Phishingerkennung mittels visuellem Ähnlichkeitsvergleich

Felix Hill
Ruhr-Universität Bochum
felix.hill@rub.de

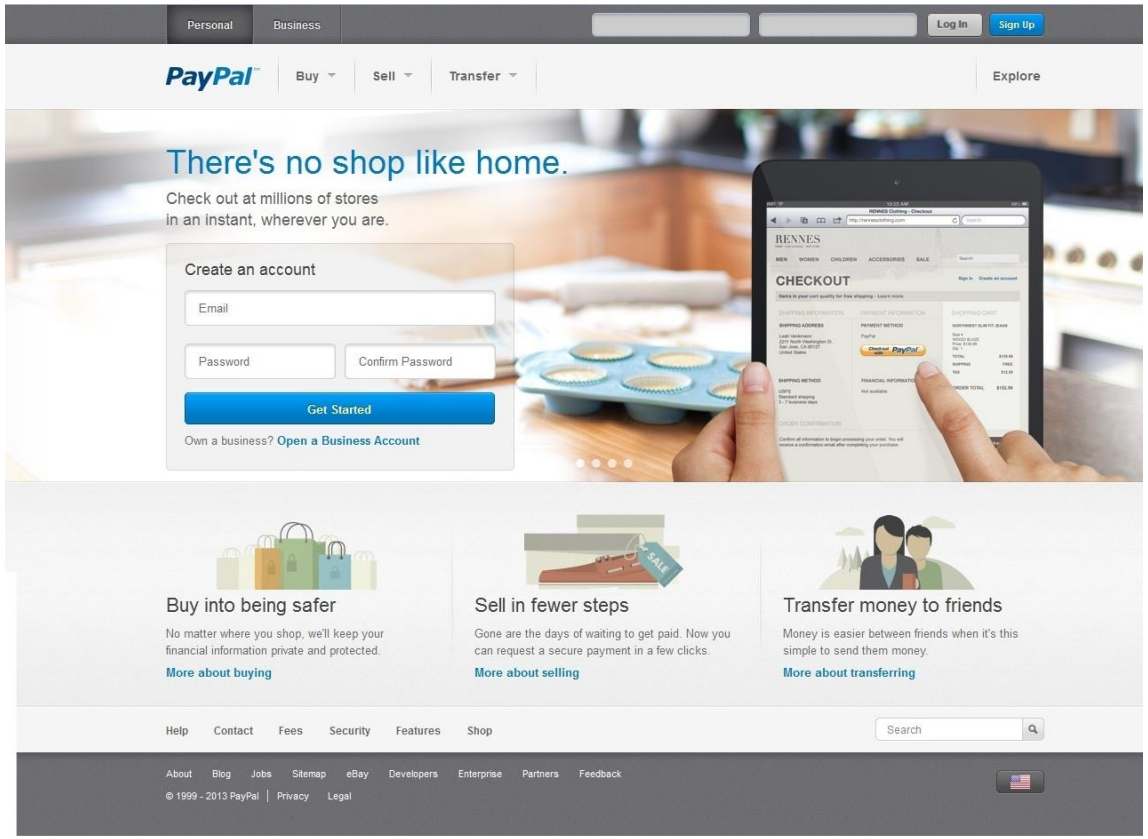
ÜBERSICHT

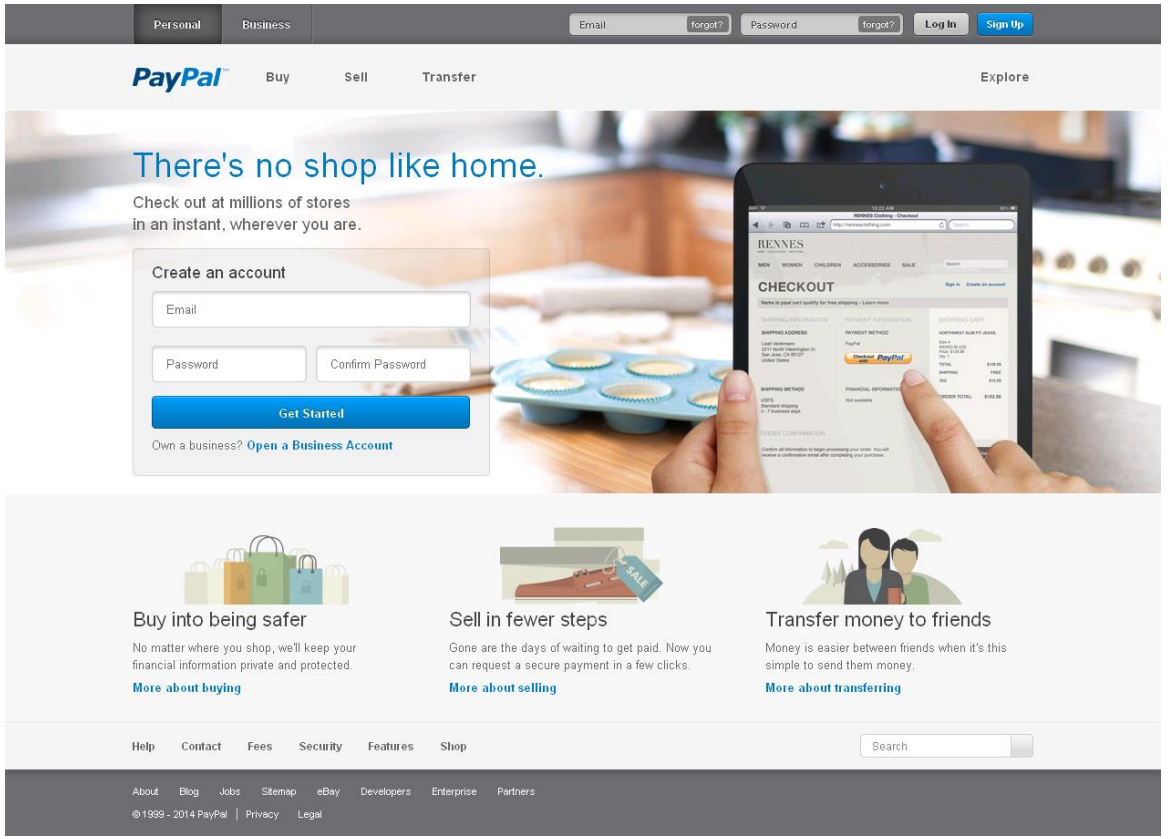
- Entwicklung im Bereich Phishing
- Ansatz
- Bilderkennung
- Evaluation

