

Ademir Rafael Marques Guedes
Victor Guimaraes

A Low-cost Attack on a Microsoft CAPTCHA

Jeff Yan

School of Computing Science
Newcastle University, UK

Ahmad Salah El Ahmad

School of Computing Science
Newcastle University, UK

Esquema de Capchas MSN



- 8 caracteres são utilizados;
- Somente letras maiúsculas e dígitos;
- Foreground (character) é azul escuro e o background(fundo) é cinza;
- Caracteres sofrem distorção
- Não há overlap de caracteres

Abordagem para segmentação

- Primeiramente tenta-se identificar e remover os arcos (riscos) aleatórios;
- Em seguida, identifica-se a posição dos caracteres na ordem correta dividindo o captcha em 8 partes;
- Observou-se 100 elementos aleatórios da base de teste para construção do algoritmo e 500 para testes;

Pré-processamento

- Converte a imagem em preto e branco utilizando um valor de threshold(limiar) determinado manualmente;



(a)



(b)



(c)

Pré-processamento

- Reúne trechos onde o caractere foi quebrado, através da transformação de pixels de background em pixels de foreground



Handwritten text "X7 N M, S Y RVE" with blue segmentation marks indicating character boundaries and internal structure.

(a)



Handwritten text "X7 N M, S Y RVE" with black segmentation marks, showing the result of the pre-processing step.

(b)

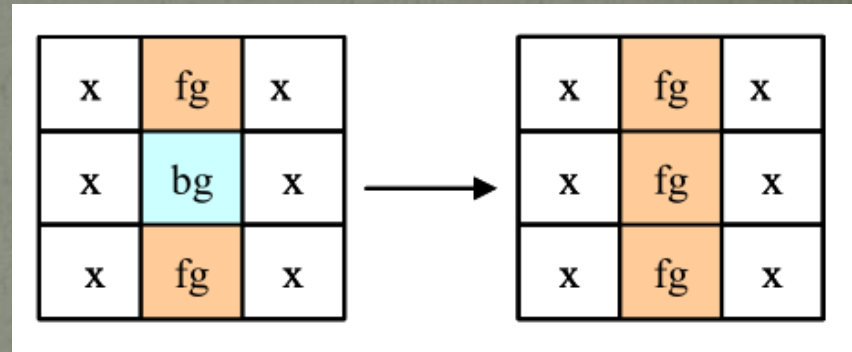
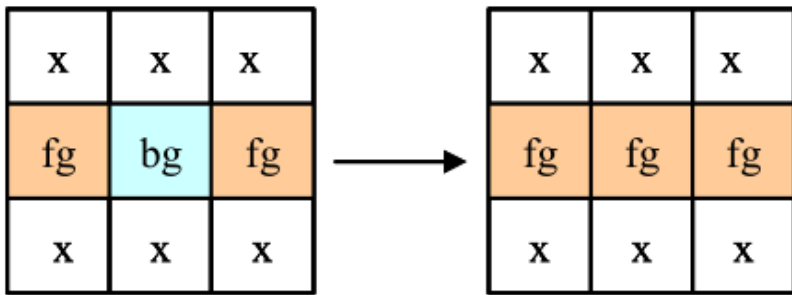


Handwritten text "X7 N M, S Y RVE" with black segmentation marks, showing the result of the pre-processing step.

(c)

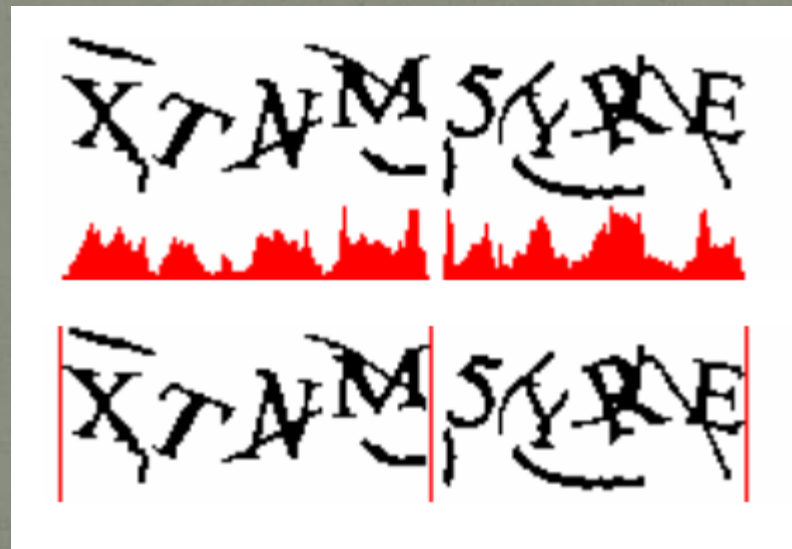
Pré-processamento

- São transformados os pixels de background que possuem pixels de foreground como vizinhos(direita e esquerda ou superior e inferior);



