



CENTRO UNIVERSITÁRIO INSTITUTO DE EDUCAÇÃO SUPERIOR DE BRASÍLIA
BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO

PEDRO ALMEIDA DIAS

APLICAÇÕES PRÁTICAS DE CRIPTOGRAFIA VISUAL EM INTERNET BANKING

Brasília - DF

2020

PEDRO ALMEIDA DIAS

APLICAÇÕES PRÁTICAS DE CRIPTOGRAFIA VISUAL EM INTERNET BANKING

Trabalho de Conclusão de Curso apresentado ao curso
de Engenharia de Computação do Centro Universitário
Instituto de Educação Superior de Brasília – IESB, para
obtenção do título de Bacharel em Engenharia de
Computação; sob orientação do Prof. Dr. Eng. Max
Eduardo Vizcarra Melgar

Brasília - DF

2020

PEDRO ALMEIDA DIAS

APLICAÇÕES PRÁTICAS DE CRIPTOGRAFIA VISUAL EM INTERNET BANKING

Trabalho de Conclusão de Curso apresentado ao curso de Engenharia de Computação do Centro Universitário Instituto de Educação Superior de Brasília – IESB, para obtenção do título de Bacharel em Engenharia de Computação; sob orientação do Prof. Dr. Eng. Max Eduardo Vizcarra Melgar

Brasília, 20 de outubro de 2020.

Banca Examinadora:

Dr. Max Eduardo Vizcarra Melgar - Orientador

Prof. Centro Universitário Instituto de Ensino Superior de Brasília - IESB

MSc. Marcos Cicero Santos Wanderlei - Membro

Prof. Centro Universitário Instituto de Ensino Superior de Brasília - IESB

Prof. Esp. Hernany Silveira Rocha

Prof. Centro Universitário Instituto de Ensino Superior de Brasília - IESB

RESUMO

Criptografia visual é uma técnica que codifica o conteúdo de uma imagem secreta em duas ou mais imagens ininteligíveis, as quais são chamadas de shares. Na definição tradicional, as shares são impressas em transparências e sobrepostas para revelar a imagem secreta original por meio do sistema visual humano.

Neste projeto é proposto um sistema de validação de dados com criptografia visual que requer apenas duas shares para ser decodificada pelo sistema visual de um usuário. A primeira share é uma lâmina impressa no material Acetato transparente (0,5 mm). A impressão utiliza tinta preta para representar pixels pretos e nenhuma tinta para representar pixels claros (transparente). A segunda share é uma imagem digital que é mostrada no visor da tela de um smartphone. Essa é uma técnica de simples implementação, mas considerada segura, pois somente é possível obter a mensagem secreta com a sobreposição das duas shares utilizadas para decodificar a mensagem. A segurança da informação do sistema proposto é incondicional desde que as shares sejam utilizadas uma única vez, comportamento típico do algoritmo One-Time Pad usado como base na geração das shares.

A utilização da criptografia visual está presente em vários campos da segurança da informação, no presente trabalho é utilizada a aplicação desse método como proposta de autenticação de transações eletrônicas. Ao mesmo tempo em que a criptografia visual é simples de implementar e segura, possui alguns problemas na implementação prática. A principal limitação é o alinhamento físico da sobreposição das shares, quanto maior a resolução espacial das shares (tamanho em pixels) o tamanho de cada pixel diminui, aumentando assim a densidade de pixel de cada lâmina. Enquanto maior é a densidade das shares, maior será a dificuldade em conseguir alinhar e sobrepor as shares para decifrar a mensagem secreta. O trabalho proposto tem como objetivo implementar um sistema de criptografia visual e encontrar/utilizar a capacidade máxima de informação cifrada em função da quantidade de pixels por polegada quadrada (densidade de pixel) em diferentes dispositivos. O resultado dos experimentos conseguiu mostrar que é possível decodificar uma mensagem secreta em caracteres em até 38.252,16 pixels por polegada quadrada (densidade de pixel).

Palavras-chave: Criptografia Visual, Java, autenticação, mensagem secreta, share, densidade de pixel..

ABSTRACT

Visual cryptography is a technique used for encoding a secret image in two or more unintelligible images, which are called shares. In the traditional definition, shares are printed on transparencies and overlaid to reveal the original secret image through the human visual system.

This project proposes a data validation system using visual cryptography with only two shares. The shares are decoded by a user's visual system. The first share is a blade printed on transparent Acetate (0,5 mm). The printer uses black ink to represent black pixels and no ink to represent light (transparent) pixels. The second share is a digital image that is shown in a smartphone screen. This is a simple implementation technique, but it is considered safe because it is only possible to obtain the secret message by overlapping the two shares used to decode the message. The information security of the proposed system is unconditional if the shares are used only once, which is a typical behavior of the One-Time Pad algorithm used for shares generation.

Visual cryptography is present in several fields of information security. In this work, this method is proposed for authentication on electronic transactions. While visual encryption is simple to implement and secure, it has some problems in practical implementations. The main limitation is the physical alignment of the shares overlap, the higher the spatial resolution of the shares (size in pixels), the size of each pixel decreases, thus increasing the pixel density of each slide. The greater the density of the shares, the greater the difficulty in being able to align and overlap the shares to decipher the secret message. The proposed work aims to implement a visual cryptography system and find/use the maximum encrypted information capacity in function of the number of pixels per square inch (pixel density) in different devices. The results of the experiments managed to show that it is possible to decode a secret message containing characters at up to 38.252,16 pixels per square inch (pixel density).

Keywords: Visual Cryptography, Java, authentication, secret message, share, pixel density.

LISTA DE ILUSTRAÇÕES

Figura 1. Esquema ataque Man-in-the-Middle	13
Figura 2. Relação alfabeto x Número.....	20
Figura 3. Cifração da mensagem.....	21
Figura 4. Decifração da mensagem.....	21
Figura 5. Representação de pixels em cores.....	22
Figura 6. Qualidade da imagem.....	22
Figura 7. Possíveis escolhas de superpixel.....	24
Figura 8. Exemplo de um esquema tradicional de CV: (a) imagem secreta. (b) Share Secreta. (c) Share de Autenticação. (d) Shares sobrepostas para revelar a imagem secreta.....	24
Figura 9. Padrões de pixels: (a) - 0; (b) - 1; (c) - 2; (d) - 3; (e) - 4; (f) – 5.	29
Figura 10. Complemento: (a) - 0; (b) - 1; (c) - 2; (d) - 3; (e) - 4; (f) – 5.	30
Figura 11. Share 96 x 96: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.....	32
Figura 12. Share 128 x 128: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.....	32
Figura 13. Share 192 x 192: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.....	32
Figura 14. Share 224 x 224: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.....	33
Figura 15. Share 384 x 384: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.....	33
Figura 16. Share 416 x 416: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.....	33
Figura 17. Share 448 x 448: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.....	34
Figura 18. Share 480 x 480: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.....	34
Figura 19. Share 1088 x 1088: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.....	35
Figura 20. Share 1120 x 1120: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.....	36
Figura 21. Share impressa.....	38
Figura 22. Share enviada para o dispositivo.	38
Figura 23. Shares sobrepostas revelando mensagem secreta.	39
Figura 24. Share impressa.	39
Figura 25. Share enviada para o dispositivo.	40
Figura 26. Shares sobrepostas revelando mensagem secreta.	40
Figura 27. Share impressa.	41
Figura 28. Share enviada para o dispositivo.	41
Figura 29. Shares sobrepostas revelando mensagem secreta.	42
Figura 30. Share impressa.	42
Figura 31. Share enviada para o dispositivo.	43
Figura 32. Shares sobrepostas revelando mensagem secreta.	43
Figura 33. Share impressa.	44
Figura 34. Share enviada para o dispositivo.	44
Figura 35. Shares sobrepostas revelando mensagem secreta.	45
Figura 36. Share impressa.	45

Figura 37. Share enviada para o dispositivo.	46
Figura 38. Shares sobrepostas mostrando que não é possível revelar mensagem secreta.	46
Figura 39. Share impressa.	48
Figura 40. Share enviada para o dispositivo.	48
Figura 41. Shares sobrepostas revelando mensagem secreta.	49
Figura 42. Share impressa.	49
Figura 43. Share enviada para o dispositivo.	50
Figura 44. Shares sobrepostas revelando mensagem secreta.	50
Figura 45. Share impressa.	51
Figura 46. Share enviada para o dispositivo.	51
Figura 47. Shares sobrepostas revelando mensagem secreta.	52
Figura 48. Share impressa.	52
Figura 49. Share enviada para o dispositivo.	53
Figura 50. Shares sobrepostas revelando mensagem secreta.	53
Figura 51. Share impressa.	54
Figura 52. Share enviada para o dispositivo.	54
Figura 53. Shares sobrepostas revelando mensagem secreta.	55
Figura 54. Share impressa.	55
Figura 55. Share enviada para o dispositivo.	56
Figura 56. Shares sobrepostas revelando mensagem secreta.	56
Figura 57. Share impressa.	58
Figura 58. Share enviada para o dispositivo.	58
Figura 59. Shares sobrepostas revelando mensagem secreta.	59
Figura 60. Share impressa.	59
Figura 61. Share enviada para o dispositivo.	60
Figura 62. Shares sobrepostas revelando mensagem secreta.	60
Figura 63. Share impressa.	61
Figura 64. Share enviada para o dispositivo.	61
Figura 65. Shares sobrepostas revelando mensagem secreta.	62
Figura 66. Share impressa.	62
Figura 67. Share enviada para o dispositivo.	63
Figura 68. Shares sobrepostas revelando mensagem secreta.	63
Figura 69. Share impressa.	64
Figura 70. Share enviada para o dispositivo.	64
Figura 71. Shares sobrepostas revelando mensagem secreta.	65
Figura 72. Share impressa.	65
Figura 73. Share enviada para o dispositivo.	66
Figura 74. Shares sobrepostas mostrando que não é possível revelar mensagem secreta.	66

LISTA DE TABELAS

Tabela 1. Relação tamanho da Share x Quantidade de caracteres.	27
Tabela 2. Relação entre dispositivo e tamanho da impressão.	28
Tabela 3. Possível visualização x Não possível visualização da informação.	67
Tabela 4. Tamanho da Share x Densidade de Pixel.	68

SUMÁRIO

1	Introdução	11
1.1	Criptografia Visual.....	11
1.2	Desafios Gerais em Segurança da Informação	11
1.3	Ataque Man-in-the-Middle.....	13
1.4	Solução Proposta	13
1.5	Tema	14
1.6	Justificativa	14
1.7	Objetivos.....	14
1.7.1	Objetivo geral	14
1.7.2	Objetivos específicos	15
1.8	Metodologia	15
1.9	Hipótese.....	15
1.10	Prévia da conclusão.....	15
2	Fundamentação Teórica	16
2.1	O Adversário moderno no atual sistema de Internet Banking	16
2.2	Autenticação em dois-fatores e dois-canais.....	17
2.3	Senhas One-Time (OTPs) e número de autenticação de transação (TAN)	18
2.4	Tokens criptográficos	19
2.5	Algoritmo One-Time Pad.....	20
2.6	Densidade de pixels.....	21
2.7	Criptografia Visual.....	23
3	O projeto.....	26
3.1	Uma solução de criptografia visual	26
3.2	Metodologia	26
3.2.1	Descrição das Shares	27
3.2.1.1	Densidade de pixel.....	28
3.3	Algoritmo de Geração de Shares	29
3.3.1	Share Secreta	29
3.3.2	Share de Autenticação	29
4	Resultados	31
4.1	Ipad 6º Geração.....	38
4.2	Iphone SE	48
4.3	Samsung A20	58
4.4	Resultados Finais	67
5	Conclusão	69

Referências	70
-------------------	----

1 INTRODUÇÃO

1.1 Criptografia Visual

A Criptografia Visual (CV) foi proposta por Naor e Shamir (NAOR, 1994) como um paradigma criptográfico de compartilhamento secreto que combina cifras perfeitas e recuperações de informação perceptível. Inicialmente, a imagem secreta é dividida em n imagens, que sozinha, não revela informações sobre o segredo. Cada share é então enviada para o usuário (MELGAR, 2019). O segredo original é recuperado somente se k ou mais dessas shares forem sobrepostas, assim um pequeno grupo de usuários podem descobrir a informação escondida. Desde de que não precise de nenhuma computação – confiando apenas na capacidade de percepção do usuário – o esquema de CV atribui uma simples e intuitiva alternativa para compartilhar um segredo entre duas ou mais partes, na qual é de interesse particular em contextos onde uma informação sensível é oferecida para usuários com nenhum ou pouco conhecimento, ou pouco ou nenhum poder computacional.

1.2 Desafios Gerais em Segurança da Informação

Com a *internet* e *mobile banking* (*e-banking* e *m-banking*, respectivamente) se tornado cada vez mais popular entre os consumidores, seus potenciais como alvo de fraudes tem também crescido. Nos últimos anos, ataques a aplicações de *e-banking* tem se tornado ameaças mais complexas e graves, habilitadas com softwares maliciosos (*malware*), que explora não somente brechas nas implementações do *e-banking*, mas também na falta de informação do usuário. Uma vez que o atacante consegue obter uma instância de malware em execução no dispositivo da vítima, garantir algum nível de segurança se torna uma difícil tarefa: o criminoso se torna capaz de observar informações que entram e que saem do dispositivo infectado; consegue gravar entrada de dados (através do teclado, mouse ou qualquer outro dispositivo de entrada) e enviá-lo para um servidor remoto; tirar fotos da tela em tempo real.

De fato, atualmente os malwares permitem que o dispositivo infectado seja controlado a tal ponto que permita ao adversário o poder indetectável representando o usuário a qualquer parte disposta a se comunicar com ele (um servidor de banco,

por exemplo) e vice-versa, assim permite manipular as transações do usuários até quando muitas camadas de autenticação são implementadas pelo sistema. Esse tipo de ataque – conhecido como Man-in-the-Middle (MitM) – tem sido tanto perigoso como factível nos últimos anos, e continua sendo o foco das atuais pesquisas (ZHAN, 2010).