ENTWICKLUNG IM BEREICH PHISHING

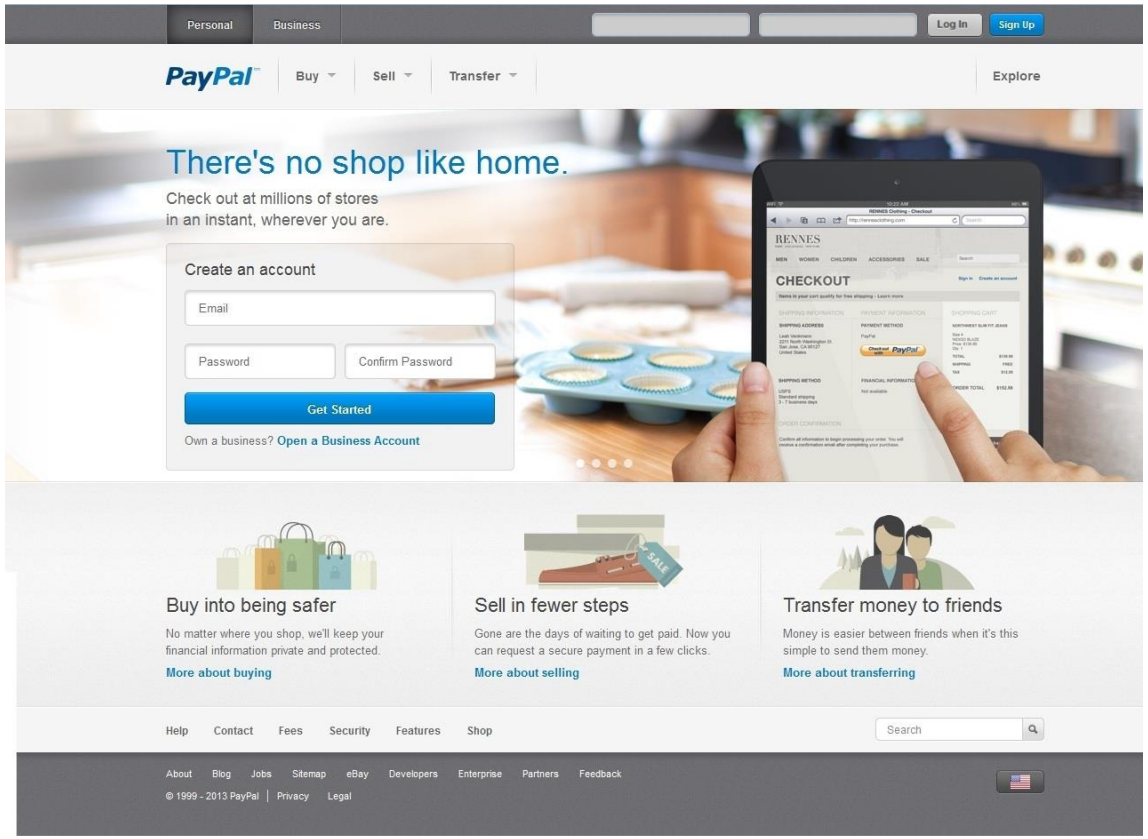
- Phishing immer attraktiver
  - Onlinebanking
  - Onlineshopping
- Phishing schwerer für den Nutzer zu erkennen
  - Weniger Rechtschreibfehler
  - Original Bilder / Layout
- Phishing schwerer automatisiert zu erkennen
  - Quelltext-Obfuskierung durch Javascript, Iframes, Flash…
  - Screenshots der originalen Webseite

ENTWICKLUNG IM BEREICH PHISHING

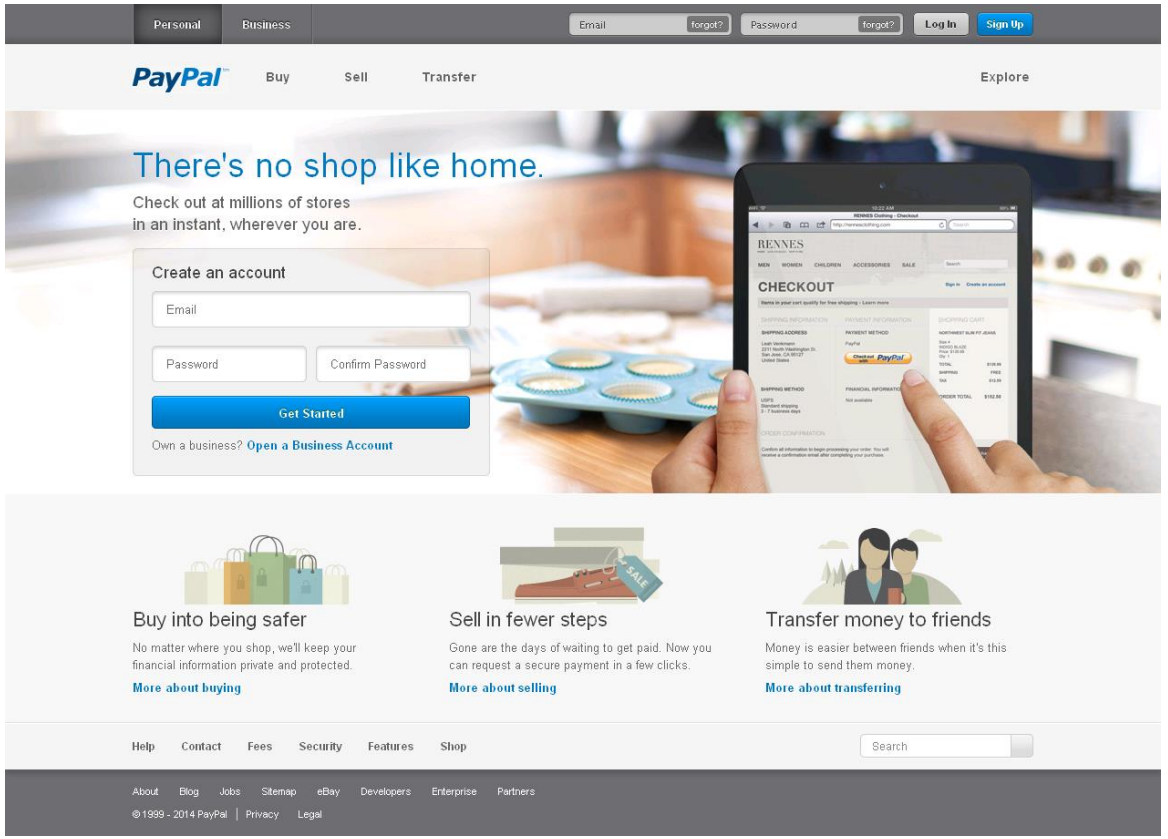




ENTWICKLUNG IM BEREICH PHISHING



Original Webseite 14.01.2014



Phishing Webseite 30.03.2015

ANSATZ

- Ausnutzung der starken Ähnlichkeit der Phishing Webseiten zum Original
- Arbeit auf Daten, die der Nutzer sieht
- Screenshot Vergleich mit originalen Webseiten
  - 100% Vergleich
  - Inhaltsbasierte Bilderkennung
- Ziel: Automatisiertes Klassifikationsverfahren
  - Minimierung der falschen Zuordnungen

ANSATZ: INHALTSBASIERTE BILDERKENNUNG

- Algorithmen, die auf die Merkmale einer Webseite eingehen
- Aus Screenshots Merkmalvektoren extrahieren
- Vektoren miteinander vergleichen
- Pro
  - Unempfindlich gegenüber leichten Änderungen
- Contra
  - Rechenintensive Extraktion
  - Viele Vergleiche von Vektoren
  - Mögliche falsche Zuordnungen

