protocol, a user has to prove his identity to a verifier and any adversary trying to pose as the user should not be able, except with small probability, to convince the verifier that he is communicating with the user.

Naor & Pinkas set up a visual identification model that serves as base for this work. That paper describes a challenge-response protocol.

The new model uses monochromatic transparencies with ten different symbols which we assume to be easily discernible from one another. A different set of symbols can be use, and then the security depends on the number of symbols in the set.

Aiming to implement the proposed protocol, we started a study that examined issues of accessibility, feasibility, usability as well as maintain the security features of the model in order to provide a better deployment of the same.

As a result, we obtained not only an implementation of that model as the proposal of a new model called Naor, Pinkas & Padovan.

By eliminating the colors from the model, we benefit not only the color-blinds, as well as cheap costs of adoption, since there is no further need of a color printer for printing of transparencies.

Keywords : identification, visual identification.

Lista de Figuras

Lista de abreviaturas, siglas e símbolos

Abreviaturas

A_r		Arquivo de identificação
e.g.	*exempli gratia*	Por exemplo
H	Harry	O usuário
i.e.	*id est*	Ou seja
P	Peggy	O atacante
S	Sally	O verificador
T_r		Transparência

Siglas

API	Application Programming Interface
BMP	Bitmap
CMYK	Cian, Magenta, Yellow & Black
NP	Modelo de identificação visual de Naor & Pinkas
NPP	Modelo de identificação visual de Naor, Pinkas & Padovan
PME	Pequenas e Medias Empresas.
RGB	Red, Green & Blue
VIC	Visual Identification Card

Símbolos

©	Copyright
ℓ	Número de identificações efetuadas

Sumário

Introdução

Atualmente nos deparamos com sistemas de identificação nos mais diferentes lugares. De estabelecimentos bancários a academias, passando pelo nosso local de trabalho, cada vez mais, estabelecimentos adotam algum sistema de identificação. Implantados nas mais variadas formas e nos mais variados materiais, nos deparamos com sistemas visuais e em papel, e.g. um rol de participantes de um evento e as etiquetas com seus nomes, a sistemas informatizados e biométricos, e.g. leitor de íris ou leitor de digitais.

A função da identificação é mapear uma quantidade conhecida, i.e. identificador ou ID, em uma entidade desconhecida, i.e. aquele que precisa de identificação, de modo a torná-la conhecida. [16]

Num protocolo de identificação, o usuário deve provar sua identidade ao verificador e qualquer adversário que tente se passar pelo usuário não deve conseguir, a exceção de uma pequena probabilidade, convencer o verificador de que ele é o usuário.

Em 1997, Naor & Pinkas estabeleceram um modelo de Identificação Visual, doravante denominado NP, que serve de base para este trabalho. Nele, os autores descrevem um protocolo baseado em "resposta a desafio".

Protocolos de resposta a desafio assumem uma ligação interativa entre o usuário e o verificador. O verificador escolhe um desafio, digamos um item num conjunto com dada propriedade. O usuário encontra a resposta nesse dado conjunto e envia para validação pelo verificador. O verificador então aceita ou rejeita, a depender da resposta recebida. [17]

Visando a implementação do protocolo proposto por [1], propusemos um estudo com o objetivo de analisar questões de acessibilidade, viabilidade, usabilidade, além de manter as características de segurança do modelo. Com o intuito de prover uma melhor implantação do mesmo, propomos a elaboração de um novo modelo denominado Naor, Pinkas & Padovan (NPP).

Para tanto, este trabalho se divide em cinco capítulos. O primeiro constitui a fundamentação teórica que dá suporte aos modelos NP e NPP. O segundo apresenta os métodos de identificação visuais NP e NPP. O terceiro, trata da implementação dos dois modelos para posterior análise. No quarto, são apresentados os testes aplicados, seus resultados e discussão. Por fim, são apresentadas as conclusões e trabalhos futuros.

Capítulo 1

Modelo e Definição de Identificação Visual

1.1 Definição: Cenário de Identificação Visual

Existem três entidades no cenário de identificação visual: H (Harry), P (Peggy) e S (Sally). H é humano e possui capacidade visual humana. P pode tanto ser humano quanto uma máquina e S é o verificador. Para cada protocolo as capacidades requeridas por H devem ser explicitadas.

Existe um parâmetro de segurança n, tal que as capacidades de armazenamento e computação de S e P são polinomiais em n.

Na fase inicial, S produz uma seqüência aleatória r, e cria uma transparência Tr e, eventualmente, alguma informação auxiliar Ar em função de r. Seus tamanhos são polinomiais em n (parâmetro de segurança). S envia Tr e Ar à H através de um meio privado off-line seguro ao qual P não possui acesso (esta é a única vez em que o meio privado é usado). Além disso, S envia para H um conjunto de instruções que devem ser seguidas por H para a execução do protocolo. Essas instruções são públicas e sabidas por P, mas ela não pode mudá-las.

Após a fase de inicialização toda a comunicação entre H e S é feita através de meio controlado por P, que pode adulterar as mensagens enviadas. [1]

Contudo, a meta do protocolo de identificação é diferente. Ele visa permitir que o usuário humano *H* prove sua identidade ao verificador *S* sem a necessidade de consultar nenhum equipamento computacional. O objetivo do adversário *P* é o de convencer o verificador (*S*) que ela (*P*) é o usuário humano.

Não faz sentido construir um protocolo de identificação visual que permita uma única identificação segura uma vez que se obtém o mesmo resultado, munindo o usuário com uma simples senha. Daqui em diante consideraremos apenas protocolos de identificação múltipla, i.e. protocolos nos quais uma mesma transparência é usada para várias autenticações. O protocolo é do tipo resposta a desafio; neste, o verificador envia o desafio ao usuário, que deve respondê-lo baseado em alguma informação secreta que possua.

1.2 Definição: Protocolo de Identificação Visual

Definimos o protocolo para a i-ésima identificação de H para S.