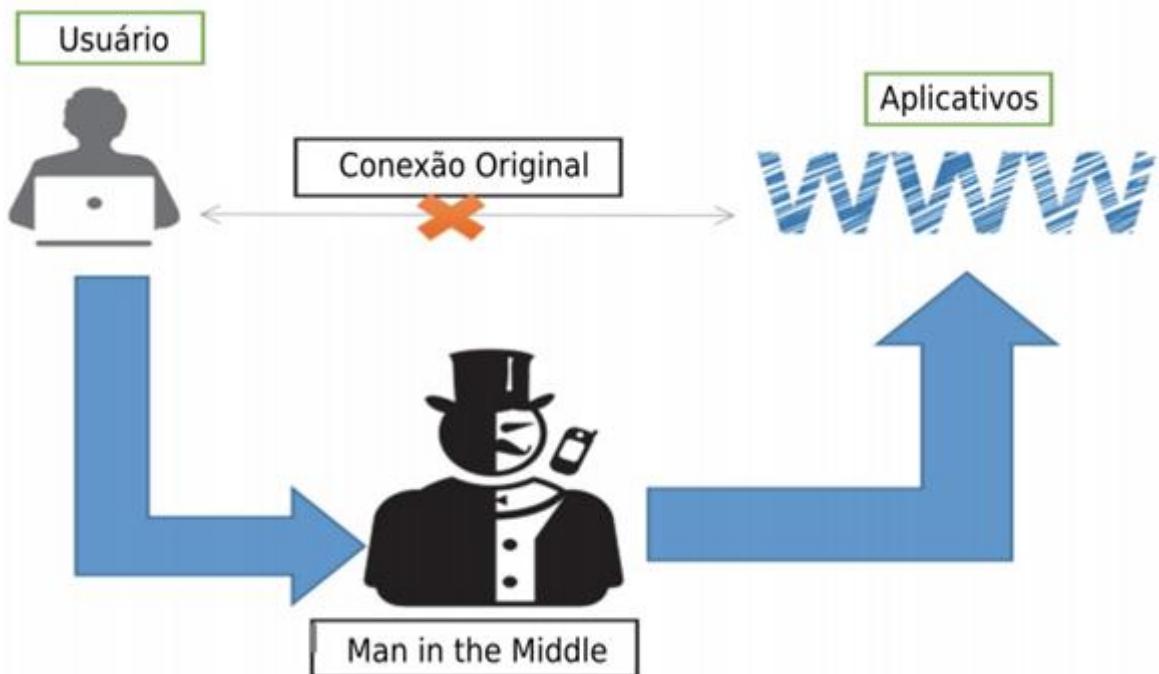
Até onde sabemos, nenhuma abordagem atualmente disponível é capaz de efetivamente enfraquecer os ataques do MitM em mecanismos de autenticação. A abordagem mais bem-sucedida para tentar inibir esses ataques é o uso da autenticação em multi-fator ou multicanal. Os primeiros dependem de dispositivos/canais de comunicação secundários para estender o protocolo de autenticação para o terminal exterior hipoteticamente corrompido – portanto adicionando uma camada extra de segurança no sistema de autenticação. O último, fortalece a precisão do processo de autenticação, usando pelo menos dois ou três fatores de autenticação como obstáculos para o adversário: senha de autenticação, por exemplo, depende do primeiro fator - “algo que o usuário sabe”; código de confirmação via SMS com intenção de verificar a identidade do usuário de acordo com o segundo fator - “algo que o usuário tem” -; e finalmente, autenticação via sistema de biometria são baseados em “algo que o usuário é”.

Os aplicativos de e-banking mais atuais contam, em sua maioria, com autenticação baseada em usuário/senha para estabelecer conexão segura entre o Usuário e o Banco. Como as senhas podem ser facilmente roubadas num cenário real, protocolo de autenticação de dois-fatores/dois-canais tornaram-se prática comum (YOU, 2010). Tais abordagens geralmente dependem de alguma forma de solicitação de login/senha como a etapa de autenticação inicial e, sempre que uma transação confidencial for solicitada pelo usuário, uma segunda etapa de autenticação – não apenas para uma verificação dupla da identidade do usuário – mas também para garantir que os parâmetros inseridos para transação (número da conta de destino, quantidade, valor etc.) não foram adulterados por nenhuma parte maliciosa antes de chegar ao Banco – ocorre. Essa segunda etapa, geralmente chamada de autenticação da transação (em oposição à autenticação do usuário), tornou-se recentemente um requisito sólido para soluções práticas em e-banking projetadas para serem robustas contra ataques do MitM e foram reconhecidos como um aspecto crucial para o futuro da segurança do e-banking.

1.3 Ataque Man-in-the-Middle

Quando se fala em criptografia e segurança dos computadores, o ataque Man-in-the-Middle (MitM) (MALLIK, 2019) é um ataque onde o atacante intercepta dados transmitidos entre duas partes que estão se comunicando. Esse modo de ataque é muitas vezes imperceptível para ambas as partes, no qual o atacante tem o objetivo de obter informações individuais, por exemplo, senhas, informações de login. Normalmente esses ataques visam clientes que utilizam e-banking. Informações obtidas de um ataque pode ser utilizado de diversas maneiras, como fraudes, enviar e receber dados, enviar dados que não tenham sido enviados pelo remetente original, suprimindo dados que deveriam chegar ao destinatário final. Figura 1 demonstra um esquema de como funciona o ataque MitM.

Figura 1. Esquema ataque Man-in-the-Middle.



Fonte: MALLIK, 2019.

1.4 Solução Proposta

A solução proposta nesse trabalho consiste na implementação de autenticação em multifatorial baseada em Criptografia Visual e ilustrada para transações em e-commerce e e-banking. Isso é novidade nos seguintes aspectos; 1) não se baseia em nenhuma suposição relativa a dispositivos descomprometidos; 2)

satisfaz ambas partes e requerimentos de autenticação nas transações sem guardar nenhuma credencial no dispositivo do usuário; 3) tem bom custo-benefício em relação soluções atuais; 4) foi projetado para ser robusto mesmo em cenário realista onde o dispositivo do usuário foi infectado por um malware; 5) protege eficientemente as transações de e-banking dos usuários contra ataques malware ataques (MitM e roubo de credenciais, por exemplo) e certos tipos de ataques de engenharia social (phishing, por exemplo). A Criptografia Visual aparece como uma alternativa a combater esse e outros tipos de ataques. Como esse método não utiliza nenhum meio computacional para a decodificação da mensagem secreta, esse tipo de ataque se torna ineficaz.

1.5 Tema

Este trabalho consiste na elaboração de um protótipo de um sistema de autenticação por via do uso da criptografia visual em celulares e lâminas impressas com a finalidade de estudar a maior densidade de pixels que pode ser utilizada em uma correta decodificação do sistema visual humano. O protótipo poderá ser utilizado como aplicação prática em diversos campos de segurança da informação, como Internet Banking e e-commerce.

1.6 Justificativa

O sistema proposto deverá permitir a autenticação segura utilizando como primitiva o princípio de segurança inquebrável da criptografia visual e uma grande quantidade de informação secreta alcançada através da utilização de shares com alta densidade de pixels.

1.7 Objetivos

1.7.1 Objetivo geral

Propor um criptossistema com base na criptografia visual e explorar os diversos casos de uso em função de tamanho de imagens, materiais utilizados e quantidade de camadas físicas compartilhadas. O sistema proposto permite a

autenticação segura utilizando como primitiva o princípio de segurança inquebrável da criptografia visual.

1.7.2 Objetivos específicos

Os objetivos específicos incluem:

- a) Criar algoritmo da Share Secreta;
- b) Criar algoritmo da Share de Autenticação;
- c) Imprimir a Share Secreta para que possa ser revelado o segredo após a sobreposição na tela do smartphone da Share de Autenticação.
- d) Obter a maior densidade de pixel utilizável para poder executar a autenticação visual com uma alta quantidade de caracteres cifrados.

1.8 Metodologia

Implementação de um algoritmo capaz de retornar duas imagens em pixels preto e branco, que sozinhas não são capazes de visualizar nenhum tipo de informação, mas quando sobrepostas a informação é revelada.

1.9 Hipótese

Essa proposta permite que a autenticação entre as duas partes seja feita de forma totalmente segura.

1.10 Prévia da conclusão

O algoritmo desenvolvido se tornou eficiente para a proposta do projeto, fazendo com que a sobreposição da share impressa com a share enviada para o smartphone seja revelado a mensagem secreta, determinando o tamanho máximo da share, a quantidade de caracteres codificados e a densidade de pixel para cada dispositivo analisado. A densidade máxima de pixels atingida para uma correta decodificação foi de 38.252,16 (pixels por polegada quadrada) no dispositivo Iphone SE.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 O Adversário moderno no atual sistema de Internet Banking

No modelo adversário clássico de Dolev-Yao (DOLEV, 1983), supõe-se que o adversário controle o canal de comunicação estabelecido entre as duas partes – podendo assim passivamente ou ativamente atacar as mensagens reenviadas, mas incapaz de comprometer o canal final. No entanto, o recente design de malware, adicionado ao não entendimento dos usuários sobre as atuais ameaças virtuais, capacita ainda mais o adversário moderno a ter o controle; isso significa que, no cenário atual, não apenas o canal de comunicação, mas também a computação embarcada nos dispositivos, pode ser monitorada e adulteradas por terceiras partes maliciosas.

Uma vez que uma instância de malware é instalada nos dispositivos da vítima, operações não autorizadas podem ser executadas remotamente e silenciosamente pelo invasor de várias formas de ataques contra aplicativos e-banking. Três classes de ataques serão apresentadas seguir: ataques de roubos de credenciais, ataques de quebra de canal e ataques de manipulação de conteúdo (OPPLIGER, 2009).

- Ataques de roubo de credencial referem-se a tentativas que o adversário possa realizar para obter as credenciais do usuário – extraíndo-as do dispositivo infectado, ou enganando os usuários para revelá-los de técnicas de phishing. Esse tipo de ataque visa obter as informações necessárias para representar com êxito o usuário em transações futuras, também são referidos como ataques off-line.
- Ataques contra quebra de canal, por outro lado, têm como objetivo quebrar o canal de comunicação hipoteticamente seguro estabelecido entre os pares. Tais ataques incluem o conhecido MitM, no qual o adversário atua como um proxy transparente entre o usuário e o banco, mantendo duas sessões simultâneas de autenticação (uma com Usuário, fingindo ser o Bank; e outra com o banco, fingindo ser o usuário). Para conseguir isso, o adversário pode tentar convencer o usuário a aceitar um certificado de e-banking inválido, ou até mesmo não usar nenhum certificado – os usuários geralmente não verificam os certificados antes de aceitar conexões autenticadas. Em oposição

ao ataque de roubo de credencial, esses ataques são realizados em tempo real, caracterizando-os como ataques online.

- Os ataques de manipulação de conteúdo podem efetivamente minar as mais conhecidas técnicas de autenticação de transações, enganando o usuário para fornecer ao banco confirmação de transações falsas e adulteradas pelo adversário. Tais ataques incluem, por exemplo, a capacidade de substituir os parâmetros originais da transação (por exemplo o número da conta bancária do usuário pode ser substituída pelo número da conta do adversário) e a capacidade de substituir o conteúdo de confirmação originado pelo banco, destinado a ser exibido ao usuário por meio da exibição do dispositivo infectado.

Pode-se notar que essas três classes de ataque não são de forma exclusiva e podem (como geralmente são) combinados pelo adversário para derrotar com sucesso a segurança e-banking. Na próxima seção, procederemos com a análise de alguns das mais comuns soluções, e discutir suas principais vantagens e desvantagens em relação às modernas capacidades adversárias que foram descrita acima.

2.2 Autenticação em dois-fatores e dois-canais

As soluções para autenticação baseada no modelo clássico de adversário geralmente dependem de protocolos de autenticação (como SSL/TLS) para estabelecer um canal seguro entre os pares para comunicação adicional de dados confidenciais da transação. Tais abordagens incluem frequentemente apenas um fator de autenticação (uma senha definida, por exemplo) e não são eficazes contra um adversário com recursos descritos anteriormente, observando uma única sessão em um protocolo de autenticação de um fator, um adversário com capacidade de roubo de credenciais pode obter facilmente as credencias do usuário, e se passar por ele em sessões futuras (HILTGEN, 2006). Além disso, um adversário com recursos de quebra de canal e manipulação de conteúdo é capaz de adulterar os parâmetros de uma transação iniciada pelo usuário, a fim de enganar o banco para enviar, por exemplo, uma quantia diferente de dinheiro para uma conta bancária de destino diferente. Por essa razão, autenticações de e-banking requerem protocolos de autenticação de dois fatores. A ideia principal de tais métodos é exigir uma inicial,

geralmente baseada em senha, no início da sessão e uma rodada de autenticação de usuários mais forte e robusta sempre que uma transação confidencial for solicitada na sessão estabelecida (transferência de dinheiro, por exemplo), em alguma abordagens, a segunda rodada de autenticação pode incluir etapas de autenticação de transação – uma tentativa do banco para garantir que os parâmetros de transação recebidos não foi adulterado por um adversário com capacidade de manipulação do conteúdo.

Observou-se que, embora a autenticação de dois fatores possa aumentar a robustez contra várias ameaças modernas, não pode ser muito mais eficaz do que autenticação de um fator se a segunda rodada estiver possivelmente comprometida. Por esse motivo, a autenticação de dois fatores torna-se amplamente adotadas no mercado financeiro. Tais abordagens, dependem da necessidade de um segundo dispositivo externo, geralmente off-line e/ou resistentes a violações no protocolo de autenticação, porque esses dispositivos secundários são independentes dos dispositivos primários, a segurança é aprimorada (OPPLIGER, 2009; ZHAN, 2010).

2.3 Senhas One-Time (OTPs) e número de autenticação de transação (TAN)

Uma abordagem bem conhecida para fornecer autenticação de dois fatores ao usuário é o uso de senhas One-time (OTP). Tais protocolos dependem de números de autenticação gerados aleatoriamente usados apenas uma vez, em um esquema baseado em desafio-resposta. Esses números podem ser gerados no momento da transação por dispositivos sincronizados ou fornecidos previamente como uma tabela de números em papel ou cartão (YOU, 2010). Como qualquer OTP é suposto ser usado apenas uma vez pelo usuário, gravá-lo para uso futuro seria de pouca ajuda para o adversário.

No entanto, mesmo que os OTPs possam, no caso de a senha de longo prazo ser roubada, dificultam a execução de futuras transações iniciadas pelo adversário, eles não conseguem fornecer autenticação na transação. Especificamente, sabe-se que apenas os métodos baseados em OTP são ineficazes contra-ataque MitM, pois o usuário pode ser levado a autenticar uma transação que foi adulterada por um adversário em tempo de execução (OPPLIGER, 2009), em outras palavras, os OTPs atenuam de modo significante os ataques off-line, mas não são robustos contra manipulação online de conteúdo.