ANSATZ: INHALTSBASIERTE BILDERKENNUNG

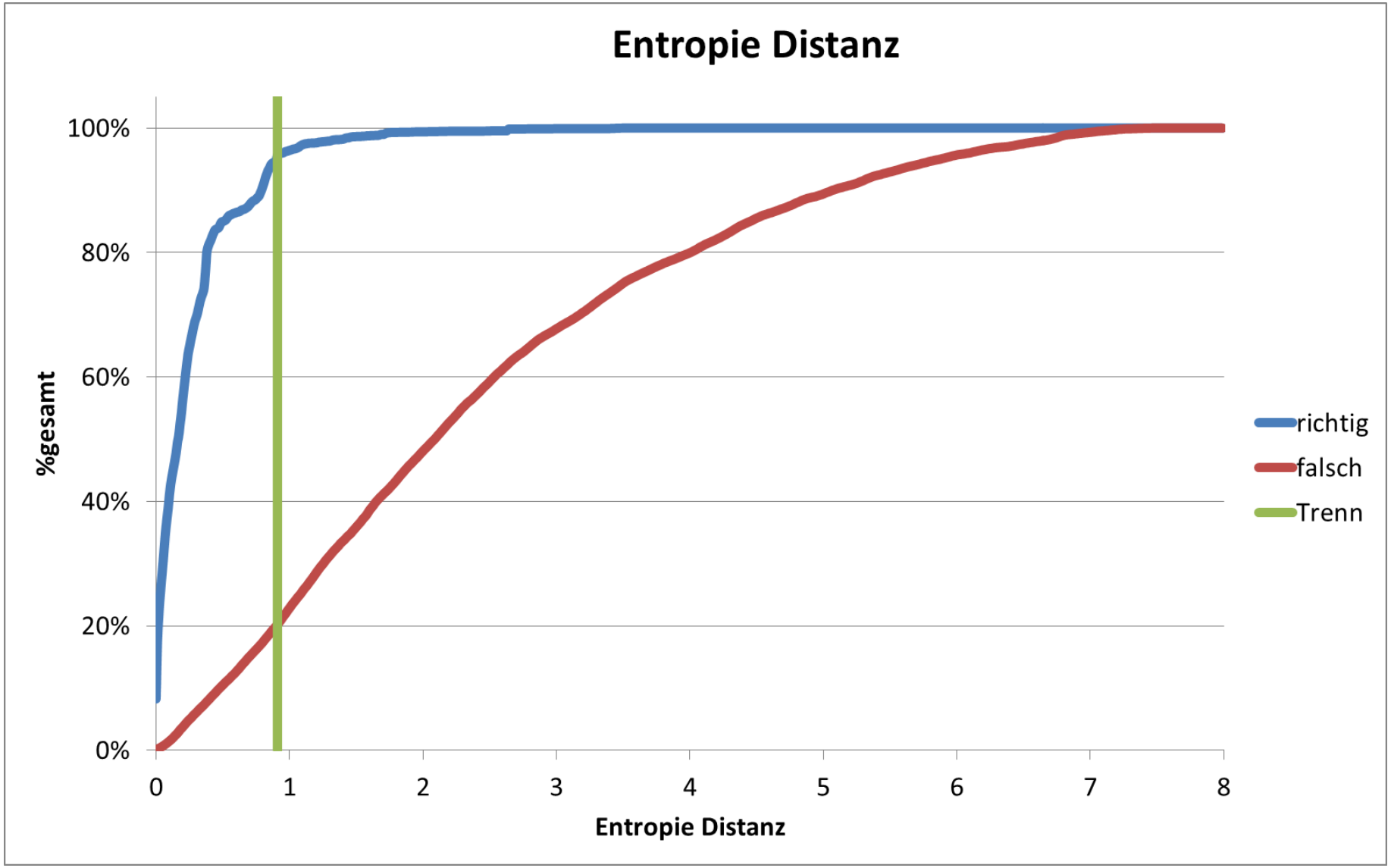
- Algorithmen, die auf die Merkmale einer Webseite eingehen
- Aus Screenshots Merkmalvektoren extrahieren
- Vektoren miteinander vergleichen
- Pro
  - Unempfindlich gegenüber leichten Änderungen
- Contra
  - Rechenintensive Extraktion
  - ~~Viele Vergleiche von Vektoren~~
  - Mögliche falsche Zuordnungen

Vorsortierung der Bilder

VORSORTIERUNG

- Betrachte folgende Attribute:
  - Grau-Entropie
  - Farb-Entropie
  - Weißanteil
  - Anzahl unterscheidbarer Farben
  - Durchschnittshelligkeit
- These: Gleiche Screenshots haben gleiche Attribute
- Betrachte % und totale Abstände

VORSORTIERUNG



VORSORTIERUNG

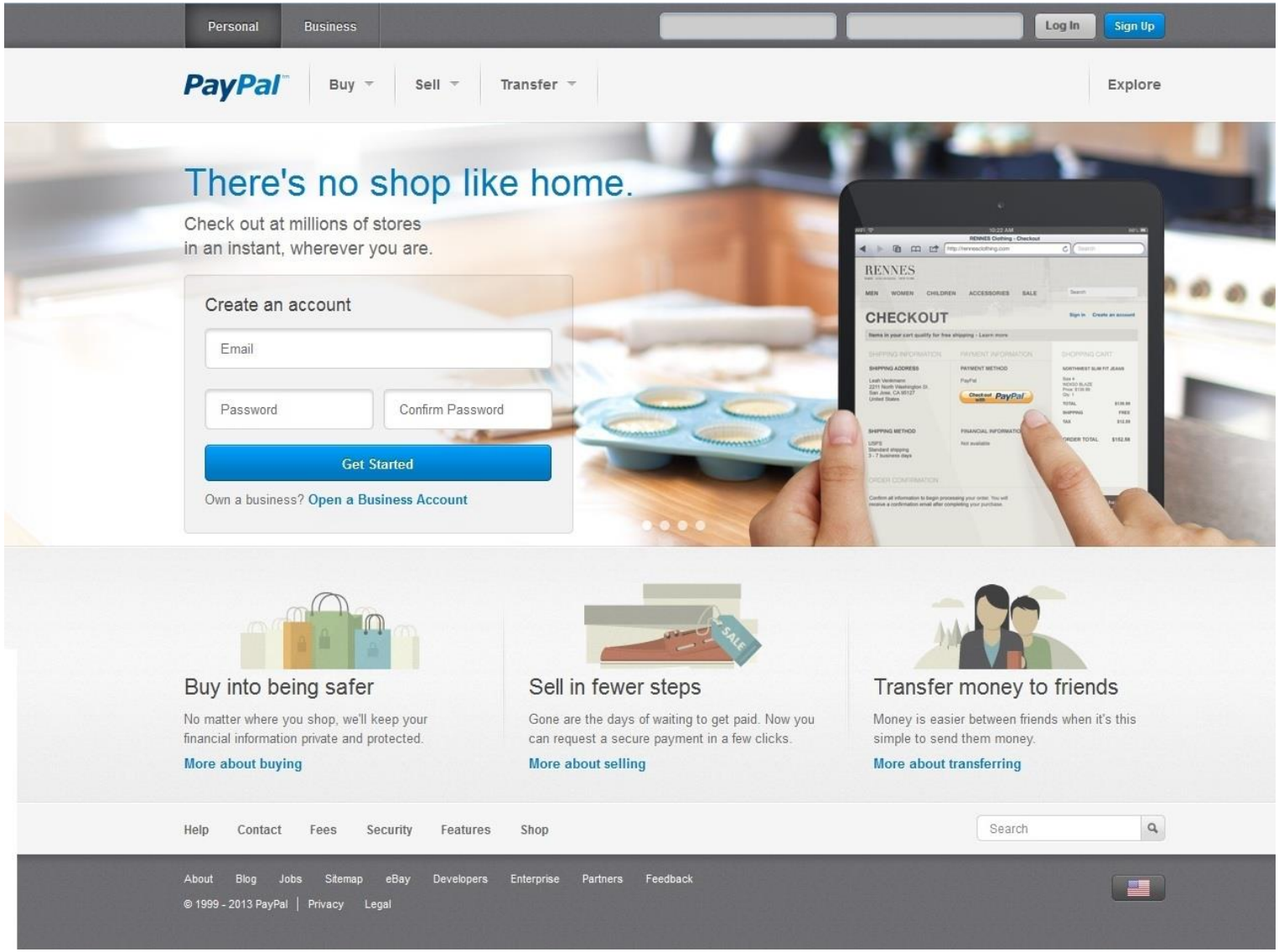
- Trennung bei größter richtig / falsch Distanz
- Ausschluss aller Werte über Trennwert
- Ergebnisse nach Kombination von 6 Attributen
  - Alle Attribute müssen ähnlich sein
  - Behalte 75% der richtigen Zuordnungen (95% der Bilderkennungen)
  - Schließe 99,53% der möglichen falschen Zuordnungen aus