- *S envia um desafio c_i à H, que é uma função do dado secreto r.*
- *Após receber c_i, o usuário humano H computa uma resposta a_i em função de c_i, T_r e A_r, e envia para S.*
- *S decide se a outra parte é H, baseado na mensagem c_i e a_i, e no dado secreto r, Ela então responde ACEITA ou REJEITA.* [1]

A adversária *P* pode tentar se passar por *H*. Nesse caso ela pode tentar indagar *H* fazendo-se passar por *S* e requerer de *H* que ele prove sua identidade. Então ela inicia o protocolo de identificação com *S* e envia uma resposta que espera convencer *S* de que a outra parte é *H*.

1.3 Definição: Protocolo de Identificação Visual ℓ-vezes (1-p)-seguro

Uma identificação visual é ℓ-vezes (1-p)-seguro se as duas condições a seguir forem verdadeiras após a adversária P ter interceptado no máximo ℓ_1 identificações respondidas por H e ter fingido ser o verificador no máximo ℓ_2 identificações com H, sujeita a restrição $\ell_1 + \ell_2 \leq \ell$.

- *S sempre aceita quando H responde de acordo com o protocolo, S aceita com probabilidade 1.*
- *Se um adversário P recebe uma mensagem c_i enviada por S e a responde com uma mensagem b_i que é função de c_i e qualquer uma das ℓ comunicações c_{i1}, b_{i1}, ... , $c_{i\ell}$, $b_{i\ell}$ (onde ℓ_1 delas foram iniciadas por S e ℓ_2 por P) então S aceita com probabilidade no máximo p.* [1]

Capítulo 2

Métodos de Identificação Visual

Os métodos sugeridos para identificação visual não usam o esquema visual de compartilhamento secreto (*2-out-of-2 visual secret sharing*) de [5] ou qualquer outro tipo de esquema visual de compartilhamento secreto, uma vez que não há a necessidade de construir uma imagem vista por *H*. Em vez disso, *H* tem que provar ao verificador *S* que ele sabe alguma propriedade da transparência.

2.1 Método de Identificação Visual de Naor & Pinkas

Este método consiste na utilização de transparências coloridas, dez cores diferentes de fácil distinção entre si. Os autores optaram pelo seguinte conjunto de cores: preto, branco, verde, azul, vermelho, amarelo, roxo, marrom, rosa e laranja. Um conjunto de cores diferentes pode ser usado, residindo assim à segurança no número de cores distintas do conjunto.

2.1.1 Esquema Seguro de Identificação Visual para um Único Verificador

A unidade básica a ser considerada na transparência são quadrados, que em nossa implementação possuem 0,5cm de lado. Na fase de inicialização o usuário *H* recebe uma transparência que é dividida em vários quadrados. Cada um é aleatoriamente colorido com uma das dez cores possíveis. A ordem das cores usadas é mantida em segredo e é sabida apenas por *H* e pelo verificador *S*.

2.1.2 Protocolo de Identificação

Seja *N* o número de quadrados na transparência, e seja *d* o número de quadrados indagados pelo protocolo. O protocolo de identificação segue da seguinte maneira:

1. *S* escolhe *d* quadrados aleatoriamente.
2. Ela envia à *H* uma imagem que é completamente preta a exceção da localização dos *d* quadrados, que são brancos.

3. O usuário H coloca sua transparência sobre a imagem recebida de S e envia para S as cores correspondentes aos quadrados brancos, em uma ordem predefinida.
4. O verificador S aceita apenas se a resposta de H estiver correta para todos os d quadrados.

2.2 Teorema

Uma transparência com N quadrados coloridos com 10 cores pode ser usada por um esquema de identificação visual ℓ-vezes $\left(1-\left(\frac{1}{10}+\frac{9d\ell}{10N}\right)^{d}\right)$-seguro, de tal forma que a cada identificação o usuário deve enviar ao verificador as cores dos d quadrados. [1]

2.2.1 Prova do Teorema

É obvio que H sempre se identifica com sucesso. Considere a situação após ℓ identificações. A melhor estratégia para P é usar essas identificações para perguntar ao usuário ℓ vezes e descobrir a cor de $d\ell$ quadrados. Quando S pergunta ao usuário ela escolhe os quadrados aleatoriamente e então a probabilidade de sucesso de P é $\sum_{i=0}^{d}\binom{d}{i}(d\ell/N)^{i}\,(1-d\ell/N)^{(d-i)}10^{-(d-i)}=\left(\frac{1}{10}+\frac{9d\ell}{10N}\right)^{d}$. A transparência com N quadrados pode, portanto ser usada por $\ell=\frac{N}{9d}$ identificações e a segurança continua maior que $1-5^{-d}$. ■

2.3 Método de Identificação Visual de Naor, Pinkas & Padovan

Este método consiste na utilização de transparências monocromáticas com dez símbolos diferentes que são de fácil distinção entre si. A figura 1 ilustra os símbolos usados na implementação. Um conjunto de símbolos diferentes pode ser usado, residindo assim à segurança no número de símbolos distintos do conjunto.

Figura 1. Símbolos usados na implementação.

Na escolha dos símbolos a serem usados, tomou-se o cuidado de evitar símbolos religiosos (e.g. cruzes, estrelas de Davi, Hilal "lua crescente", Yin e yang ou o Om)[6] no intento de tornar o mais laico e universal a implementação. Também se

evitou o uso de símbolos que remetam a violência, ódio ou tragédias (e.g. como suásticas, bombas, facas, armas). Poder-se-ia usar letras ou algarismos, uma vez que se optou por usar apenas dez símbolos; contudo, devido ao seu número limitado (26 letras e 10 algarismos) e principalmente por questões tipográficas, optou-se pelo uso de símbolos.

No intuito de tornar o modelo mais acessível e favorecer os daltônicos, buscou-se eliminar do modelo a necessidade de distinguir entre cores.

O daltonismo (também chamado de discromatopsia ou discromopsia) é uma perturbação da percepção visual caracterizada pela incapacidade de diferenciar todas ou algumas cores, manifestando-se muitas vezes pela dificuldade em distinguir o verde do vermelho. Esta perturbação tem normalmente origem genética, mas pode também resultar de lesão nos órgãos responsáveis pela visão, ou de lesão de origem neurológica. [2]

Estima-se que entre 5 a 8% da população masculina seja portadora do distúrbio, embora menos de 1 % das mulheres sejam atingidas. [3]

Os códigos de cores geralmente se apresentam como um problema para os daltônicos, uma vez que sua percepção por estes se torna difícil ou impossível, a depender do tipo de daltonismo que eles apresentem.