Outra desvantagem das tabelas TAN é que elas introduzem um grau inconveniente indiscutivelmente pequeno para o usuário, uma vez que é necessário carregar a tabela de TAN todas as vezes que quiserem realizar uma transação de e-banking (OPPLIGER, 2009). Mais que inconveniente, o problema reside na facilidade com que o usuário pode, por conveniência simplesmente digitalize sua tabela TAN (ou simplesmente copie seu conteúdo para um arquivo texto) e armazene-o em uma forma em que seu dispositivo controlado pelo adversário – permitindo que assim o invasor copio-o e atenuar ainda mais os aprimoramentos de segurança fornecidos pela solução.

2.4 Tokens criptográficos

Outra abordagem para minimizar os efeitos de um dispositivo comprometido na autenticação é usar a ferramenta PKI com credenciais armazenadas externamente. Tokens criptográficos (HILTGEN, 2006) são dispositivos resistentes a violação que podem ser conectados ao computador do usuário (geralmente através de uma interface USB) durante a transação, mediante solicitação do banco, e que pode conter par de chaves públicas e privadas. Esses dispositivos são projetados para proibir seu conteúdo para serem copiado por aplicativos externos (ou seja, pelo adversário), e pode ser incorporado com recursos de computação (criptografia / decifração, assinatura / verificação). Atualmente, os tokens estão disponíveis de forma variável – a partir de um simples armazenamento USB, a gadgets com tela / teclado – na tela equipada, o usuário pode com segurança verificar os parâmetros da transação antes de assiná-la – pois as habilidades de manipulação de conteúdo estão limitadas ao computador infectado da vítima – e portanto a autenticação pode ser garantida. Se não, no entanto, o usuário não tem controle sobre o que está assinado / criptografado dentro do token, nesses casos, o adversário pode ainda ser capaz de substituir as informações enviadas pelo banco pelo token de autenticação e conseguir fazer alterações.

Infelizmente, os dispositivos de tokens permanecem relativamente caros (YOU, 2010) para serem amplamente distribuídos para os clientes – especialmente aqueles mais equipados com extensões de entrada e saída para autenticação da transação. Além disso, no caso de uma perda do token comprometido, a remissão da credencial pode levar a custos maiores.

2.5 Algoritmo One-Time Pad

O algoritmo de criptografia One-Time Pad pode ser generalizado utilizando a Equação 1, onde O é a operação de criptografia, M_i é o i -ésimo caractere da mensagem a ser criptografada, K_i é o i -ésimo byte da chave (gerada aleatoriamente) usada para cifrar a mensagem, C_i é o i -ésimo caractere da mensagem cifrada e n o tamanho da chave (RABAH, 2005).

$$C_i = O(M_i, K_i) \text{ para } i = 1, 2, 3 \dots n \quad (1)$$

Para cifrar uma mensagem, M , com uma chave, K , produzindo a mensagem cifrada, C , basta fazer a operação XOR (ou exclusivo) bit-a-bit entre a mensagem e a chave, e para decifrar essa mensagem basta realizar a operação XOR entre a mensagem cifrada e a chave. É um algoritmo simples e seguro, desde que a chave seja aleatória, usada apenas uma vez e seja compartilhada apenas entre as partes interessadas na decifração.

Para cifrar a seguinte mensagem “IESB” pode-se seguir os 3 passos seguintes:

- Passo 1 – Criar a chave (K): a chave é um bloco de números ou bits, usados para transformar a mensagem original (M) na mensagem cifrada (C). primeiramente é criada a chave aleatória, após ser criada determina-se um método para converter o alfabeto em números, como pode ser visto na Figura 2. Assumindo a chave aleatória FSDN, é convertida em números, tornando-se 06 19 04 14.

Figura 2. Relação alfabeto x Número.

A 1	B 2	C 3	D 4	E 5	F 6	G 7	H 8	I 9	J 10	K 11	L 12	M 13
N 14	O 15	P 16	Q 17	R 18	S 19	T 20	U 21	V 22	X 23	W 24	Y 25	Z 26

Fonte: RABAH, 2005.

- Passo 2 – Cifrar a mensagem: primeiramente a mensagem é também convertida em números, torando-se 09 05 19 02. Agora basta realizar a operação como na Figura 3.

Figura 3. Cifração da mensagem.

Mensagem	09	05	19	02
Chave	06	19	04	14
+				
Mensagem cifrada	15	24	23	16
O	W	X		P

Fonte: RABAH, 2005.

Agora a mensagem cifrada está pronta para ser mandada ao receptor.

- Passo 3 – Decifrar a mensagem: para decifrar a mensagem basta reverter os cálculos, como mostrado na Figura 4.

Figura 4. Decifração da mensagem.

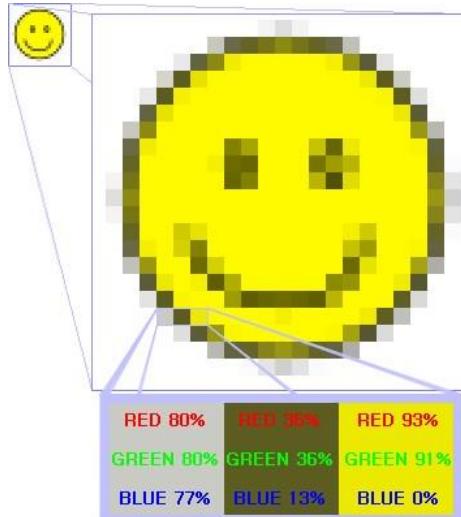
Mensagem cifrada	15	24	23	16
Chave	06	19	04	14
-				
Mensagem decifrada/original	09	05	19	02
I	E	S		B

Fonte: RABAH, 2005.

2.6 Densidade de pixels

Antes de se falar em densidade de pixels, é importante saber o conceito de pixel. O pixel é a menor unidade de composição de uma imagem digital (SLIDEShare, 2020), sendo eles representados com um sistema de três cores (vermelho, verde e azul), cada uma dessas cores é utilizado $8 + 8 + 8 = 24$ bits assumindo $256 \times 256 \times 256 = 16.777.216$ possíveis tonalidades (Figura 5). Nas imagens monocromáticas, cada pixel apresenta vários tons de uma única cor, sendo representado por 8 bits compreendido por um valor entre [0, 255]. A imagem digital é formada por uma matriz (x, y) de pixels agrupados em linhas e colunas.

Figura 5. Representação de pixels em cores.



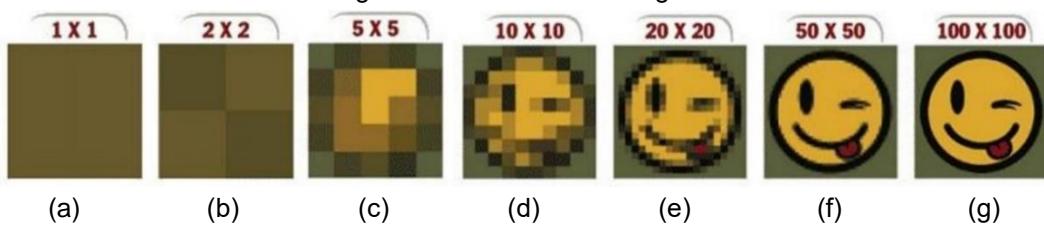
Fonte: SLIDEShare.

A densidade de pixel pode ser calculada através da Equação 2, definida pelos parâmetros: Quantidade de pixel em x (Q_x); Quantidade de pixel em y (Q_y); Área da imagem em polegadas (A_{pol}); Densidade de pixel (D_{pixel}).

$$D_{pixel} = (Q_x) * (Q_y) / A_{pol} \quad (2)$$

Exemplificando como a densidade de pixels influencia na qualidade de uma imagem, a Figura 6 mostra uma mesma imagem sendo representada por diferentes quantidades de pixels, à medida que a quantidade de pixels aumenta, maior volume de informação é armazenado na imagem. Desse modo a qualidade de uma imagem depende de quantos pixels a compõem em uma polegada quadrada, podendo ser observado na Figura 6 (g),

Figura 6. Qualidade da imagem.



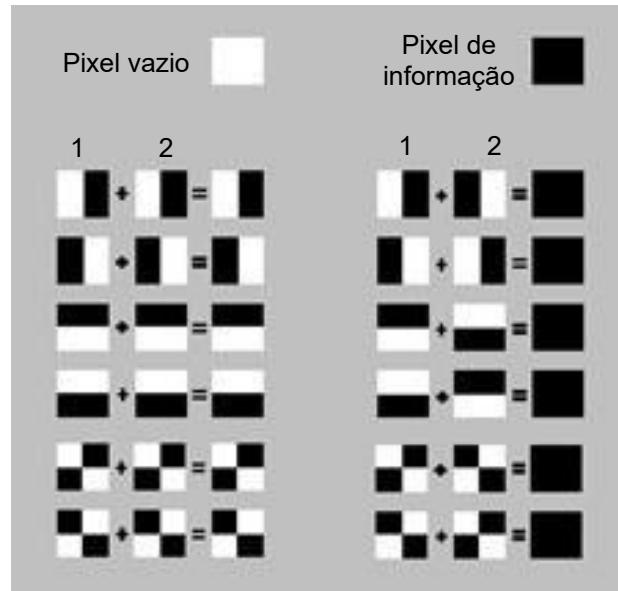
Fonte: SLIDEShare.

2.7 Criptografia Visual

O conceito original da Criptografia Visual (NAOR, 1994) foi proposto como um método alternativo para compartilhar um segredo entre partes que não contém, ou pelas limitações ou recursos inexistentes, um sistema computacional tradicional. A ideia principal por trás do método clássico, é converter o segredo em uma imagem, com formato bitmap, preta e branca, de baixa resolução e redimensionar de certo modo que cada pixel (será referido a partir de agora como subpixel) seja representado por uma matriz quadrada de pixel (será referido como superpixel); a imagem é então subdividida em um número predefinido de shares (neste projeto será utilizado duas shares).

Nessa aplicação específica de duas shares, a imagem secreta é inicialmente estendida por um fator de 2 – no qual os resultados estendidos da imagem secreta são compostos por 2 x 2 superpixel formado por quatro subpixels pretos (superpixel de informação) ou quatro subpixels brancos (superpixel sem informação) (PIVA, 2014). O par de shares para serem recuperados é então construído da seguinte maneira: primeiro, 2 x 2 superpixels composto por quatro subpixels brancos ou pretos são selecionados aleatoriamente de seis padrões possíveis e gerada na primeira share (ou share secreta). Finalmente, os superpixels da segunda share (ou share de autenticação) são escolhidas para serem idênticos ao equivalente da primeira share (se o equivalente na imagem secreta estendida for um super pixel não-informativo) ou complementar a ele (se o equivalente na imagem secreta estendida for um super pixel de informação). Figura 7 ilustra todas as escolhas possíveis de superpixels para compor a primeira e segunda shares.

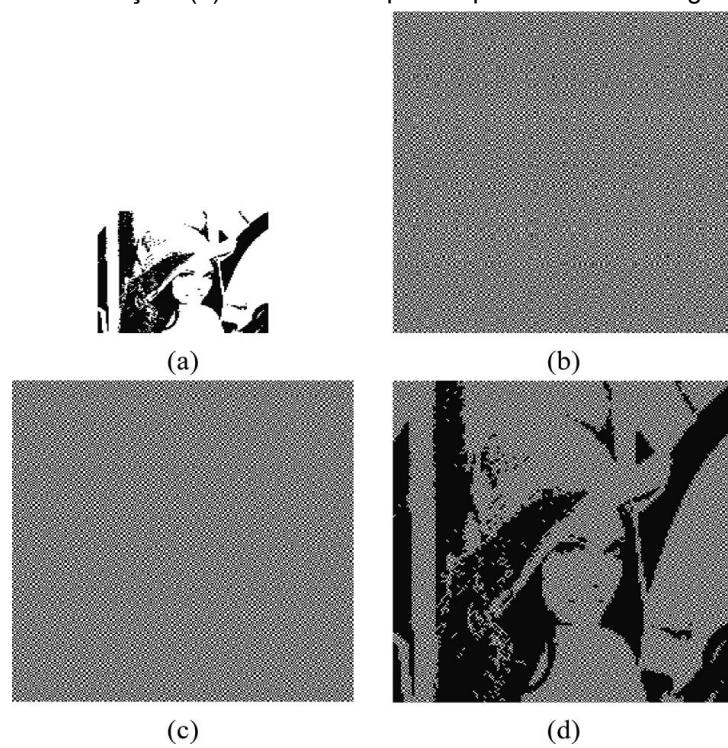
Figura 7. Possíveis escolhas de superpixel.



Fonte: Visual Cryptography. How Visual Cryptography works.

Depois que o par de shares são gerados, cada share é finalmente dada a cada parte, e somente pode ser possível recuperar a imagem secreta original se as duas shares forem empilhadas e alinhadas corretamente. Esse processo é referido como sobreposição. A Figura 8 ilustra a imagem secreta recuperada a partir da share secreta e a share de autenticação.

Figura 8. Exemplo de um esquema tradicional de CV: (a) imagem secreta. (b) Share Secreta. (c) Share de Autenticação. (d) Shares sobrepostas para revelar a imagem secreta.



Fonte: MELGAR, 2019.

Os superpixels sem informação na sobreposição são recuperados em tons de cinza, enquanto os superpixels de informação aparecem em preto. Esse aspecto “preto e cinza” da imagem recuperada representa uma perda de contraste de 50% em comparação com a imagem secreta estendida (preto e branco) original, que não é suficiente para debilitar a visualização da imagem.

3 O PROJETO

A pesquisa surgiu com o intuito de obter um sistema no qual a autenticação de transações seja segura contra ataques, com proposta de ter uma share de autenticação impressa em material Acetato transparente e outra share secreta enviada para o smartphone do usuário e ao serem sobrepostas, revelando a mensagem secreta.

3.1 Uma solução de criptografia visual

Os dispositivos móveis são considerados plataformas convenientes e relativamente econômicas para implementação de soluções de autenticação de dois-fatores e dois-canais de e-banking. Para fornecer, simultaneamente, autenticação mútua de usuário e autenticação de transação, a solução proposta conta com o dispositivo móvel do usuário principalmente por suas características de saída. Especificamente, consideramos o dispositivo móvel capaz de receber e exibir informações bancárias, resistentes a violações, cifradas em CV e dependentes de transações, que só podem ser recuperadas pelo usuário através da posse de um segredo compartilhado previamente estabelecido.

