Um sistema de autenticação de produtos que emprega a criptografia visual

Cicareli, Rodrigo dos Santos
Departamento de Engenharia Elétrica
Universidade Federal de São Carlos
São Carlos (SP), Brasil
rodrigo.cicareli@gmail.com

Pizolato Junior, José Carlos
Departamento de Engenharia Elétrica
Universidade Federal de São Carlos
São Carlos (SP), Brasil
jcpizolato@yahoo.com.br

***Abstract* - In the commercial sphere, attempts at fraud and counterfeiting have caused several problems for manufacturers and the consumer market. In view of this scenario, in order to promote greater reliability and security in commercial transactions, several techniques are being used to verify the authenticity of physical products. Among them, the most used are QR Codes (Quick Response Code), holographic stamps and RFID (Radio Frequency Identification). In this work, a product authentication system that uses the visual encryption developed by Naor and Shamir is proposed. This system uses two computationally generated masks that when overlapped allow visual authentication without the need for any computational processing by the customer. With visual encryption, this authentication system was proposed by Cicareli in submitted work [18].**

Resumo – No âmbito comercial as tentativas de fraudes e falsificações têm provocado diversos problemas a fabricantes e ao mercado consumidor. Diante deste panorama, a fim de promover maior confiabilidade e segurança nas transações comerciais, diversas técnicas estão sendo empregadas para a verificação da autenticidade de produtos físicos. Dentre elas, as mais utilizadas são: QR Codes (Quick Response Code), selos holográficos e RFID (Radio Frequency Identification). Neste trabalho é proposto um sistema de autenticação de produtos que emprega a criptografia visual desenvolvida por Naor e Shamir. Este sistema utiliza duas máscaras geradas computacionalmente que, quando sobrepostas, permitem a autenticação visual sem a necessidade de qualquer processamento computacional por parte do cliente. Com o uso da criptografia, este sistema de autenticação foi proposto por Cicareli em trabalho submetido [18].

Keywords— Sistemas, segurança, autenticação, máscaras, criptografia visual.

I. INTRODUÇÃO

A intensificação de compra e venda de produtos no mercado mundial, promovido pela globalização, trouxeram alguns infortúnios. Dentre eles está o aumento de fraudes quanto a falsificação de produtos comercializados em estabelecimentos físicos e virtuais.

No Brasil, de acordo com a Associação brasileira de combate à falsificação [1], em 2017 a comercialização de produtos falsificados causou um prejuízo de cerca de 145 bilhões de reais.

Entre os anos de 2016 e 2018 [1], R$395 bilhões deixaram de entrar nos cofres públicos e empresariais, principalmente nos setores de cigarros, autopeças, produtos ópticos e combustíveis. Pelos EUA, a U.S. Customs and Border Protection Office of Trade [2] nos informa que o prejuízo causado em 2018 foi de aproximadamente $1,4 bilhão. Dentre os produtos mais apreendidos, estão os calçados, relógios, equipamentos eletrônicos e roupas.

Diante deste panorama, diversos estudos surgem diariamente com o intuito de combater as falsificações e aumentar a segurança nas transações comerciais de compra e venda de produtos físicos.

A intenção é apresentar com transparência ao cliente informações vinculadas aos produtos, como informações das empresas, procedência, número de série, entre outras coisas. Dentre as técnicas mais aplicadas destacam-se: o código de barras [3], o selos holográficos [4], o QR Code (Quick Responde Code) [5] e o RFID (Radio Frequency Identification) [6].

Por sua facilidade de implementação e conhecimento de todos, o modelo mais difundido, principalmente em mercado é o código de barras. O RFID vem em contramão ao quesito facilidade. É um sistema de difícil implementação e custoso, que fornece ao usuário informações em tempo real do produto, além da localização do mesmo. Sua implantação costuma ser feita em empresas para verificar o trâmite dos deslocamentos das mercadorias. Outro empecilho é a interferência eletromagnética. O QR Code é uma opção diferente de divulgação. Pode ser exposto em qualquer lugar e possui uma codificação rápida e segura. Ele armazena diferentes tipos de informações, e pode ser transmitido em aparelhos que possuem câmeras de baixa qualidade. A principal desvantagem se dá ao quesito segurança. Pode ser utilizado para veicular conteúdo ilegal, como vírus, malware e outros códigos maliciosos, além dos leitores empresariais serem geralmente caros. Outra opção vem dos selos holográficos. Produzidos em larga escala, podem ter seus custos reduzidos e viáveis para muitas aplicações. São geralmente colados ao produto físico e a tentativa de adulteração ou uso incorreto do produto danifica o selo. Seu principal ponto negativo é a necessidade de produção em larga escala para a redução dos custos, impossibilitando a personalização com uma maior agilidade e facilidade.