ALGORITHMEN

- 14 verschiedene Algorithmen
  - Inhaltsbasierte Bilderkennungsalgorithmen
  - Erstellung eines Merkmalvektors aus dem Bild
  - Berechnung eines Distanzwertes zwischen Vektoren

- Analyse der ursprünglichen Anwendungsgebiete

MERKMALE EINER WEBSEITE



ALGORITHMEN

- Unpassende Anwendungsgebiete
  - Iriserkennung
  - Fingerabdruckerkennung
  - Rotationserkennung

- Es bleiben 11 Algorithmen für weitere Tests

ALGORITHMEN

- Tests der verbleibenden Algorithmen auf Testset
- Betrachten der Bildpaare nach der Vorsortierung
- Finden eines Schwellwertes für jeden Algorithmus
  - Max. 0.1% falsche Zuordnungen
  - Keine falsche Zuordnung mit Abstand 0

ALGORITHMEN

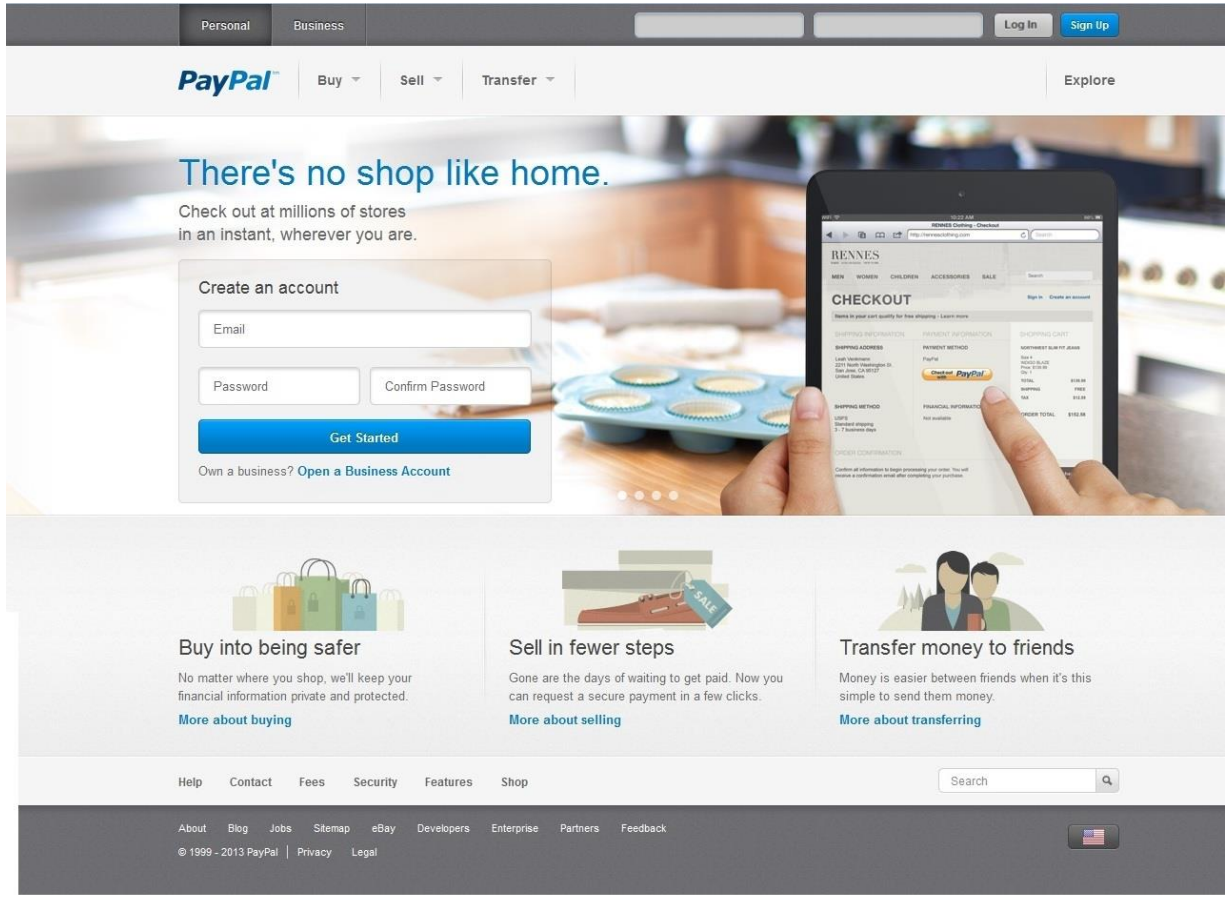
- Es verbleiben 3 Algorithmen:
  - Color Layout Descriptor (CLD)
  - Auto Color Correlogram (ACC)
  - Edge Histogram Descriptor (EHD)
- Hohe Erkennungsraten durch großes Signaturset
- Erkennungsraten:
  - 45-69% Erkennung
  - <0,1% Falschzuordnungen

ALGORITHMEN: CLD

- Entwickelt im MPEG-7 Standard
- Arbeitet auf 8x8 Bild
- Nutzt diskrete Kosinustransformation auf YCbCr Darstellung
- Speichert nur niedrige Frequenzen