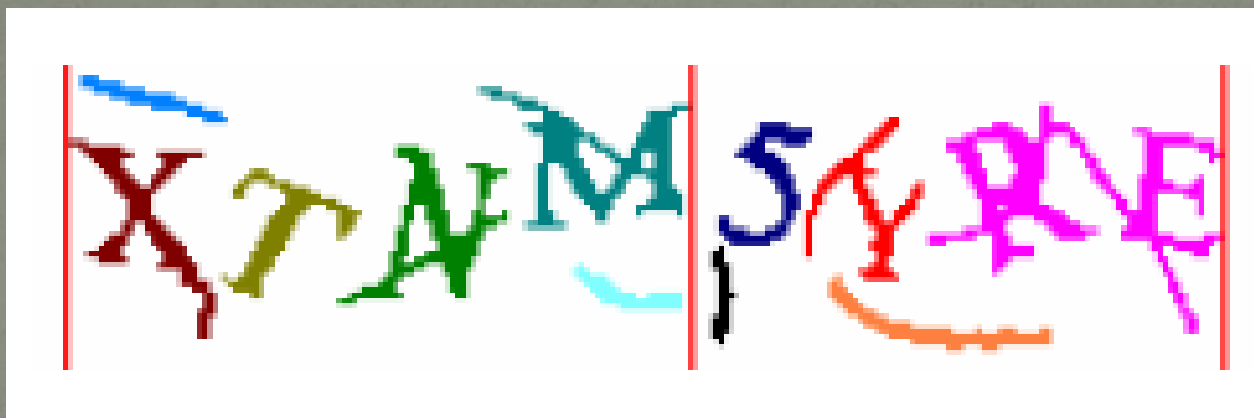
Segmentação Vertical

- Geração de um histograma, calculando a quantidade de pixels pretos por coluna e segmentação nas colunas de valor 0.



Segmentação por coloração

- Coloração aplicada a cada pedaço gerado anteriormente a fim de separar cada pedaço em objetos (cada objeto identificado com uma cor)

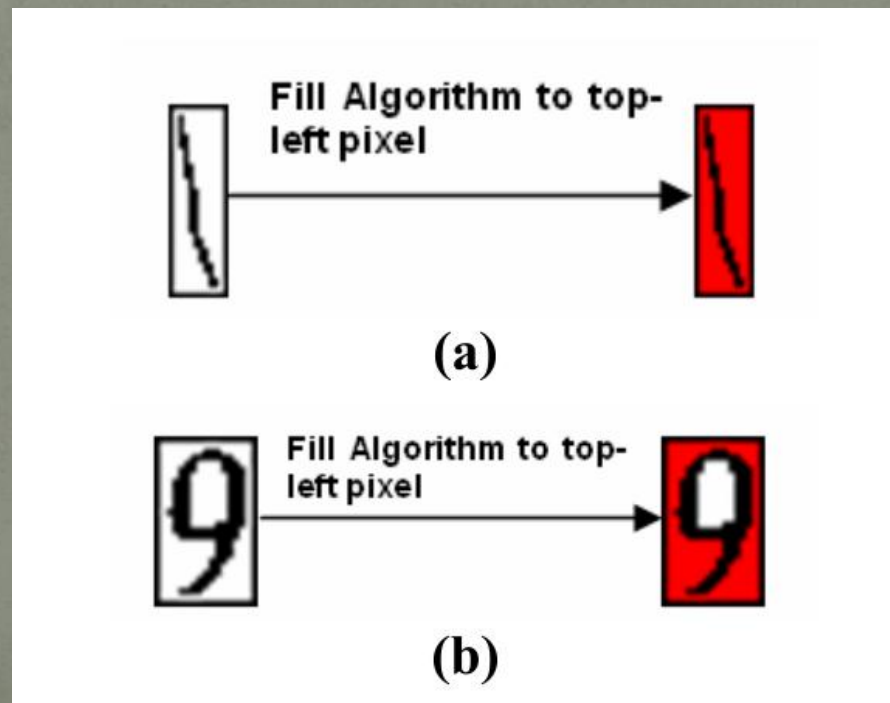


Remoção de Riscos Grossos

- Baseado nas singularidades dos riscos
 - Quantidade de pixels: geralmente poucos
 - Localização: riscos grossos geralmente próximos das bordas e não intersejam caracteres
 - Formato: não possuem “círculos”(curvas fechadas)