Faz-se necessário, portanto não só o uso de um código de cor, mas o uso de contrastes de cores e formas para melhor expressar informações; isso não só ajuda os daltônicos, como também melhora a compreensão por parte das pessoas não portadoras da doença.

Outro fator que se deve levar em conta é o material usado. Estudos mostram que uma simples mudança no material usado para se confeccionar um artefato pode levar a uma mudança quanto à percepção de suas cores. [15] Por exemplo, alguns daltônicos conseguem distinguir melhor as cores em materiais sintéticos, como plástico ou acrílico, que em materiais naturais, como papel e madeira. Um daltônico incapaz de distinguir cores num mapa impresso em papel não apresenta a mesma dificuldade quando observa o mesmo mapa numa tela de computador. Esse exemplo nos chama a atenção para o objeto ser ou não um emissor primário de luz.

Outros fatores importantes como a espessura de uma linha, as formas adjacentes a uma figura e suas respectivas cores influem diretamente em sua percepção. Isso não é uma exclusividade dos daltônicos como podemos comprovar nos exemplos abaixo.

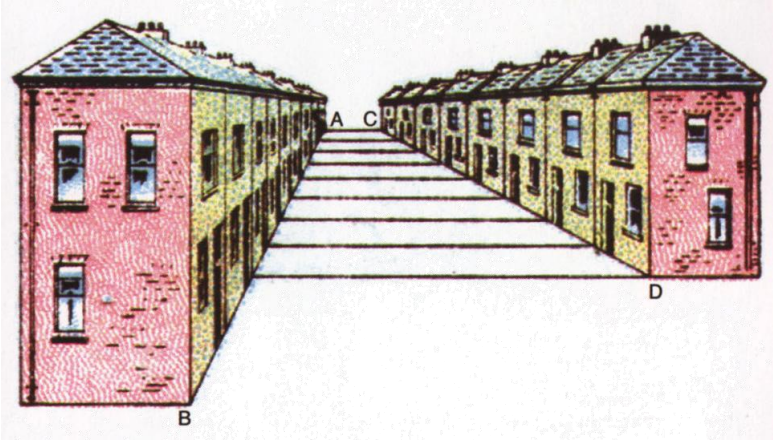

Figura 2. Ilusão de ótica (perspectiva). Os segmentos AB e CD são congruentes. [4]

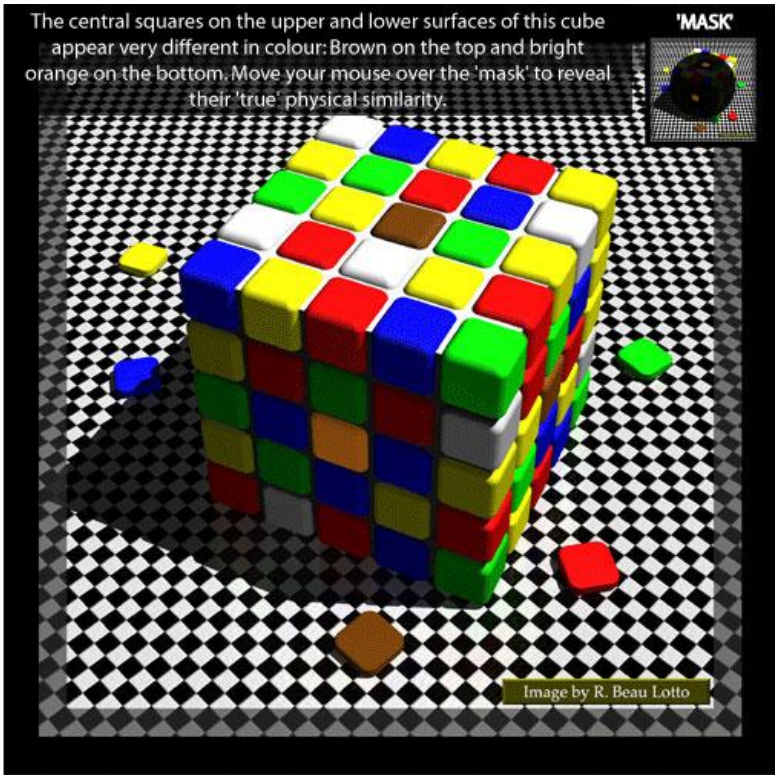

Figura 3. Ilusão de ótica (cores). O quadrado marrom na face superior e o quadrado laranja na face dianteira têm a mesma cor. [7]

Os brasileiros - principalmente usuários finais e a pequena e média empresa (PME) - foram responsáveis pela compra de quase um milhão de impressoras em 2007, totalizando 4,326 milhões de unidades. [11]

Ao eliminar as cores do modelo, não só beneficiamos os daltônicos como universalizamos, englobando usuários de impressoras monocromáticas, e barateamos os custos de adoção, visto que não há mais a necessidade de uma impressora jato de tinta ou laser colorida para a impressão das transparências.

2.3.1 Esquema Seguro de Identificação Visual para um Único Verificador

A unidade básica a ser considerada na transparência são quadrados, que na implementação possuem 0,5cm de lado. Na fase de inicialização, o usuário *H* recebe uma transparência que é dividida em vários quadrados. A cada quadrado é aleatoriamente atribuído um símbolo dos dez possíveis. A ordem dos símbolos usados é mantida em segredo e é sabida apenas por *H* e pelo verificador *S*.

2.3.2 Protocolo de Identificação

Seja *N* o número de quadrados na transparência, e seja *d* o número de quadrados indagados pelo protocolo. O protocolo de identificação segue da seguinte maneira:

1. *S* escolhe *d* quadrados aleatoriamente.
2. *S* envia à *H* uma imagem que é completamente preta a exceção da localização dos *d* quadrados, que são brancos.
3. O usuário *H* coloca sua transparência sobre a imagem recebida de *S* e envia para *S* os símbolos correspondentes aos quadrados brancos, em uma ordem predefinida.
4. O verificador *S* aceita apenas se a resposta de *H* estiver correta para todos os *d* quadrados.

O protocolo é comprovado pelo Teorema vide 2.2 e 2.2.1.