Diante deste panorama, alguns trabalhos foram propostos para o emprego da criptografia visual de Naor e Shamir [7] na implementação de sistemas de segurança. Em sistemas bancários, algumas sugestões foram propostas. Em [9] foi proposto a utilização da criptografia visual no momento da confirmação da transação bancária e em [10] o mesmo é empregado num sistema para autenticação de assinaturas.

Nestes trabalhos, destaca-se o emprego do processamento visual para a verificação da autenticidade, uma vez que o usuário visualiza as informações sem a necessidade de qualquer processamento computacional. Outro aspecto atrativo da técnica corresponde ao baixo

custo computacional no projeto das máscaras, em que não há a necessidade de algoritmos complexos de processamento. Entretanto, o processo de recuperação visual necessita de um preciso alinhamento das máscaras codificadas para uma visualização nítida e bem definida. Este tema foi abordado em diversos trabalhos. Em [11], para casos onde apenas uma transparência é deslocada, é mostrado que as máscaras não precisam ser perfeitamente alinhadas para uma visualização da imagem original recuperada. Já em [12], foi desenvolvido um sistema de alinhamento automático baseado em transformada de Fourier para imagens digitais.

No mercado de comercialização de produtos de áudio, as fraudes também representam um problema que provoca prejuízos financeiros [13]. Desta forma, este setor do mercado também necessita de sistemas de autenticação que reduzam problemas de falsificação e adulteração de produtos. Diante disto, neste trabalho são apresentados sistemas de autenticação visual já desenvolvido e apresentado por Cicareli e Pizolato [18] e [19]. Neles, são propostos sistemas de autenticação de produtos, no caso foi aplicado para um equipamento específico de áudio em questão, pedal de efeito [14]. O sistema proposto utiliza a técnica de Naor e Shamir [7] juntamente com as peculiaridades da aplicação considerando as necessidades da empresa (neste caso a Trefilio Pedais) e dos seus usuários.

Os sistemas propostos têm como função autenticar o produto (pedal de efeito) através da produção e envio ao cliente juntamente com as máscaras codificadas. A sobreposição delas permitirá a visualização de dados que comprovará a autenticidade do produto vendido. O maior desafio é garantir um perfeito alinhamento das máscaras sobrepostas para que a técnica garanta sua funcionalidade com uma ótima definição. Este problema foi abordado analisando o tamanho dos pixels ao produzir um dispositivo que facilite o alinhamento das máscaras, através do auxílio de uma placa de acrílico.

O trabalho será apresentado na seguinte ordem. Primeiramente serão abordados os conceitos de segurança relacionado a produtos em geral. Em seguida é abordada a técnica de criptografia visual, suas aplicações, vantagens e desvantagens. Na seção seguinte, são abordados os sistemas de autenticação propostos por Cicareli e Pizolato [18] e [19]. Em *análise de desempenho dos sistemas propostos*, são realizados os testes e melhorias do projeto. Na conclusão é apresentado a viabilidade das propostas para a autenticação de produtos segundo os testes de avaliação descritos e a eficiência dos mesmos.

II. SEGURANÇA NA COMERCIALIZAÇÃO DE PRODUTOS

As fraudes no setor de comercialização de produtos podem ser divididas em cinco categorias [17]: falsificação, adulteração, duplicação, violação e simulação. A duplicação é mais comum nos meios digitais. Já a falsificação reproduz exatamente todos os elementos de segurança do produto, chegando até mesmo a passar por verdadeiro aos olhos periciais. A adulteração é a modificação de partes do documento ou produto. Na simulação há a reprodução aproximada do produto com o objetivo de enganar os olhos leigos. E a violação em que há a abertura da embalagem ou invólucro do produto, levando a sua substituição, danos ou subtração de partes do mesmo.

Diante do panorama acima várias técnicas vêm sendo utilizadas para evitar os problemas mencionados. Dentre elas: QR Code, código de barras, selos holográficos e RFID.

Entretanto, nos últimos anos, a técnica de criptografia visual, proposta em [7], vem sendo utilizada na implementação de sistemas de segurança [17]. A principal vantagem desta técnica refere-se à inexistência de processamento computacional na fase de autenticação, sendo que neste caso há um processamento visual da informação. Um inconveniente da técnica é a necessidade de um alinhamento adequado dos componentes de autenticação, neste caso máscaras geradas no projeto do sistema.

Nos trabalhos propostos por Cicareli e Pizolato [18] e [19], foi proposto um sistema de autenticação de produtos utilizando a criptografia visual de [7] para a geração de duas máscaras codificadas que quando sobrepostas recuperam uma informação desejada. O sistema proposto foi utilizado para autenticação de produtos de uma empresa de áudio que fabrica pedais de efeito utilizado em instrumentos musicais. O problema do alinhamento foi analisado e abordado segundo as peculiaridades específicas para a aplicação em questão. A modelagem matemática da técnica de criptografia visual será apresentada em detalhes na seção seguinte.