Remoção de Riscos Grossos

1. Detecção de círculos por preenchimento. Se objeto contém um círculo, ele não é um risco e os próximos passos são ignorados



Remoção de Riscos Grossos

2. Objetos com menos de 50 pixels são removidos
3. Remoção através da detecção da posição relativa dos objetos. Posição dos caracteres tende a formar uma linha horizontal, logo são removidos objetos acima ou abaixo da linha formada pelos demais



Remoção de Riscos Grossos

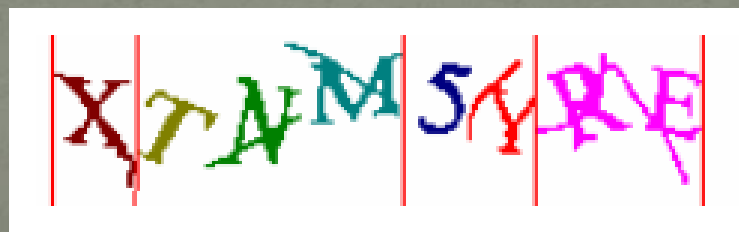
4. Novo histograma e separação vertical por colunas em que a contagem de pixel é o
5. Contagem do número de objetos: caso o número de objetos seja maior que o, remove-se sucessivamente os objetos que não contém círculos com menor número de pixels

Localização de objetos conectados

- Caso o número de objetos for menor que 8, existe pelo menos 2 caracteres ligados em um objeto;
- Por observação notou-se que:
 - Sempre existem 8 caracteres;
 - Conexões sempre são horizontais, nunca verticais;
 - Cada pedaço com mais de 35 pixels possui mais de um objeto;
- Realizada através da relação entre o número de pedaços, o número de objetos e o tamanho dos pedaços.

Localização de objetos conectados

- Por exemplo, num captcha que foi dividido em 4 pedaços existem os seguintes casos:
 1. Quatro pedaços, cada um com 2 objetos;
 2. Um pedaço com 3, dois com 2 e um com 1 caracter;
 3. Um pedaço com 4, um com 2 e dois com 1 caracter;
 4. Dois pedaços com 3 caracteres e dois com 1 caracter;
 5. Um pedaço com 5 caracteres e três com 1 caracter;
- Se três pedaços forem maiores que 35px, elimina-se 3,4 e 5.



Segmentação de Caracteres Conectados

- Após identificar quais pedaços possuem dois ou mais caracteres, simplesmente divide-se o pedaço em partes de tamanho igual de acordo com o número de objetos identificados



Resultados

- Taxa de acerto de 91% no conjunto de exemplo, composto por 100 elementos;
- Taxa de acerto de 92% no conjunto de teste, composto por 500 elementos;

Resultados

- Tipos de falhas encontradas:
 - Alguns arcos grossos não foram detectados e consequentemente não removidos;
 - Algumas letras, como o W, foram entendidas com caracteres conectados quando muito largos.
 - Alguns traços grossos foram reconhecidos como caracteres;
 - O método de segmentar caracteres conectados em partes de igual tamanho nem sempre funciona;

Resultados

- Método rápido e com 92% de acerto, porém somente focado na segmentação dos captchas. Pode ser associado a outro método do estado da arte para reconhecimento dos caracteres.

Speed (ms/challenge)	Average	Max	Min
Sample set	82.8	91.4	81.4
Test set	84.2	95.5	82.8

Resultados em outros trabalhos

- O mesmo método de segmentação, com pequenas modificações, foi aplicado a captchas dos serviços do Yahoo e do Google, com taxas de sucesso de 77% e 12%, respectivamente.
- O resultado acima mostra que o método é totalmente dependente de características específicas da base de dados a ser utilizada como, por exemplo, número fixo de caracteres por captcha.