Capítulo 3

Implementação

A implementação descrita a seguir serve mais como prova de conceito e viabilidade que como aplicação comercial. Não foi em momento algum intenção do autor desenvolver tal aplicativo para fins comerciais uma vez que tal desenvolvimento requer um estudo mais detalhado dos cenários de uso, diversidade e qualidade dos agentes envolvidos, ataques externos entre outros. Tal estudo é fundamental para uma implementação comercial. Por exemplo, ataques de *buffer overflow* constituem a maioria dos ataques registrados em programas, simplesmente porque esse tipo de vulnerabilidade é muito freqüente [9] e de fácil exploração. [10]

Este trabalho não provê uma Application Programming Interface (API) ou um conjunto de métodos que possibilitam a inserção de um módulo de identificação visual em aplicações de terceiros.

A implementação consiste em dois aplicativos: um gerador de transparências e um verificador. Esta divisão se dá devido à necessidade de um meio seguro para a transmissão e armazenamento das transparências geradas e da diversidade de plataformas existentes para a implantação do verificador.

Ambos os aplicativos apresentam uma interface simples e intuitiva visando uma maior acessibilidade. Os aplicativos apresentam interface em língua inglesa para abarcarem um público maior de usuários, sendo possível sua tradução para o português.

3.1 Gerador

O gerador é o aplicativo responsável por gerar as transparências (T_r), citadas no cenário de identificação visual (vide 1.1), e armazená-las de forma segura.

3.1.1 Transparências

No intuito de tornar o aplicativo o mais viável e próximo de uma versão comercial, optou-se por construir as transparências, doravante denominadas por

Visual Identification Cards (VIC) como matrizes de 112 quadrados de 0,5 cm de lado organizados em 8 linhas e 14 colunas mais uma tarja orientadora. As figuras abaixo ilustram tal construção.

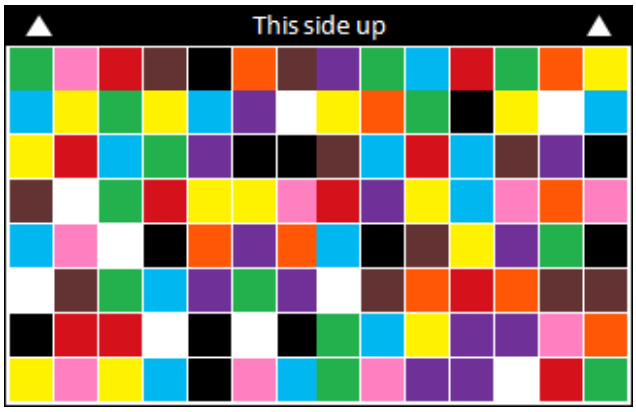

Figura 4. Exemplo de VIC NP em tamanho natural.

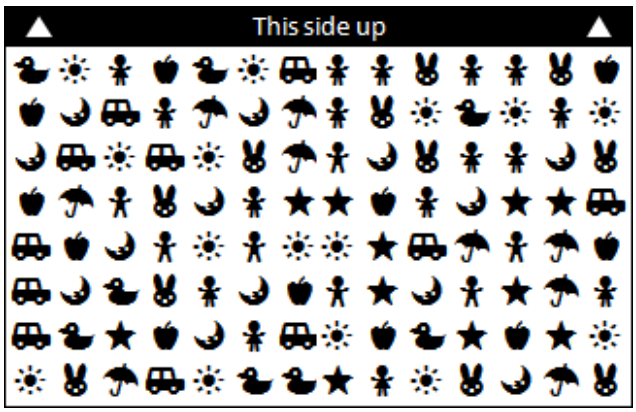

Figura 5. Exemplo de VIC NPP em tamanho natural.

Tal construção nos propicia um VIC de 8,2 cm de comprimento e 5,2 cm de altura, i.e. um pouco menor que um cartão bancário (8,5 x 5,4 cm), o que facilita seu transporte e manuseio. Uma versão um pouco menor (6,8 x 4,3 cm) também foi testada com o intuito de propiciar a implementação dos modelos em dispositivos móveis, e.g. iPhones©[1], handhelds e celulares.

Como decorrência da configuração adotada na implementação, temos pelo teorema 2.2 que a vida útil de uma transparência ℓ, i.e. número de identificações efetuadas, é dada pela seguinte fórmula: $\left(1-\left(\frac{1}{10}+\frac{27\ell}{1120}\right)^3\right)$. A figura 6 ilustra ℓ - o número de identificações efetuadas versus o percentual de segurança do sistema.

[1] Copyright © 2009 Apple Inc. All rights reserved

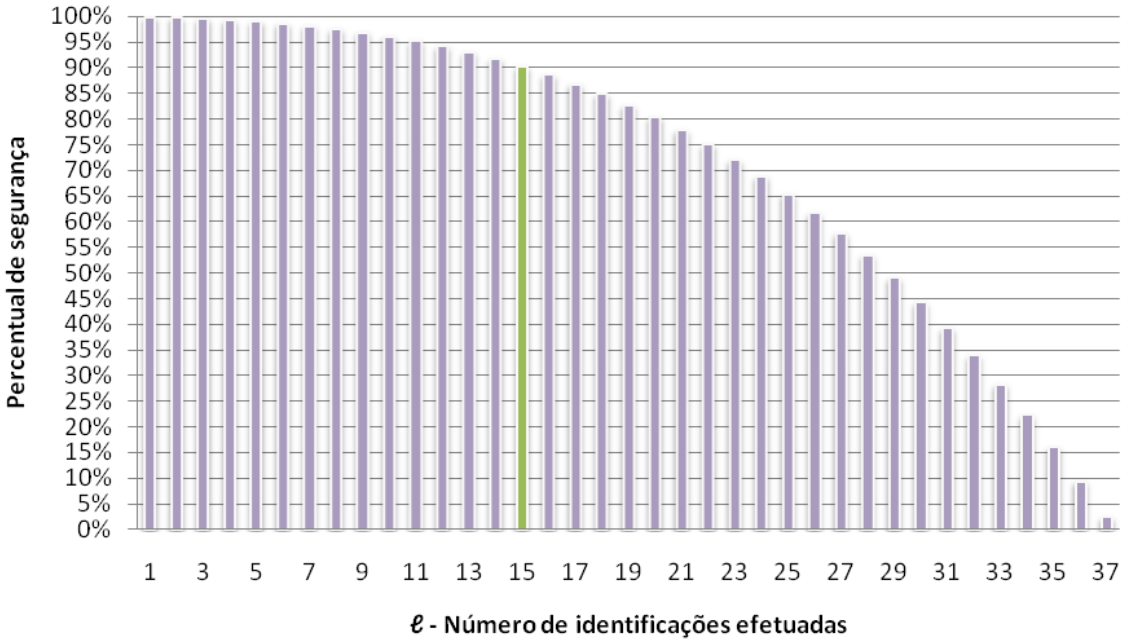

Figura 6. Variação da vida útil do VIC com o uso.