III. A TÉCNICA DE CRIPTOGRAFIA VISUAL

A técnica de Criptografia Visual proposta por Naor e Shamir [7] tem por objetivo transformar o conjunto de pixels brancos e pretos de uma imagem original em *n* versões modificadas (chamadas de máscaras), uma para cada transparência.

O processo de geração das máscaras está ilustrado na figura 1. O pixel da imagem original é transformado em quatro sub-píxels pretos e brancos. Em cada máscara há um conjunto de *m* sub-pixels, dispostos de tal forma que a visão humana considera apenas a média de suas contribuições via um processamento visual. A estrutura formada é descrita pela matriz *n* x *m* Booleana $S = [S_{ij}]$, onde:

$S_{ij} = 0$ se o sub-pixel *j* na transparência *i* é preto e
$S_{ij} = 1$ se o sub-pixel *j* na transparência *i* é branco

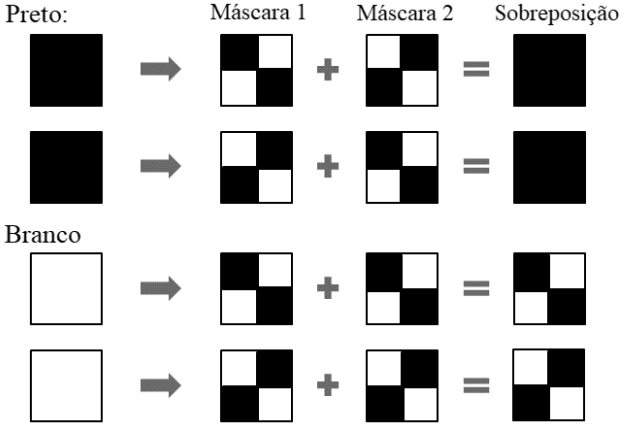


Fig. 1 – Processo exemplo de geração dos sub-pixels e sobreposição. Fonte: [19].

As figuras 2 e 3 mostram a implementação do modelo matemático básico da criptografia visual, onde cada pixel é transformado em um conjunto de quatro sub-pixels pretos e brancos ($m = 4$) rearranjados em matrizes 2x2 ($n = 2$) em suas respectivas máscaras. Cada máscara segundo a técnica, terá seu tamanho dobrado em relação a imagem original. Assim,

M_1 = {todas as matrizes obtidas permutando as colunas de $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$}; (1)

M_2 = {todas as matrizes obtidas permutando as colunas de $\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$}; (2)

As escolhas dos sub-pixels pretos e brancos são feitas de forma randômica pelo software (Matlab). A sobreposição das máscaras 1 e 2, mostradas na figura 2, quando devidamente codificadas, será um conjunto de quatro sub-pixels pretos para o pixel original preto e a de pelo menos um sub-pixel branco para o pixel original branco. A tonalidade do cinza identificada pelo olho humano decorre da quantidade de sub-pixels brancos em relação aos pretos em cada conjunto.

O exemplo de aplicação da técnica para duas máscaras das figuras 2-3, foi aplicado sobre a logomarca da empresa Trefilio Pedais.

A figura 2 mostra as máscaras geradas a partir da imagem original e a figura 3 o resultado da sobreposição delas. As marcações presentes nas laterais e no centro foram inseridas para facilitar o alinhamento.

A técnica de criptografia visual para o modelo de duas máscaras possui um alto grau de confiabilidade conforme [8], já que se o fraudador possuir apenas uma delas, não é possível decifrar a informação desejada.

Um dos desafios na implementação da técnica conforme descrito por Cicareli e Pizolato [18] e [19] foi o alinhamento das máscaras de forma manual com precisão, já que os pixels devem estar precisamente combinados para uma visualização desejada. O grau de dificuldade de alinhamento depende da resolução e definição escolhidas e geradas através da técnica de criptografia visual.

Quanto maior a resolução e definição da imagem a ser recuperada, menor o tamanho dos pixels e consequentemente maior a dificuldade de alinhamento. Desta forma, o desafio é encontrar um ponto ótimo entre resolução da imagem e capacidade de alinhamento. Em testes realizados com resoluções acima de 150x150 pixels se mostraram inviáveis para a realização física e abaixo de 75x75 pixels a qualidade da informação se tornou baixa. Nos trabalhos de Cicareli e Pizolato [18] e [19], a técnica de criptografia será aplicada em propostas para autenticar pedais de efeito da empresa Trefilio Pedais. As necessidades da empresa em questão para realizar o projeto serão apresentadas na seção *os sistemas de autenticação de produtos*.