Como a decifração é executada pelos olhos do usuário e não requer o uso da computação, o compartilhado entre as duas partes não é armazenado em nenhum dispositivo que possa ser comprometido por malware. Isso impossibilita que o adversário realize ataques de roubo de credenciais por meio de infecção por malware.

3.2 Metodologia

O método de CV tem duas limitações principais que dizem respeito à aplicação proposta: primeiro cada par de shares podem revelar apenas uma imagem secreta predefinida. Isso significa que cada interação a respeito do compartilhamento do segredo entre duas partes requer a geração e distribuição de novos pares de shares.

Segundo reutilizar diretamente qualquer share gerada anteriormente (especificamente, a primeira share) em um novo par com intenção de recuperar uma imagem secreta diferente torna-se inseguro. Por exemplo, em um cenário no qual uma share particular queira ser reutilizada na geração de outras diferentes segundas

shares, destinados à recuperação de várias imagens secretas, mesmo um adversário clássico seria capaz de reconstruir a primeira share observando não mais que duas transações. Esse é o comportamento típico do algoritmo One-Time Pad, onde é recomendado ser utilizado apenas uma vez para cifrar e decifrar a mensagem secreta desejada.

3.2.1 Descrição das Shares

Para o algoritmo de geração das shares, foi utilizado o ambiente de programação em Java. Determinando assim, a Share Secreta e a Share de Autenticação. A proposta para este projeto será de uma imagem secreta (gerando números e letras aleatórias), que se limita a um tamanho de 32 x 32 pixels sendo analisadas em três diferentes dispositivos: Iphone SE, Ipad 6^a Geração e Samsung A20.

Prosseguindo com a geração das shares será determinado tamanhos diferentes de imagens partindo de 64 x 64 pixels e aumentado gradativamente em 32 x 32 pixels até alcançar o tamanho máximo avaliado de 1120 x 1120 pixels, afim de determinar até qual tamanho será possível ter uma boa visualização e quantidade de caracteres da mensagem secreta após a sobreposição das duas shares nos três diferentes dispositivos, como mostra na Tabela 1.

Tabela 1. Relação tamanho da Share x Quantidade de caracteres.

Tamanho da Share (pixels)	Quantidade de caracteres
64 x 64	4
96 x 96	9
128 x 128	16
...	...
1056 x 1056	1089
1088 x 1088	1156
1120 x 1120	1225

Fonte: Própria.

Após ter gerados as duas shares, a Share de Autenticação é impressa em material de Acetato transparente de 0,5 milímetros (onde os pixels brancos tornam-

se transparentes) – utilizando a impressora AccurioPrint C2060L (com resolução de 1200 x 1200 dpi x 8 bit) em sua máxima qualidade – enquanto a Share Secreta será enviada para o dispositivo.

Utilizando a Equação 3 e a Equação 4, será determinado o tamanho de impressão para cada Share de Autenticação a cada dispositivo (Tabela 2) (foi considerado o máximo de casas decimais para que se tenha a melhor precisão quando as shares forem sobrepostas), definindo como parâmetros: P_h (pixels horizontais), P_y (pixels verticais), H_{mm} (hipotenusa em milímetros), H_p (hipotenusa em pixel), T_{mm} (tamanho da impressão por lado em mm), T_{pol} (tamanho da impressão por lado em polegadas). Para a impressão da share foi considerado o tamanho horizontal de cada dispositivo para que seja compatível com o formato quadrado das shares e tenha o aproveitamento máximo do tamanho da tela, para a visualização das shares sobrepostas é considerado o dispositivo na posição vertical.

$$(H_p)^2 = (P_h^2 * P_y^2) \quad (3)$$

$$T_{mm} = (H_{mm} * P_h)/H_p \quad (4)$$

Tabela 2. Relação entre dispositivo e tamanho da impressão.

Dispositivo	H_{mm}	P_y	P_h	H_p	T_{mm}	T_{pol}
Ipad 6ª Geração	246,38	2048	1536	2560	147,828	5,8200
Samsung A20	162,56	1560	720	1718,1	68,122	2,6820
Iphone SE	101,6	11136	640	1303,8772	49,8697	1,9634

Fonte: Própria.

3.2.1.1 Densidade de pixel

Neste projeto a densidade de pixel é determinada pela Equação 5, definindo como parâmetros: Tamanho da share em pixels (T_{sha}); Área da share em polegadas (A_{pol}) calculada a partir do tamanho da impressão; Densidade de pixel de cada share (D_{sh}). Para cada share é calculada sua densidade de pixel, essa informação é importante para determinar a quantidade de pixels que uma share pode assumir para que seja possível a visualização da mensagem secreta.

$$D_{sh} = (T_{sha})^2/A_{pol} \quad (5)$$

3.3 Algoritmo de Geração de Shares

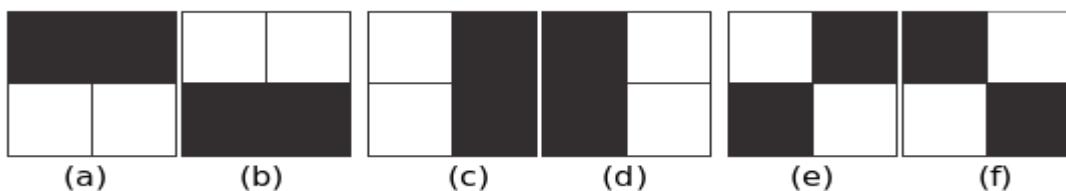
Nesta seção será apresentado o algoritmo capaz de gerar as Shares Secreta e de Autenticação, sendo disponibilizado em: <https://github.com/pedrosaid/Visual-Cryptography.git>

3.3.1 Share Secreta

Nesta etapa é definido primeiramente o tamanho da share. Com esses tamanhos e utilizando a Classe `BufferedImage` e `Graphics2D` é criado uma imagem.

Para geração da share será criado um vetor de pixels com números aleatórios, de 0 até 5, que serão utilizados para representar cada padrão demonstrado na Figura 9.

Figura 9. Padrões de pixels: (a) - 0; (b) - 1; (c) - 2; (d) - 3; (e) - 4; (f) - 5.



Fonte: MELHAR, 2019.

Após o vetor de pixels ter sido criado, será percorrida toda a imagem comparando com esse vetor e será pintado cada padrão correspondente. Após ter a imagem criada com seus pixels aleatórios será salva em formato bitmap, para que seja enviada posteriormente ao smartphone.

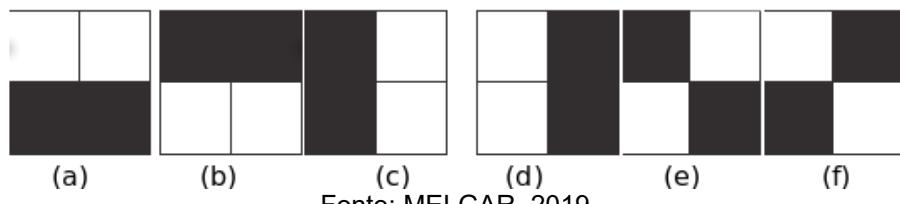
3.3.2 Share de Autenticação

A share de autenticação reutiliza os pixels da share secreta para que sejam geradas shares idênticas.

A partir de vetores numéricos, representando graficamente a imagem secreta (neste caso serão letras e números), serão definida aleatoriamente os números a serem codificados nesta share (para cada tamanho da share, será uma quantidade de número diferentes), como na etapa anterior também será percorrido toda a imagem comparando agora com o vetor de cada número da mensagem secreta, mas pintando cada pixels que combine com o vetor da mensagens secreta com seu complemento (obtendo os pixel de informação) representados na Figura 10, salvando também a

imagem em formato bitmap, para que possa ser impressa e ao ser sobreposta com a share de secreta (enviada para o smartphone) a mensagem secreta é revelada.

Figura 10. Complemento: (a) - 0; (b) - 1; (c) - 2; (d) - 3; (e) - 4; (f) – 5.



Fonte: MELGAR, 2019.

4 RESULTADOS

Após a geração do par de shares para cada tamanho indicado na Tabela 1, foram feitas as análises para cada dispositivo afim de se obter qual o tamanho máximo para que seja possível a visualização da mensagem secreta. Foram feitas duas análises, a primeira considerando que tenha sido possível visualizar a mensagem secreta com a visão humana e a outra através de uma câmera de celular, esses resultados foram evidenciados com a câmera de um smartphone Xiaomi Redmi Note S9 a uma distância de aproximadamente 40 centímetros.

Nas duas análises feitas, foram observados diferentes resultados em relação ao tamanho das shares, quantidade de caracteres decifrados e densidade de pixels para cada dispositivo.

A princípio é possível observar todos os caracteres da mensagem secreta, mas de modo que vai aumentando o tamanho das shares a cada 32×32 pixels a decifração da mensagem secreta vai se limitando a regiões cada vez menores. A decifração por regiões quando analisadas pela visão humana é feita dependendo da inclinação em que se olha as shares sobrepostas, e quando analisadas pela câmera do celular depende da posição da câmera em relação das shares sobrepostas.

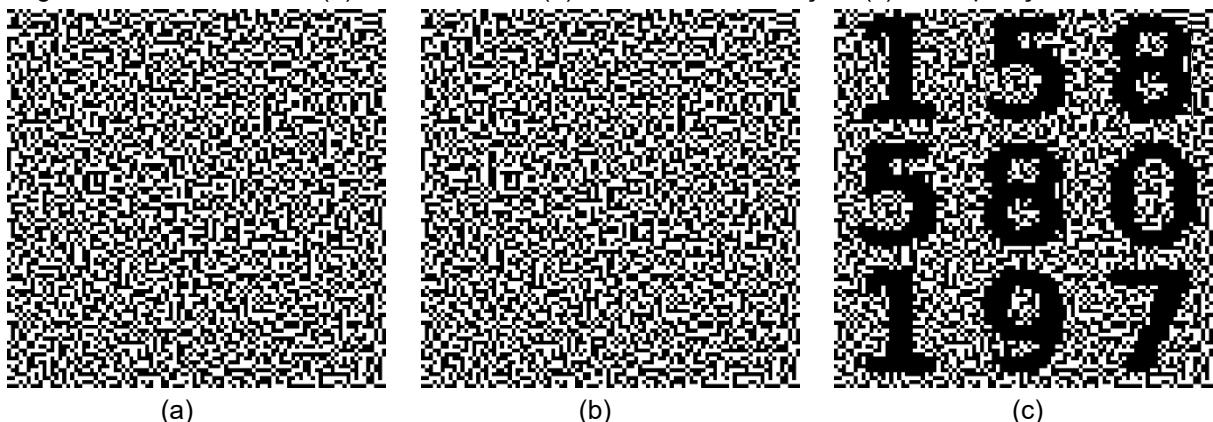
A melhor visualização possível dos caracteres decifrados é quando o observador ou a câmera do smartphone está com uma inclinação de 90° em relação a tela das shares sobrepostas, quando o observador se distancia dessa inclinação, a visualização vai se tornando impossível. Essa propriedade física aumenta a segurança contra ataques de engenharia social como o *Shoulder Surfing*¹.

A impressão das shares foram feitas em uma folha de acetato transparente no tamanho A3 (com uma área de 193,3472 polegadas quadradas) custando R\$ 20,00, sendo o custo para impressão da share por polegada quadrada é igual a R\$ 0,10.

Afim de exemplificação nas Figuras 11, 12, 13, 14, 15, 16, 17, 18, 19 e 20 serão apresentadas o resultado esperado na sobreposição da share secreta, share de autenticação.

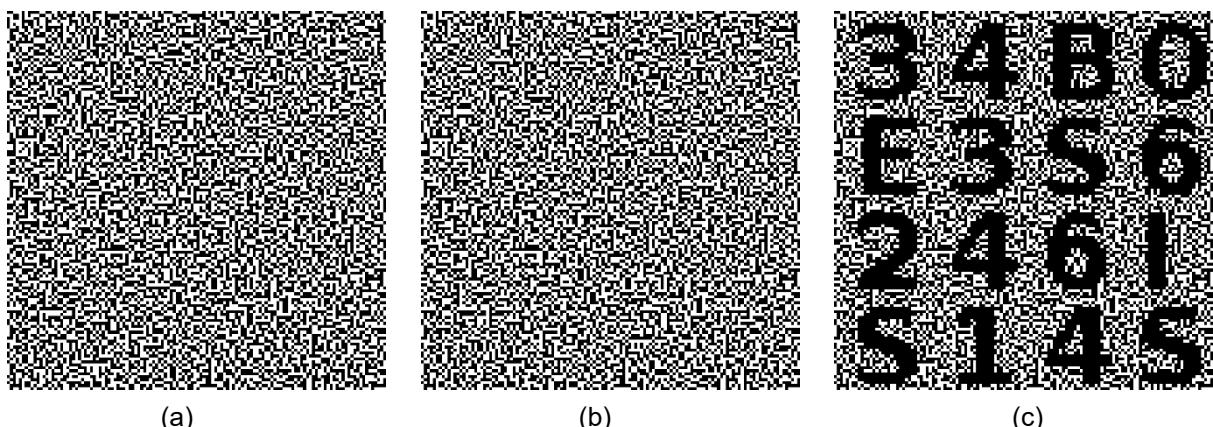
¹ Este tipo de ataque ocorre quando uma das partes é capaz de olhar sobre o ombro de outro ou espionar a tela do outro.

Figura 11. Share 96 x 96: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.