3.1.2 Funcionalidades

Este aplicativo gera os VICs tanto do modelo Naor & Pinkas quanto o proposto, denominado Naor, Pinkas & Padovan no aplicativo. Quando selecionado o modelo, o aplicativo gera então um VIC e as opções *print* e *save* são apresentadas.

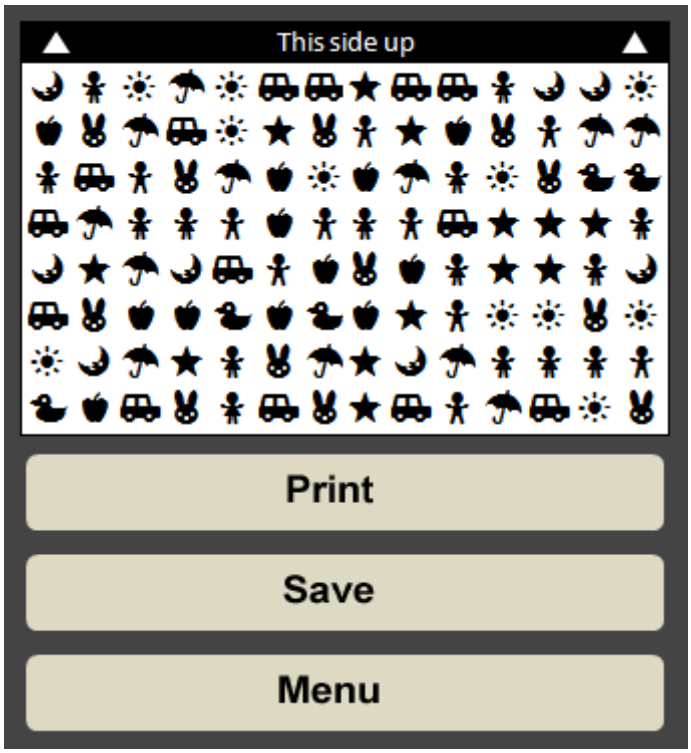

Figura 7. Tela do gerador após geração do VIC NPP.

3.1.2.1 Print

Imprime o VIC gerado e em seguida salva o arquivo de identificação (VIC.id). O arquivo de identificação (A_r), citado no cenário de identificação visual (vide 1.1), contém o código referente ao VIC armazenado. Este arquivo é necessário para podermos identificar qual usuário está associado a qual identidade, e.g. numa implementação web o mesmo estaria armazenado num *cookie*.

3.1.2.2 Save

Salva uma cópia do VIC num arquivo *bitmap* (.BMP) e o arquivo de identificação (A_r). A escolha do formato se dá por ser *lossless* (sem perda) e de fácil manuseio.

3.2 Verificador

O verificador é o aplicativo responsável por efetuar a identificação do usuário por meio do seu VIC. Em sua tela inicial possui duas funcionalidades: Calibrate, serve para calibrar o monitor, e Verify ID, o verificador.

3.2.1 Calibrate

No intuito de tornar o aplicativo mais adaptável, construiu-se um calibrador que permite ao usuário redimensionar o retângulo que contém o desafio. Essa calibração deve ser feita uma única vez, preferencialmente durante a primeira execução. O aplicativo guarda os valores da calibração num arquivo de configuração. Inicialmente o aplicativo vem calibrado para telas de proporções 4:3 e 16:9.

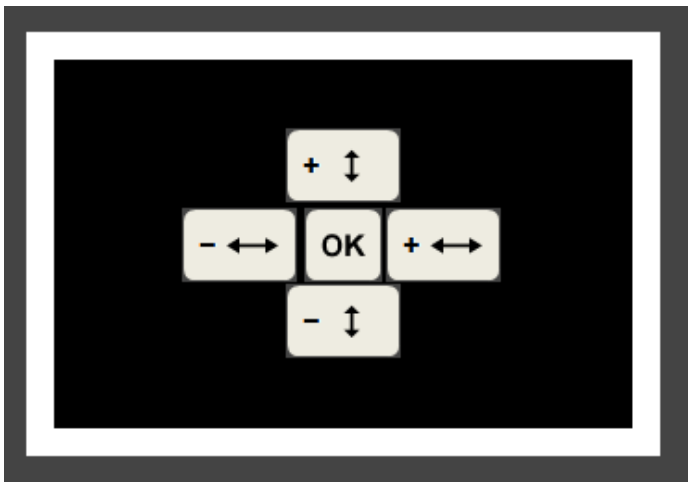

Figura 8. Tela do calibrador.

3.2.2 Verify ID

Esta é a funcionalidade que prove a verificação da identidade. O seu funcionamento se dá da seguinte forma:

1. Logo ao iniciar o programa, *H* é questionado sobre a localização do seu arquivo de identificação (A_r). Esse arquivo é lido e dele é extraído o código do usuário que está tentando se identificar.
2. De posse do A_r o programa então acessa o VIC correspondente, de onde retira as seguintes informações:
    a. Número de identificações já efetuadas;
    b. Modelo do VIC;
    c. Os símbolos ou cores sorteados aleatoriamente.

    Caso o número de identificações exceda 15, o programa exibe a seguinte mensagem de erro: *Your VIC expired. Please get a new and try again*, i.e. Seu VIC expirou. Por gentileza obtenha um novo e tente novamente. Esse número foi escolhido uma vez que dada a implementação após 15 identificações o sistema possui uma segurança menor que 90%.