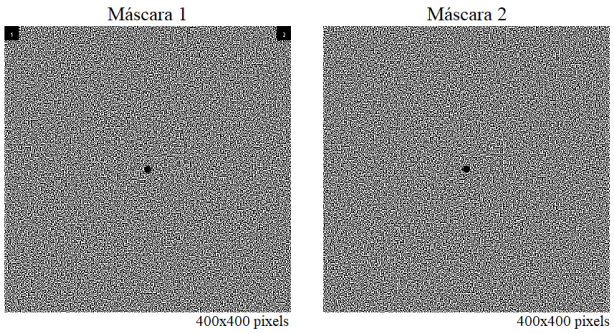


Fig. 2 – Exemplo de máscaras criadas. Fonte: [19]

Fig. 3 – Máscaras 1 e 2 sobrepostas. Fonte: [19]

IV. SISTEMAS DE AUTENTICAÇÃO DE PRODUTOS

De acordo com as necessidades da empresa [18], adotar a criptografia visual para autenticação se torna mais vantajosa em relação aos selos holográficos, um exemplo é mostrado na figura 4. Este modelo é adotado por várias empresas por motivos de custos e facilidade de personalização. Entretanto, tais selos são fabricados em larga escala para redução de custos, sendo uma alternativa inviável quando necessita-se de ajustes para personalização de produtos para produção em baixa escala.

Fig. 4 – Exemplo de um selo holográfico. Fonte: [15]

A técnica de criptografia visual já abordada na seção anterior foi utilizada nas propostas de Cicareli e Pizolato [18] e [19] conforme abaixo.

A imagem exemplo da figura 5 foi escolhida para a realização dos testes de autenticação. Esta imagem possui quatro dígitos e simula a identificação e visualização de um código, que deverá ser recuperado no processo de autenticação.

Fig. 5 – Imagem teste de 75x75 pixels. Fonte: [18]

A imagem teste da figura 5 (resolução de 75x75 pixels), foi utilizada como imagem a ser autenticada da criptografia visual. O algoritmo descrito na seção *A técnica de criptografia visual*, foi implementado no software Matlab para gerar duas máscaras de dimensões (150 x 150 pixels)

Cicareli e Pizolato [18] e [19] propuseram duas diferentes abordagens para o sistema de autenticação de produtos que serão abaixo explicitadas como modelo A e modelo B.

A. Modelo A

O sistema proposto por Cicareli e Pizolato [18] neste caso está ilustrado na figura 6.

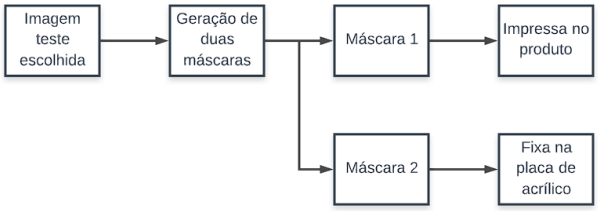


Fig. 6 –Sistema de autenticação A proposto. Fonte: [18]

A máscara 1 da figura 7(a) será impressa na parte interna do invólucro do produto e a máscara 2 da figura 7(b) fixada em uma placa de acrílico e enviada dentro de um envelope juntamente com o produto. Neste envelope estará o endereço eletrônico de contato do fabricante e a informação de como proceder para a verificação da autenticidade do produto.

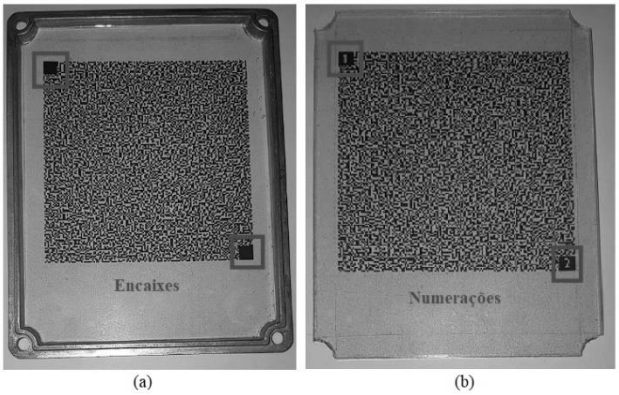


Fig.7 – Máscara 1 instalada no invólucro do pedal Silverado (a) e Máscara 2 fixada em uma placa de acrílico (b). Fonte: [18]

No momento da venda, o cliente é instruído pelo lojista a realizar um cadastro de garantia onde constará um número de série da nota fiscal, assim como os dados do comprador. A partir deste cadastro, um e-mail (ou mensagem digital) é enviada ao cliente contendo as explicações de como proceder com a autenticação. As etapas que serão realizadas pelo comprador são descritas na figura 8.