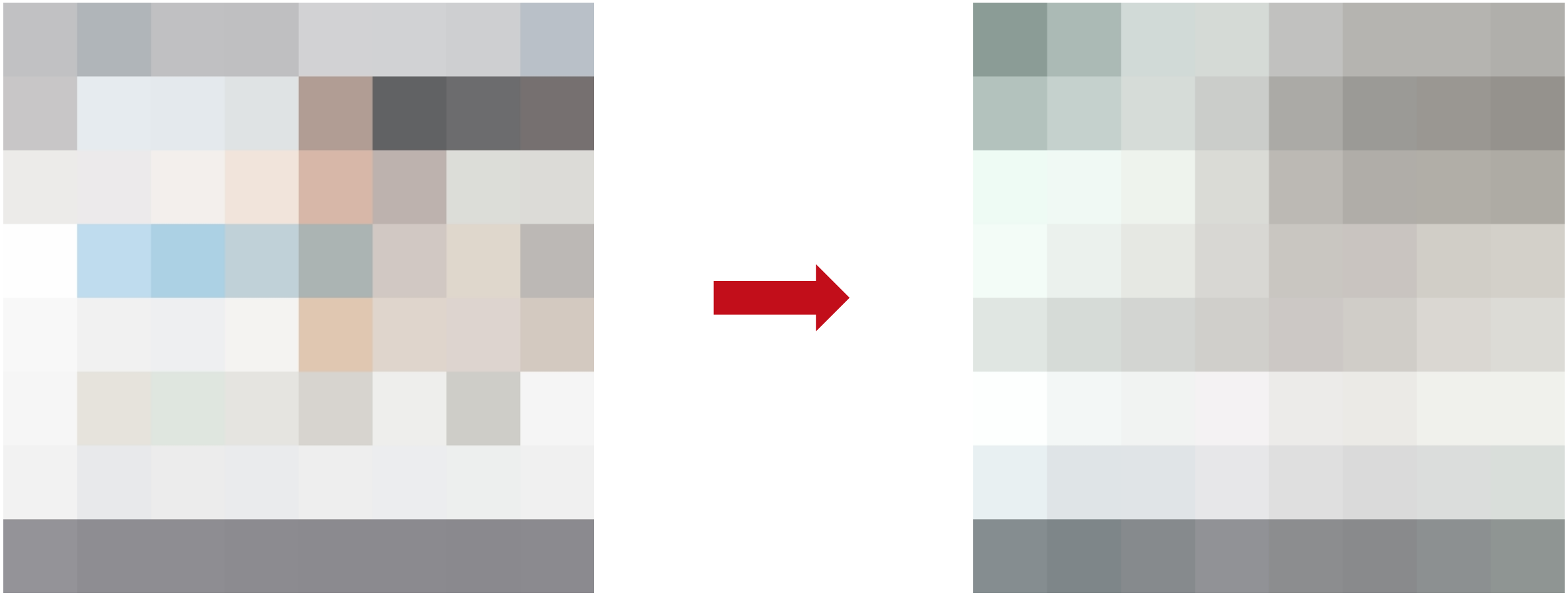
ALGORITHMEN: CLD

- Arbeitet auf 8x8 Bild

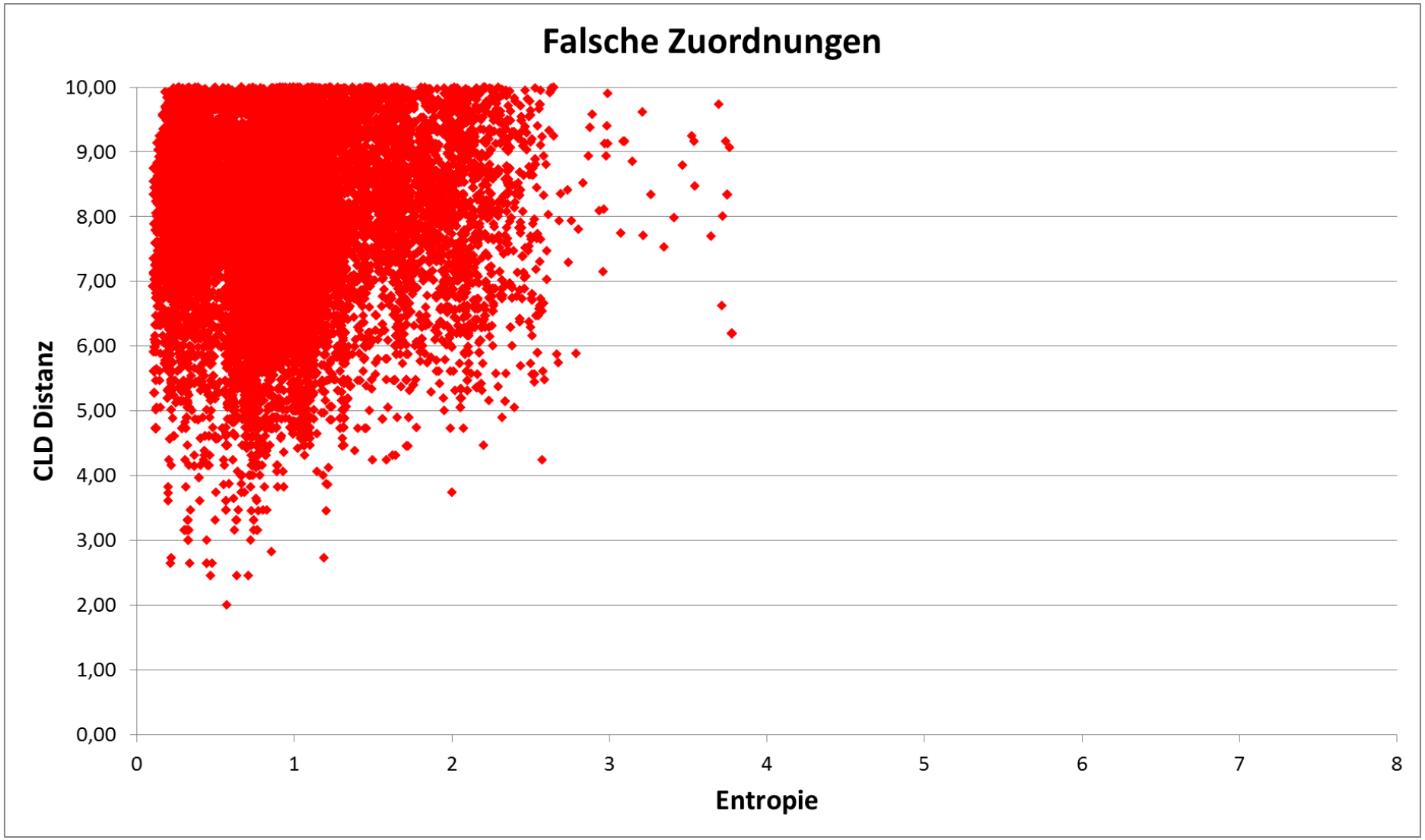


ALGORITHMEN: CLD

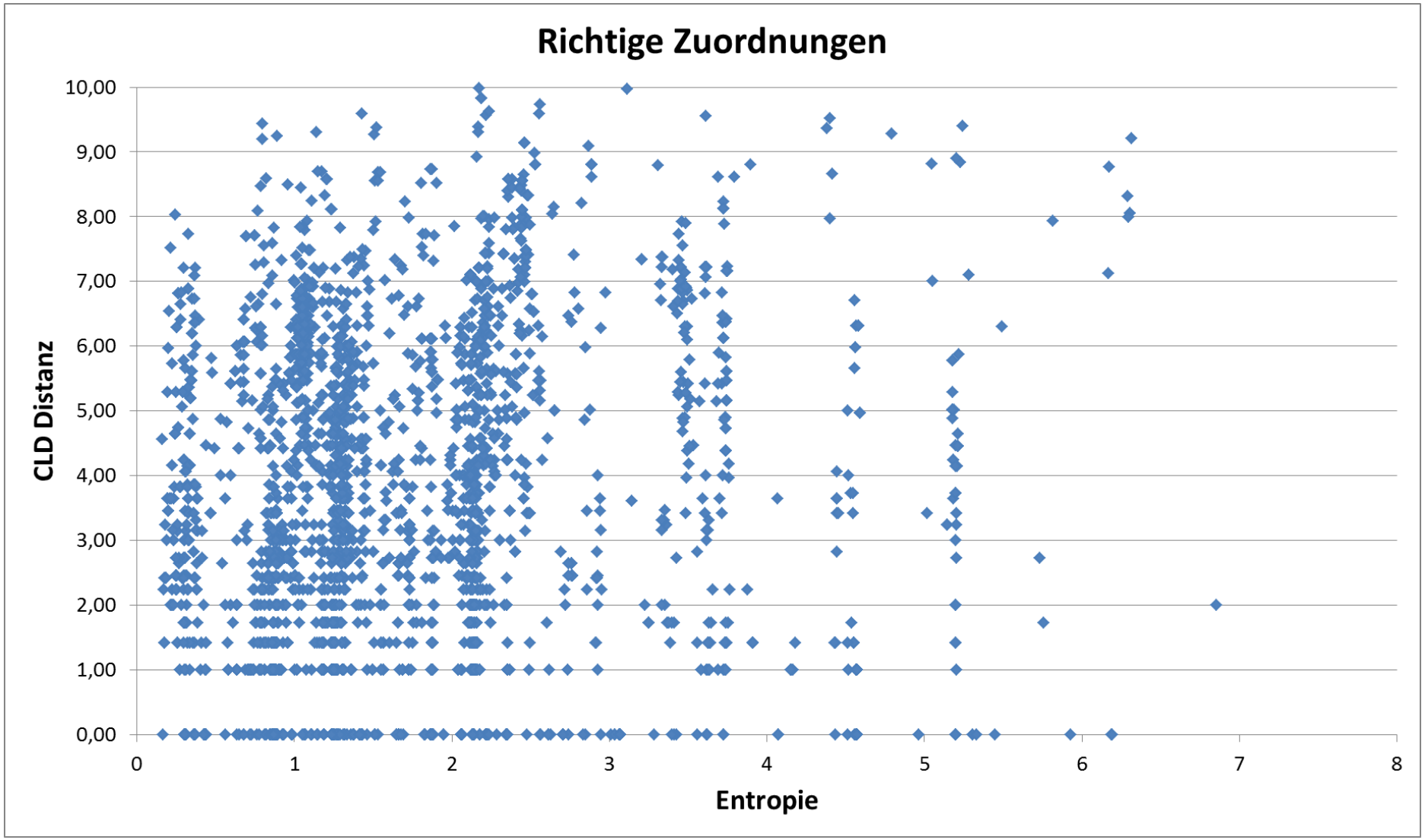
- Speichert nur niedrige Frequenzen



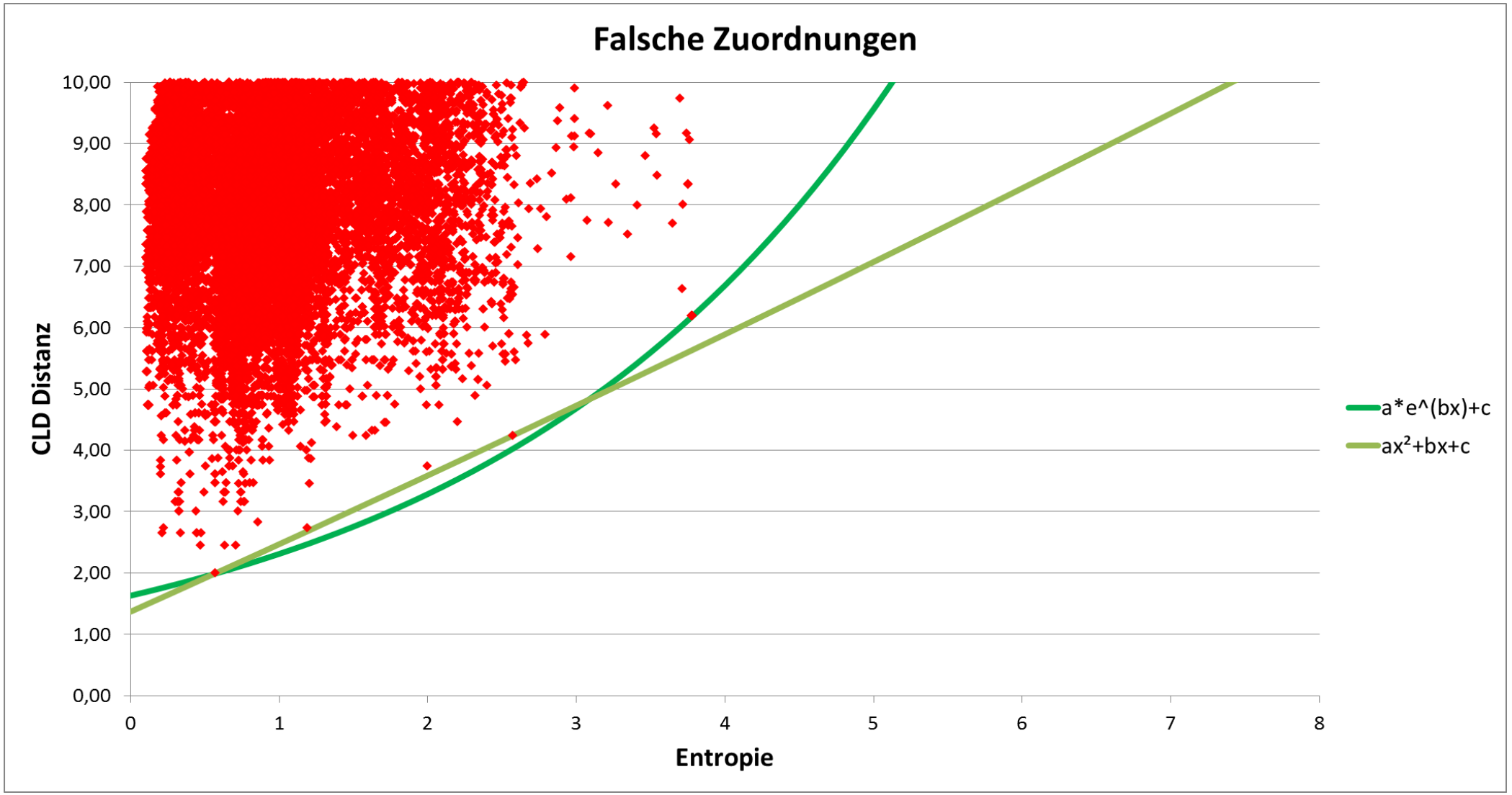
GRENZWERTBESTIMMUNG



GRENZWERTBESTIMMUNG



GRENZWERTBESTIMMUNG



GRENZWERTBESTIMMUNG

- Grenzwerte abhängig von Attributen