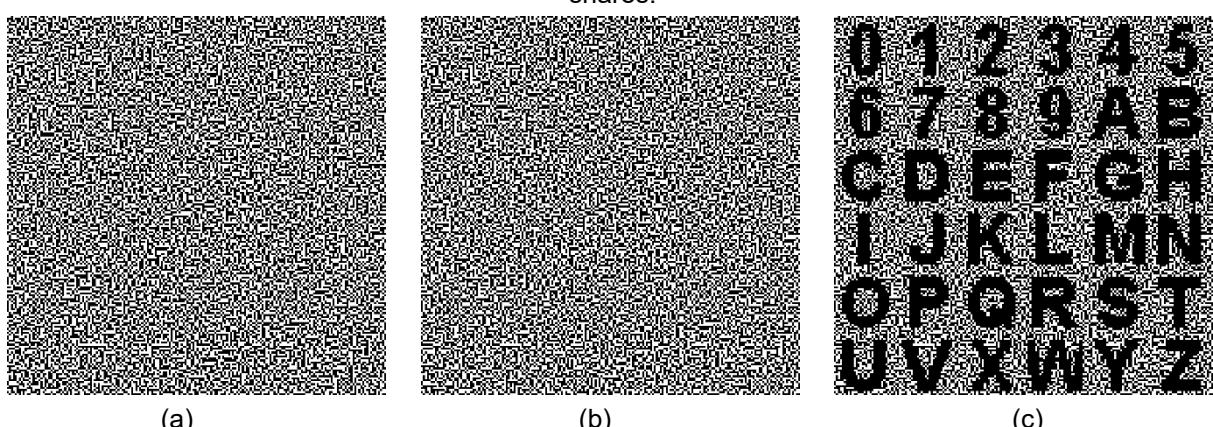
Fonte: Própria.

Figura 12. Share 128 x 128: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.



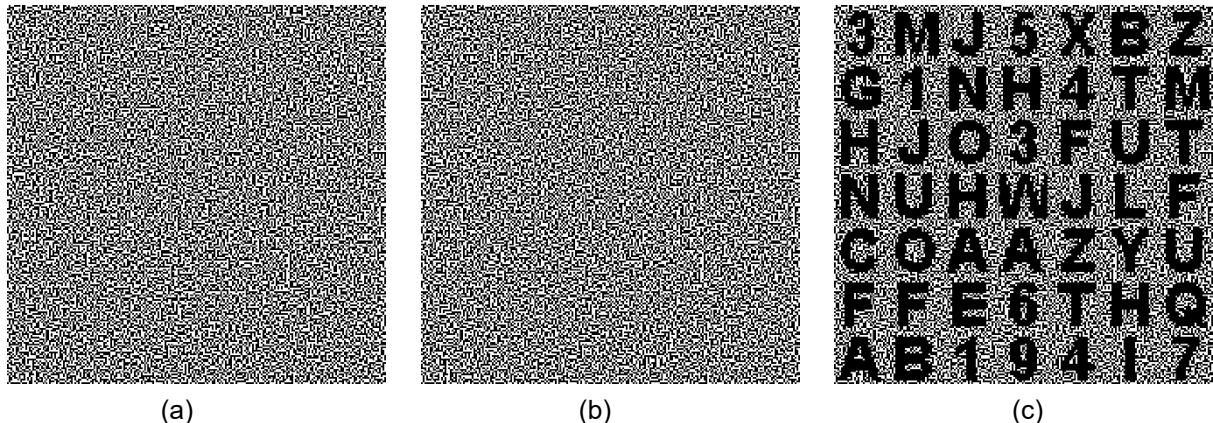
Fonte: Própria.

Figura 13. Share 192 x 192: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.



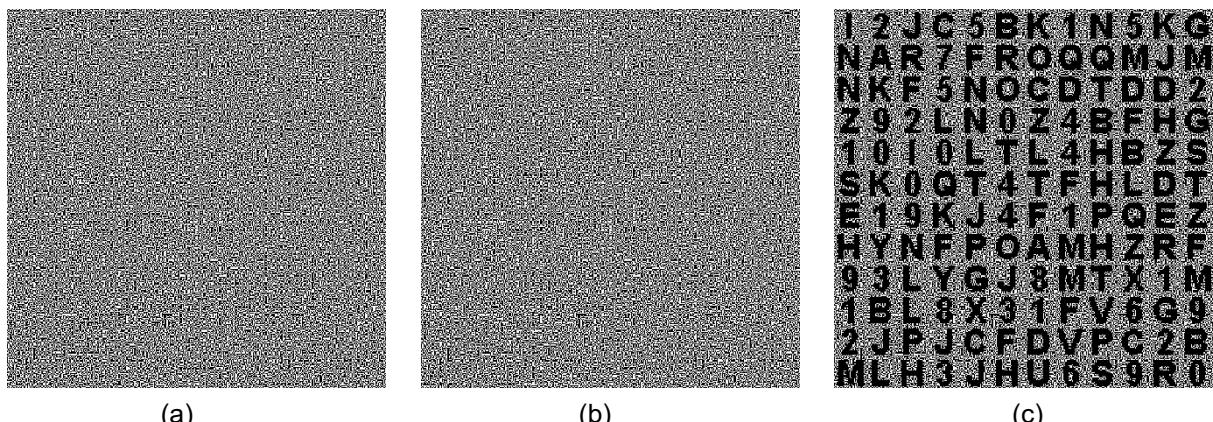
Fonte: Própria.

Figura 14. Share 224 x 224: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.



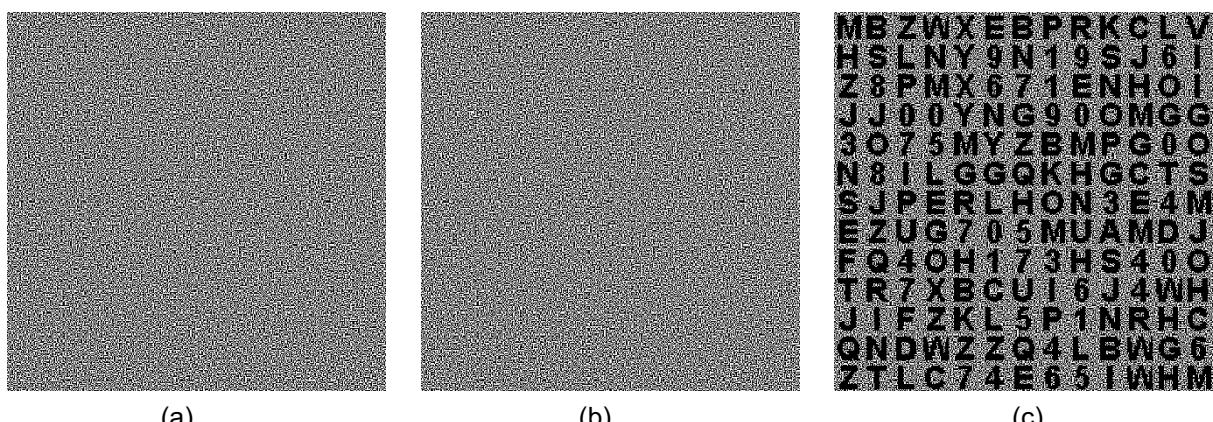
Fonte: Própria.

Figura 15. Share 384 x 384: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.



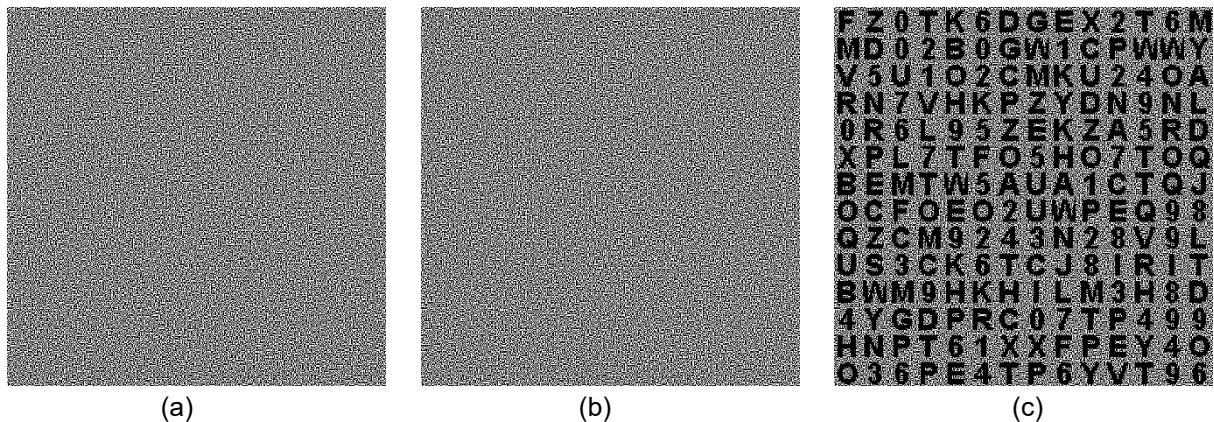
Fonte: Própria.

Figura 16. Share 416 x 416: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.



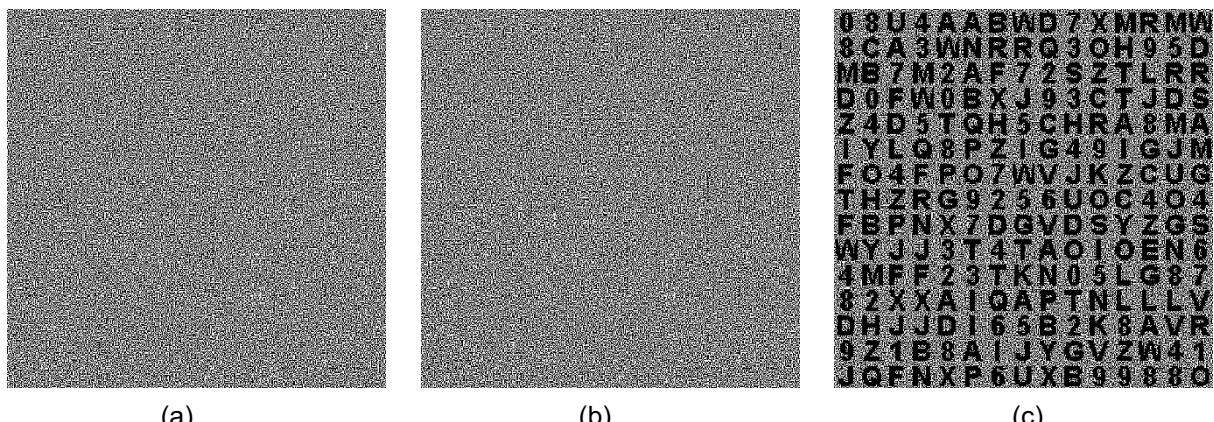
Fonte: Própria.

Figura 17. Share 448 x 448: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.



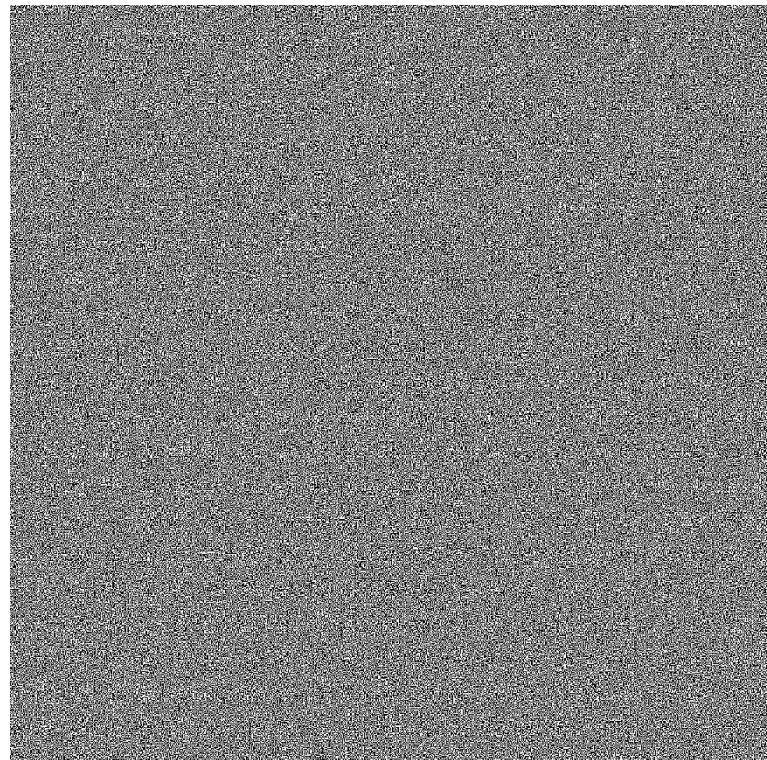
Fonte: Própria.

Figura 18. Share 480 x 480: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.

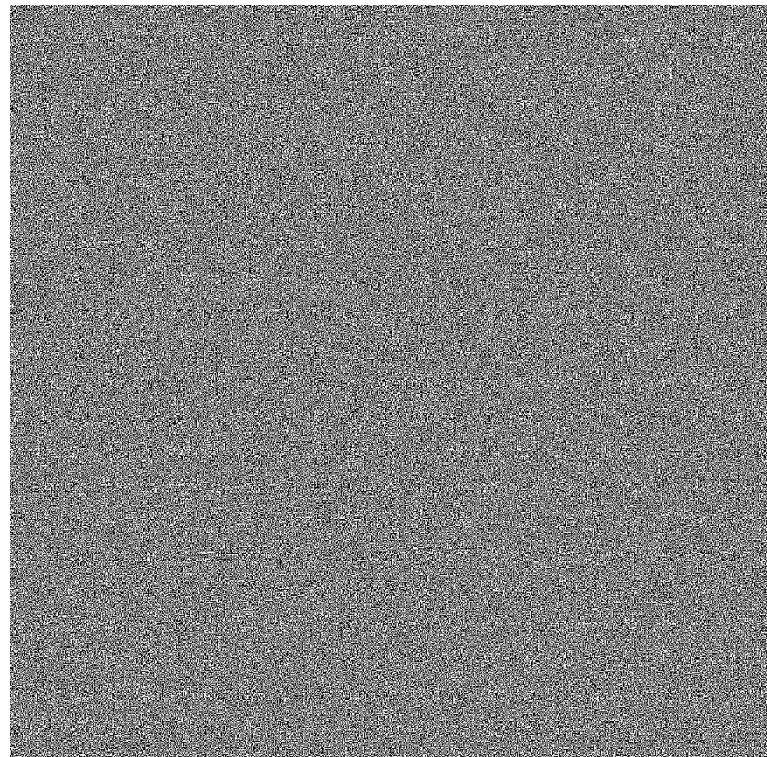


Fonte: Própria.

Figura 19. Share 1088 x 1088: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.