Fig. 8 – Procedimento de autenticação A. Fonte: [18]

O cliente então após abrir o invólucro metálico do pedal, como mostrado na figura 9(a), encontrará a máscara 1 em sua parte traseira, como mostrado na figura 9(b). Na sequência, a máscara 2 mostrada na figura 10(a), enviada juntamente com o produto num envelope, será sobreposta e alinhada à máscara 1 da figura 9(b). O processo de alinhamento é facilitado pelo encaixe correto e pelas numerações existentes, como observados nas figuras 7(a-b). Após o alinhamento adequado, a informação criptografada pode ser visualizada com nitidez em tons de cinza como mostrado na figura 10(b).

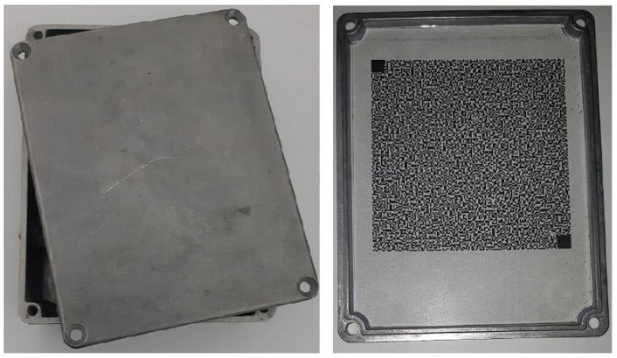


Fig. 9 – Invólucro traseiro metálico do pedal (a) e máscara 1 instalada (b). Fonte: [18]

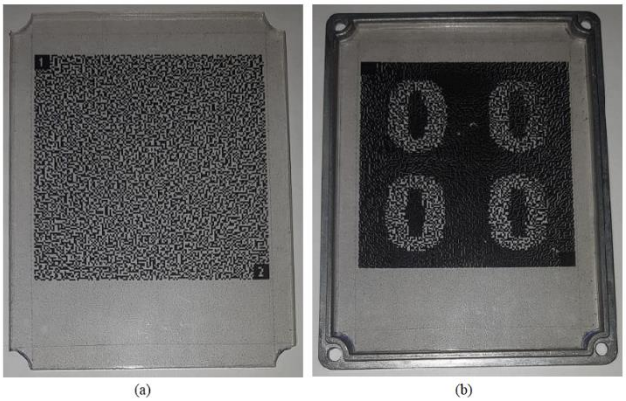


Fig. 10 – Máscara 2 fixa na placa de acrílico (a) e Resultado visual da sobreposição das máscaras 1 e 2. Fonte: [18]

O sistema de autenticação proposto acima poderá resultar nos seguintes casos:

• O código de autenticação foi recuperado com sucesso e comprova a originalidade do produto;

• O código correto do produto em questão não apareceu ou nada foi visualizado. Neste caso, o produto é falso;

• O comprador enviou e-mail perguntando a respeito do dispositivo acrílico encontrado no envelope. Neste caso o cliente não fez o cadastro da garantia (o lojista não informou o cliente por despreparo ou agiu de má fé) e isto será analisado pela fabricante do produto;

• Surgiram dois cadastros com mesmo número de série, portanto um deles será falso. O rastreamento da origem do número de série permitirá um processo de investigação;

• O comprador recebeu o e-mail, mas não encontrou alguma das máscaras ou nenhuma delas junto ao produto. Neste caso a fabricante do produto de posse no número de série da nota fiscal poderá solucionar o problema.

B. Modelo B

Já nesta segunda proposta de Cicareli e Pizolato [19], a máscara 1 é disponibilizada de forma digital através de um link enviado para o cliente ou na aba autenticação do site da empresa. A máscara 2 continua fixada na placa de acrílico e enviada para o cliente da mesma forma que no caso anterior.

A figura 11 ilustra o procedimento de implementação proposto para os produtos segundo as necessidades da empresa Trefilio Pedais.

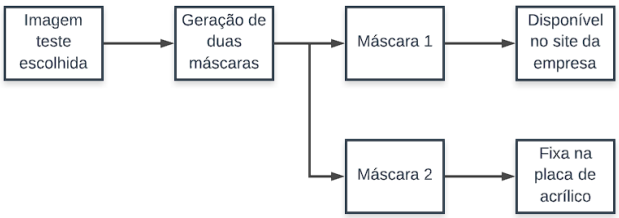


Fig. 11 – Sistema de autenticação B proposto. Fonte: [19]

Assim como no primeiro modelo, o cliente é instruído a realizar o cadastro de garantia e receberá as informações pertinentes via e-mail ou mensagem digital. Os passos necessários estão descritos na figura 12. O cliente irá acessar o link enviado para realizar a autenticação (também poderá ser acessado pelo site da empresa, que no caso é a Trefilio Pedais entrando na aba de autenticação). Neste local, haverá a opção de inserir o número da nota fiscal (figura 13). Após a inserção deste número e o acesso, surgirá uma máscara digital para realizar a sobreposição, como indicado na figura 14. A ideia é pressionar a máscara 2 fixada no acrílico em cima da tela do computador nos pontos de alinhamento indicados, de forma que ocorra a sobreposição das duas máscaras e os quatro dígitos apareçam. A barra presente tem a função de redimensionar a máscara para mantê-la do mesmo tamanho da máscara fixa no acrílico. A figura 15(a-b) mostram como é feito na prática a sobreposição.