  - 5 Grenzwert-Kurven
  - ODER Kombination

	Erkennung statisch	Erkennung dynamisch
CLD	58%	71%
EHD	45%	57%
ACC	69%	85%

GRENZWERTBESTIMMUNG

- Verbesserung der Algorithmen
  - Frequenzfilter verändern
  - Betrachtungsbereich verändern

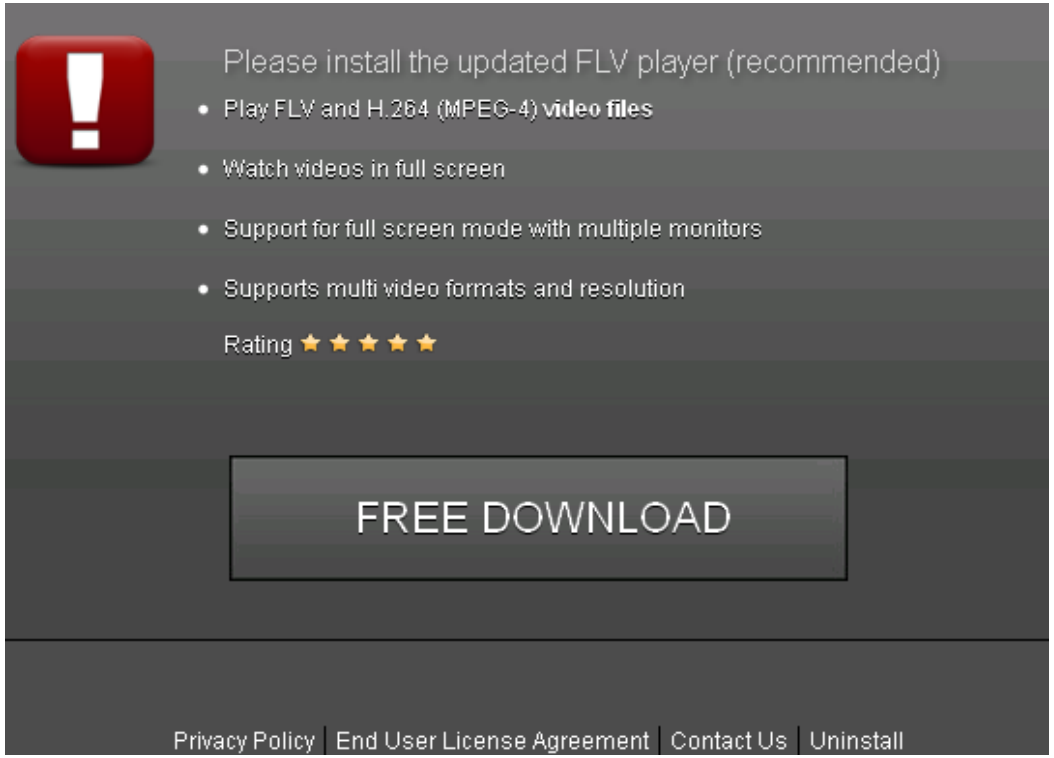
	Erkennung statisch	Erkennung dynamisch	Erkennung dynamisch 2
CLD	58%	71%	77%
EHD	45%	57%	-
ACC	69%	85%	85%