(a)



(b)

```

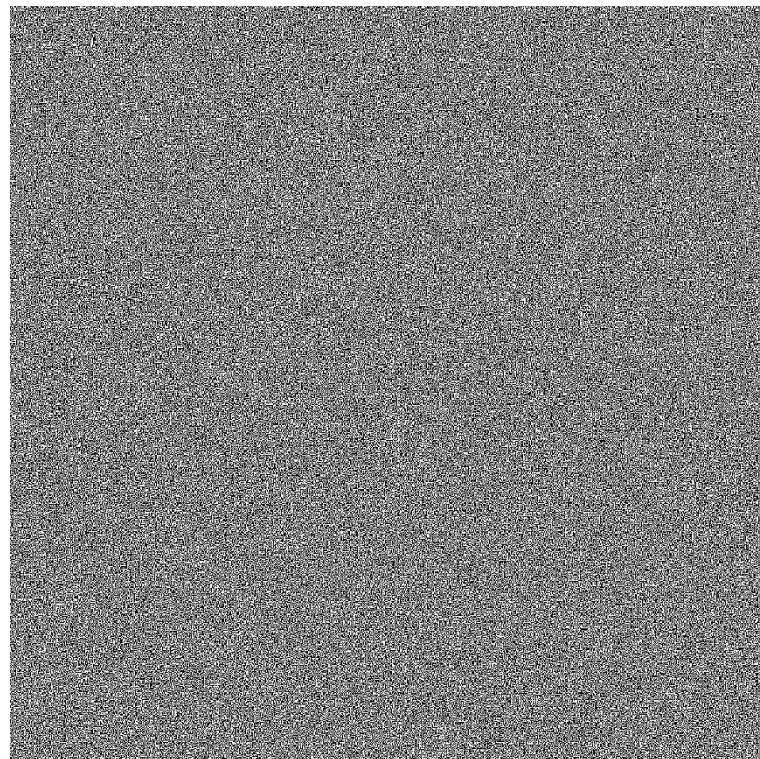
BR5K1SOU9YUXGKU6H3HIIMLLDG4VMEIP543
EZCGH9L4XDZVQPOSMAZ2PP0WTIT96FDYHD
VMPNEWT7ZCKX86YCNSZ95A1GMYFJBK4AUT
ESMDG2LP1YHZQ1C7141R7B1MOXY0H53ZU
J9ZP3B7G1ZB4FKGLGFLRB70PPLERWYR
51W0UO9FZI1ZXPV43FUFT2GW7DG9VRABON
07LBD28DUAAEKB1NEB7XRBO4MEKSUVGC0
753CD5F7ZGJYJV18BANVXPR730GMANR0
J8WKZ13TR2PLYMTUP3MXR0804WXSR3GNUB
XSYKU6VDGSTP91SB91XMMWPNKODL25JGL
VKZTT49X4AS0YQJCJD5BHST1ZXNYVOZGR0
YEXGDFWI2DHIREBJSXL17VFRSGAOFD9WINS
0TWY7PIHGF30ZV0L007H2ZG1FDLDWH9LSJ
XJHSURVG1S7HSLT4LEMZH1SGMRWM7WGZOY
ZUMSE39J1SRJKHZGYZ1HWJQR8111UVGDE
LY92G1JX8XPU6EH13L3ADJJB7V2MDT3Q38
K10AVK15EHKG26KAEG612V2LH0PI0AMP
5PVBXNXSGOKK6ROX4C0NNNYLL1HBRUS6NP
69DCKVT8N1Z8C0HS1DPKXNFGOO48UTF
WDWFQG-N06QPDONJ0R PY DHGNDGXW/BDD E6
YPXDF1PB6X61GJIJCM5C09UU1SZZGIZDIL
OBE4JG1DC9SH7JP06H6SGU7CGCRK3L2G
5PTDRXHZ19M106WMX478FJZ2131MQX01R0
60EFT1KOXG00MRU7STIWTJS9XVB41PGZBT
51HD2J1HLVAOC1R284TNSA6YG1Z17XEZDO
Y0BVEKUKFGY3YRFPT4ABEMJYYALEIN71H0
GBDLFX1D5HFPJ71P71BZG3R6GUSNUSQKMA
P6ZJ1703B9N0QWTAGSJ466Y3KSLMBGLMF
5QT95J16BXVVAZ17VB3YBHJZGVJCB8NH50
H61789CH3CEVYN1H002H1R212FU7Z3QJ3L
5K13P71AG6CZCKONYAGY6YZ0BZYDD5W970
H1MZ3DJGIX07157RAAPPXCGY0IHQ0D1ZYX
7MQU3CHLD5M96PMPUF0H17YE61F2V97H1B
1OG0NNUGWSZBL4JRNRJJM5JRDBLR54MNZ

```

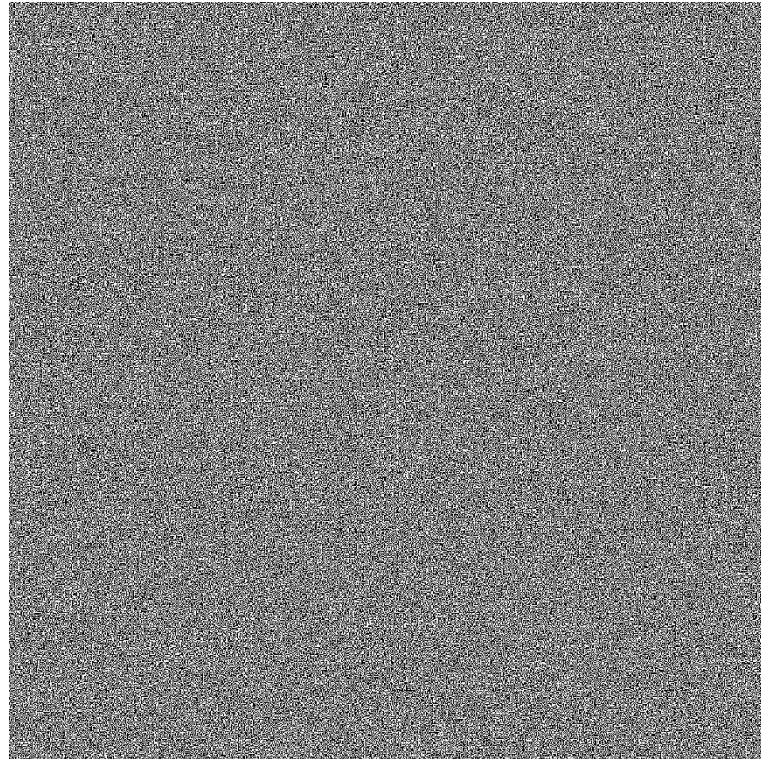
(c)

Fonte: Própria.

Figura 20. Share 1120 x 1120: (a) Share secreta, (b) Share de autenticação, (c) Sobreposição das shares.



(a)



(b)

YQLOQAWM3TADG7G1ZDNINMOKTRJB5AW4MM5
 SKTSGSMDH5SNNIX9G193SH5XE3BC2VNHSQR
 NOST1UVNJKR3N9PBVF4VMD9CJUUPXCHACEA
 H9XEKMGVFL49R3L1TAW5SURJ0MFXXK7EHP5C
 I1DHWMEEHYRRHP1L615MA07NOA5RGACPR5Z
 ALIG09THN8GB9MHEINEJSK855IKV2JRNGQY
 EN9DL0D28MV67QZIPP5HM56XW3HOPZRNNE
 TG760FHDSD0ESEMOXHEGH834KIKOOT2RT07X
 MDX3R8FWWQHMAQ4XUPKKJZOZFLFSAT3RXV
 PEW41UYP0K1NBB1804RQ75JJG3FT94Q01R
 M1FX21VN015V4WJ67GL9EA4YADBDDYH2Y3
 64ZBZ7MKLQ7MGAT9T1HOZAEYUNVI9ANVZDO
 51NKDGEG8UT39AAJNLRBZU122MF8RML7MZIK
 V72MSK31HRGNX5WUDELVM2HF73028KUQGETS
 DS1KEVXFH1M1E1JK5LQIPKNNAHXKA704CBL
 ZC60V12WSURKIJSTNB21UTLK23X5FAGAIN
 FRUT94K5RPR4XAXIT3DZ73LE3P1BKZMKCK
 JKYGUV90JV7AXC1U47UE0HOTPP6Q3DBNG8J
 160FMICPG6P1OAX5TTAL5JOSLT3H9CV76P
 NSX79HB2AGGGID0UNCANY0PKZ63TPMVDAJ06
 TEROX0631F8DAUCNFKOHL77PYPG5QNU6H
 W057QK9NVUABORJMIET2BP4MU19CN8HNTG9
 HD0IV1063WLTSSJ7DWZXSNCZEJ7ZWAGAEKB
 D007LUM5KRA3RT7T4Z0A51S5T2R61DK55
 AWTWB5ETHUCQA1WNQP37D1PYS19ZBKQEZZJD
 1QCYBY3YY3XDNMHOBJ824P57REKXU0FOMRC
 001CJB9WRR5P19CGIMI0CP93TQKE1VOL1TR
 U4T3JF5Q9TZKFD228N880206R7GLUD0EQQ
 TA41YPOBERJW1BK71CCBZSF38160DRPC711
 7J3RZBGL8QHLHIU6NRZ1DK519JHZJ4HEVBE
 GW8A6QD6NSZE1PT1AYHMRLX0PWVB-LU3QYXTV
 PV7FUYSM6PY8T97LRXTNG3RBQRD62M5ESY0
 D9XG7HJMOYEKJNAT13KXC7SIEYHJ9D2TFZY
 F1W74XN91E917E7A2DJ07557KGHUUVY151SU
 DPDRVTANSVOODS0HUZWEU1SQH52PW47YD7C1

(c)

Fonte: Própria.

A seguir serão apresentados os resultados para cada dispositivo analisado.

4.1 Ipad 6º Geração

4.1.1 Tamanho 96 x 96 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 21, 22, 23 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 21. Share impressa.



Fonte: Própria.

Figura 22. Share enviada para o dispositivo.



Fonte: Própria.

Figura 23. Shares sobrepostas revelando mensagem secreta.



Fonte: Própria.

4.1.2 Tamanho 128 x 128 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 24, 25, 26 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 24. Share impressa.



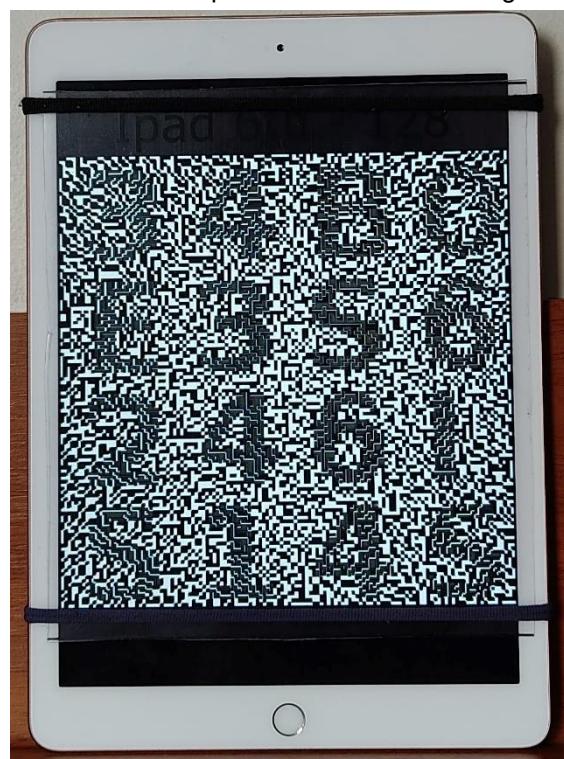
Fonte: Própria.

Figura 25. Share enviada para o dispositivo.



Fonte: Própria.

Figura 26. Shares sobrepostas revelando mensagem secreta.

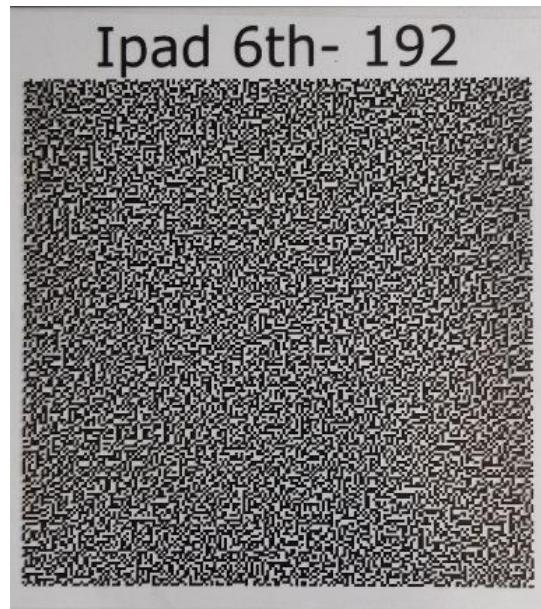


Fonte: Própria.

4.1.3 Tamanho 192 x 192 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 27, 28, 29 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 27. Share impressa.



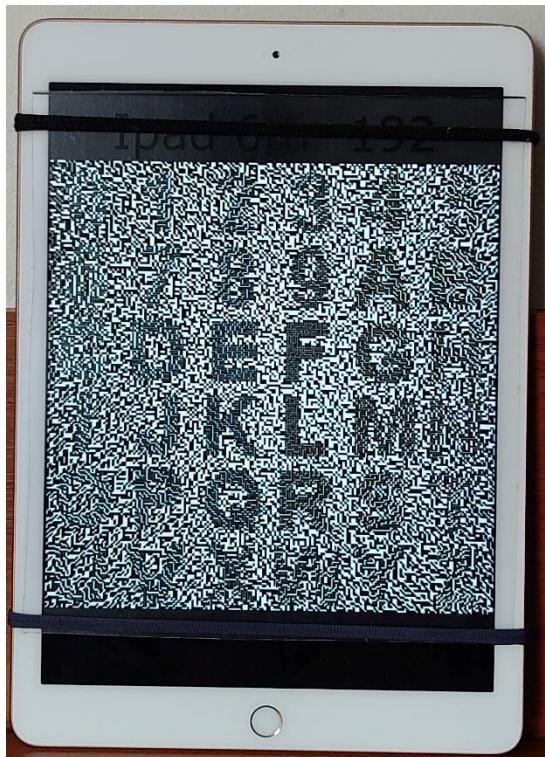
Fonte: Própria.

Figura 28. Share enviada para o dispositivo.



Fonte: Própria.

Figura 29. Shares sobrepostas revelando mensagem secreta.