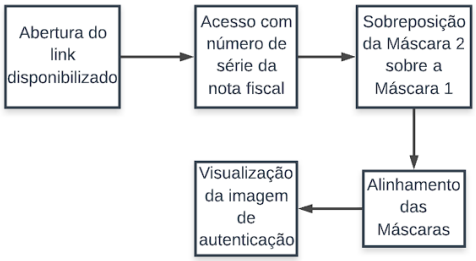


Fig. 12 – Procedimento de autenticação B. Fonte: [19]

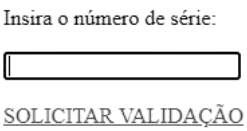


Fig. 13 – Acesso a máscara 1 através do nº de série da nota fiscal. Fonte: [19]

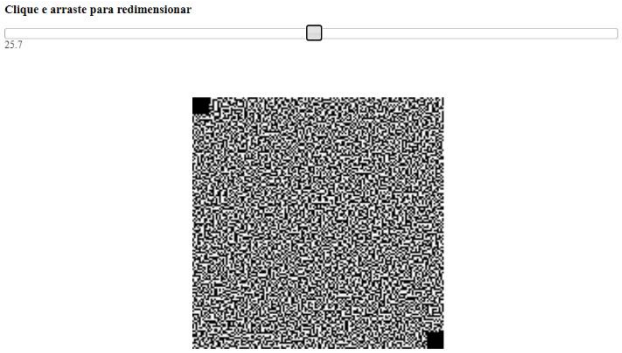
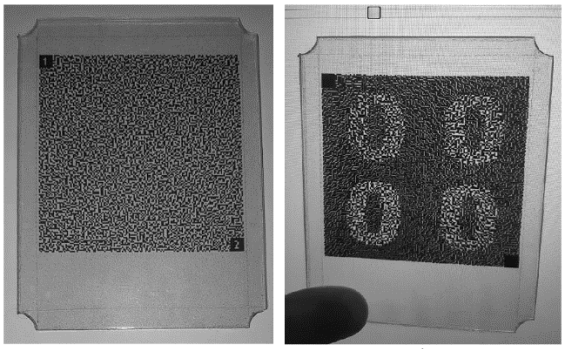


Fig. 14 – Máscara 1 após o acesso. Fonte: [19]



(a) (b)

Fig. 15 – Máscara 2 fixada no acrílico (a) e sobreposição de 2 em 1 na tela de um computador (c). Fonte: [19]

O sistema de autenticação proposto resultará em um dos seguintes casos:

• O código de autenticação foi recuperado e o produto se prova ser original;

• Nada pode ser visualizado. Neste caso o produto é falso ou o cliente não conseguiu alinhas as duas máscaras.

• O comprador entrou em contato para perguntar para que serve acrílico com a máscara. Neste caso, é comprovado que o cliente não fez o cadastro de garantia (o lojista não o instruiu ou agiu de má fé) e isto será analisado pelo fabricante do produto.

• O cliente não recebeu a máscara juntamente com o produto. Neste caso, o fabricante em posse do número da nota fiscal pode resolver o problema.

Em compras diretas com o fornecedor, não há risco de fraudes, e, portanto, as informações de como proceder são enviadas diretamente com o produto.

Deve-se atentar para alguns detalhes na hora da implementação de ambos os modelos. A escolha da dimensão da imagem teste (figura 5) e consequentemente das máscaras criadas foram escolhidas após uma análise de nitidez das informações recuperadas. Neste caso, a dimensão e número dos pixels devem contribuir de forma com que o alinhamento seja preciso e facilitado para a autenticação manual para o comprador. Foi verificado por meio de testes, que as dimensões deveriam estar entre 75 e 150 pixels. Abaixo disso a nitidez fica muito prejudicada e acima disso, o alinhamento manual se torna complicado.

Em seguida, foi necessário descobrir como a sobreposição seria feita. A necessidade de imprimir as

imagens com alta resolução e em transparências impossibilitou o envio das máscaras eletronicamente para o cliente para que este as imprimisse, pois são poucas as pessoas que possuem acesso a uma impressora de alto nível e a folhas de acetato ou fotolito para a impressão. Foi realizado a inversão dos pixels pretos e brancos também, já que isto facilitou a visualização da imagem final em ambientes de menor luminosidade.

O processo de sobreposição entre a máscara e a tela do computador, também se mostrou desafiador. A existência de ar entre a placa de acrílico e a tela do computador gera um efeito de paralaxe [16] impedindo a visualização correta da sobreposição para determinados ângulos de visão. A necessidade do alinhamento preciso também é um obstáculo, e para reduzir este problema, foram colocados pontos de referência nas duas máscaras conforme mostrado na figura 7.