    Nesse caso um ataque possível seria *S* fraudar o arquivo de identificação (A_r) para conter o código de outro usuário, e.g. *Sally* usar um A_r falso com o código de *Harry*. No entanto, como o número de identificações efetuadas também fica armazenado no verificador, o programa automaticamente detecta o ataque e pede para *H* obter novo VIC.

    Na atual implementação são escolhidas aleatoriamente três quadrados. O sorteio dos quadrados usados no desafio c_i só é realizado após validação do número de identificações do VIC.

3. O desafio c_i é então apresentado à *H* como ilustrado abaixo.

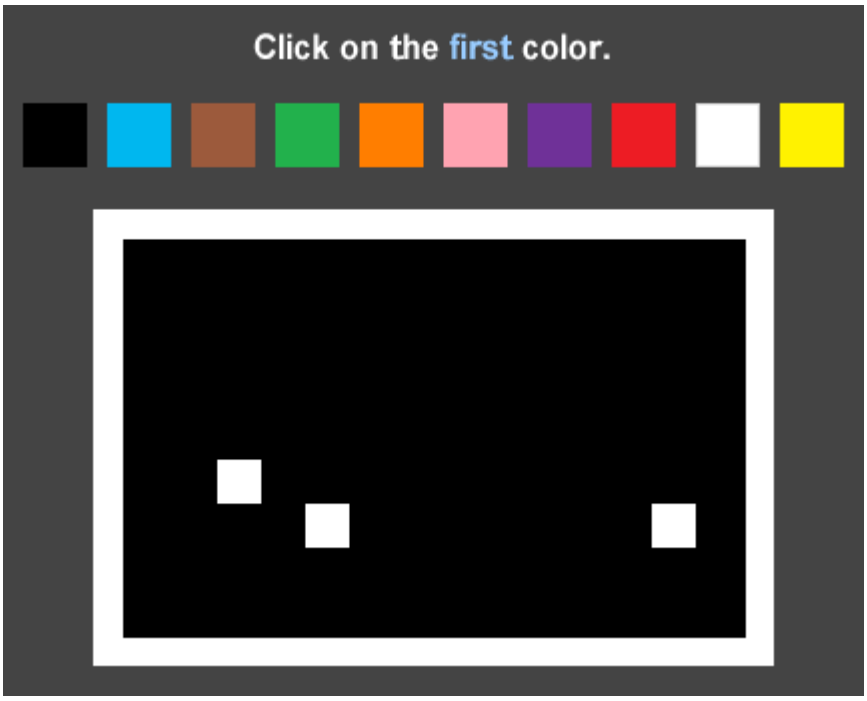

Figura 9. Tela do desafio c_i para o modelo Naor & Pinkas.

4. O usuário H coloca sua transparência sobre a imagem dentro do retângulo delimitador. A adoção do retângulo foi necessária para facilitar o correto posicionamento do VIC sobre a tela.

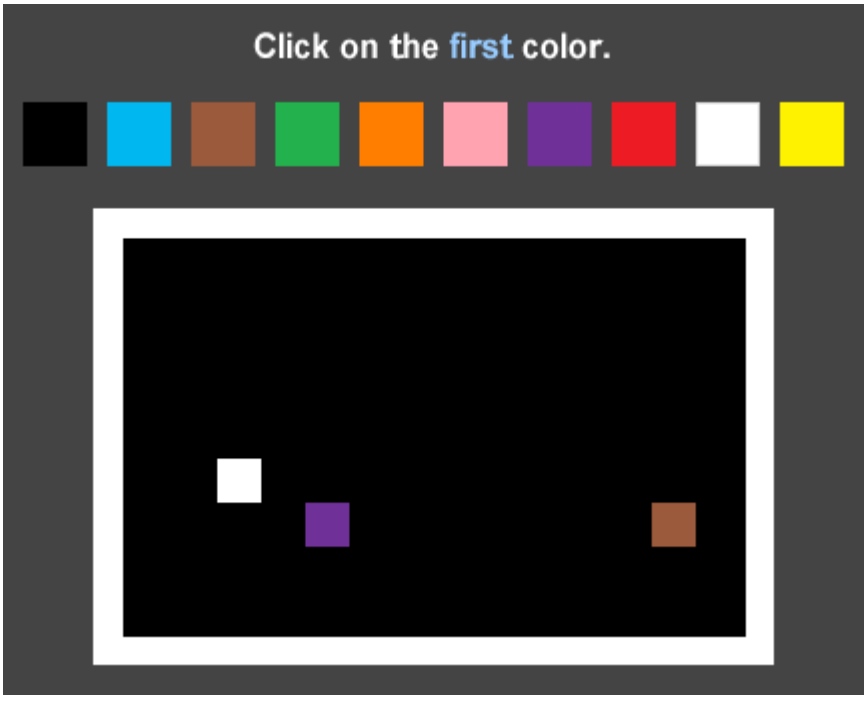

Figura 10. Tela do desafio c_i para o modelo Naor & Pinkas com VIC.

5. *H* deve identificar qual cor apresentada corresponde à cor do primeiro quadrado.
6. A etapa 5 é repetida para os demais quadrados.
7. O verificador *S* aceita apenas se a resposta de *H* estiver correta para todos os três quadrados.
8. Os passos para o modelo Naor, Pinkas & Padovan são análogos.

Capítulo 4

Testes Aplicados

Para tal, foram entrevistadas 10 pessoas, com a distribuição dada na tabela abaixo, as quais foram avaliadas em 3 testes que visaram analisar o desempenho dos modelos (NP e NPP) sob determinados aspectos.

Total de entrevistados							
10							
Sexo							
Masculino				Feminino			
5				5			
Faixa etária							
0 - 20	21 – 40	41 - 60	61 - +	0 - 20	21 - 40	41 - 60	61 - +
1	3	1	0	0	3	1	1

Apesar de uma porcentagem relativamente baixa de daltônicos (10% dos entrevistados), não podemos omitir o fato, principalmente no mundo atual, onde a inclusão social é cada dia maior, fazendo-se necessária e presente em todos os setores da vida.