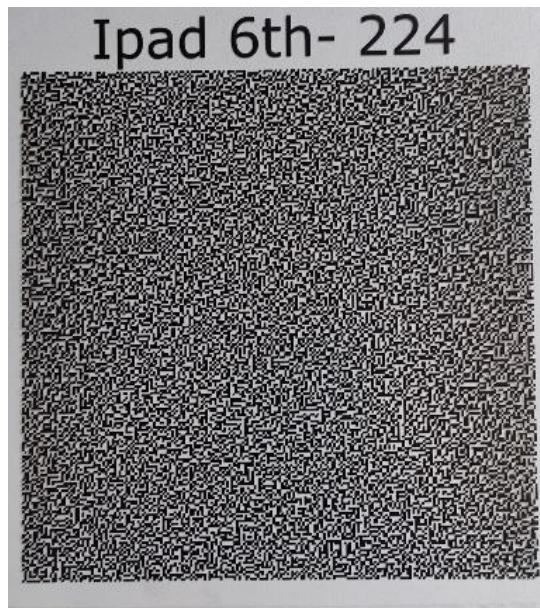


Fonte: Própria.

4.1.4 Tamanho 224 x 224 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 30, 31 e 32 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 30. Share impressa.



Fonte: Própria.

Figura 31. Share enviada para o dispositivo.



Fonte: Própria.

Figura 32. Shares sobrepostas revelando mensagem secreta.

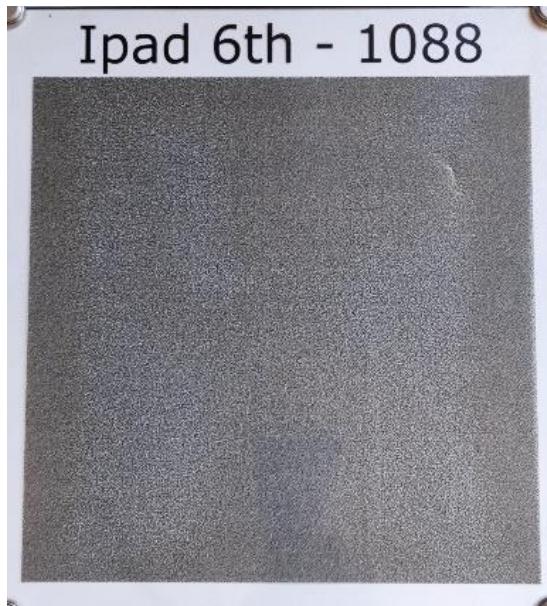


Fonte: Própria.

4.1.5 Tamanho 1088 x 1088 pixels

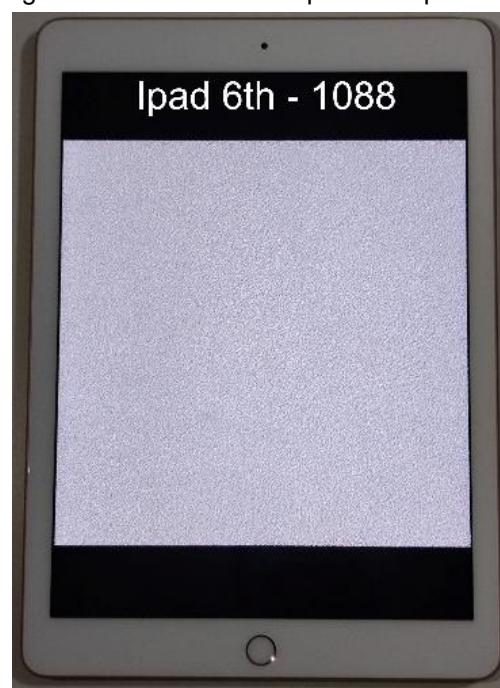
Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 33, 34 e 35 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 33. Share impressa.



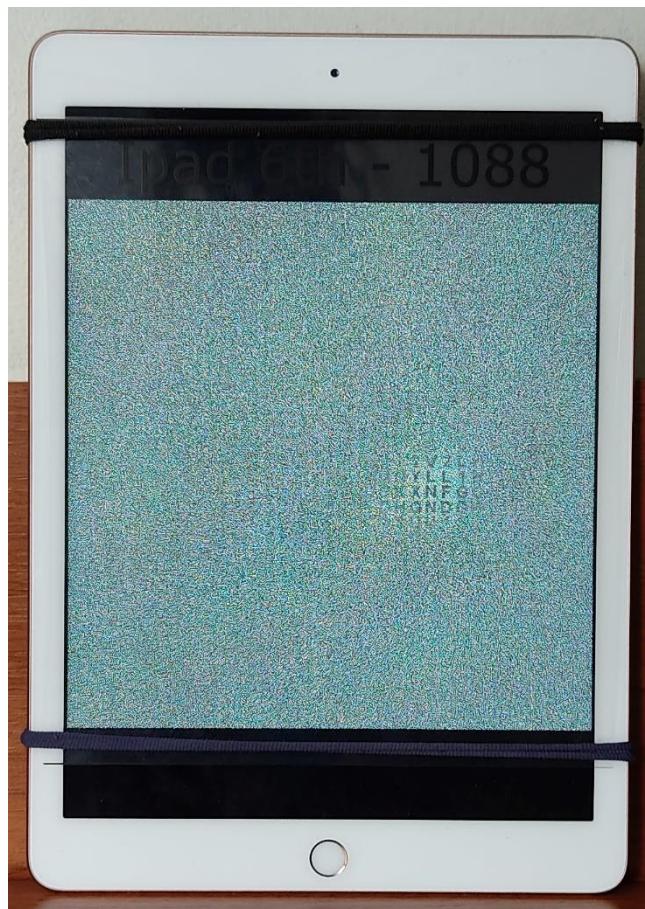
Fonte: Própria.

Figura 34. Share enviada para o dispositivo.



Fonte: Própria.

Figura 35. Shares sobrepostas revelando mensagem secreta.



Fonte: Própria.

4.1.6 Tamanho 1120 x 1120 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 36, 37 e 38 respectivamente, não tendo um resultado satisfatório pois a mensagem secreta não pôde ser visualizada.

Figura 36. Share impressa.



Fonte: Própria.

Figura 37. Share enviada para o dispositivo.



Fonte: Própria.

Figura 38. Shares sobrepostas mostrando que não é possível revelar mensagem secreta.



Fonte: Própria.

Nas análises feitas no Ipad 6^a Geração é possível que tenha uma visualização completa de toda a mensagem secreta até a share de tamanho 128 x 128 pixels (contendo 16 caracteres) com uma quantidade de 483,70 pixels por polegada quadrada e o tamanho máximo que possa ser visualizada a mensagem por regiões tem-se a share de tamanho 1088 x 1088 (contendo 1156 caracteres) com uma quantidade de 34.947,1546 pixels por polegada quadrada, considerando a visualização através da câmera do smartphone. Considerando a análise feita pela visão humana o limite possível para que a mensagem seja visualizada tem-se uma share de tamanho 1024 x 1024 (contendo 1024 caracteres) com uma quantidade de 30.956,65 pixels por polegada quadrada.

Está disponível dois vídeos no links a seguir, <https://youtu.be/axTvzwcJ0bs> e <https://youtu.be/NvDZfHsW8DM>, das shares 1088 x 1088 e 1120 x 1120 pixels para evidenciar a visualização por regiões dos caracteres revelados, foram gravados com a câmera do celular Xiaomi Redmi Note 9S com uma distância de 40 centímetros.

4.2 Iphone SE

4.2.1 Tamanho 96 x 96 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 39, 40 e 41 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 39. Share impressa.



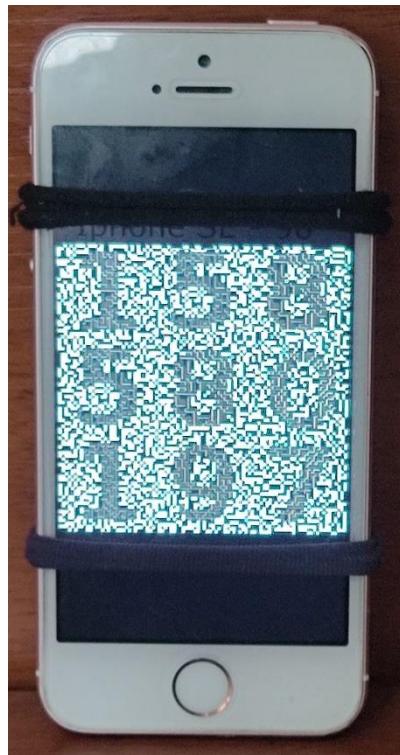
Fonte: Própria.

Figura 40. Share enviada para o dispositivo.



Fonte: Própria.

Figura 41. Shares sobrepostas revelando mensagem secreta.



Fonte: Própria.

4.2.2 Tamanho 128 x 128 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 42, 43 e 44 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 42. Share impressa.



Fonte: Própria.

Figura 43. Share enviada para o dispositivo.



Fonte: Própria.

Figura 44. Shares sobrepostas revelando mensagem secreta.



Fonte: Própria.

4.2.3 Tamanho 192 x 192 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 45, 46 e 47 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 45. Share impressa.



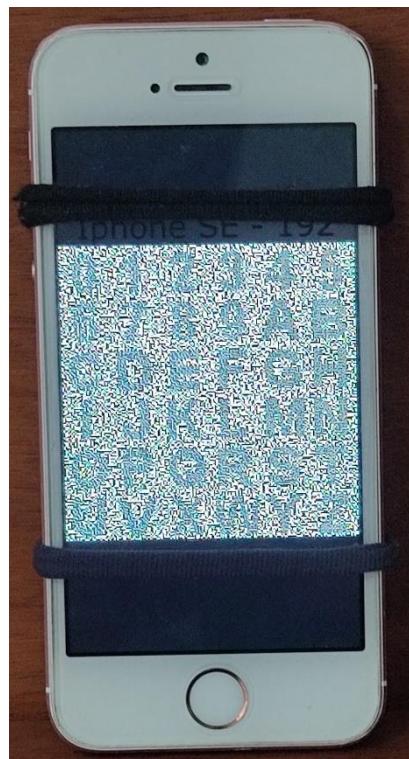
Fonte: Própria.

Figura 46. Share enviada para o dispositivo.



Fonte: Própria.

Figura 47. Shares sobrepostas revelando mensagem secreta.



Fonte: Própria.

4.2.4 Tamanho 224 x 224 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 48, 49 e 50 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 48. Share impressa.



Fonte: Própria.

Figura 49. Share enviada para o dispositivo.



Fonte: Própria.

Figura 50. Shares sobrepostas revelando mensagem secreta.



Fonte: Própria.

4.2.5 Tamanho 384 x 384 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 51, 52 e 53 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 51. Share impressa.



Fonte: Própria.

Figura 52. Share enviada para o dispositivo.



Fonte: Própria.

Figura 53. Shares sobrepostas revelando mensagem secreta.



Fonte: Própria.

4.2.6 Tamanho 416 x 416 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 54, 55 e 56 respectivamente, não tendo um resultado satisfatório pois a mensagem secreta não pôde ser visualizada.

Figura 54. Share impressa.



Fonte: Própria.

Figura 55. Share enviada para o dispositivo.



Fonte: Própria.

Figura 56. Shares sobrepostas revelando mensagem secreta.



Fonte: Própria.

Nas análises feitas no Iphone SE é possível que tenha uma visualização completa de toda a mensagem secreta até a share de tamanho 192 x 192 pixels

(contendo 36 caracteres) com uma quantidade de 9.563,04 pixels por polegada quadrada e o tamanho máximo que possa ser visualizada a mensagem por regiões tem-se a share de tamanho 384 x 384 (contendo 144 caracteres) com uma quantidade de 38.252,16 pixels por polegada quadrada, considerando a visualização através da câmera do smartphone. Considerando a análise feita pela visão humana o limite possível para que a mensagem seja visualizada tem-se uma share de tamanho 352 x 352 (contendo 121 caracteres) com uma quantidade de 32.142,44 pixels por polegada quadrada e

Está disponível dois vídeos no links a seguir, <https://youtu.be/x7UkLLnw0ec> e <https://youtu.be/zUiPpJ2fXMk>, das shares 384 x 384 e 416 x 416 pixels para evidenciar a visualização por regiões dos caracteres revelados, foram gravados com a câmera do celular Xiaomi Redmi Note 9S com uma distância de 40 centímetros.

4.3 Samsung A20

4.3.1 Tamanho 96 x 96 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 57, 58 e 59 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 57. Share impressa.



Fonte: Própria.

Figura 58. Share enviada para o dispositivo.



Fonte: Própria.

Figura 59. Shares sobrepostas revelando mensagem secreta.



Fonte: Própria.

4.3.2 Tamanho 128 x 128 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 60, 61 e 62 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 60. Share impressa.



Fonte: Própria.

Figura 61. Share enviada para o dispositivo.



Fonte: Própria.

Figura 62. Shares sobrepostas revelando mensagem secreta.



Fonte: Própria.

4.3.3 Tamanho 192 x 192 pixels

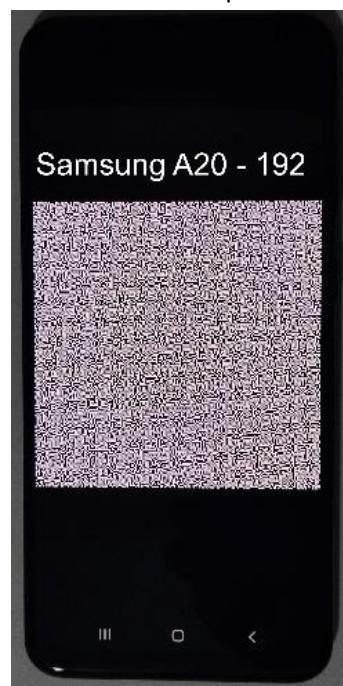
Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 63, 64 e 65 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 63. Share impressa.



Fonte: Própria.

Figura 64. Share enviada para o dispositivo.



Fonte: Própria.

Figura 65. Shares sobrepostas revelando mensagem secreta.



Fonte: Própria.

4.3.4 Tamanho 224 x 224 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 66, 67 e 68 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 66. Share impressa.