A análise de desempenho dos modelos foi realizada por testes com pessoas e os resultados são descritos na seção *Análise de desempenho dos sistemas propostos*.

V. ANÁLISE DE DESEMPENHO DOS SISTEMAS PROPOSTOS

A otimização do sistema foi feita segundo as necessidades da empresa, no caso a Trefilio Pedais e dos usuários [18]. Os testes de ambos os modelos foram feitos com 50 pessoas que simularam o procedimento das figuras 8 e 12. Os seguintes parâmetros foram avaliados: facilidade de alinhamento, observação visual da informação e viabilidade. Os resultados das pesquisas estão destacados na tabela a seguir.

TABELA I – RESULTADOS DOS TESTES SIMULADOS COM 50 PESSOAS. Fonte: [18]

Proposta	**Modelo A**	**Modelo B**
É facil alinhar?	100%	84%
A imagem visualizada é nítida	100%	100%
O sistema parece efetivo?	100%	94%

Ao fim da pesquisa, foi questionado aos entrevistados sugestões de melhorias para aumentar a viabilidade dos sistemas.

A sugestão mais aparente foi a inserção das instruções via WhatsApp, pois nem todos utilizam com frequência seus e-mails. A segunda sugestão foi aumentar a nitidez da imagem final. Para isto, foram realizados testes e observou-se que a quantidade de pixels pretos em relação aos brancos estava muito baixa. Manter a proporção destes pixels seria adequado tanto para uma melhor visualização quanto para a segurança. Na terceira sugestão os usuários solicitaram que no modelo B, houvesse uma melhoria na facilidade de alteração do tamanho da máscara 1. Para a terceira sugestão, a barra de movimentação que permitia alterar o tamanho da máscara 1 passou a ser controlada também através das setas direcionais do teclado.

Em conjunto com o fabricante do produto, as ideias dos entrevistados foram atendidas. Adotadas todas as sugestões, foi necessário testar a robustez do sistema no critério segurança. Dois critérios foram adotados. A existência de padrões que se repetem ao longo das máscaras e o equilíbrio na distribuição dos pixels.

As figuras 16, 17 e 18 destacam a visualização dos pixels para uma mesma região para as duas máscaras e com elas sobrepostas. Pode-se notar que não há vestígios de padrões bem definidos que permitem a quebra de segurança da proposta.

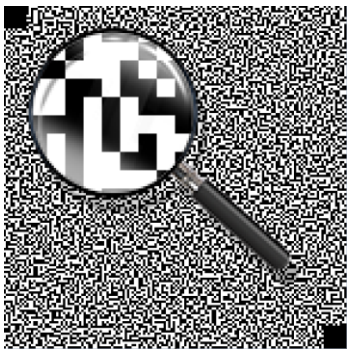


Fig. 16 – Máscara 1 com uma parte ampliada. Fonte: [19]

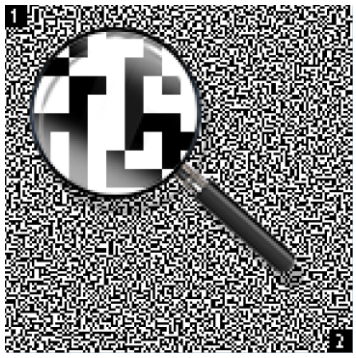


Fig. 17 – Máscara 2 com uma parte ampliada. Fonte: [19]

Fig. 18 – Máscaras 1 e 2 sobrepostas com parte ampliada. Fonte: [19]

Outro critério foi analisar a distribuição dos pixels ao longo de cada máscara. Permitindo uma distribuição uniforme, pode-se evitar a identificação de vestígios da informação a ser autenticada. Pelas tabelas 2 e 3 nota-se que a distribuição de pixels pretos e brancos está praticamente uniforme.

TABELA II – RELAÇÃO DE PIXELS PRETOS E BRANCOS NA MÁSCARA 1. Fonte: [19]

Máscara 1	**Resolução**	150x150 pixels
Pixels totais	22500	
Pixels pretos	11314	50,28%
Pixels brancos	11186	49,72%

TABELA III – RELAÇÃO DE PIXELS PRETOS E BRANCOS NA MÁSCARA 2. Fonte: [19]

Máscara 2	**Resolução**	150x150 pixels
Pixels totais	22500	
Pixels pretos	11307	50,25%
Pixels brancos	11193	49,75%

Através das análises acima pode-se afirmar que os modelos propostos são viáveis para a autenticação de produtos.

VI. CONCLUSÃO

A comercialização de produtos requer um alto nível de segurança para evitar fraudes e proteger as empresas e consumidores.