4.1 Material para Confecção do VIC para Naor & Pinkas

Este experimento durou de 1 a 3 minutos para ser realizado e aferiu qual o melhor material para se confeccionar o VIC do modelo NP.

4.1.1 Procedimento

O experimento consistiu em efetuar uma identificação utilizando dois VICs confeccionados em materiais diferentes, transparência de poliéster e papel branco com gramatura de 75g/m^2.

4.1.2 Requerimentos

Computador com Monitor em resolução de 800 x 600 pixels ou superior, uma transparência de poliéster, uma folha de papel branco com gramatura de 75g/m^2 e uma impressora colorida.

4.1.3 Notas

Ambos os VICs foram impressos na mesma impressora em seus respectivos modos de impressão para não comprometer os resultados do experimento. Também foi usado o mesmo equipamento, tela LCD de 17 polegadas, em todos os testes.

4.1.4 Resultados e Discussão

Os testes apontaram para uma quase unanimidade quanto ao material preferido ser a transparência de poliéster. Apenas um entrevistado disse não fazer diferença.

A maioria dos entrevistados teve certa dificuldade em distinguir as cores: marrom, vermelho, rosa e laranja. Isso, devido ao uso de *gamuts* diferentes na impressão e na tela.

Gamuts de cor são os vários níveis de cores que potencialmente podem ser exibidos por um dispositivo. Existem dois tipos de *gamuts* de cor, aditivo e subtrativo.

Aditivos são aqueles em que as cores são obtidas através da mistura de luzes coloridas para gerar uma cor final. Este é o tipo usado em monitores, televisores e outros dispositivos. Geralmente é denominado de RGB devido ao uso das cores *red*, *green* e *blue*, i.e. vermelho, verde e azul, para a geração das demais cores.

Subtrativos são aqueles em que as cores são obtidas através da mistura de tons que previnem a refração da luz que então produz a cor. Este é o tipo usado por todo tipo de impresso, e.g. fotos, revistas e livros. Geralmente é denominado de CMYK *cyan*, *magenta*, *yellow* e *black*, i.e. ciano, magenta, amarelo e preto, devido as cores usadas. [12]

Tal análise mostra que o problema da discrepância entre as cores exibidas na tela e no VIC reside no fato do *gamut* CMYK ser menor, consistindo apenas de cores que podem ser impressas usando tintas. [13] Quando cores que não podem ser impressas são exibidas na tela, elas são mapeadas em cores próximas, pertencentes ao *gamut* para serem impressas. Nessa transformação ocorrem perdas que na maioria das vezes ocasionam uma diferença de tonalidade. [14]

Vale salientar que vários dos entrevistados retiraram o VIC da tela e usaram uma fonte de luz indireta, luz ambiente, para analisarem a cor questionada a fim de completarem a tarefa.

4.2 Material para Confecção do VIC para Naor, Pinkas & Padovan

Este experimento também durou de 1 a 3 minutos para ser realizado e aferiu qual o melhor material para se confeccionar o VIC do modelo NPP.

4.2.1 Procedimento

O experimento consistiu em efetuar uma identificação utilizando dois VICs confeccionados em materiais diferentes, transparência de poliéster e papel branco com gramatura de 75g/m^2.

4.2.2 Requerimentos

Computador com Monitor em resolução de 800 x 600 pixels ou superior, uma transparência de poliéster, uma folha de papel branco com gramatura de 75g/m^2 e uma impressora.

4.2.3 Notas

Ambos os VICs foram impressos na mesma impressora em seus respectivos modos de impressão para não comprometer os resultados do experimento. Também foi usado o mesmo equipamento, tela LCD de 17 polegadas, em todos os testes.

4.2.4 Resultados e Discussão

Os testes apontaram uma leve predileção pelo VIC confeccionado em transparência de poliéster; contudo, quando indagados sobre o VIC de papel, os entrevistados foram categóricos em afirmar que a legibilidade era quase tão boa quanto à do VIC de poliéster.

Também foi mencionado que o modelo NP quando usado VIC de papel, não possuía a mesma legibilidade que o modelo NPP no mesmo material.

4.3 Teste de Desempenho

Este experimento durou de 3 a 7 minutos para ser realizado e aferiu em qual modelo o usuário se identificava mais facilmente.

4.3.1 Procedimento

O experimento consistiu em efetuar duas identificações, cada uma num modelo, utilizando os respectivos VICs confeccionados em transparência de poliéster. O usuário efetuou as duas identificações e os tempos gastos para a execução de cada identificação foi anotado.

4.3.2 Requerimentos

Computador com Monitor em resolução de 800 x 600 pixels ou superior, uma transparência de poliéster e uma impressora colorida.

4.3.3 Notas

Ambos os VICs foram impressos na mesma impressora em seus respectivos modos de impressão para não comprometer os resultados do experimento. Também foi usado o mesmo equipamento, tela LCD de 17 polegadas, em todos os testes.

4.3.4 Resultados e Discussão

Por ocasião da análise dos resultados, foi constatado que, quando os participantes do experimento foram argüidos sobre cores de fácil distinção, e.g. verde, amarelo, azul e roxo, os tempos para realizar a tarefa no modelo NP, foram próximos dos gastos para realizar a mesma tarefa no modelo NPP. No entanto, quando as cores perguntadas foram - laranja, rosa, marrom e vermelho – o tempo de resposta aumentou significativamente.

Foi constatado também que à medida que o usuário efetuava mais identificações usando os VICs coloridos, ele decorava qual era a correspondência certa entre a cor vista no cartão e as alternativas.

Outro fato que chamou à atenção foi a maior facilidade que as mulheres apresentaram em distinguir e acertar cores conflitantes.

Capítulo 5
Conclusões

A diferença entre os *gamuts* usados pelo sistema foi a principal causa de erro entre não daltônicos. Essa diferença entre os *gamuts* usados para representar as cores na tela e no VIC induz a perdas que levam a uma má interpretação das cores e, conseqüentemente, a resultados errôneos.

Ao eliminar as cores do modelo, não só beneficiamos os portadores de daltonismo, como barateamos os custos de adoção, visto que não há mais a necessidade de uma impressora colorida para obtenção das transparências do modelo NP.