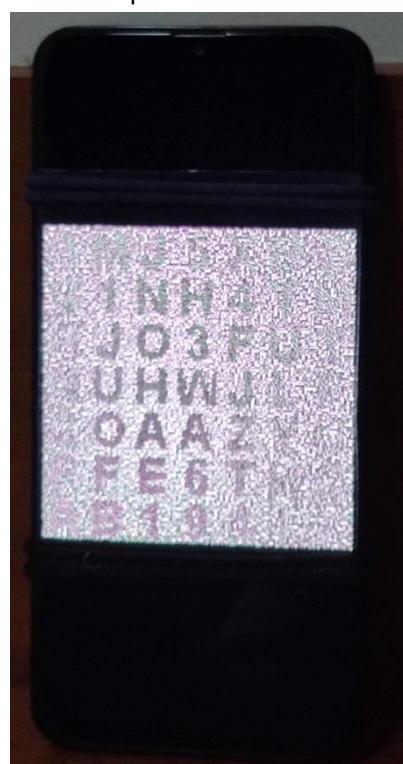
Fonte: Própria.

Figura 67. Share enviada para o dispositivo.



Fonte: Própria.

Figura 68. Shares sobrepostas revelando mensagem secreta.

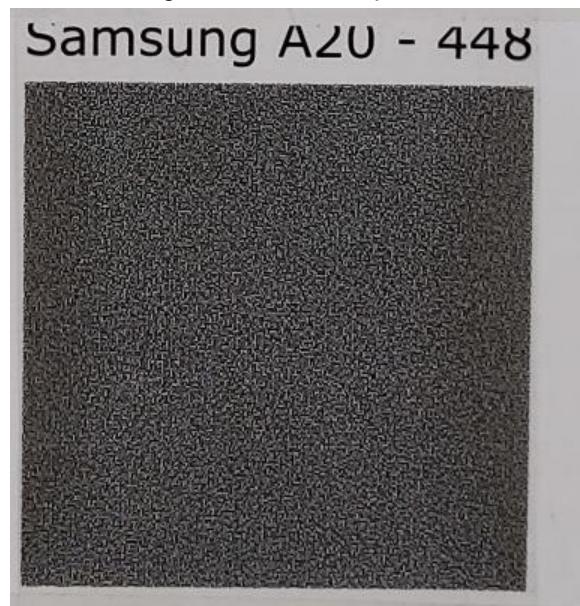


Fonte: Própria.

4.3.5 Tamanho 448 x 448 pixels

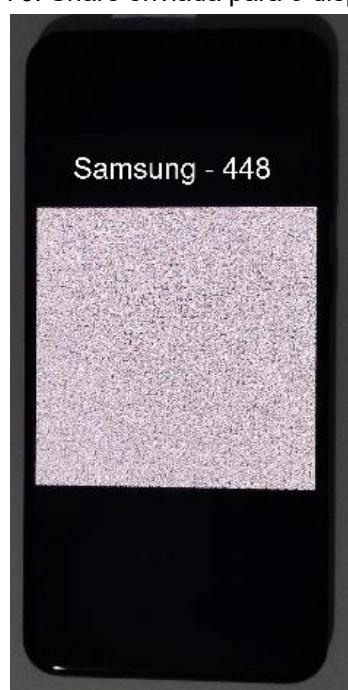
Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 69, 70 e 71 respectivamente, tendo um resultado satisfatório ao poder ser visualizada a mensagem secreta.

Figura 69. Share impressa.



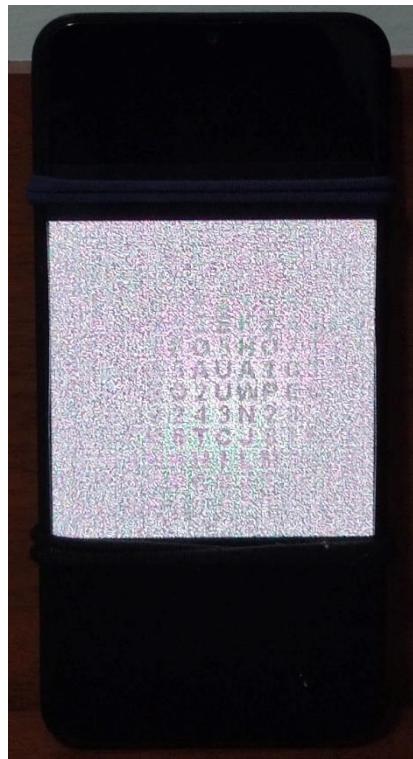
Fonte: Própria.

Figura 70. Share enviada para o dispositivo.



Fonte: Própria.

Figura 71. Shares sobrepostas revelando mensagem secreta.



Fonte: Própria.

4.3.6 Tamanho 480 x 480 pixels

Pode-se observar a Share Secreta, de Autenticação e o segredo revelado ao serem sobrepostas, representadas pelas Figuras 72, 73 e 74 respectivamente, não tendo um resultado satisfatório pois a mensagem secreta não pôde ser visualizada.

Figura 72. Share impressa.



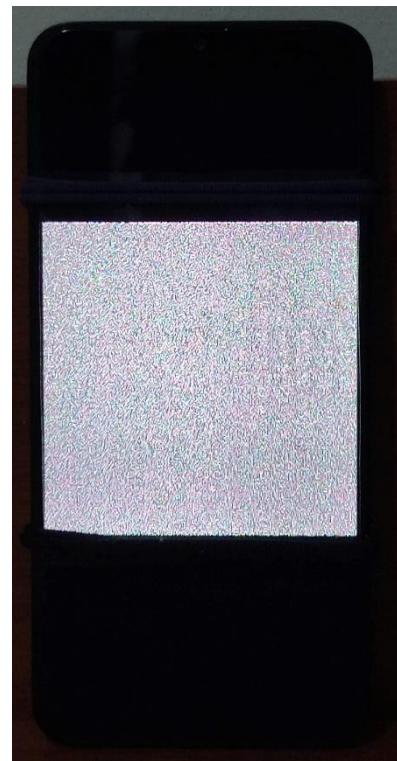
Fonte: Própria.

Figura 73. Share enviada para o dispositivo.



Fonte: Própria.

Figura 74. Shares sobrepostas mostrando que não é possível revelar mensagem secreta.



Fonte: Própria.

Nas análises feitas no Samsung A20 é possível que tenha uma visualização completa de toda a mensagem secreta até a share de tamanho 128 x 128 pixels

(contendo 16 caracteres) com uma quantidade de 2.277,78 pixels por polegada quadrada e o tamanho máximo que possa ser visualizada a mensagem por regiões tem-se a share de tamanho 448 x 448 pixels (contendo 196 caracteres) com uma quantidade de 27.902,78 pixels por polegada quadrada, considerando a visualização através da câmera do smartphone. Considerando a análise feita pela visão humana o limite possível para que a mensagem seja visualizada tem-se uma share de tamanho 384 x 384 pixels (contendo 144 caracteres) com uma quantidade de 20.500,00 pixels por polegada quadrada.

Está disponível dois vídeos nos links a seguir, <https://youtu.be/RhIMG84-1nY> e <https://youtu.be/cQU8e-PVZfA>, das shares 448 x 448 e 480 x 480 pixels para evidenciar a visualização por regiões dos caracteres revelados, foram gravados com a câmera do celular Xiaomi Redmi Note 9S com uma distância de 40 centímetros.

4.4 Resultados Finais

Após as análises feitas em cada dispositivo, a Tabela 3 apresenta o tamanho da share e a quantidade de caracteres decifrados quando possível ou não serem visualizados através da câmera do smartphone e a visão humana.

Tabela 3. Possível visualização x Não possível visualização da informação.

Dispositivo	Gravado com Xiaomi Redmi Note S9		Visão humana		Área da share em polegadas
	Visualização possível	Visualização não possível	Visualização possível	Visualização não possível	
Ipad 6ª Geração (Qtd de caracteres)	1088 x 1088 1156	1120 x 1120 1225	1024 x 1024 1024	1056 x 1056 1089	33,8724
Samsung A20 (Qtd de caracteres)	448 x 448 196	480 x 480 225	384 x 384 144	416 x 416 169	7,1930
Iphone SE (Qtd de caracteres)	384 x 384 144	416 x 416 169	352 x 352 121	384 x 384 144	3,8548

Fonte: Própria.

Analizando o tamanho das share e sua densidade de pixels obteve-se os resultados descritos na Tabela 4. Nota-se que existe uma diferença nas quantidades de densidade de pixel para cada dispositivo, essa diferença é explicada com a

qualidade que cada dispositivo apresenta em suas telas. O Ipad 6^a Geração tem uma tela de 2048 x 1536 pixel com um tamanho de 9,7 polegadas e 264 pixels por polegada, o Samsung A20 tem uma tela de 1560 x 720 pixel com um tamanho 6,4 polegadas e 268 pixels por polegada e o Iphone SE tem uma tela de 1136 x 640 com um tamanho de 4 polegadas e 326 pixel por polegada.

O Iphone SE apresenta uma maior quantidade de pixels visíveis pois sua tela apresenta uma densidade de pixels maior em comparação com as outras analisadas.

Entre o Ipad 6^a Geração e o Samsung houve uma grande diferença entre a quantidade de pixels visíveis mesmo suas telas apresentando uma densidade de pixels bem próximas, como as marcas utilizam diferentes tecnologias para implementar suas telas (o Ipad 6^a Geração apresenta uma tela com tecnologia IPS e o Samsung A20 apresenta uma tela com tecnologia Super AMOLED), esse pode ser um motivo para tal diferença na quantidade de pixels visíveis.

Tabela 4. Tamanho da Share x Densidade de Pixel.

Dispositivo		Tamanho da Share	Densidade de Pixel	Quantidade de caracteres por polegada quadrada
Ipad 6 ^a Geração	Câmera do smartphone	1088 x 1088 pixels	34.947,1546	34,1281
	Visão humana	1024 x 1024 pixel	30.956,65	30,2311
Samsung A20	Câmera do smartphone	448 x 448 pixels	27.902,78	27,2488
	Visão humana	384 x 384 pixels	20.500,00	20,0195
Iphone SE	Câmera do smartphone	384 x 384 pixels	38.252,16	37,3556
	Visão humana	352 x 352 pixels	32.142,44	31,3891

Fonte: Própria.

Com o aumento no tamanho das shares, os pixels ficam cada vez menores e isso traz uma grande dificuldade para o alinhamento das Shares Secreta e de Autenticação. Foram utilizados dois elásticos para fixar as shares e buscar o alinhamento necessário e ser possível a visualização da mensagem secreta.

5 CONCLUSÃO

Neste trabalho foram tratados assuntos relacionados à segurança da informação e autenticação em transações propondo um método de criptografia capaz de diminuir ataques invasores fazendo com que as transações se tornem mais seguras. O trabalho explora a propriedade principal da criptografia visual: utilização do sistema visual humano para decifrar a mensagem sem necessidade de um sistema computacional.

Com os resultados observados na seção 4, conclui-se que o método utilizado para a criptografia visual obteve um resultado ótimo para o tamanho das shares de até 128 x 128 quando considerado a visualização completa de todos os caracteres, e para a visualização da mensagem por regiões em cada dispositivo pode-se observar o tamanho máximo da shares apresentados na Tabela 3. Além disso, na relação entre a densidade de pixel e tamanho das shares apresentada na Tabela 4, pode-se concluir que utilizando a câmera do smartphone para visualizar a mensagem existe em média uma quantidade de 33.700,70 pixel por polegada quadrada, e utilizando a visão humana para visualizar a mensagem existe uma quantidade de 27.866,36 pixel por polegada quadrada.

Até onde foi investigado, esse trabalho é o primeiro na literatura que permite alcançar uma alta quantidade de caracteres ou informações cifradas em pixels por polegada quadrada por meio da utilização de uma câmera digital (em outro dispositivo) na decodificação. Além de uma proposta de implementação de criptografia visual, o trabalho mostra que é viável atingir a taxa de codificação de 38.252,16 pixels por polegada quadrada.

Uma das maiores dificuldades encontradas neste projeto foi de se obter um alinhamento perfeito entre as shares, sendo difícil em ter uma boa visualização da mensagem revelada.

Em trabalhos futuros, pretende-se aprimorar o método de alinhamento entre as shares fazendo com que seja possível melhorar a visualização da mensagem revelada, assim como uma análise mais profunda onde o smartphone está efetivamente infectado com malware bancário.

REFERÊNCIAS

- NAOR, M.; SHAMIR, A. VISUAL CRYPTOGRAPHY. IN: WORKSHOP ON THE THEORY AND APPLICATION OF OF CRYPTOGRAPHIC TECHNIQUES. 1994. 12P.
- MALLIK, A. et al. Man-in-the-middle-attack: Understanding in simple words. **International Journal of Data and Network Science**, v. 3, p. 16, 2 Janeiro 2019.
- Visual Cryptography. How Visual Cryptography works. Disponível em: <<http://users.telenet.be/d.rijmenants/en/visualcrypto.html>>. Acesso em: 17 Setembro 2019.
- DOLEV, D.; YAO, A. C. On the Security of Public Key Protocols. **IEEE TRANSACTIONS ON INFORMATION THEORY**, v. 29, n. 2, p. 198-208, Março 1983.
- HILTGEN, A.; KRAMP, T.; WEIGOLD, T. Secure Internet banking authentication. **IEEE Security & Privacy**, v. 4, n. 2, p. 21-29, Março 2006
- OPPLIGER, R; RYTZ, R.; HOLDEREgger, T. Internet Banking: Client-Side Attacks and Protection Mechanisms. **Computer**, v. 42, n. 6, p. 27-33, Julho 2009
- YOU, H. et al. A Study on the Two-channel Authentication Method which Provides Two-way Authentication using Mobile Certificate in the Internet Banking Environment. **5th International Conference on Computer Sciences and Convergence Information Technology**, p. 539-543, Dezembro 2010
- ZHAN, Justin; FANG, Xing. Online Banking Authentication Using Mobile Phones. **2010 5th International Conference on Future Information Technology**, p. 6, 21 Maio 2010
- MELGAR, M. E. V.; FARIA, M. C. Q. A (2,2) XOR-based visual cryptography scheme without pixel expansion. **Journal of Visual Communication and Image Representation**, v. 63, p. 10, 28 Julho 2019.
- PIVA, F. R. **Addressing human factors in the design of cryptographic solutions:** a two-case study in item validation and authentication. 49-p. Tese (Ciência da Computação) - Universidade Estadual de Campinas, 2014.
- K.V.O. RABAH , 2005. **Implementation of One-Time Pad Cryptography.** Information Technology Journal, 4: 87-95.
- SLIDEShare. Comunicação Gráfica e Design: Processamento de Imagens. Disponível em: https://www.slideshare.net/AlineAntunes25/comunicao-grfica-e-design-aula-7-processamento-de-imagens?from_action=save. Acesso em: 17 Setembro 2020.