Neste trabalho, é apresentado duas versões sobre um sistema de autenticação de produtos [18] e [19] para a empresa Trefilio Pedais que empregam a técnica de criptografia visual [7]. A implementação foi feita para o produto pedal de efeito utilizado em instrumentos musicais. A técnica envolve a geração de duas máscaras codificadas, que quando sobrepostas, revelam informações pertinentes da empresa ao cliente para realizar uma autenticação de produto. O processo ocorre de forma visual sem necessitar de processamento computacional.

A maior dificuldade foi o alinhamento preciso entre as máscaras para não interferir na nitidez e, portanto, prejudicar o processo de autenticação. Esta dificuldade foi abordada conforme as necessidades e peculiaridades do produto em questão, como descrito nas seções *Sistemas de autenticação de produtos* e *Análise de desempenho dos sistemas propostos*. Além disso, na seção *Análise de desempenho dos sistemas propostos* uma pesquisa realizada com 50 pessoas revelou uma aprovação de 100% do modelo A e 94% do modelo B. Segundo resultados da pesquisa realizada, melhorias futuras sobre o procedimento de alinhamento do modelo B merecem ser investigadas, já que nem todos os entrevistados sentiram tanta facilidade nesta tarefa.

Ao analisar os sistemas propostos por Cicareli e Pizolato [18] e [19], foi verificado conforme opiniões de usuários e análise de segurança, que ambos os modelos possuem um grau de segurança aceitável para a aplicação em questão.

Em suma, os sistemas de autenticação propostos por Cicareli e Pizolato [18] e [19] demonstram ser viáveis tanto na aplicação quanto na segurança.

REFERÊNCIAS

[1] ABCF. Associação Brasileira de combate à falsificação. [Online]. Disponível: <https://abcf.org.br/abcf-news/>. 2017. [Acesso: 13-Dez-2019].

[2] CBP. U.S. Customs and Border Protection Office of Trade. [Online] Disponível em < https://www.cbp.gov/sites/default/files/assets/documents/2019-Aug/IPR_Annual-Report-FY-2018.pdf>. 2018. [Acesso: 13-Dez-2019].

[3] Bushnell, R. D. and Meyers, R. B., "Getting Started with Bar Codes: A Systematic Guide", 5th ed, 1999).

[4] BJELKHAGEN, H. I., "Holography & Philately: Postage Stamps with Holograms." Hansholo Consulting Ltd, 2017.

[5] B. Tara *et al*., "Digital Wine: How QR Codes facilitate new markets for small wine industries". Springer-Verlag Singapur, 2014.

[6] KARAGIANNAKI, A; PRATAMARI, K., "Leveraging RFID-enabled Traceability for the Food Industry: a Case Study", 2011.

[7] NAOR, M; SHAMIR, A., "Visual cryptography. Advances in Cryptology". EUROCRYPT'94, páginas 1-12. Springer, 1995.

[8] FEIJÓ, E. A., "Proteção dos direitos autorais de imagem estática usando Criptografia Visual e Marca d`Água". Instituto de Matemática e Estatística da Universidade de São Paulo, 2016.

[9] RAJGURU *et al.*, "Securing Online Transaction Using Visual Cryptography". Journal of Telecommunications System & Management, 2018.

[10] SRIKANTH. B. *et al.*, "Secured Bank Authentication using Image Processing and Visual Cryptography". International Journal of Computer Science and Information Technologies, Vol. 5, 2014.

[11] LIU, F. *et al.*, "The alignment problem of visual cryptography schemes". Springer, 2008.

[12] MACHIZAUD, J. *et al.*, "Fourier-based automatic alignment for improved visual cryptography schemes". Optics Express, 2011.

[13] PROSOUND. Prosound Newsletter. [Online]. Disponível: https://www.prosoundnetwork.com/business/busted-counterfeit-pro-audio-gear-seized-in-china. [Acesso: 13-Dez-2019].

[14] JANONES, U. O., "Um novo olhar sobre os pedais de efeito". Universidade Federal de Uberlândia, 2018.

[15] DOTTER. [Online]. Disponível: https://dotter.com.br/selos-holograficos. Acesso: 20-Mai-2020.

[16] ŽIŽEK. S., "The Parallax View". The MIT Press, 2006.

[17] PRIMI. [Online]. Disponível: https://www.primi.com.br/selo-holografico/. [Acesso: 16-Set-2019].

[18] CICARELI, R. S.; PIZOLATO JUNIOR, J. C. "Um sistema alternativo para a verificação da autenticidade de produtos utilizando criptografia visual." Universidade Federal de São Carlos. Semina: Ciências Exatas e Tecnológicas. 2020. No prelo.

[19] CICARELI, R. S.; PIZOLATO JUNIOR, J. C. "Proposta de um sistema de autenticação de produtos de forma virtual e visual." Universidade Federal de São Carlos. Revista Principia. 2020. No prelo.