No tocante ao material empregado na confecção dos VICs, observamos que a transparência de poliéster é o melhor material para a confecção dos VICs NP. Para a confecção dos VICs NPP, pode-se lançar mão não só de transparências de poliéster, como de papel, desde que branco ou de cor clara.

Isso nos possibilita cogitar a adoção do modelo em caixas eletrônicos, pelo menos como unidades emissoras de VICs. Uma vez que todos os caixas são equipados com impressora com resolução suficiente para emitir os VICs e o papel usado por eles possui gramatura inferior a $75g/m^2$, o que os torna mais transparentes.

Referente à comparação entre os modelos NP e NPP, constatou-se que, quando os participantes foram argüidos sobre cores de fácil distinção, e.g. verde, amarelo, azul e roxo, os tempos para realizar a tarefa no modelo NP, foram próximos dos gastos para realizar a mesma tarefa no modelo NPP.

No entanto, quando as cores perguntadas foram - laranja, rosa, marrom e vermelho – o tempo de resposta aumentou significativamente. Contudo, pelo exposto acima, quando consideradas a diversidade de impressoras, monitores e condições de iluminação, os resultados tendem a favor do modelo NPP.

5.1 Trabalhos Futuros

Ao realizarmos o presente trabalho, identificamos vários outros pontos que merecem uma abordagem mais aprofundada. Uma vez que nossas observações nos levam a novos questionamentos e novas luzes surgem face ao atual problema.

Entre outros destacamos:

A adequação do problema a portadores de deficiências visuais diversas. Desde baixa visão até cegueira.

Desenvolvimento de uma API ou framework, para desenvolvimento de aplicações seguras baseadas em identificação visual.

Novos materiais para a confecção dos VICs.

Extensão do atual modelo ou proposição de novos métodos de identificação visual.

Referências

[1] M. Naor & B. Pinkas. Visual Authentication and Identification. In *Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology,* LNCS 1294, pp.322–336, 1997.

[2] Wikipedia. Daltonismo [homepage na Internet]. Wikimedia Foundation, Inc.; c2001-2009 [atualizada em 2009 Maio 05; acesso em 2009 Maio 20]. Daltonismo - Wikipédia, a enciclopédia livre; [1 tela]. Disponível em: http://pt.wikipedia.org/wiki/Daltonismo

[3] Sharpe, LT; Stockman A, Jägle H, Nathans J (1999). "Opsin genes, cone photopigments, color vision and color blindness". In Gegenfurtner KR, Sharpe LT. Color Vision: From Genes to Perception. Cambridge University Press.

[4] Seckel, Al. *Incredible Visual Illusions (You won't believe your eyes!)*, Arcturus Publishing, Ltd., pp 63, 2006.

[5] Naor M. and A. Shamir, Visual Cryptography, *Eurocrypt '94*, Springer-Verlag LNCS Vol. 950, Springer-Verlag, 1995, 1-12.

[6] Bowker, John. Para Entender as Religiões, Editora Ática, SP, pp 27, 1997.

[7] R.Beau Lotto. Illusions of Light. [homepage na Internet]. Londres: Lottolab Studio; c2008-2009 [atualizada em 2008; acesso em 2009 Abril 13]. visual demo; [2 telas]. Disponível em: http://www.lottolab.org/articles/illusionsoflight.asp

[9] Michele Crabb. Curmudgeon's Executive Summary. In Michele Crabb, editor, *The SANS Network Security Digest*. SANS, 1997. Contributing Editors: Matt Bishop, Gene Spafford, Steve Bellovin, Gene Schultz, Rob Kolstad, Marcus Ranum, Dorothy Denning, Dan Geer, Peter Neumann, Peter Galvin, David Harley, Jean Chouanard.

[10] "Aleph One". Smashing The Stack For Fun And Profit. *Phrack*, 7(49), November 1996.

[11] Daniela González. PCWorld [homepage na Internet]. São Paulo: IDG Brasil Ltda. [atualizada em 2008 Fevereiro 6; acesso em 2009 Abril 13]. Laser e jato de tinta: mercado de impressoras continua em expansão; [1 tela]. Disponível em: http://pcworld.uol.com.br/reportagens/2008/02/06/laser-e-jato-de-tinta-mercado-de-impressoras-continua-em-expansao/IDGNoticiaPrint_view

[12] Mark Kyrnin. LCD Monitors and Color Gamuts [homepage na Internet]. Nova Yorque: 2009 About.com, a part of The New York Times Company; [atualizada em 2009; acesso em 2009 Abril 13]. LCD Monitors and Color Gamuts; [1 tela]. Disponível em: http://compreviews.about.com/od/monitors/a/LCDColorGamut.htm

[13] Color gamuts (Photoshop). San Jose: Adobe Systems Incorporated; [atualizada em 2002; acesso em 2009 Abril 13]. Adobe Phtoshop Help; [1 tela]. Disponível em: http://www.cellbio.duke.edu/Faculty/Klingensmith/Adobe%20Photoshop%207/Help/1_6_2_0.html

[14] Wikipedia. Gamut [homepage na Internet]. Wikimedia Foundation, Inc.; c2001-2009 [atualizada em 2009 Maio 22; acesso em 2009 Maio 25]. Gamut - Wikipédia, the free encyclopedia; [1 tela]. Disponível em: http://en.wikipedia.org/wiki/Gamut

[15] Brainard, D. H., & Maloney, L. T. (2004). Perception of color and material properties in complex scenes. *Journal of Vision*, 4(9):i, ii-iv, http://journalofvision.org/4/9/i/, doi:10.1167/4.9.i.

[16] Wikipedia. Identification (information) [homepage na Internet]. Wikimedia Foundation, Inc.; c2001-2009 [atualizada em 2009 Maio 10; acesso em 2009 Maio 25]. Identification (information) - Wikipédia, the free encyclopedia; [1 tela]. Disponível em: http://en.wikipedia.org/wiki/Identification_(information)

[17] Wikipedia. Proof-of-work system [homepage na Internet]. Wikimedia Foundation, Inc.; c2001-2009 [atualizada em 2008 Dezembro 20; acesso em 2009 Maio 25]. Proof-of-work system - Wikipédia, the free encyclopedia; [1 tela]. Dis-ponível em: http://en.wikipedia.org/wiki/Proof-of-work_system