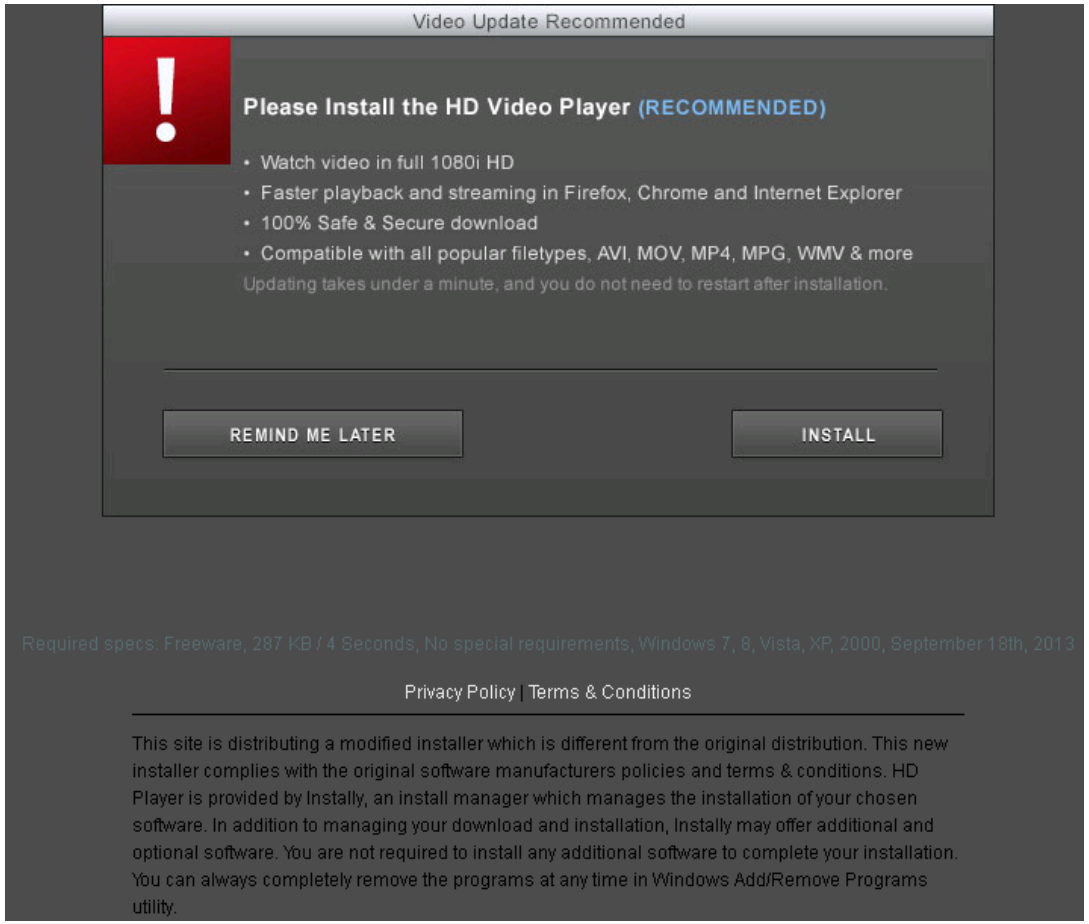
EVALUATION

- Set aus Livedaten
  - Alte Signaturbilder
  - 500.000 Screenshots
  - Nicht nur Webseiten
- EHD und ACC haben hohe FP-Raten
- CLD gute Ergebnisse

EVALUATION: CLD

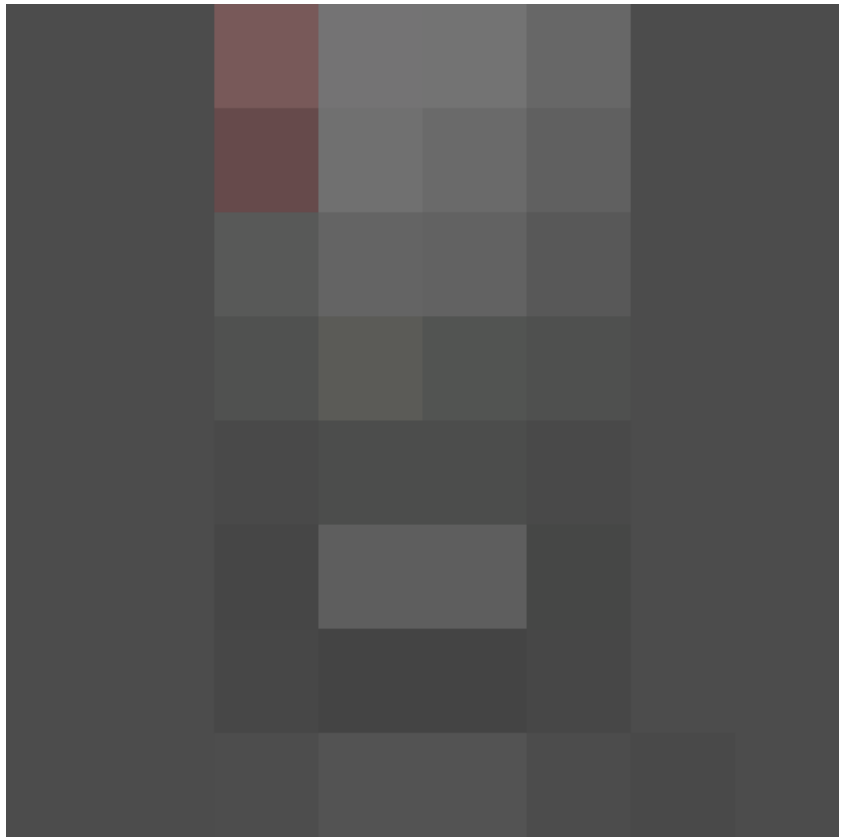
- 33.000 Webseiten erkannt
- 7 falsche Zuordnungen





EVALUATION: CLD

- 33.000 Webseiten erkannt
- 7 falsche Zuordnungen



…VIELEN DANK!

TESTSET

- Signaturset aus 1.500 Screenshots von 811 Webseiten
  - Unterschiedliche Werbung
  - Unterschiedliche Sprachen

- Testset aus 50.000 Screenshots
  - 74.990.258 mögliche falsche Zuordnungen
  - 9.742 mögliche richtige Zuordnungen

ALGORITHMEN: EHD

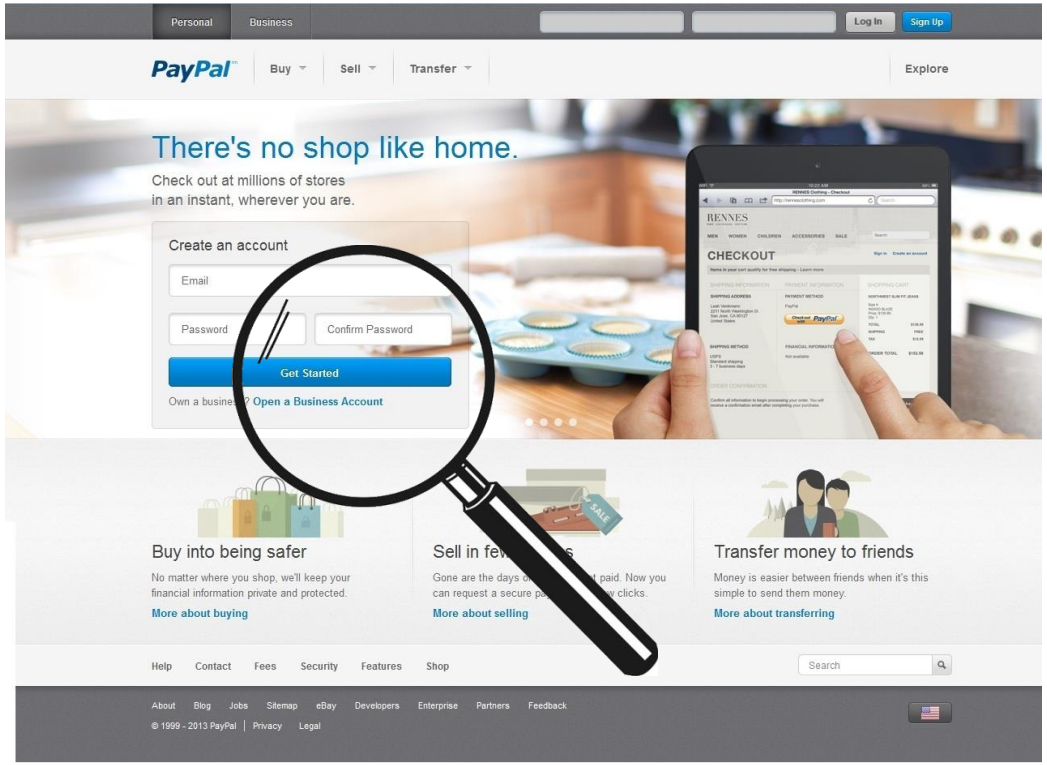
- Im MPEG-7 Standard entwickelt
- Betrachtet Kantenverteilung
  - Globale Kantenverteilung
  - Kanten in 16 Unterbildern
- 5 mögliche Kantenrichtungen
- Farben werden ignoriert
- 45% Erkennung im Test

ALGORITHMEN: ACC

- Betrachtet Farbnachbarschaft
  - Nachbarschaft eines Bildpunktes
  - Bis zu 3 Punkte entfernt
  - Zählt nur Punkte gleicher Farbe
- Positionsunabhängig
- 69% Erkennung im Test

ALGORITHMEN: ACC

- Betrachtet Farbnachbarschaft

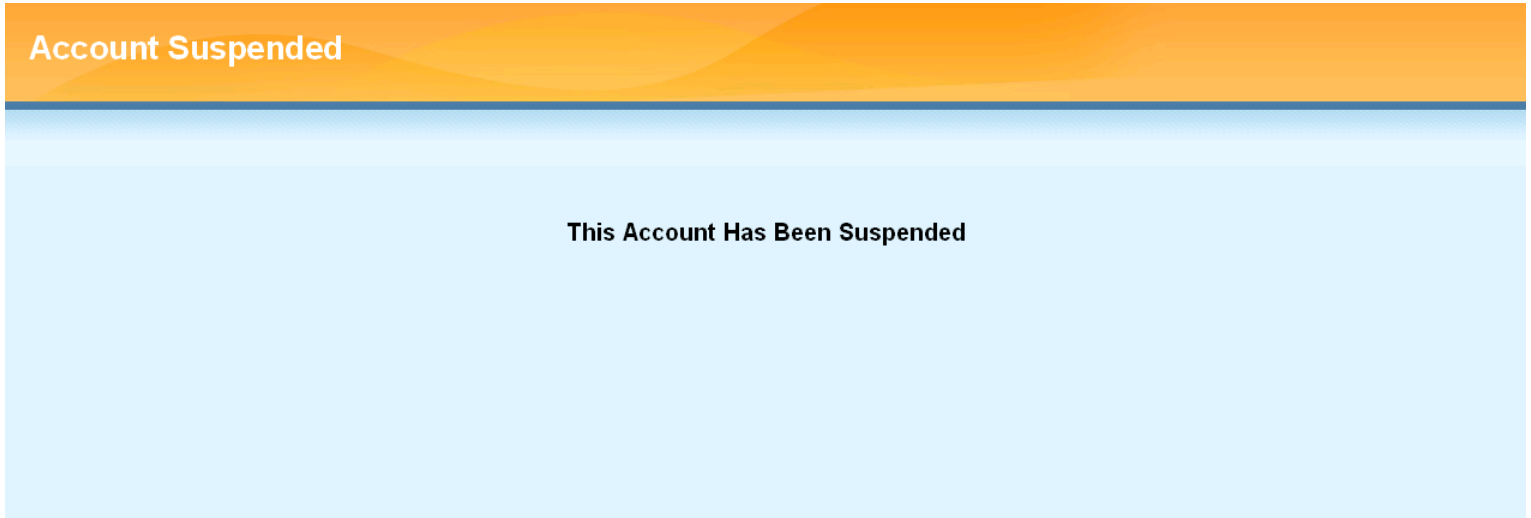


EVALUATION: EHD

- Grundannahme:
  - Kantenerkennung reicht, um eine Webseite zu identifizieren
  - Probleme bei gleich aufgebauten Webseiten

- Es kommt zu fehlerhaften Zuordnungen mit geringer Distanz
  - Algorithmus ist nicht automatisiert nutzbar

EVALUATION: EHD



EVALUATION: ACC

- Grundannahme:
  - Farbnachbarschaft genügt, um eine Webseite zu identifizieren
  - Probleme bei gleichfarbigen Seiten

- Es kommt zu fehlerhaften Zuordnungen mit geringer Distanz
  - Webseiten mit ausschließlich Textinhalten werden einander zugeordnet
  - Signaturset darf keine Webseiten ohne Farbinhalt enthalten

EVALUATION: ACC

Strict Standards: Non-static method JLoader::import() should not be called statically in **/home/octify/public_html/libraries/joomla/import.php** on line **29**

Strict Standards: Non-static method JLoader::register() should not be called statically in **/home/octify/public_html/libraries/loader.php** on line **71**

Strict Standards: Non-static method JLoader::import() should not be called statically in **/home/octify/public_html/libraries/joomla/import.php** on line **32**

ATENÇÃO

O endereço IP de sua conexão encontra-se bloqueado neste servidor.
Leia atentamente as informações abaixo para evitar recorrencia deste bloqueio.

Por que isto ocorre?

Os principais motivos de bloqueios são

1. Erros consecutivos de senha ou usuário no login nos serviços **cPanel**, **WebMail**, **WHM**, **FTP**, **E-mail (SMTP, POP e IMAP)** ou **diretórios protegidos pelo serviço HTTP (sites protegidos por senha)**.
2. Contas de email configuradas com senha ou login incorretos em clientes de email local tais como Outlook, Thunderbird ou similares.
3. Ocorrência de alguma ação suspeita ou acesso não autorizado a partir do seu IP.
4. Excesso de conexões ao serviço de email **POP3** (acima de 60 conexões por hora), para previnir este tipo de bloqueio aumente o intervalo de checagem de novos e-mails em seu cliente de e-mail para ao menos uma vez a cada 5 minutos.
5. **Mais de 50 conexões simultâneas ao Serviço HTTP (acesso a páginas)** a partir de um mesmo endereço IP, comum em usuários de internet a rádio ou em empresas que compartilham a mesma conexão de internet para todos os usuários da rede.

O que devo fazer?

A maioria dos bloqueios são temporários e tem limite de aproximadadamente 5 minutos, caso continue a ver esta mensagem mesmo após este período entre em contato com seu serviço de hospedagem.

Dados de seu acesso

IP bloqueado: **91.52.210.197**

Site acessado: **www.transpavimentacao.com.br**

Data: **Sexta-feira, 20 de Dezembro de 2013**

Caso seja necessário entrar em contato com o suporte informe os dados acima.

AUSBLICK

- Automatisierte Erkennung im Browser
- Erkennung von Phishingtrends / neuen Kampagnen
  - Clustering der Daten eines Eingangsstroms

FORSCHUNGSSTAND

- Visuelle Erkennung möglich

- ABER: In der Praxis nicht eigenständig nutzbar
  - Zu viele falsche Erkennungen (11%)

FORSCHUNGSSTAND

- Visuelle Erkennung möglich

- ABER: In der Praxis nicht eigenständig nutzbar
  - Zu viele falsche Erkennungen (11%)