Partielle Verschlüsselung von JPEG2000 Fingerprints

By the pricking of my thumbs,
something wicked this way comes.

M. Draschl , S. Ramp , M. Perfler

Inhalt

- Motivation und Ziele
- Jpeg2000 Bildformat
- NIST Fingerprint Matching Suite
- Workflow und Ergebnisse

Motivation und Ziele

- Partielle Verschlüsselung von Fingerprints
- Verminderung der Matching-Genauigkeit
- Ermitteln einer Mindest-Verschlüsselungs-Rate

JPG 2000 Bildformat

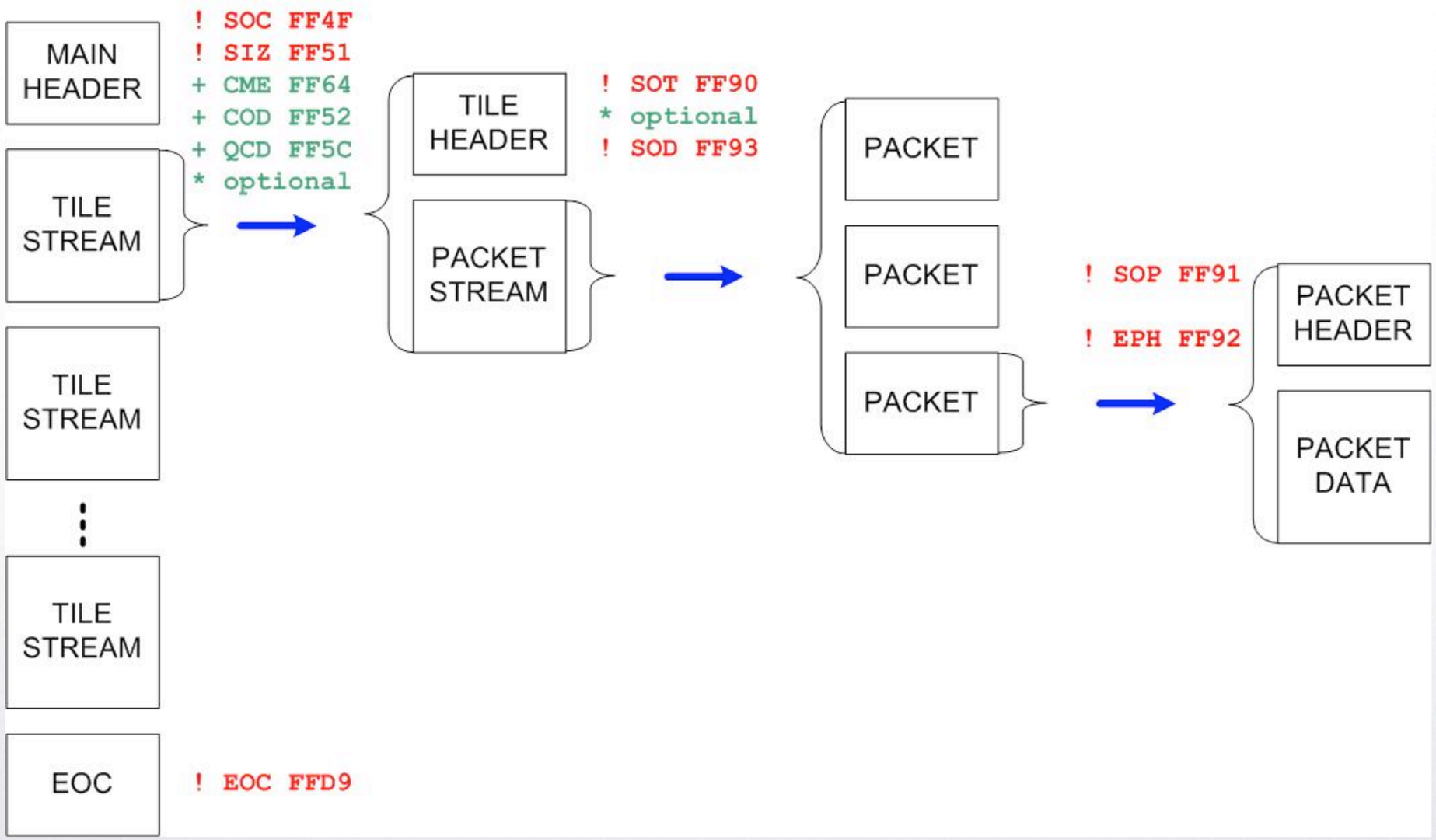
- Nachfolger JPG, mit verlustloser Kompression
- Keine Artefaktbildung (JPG: 8x8)
- Erweitertes Featureset (RoI,..)

Encoding

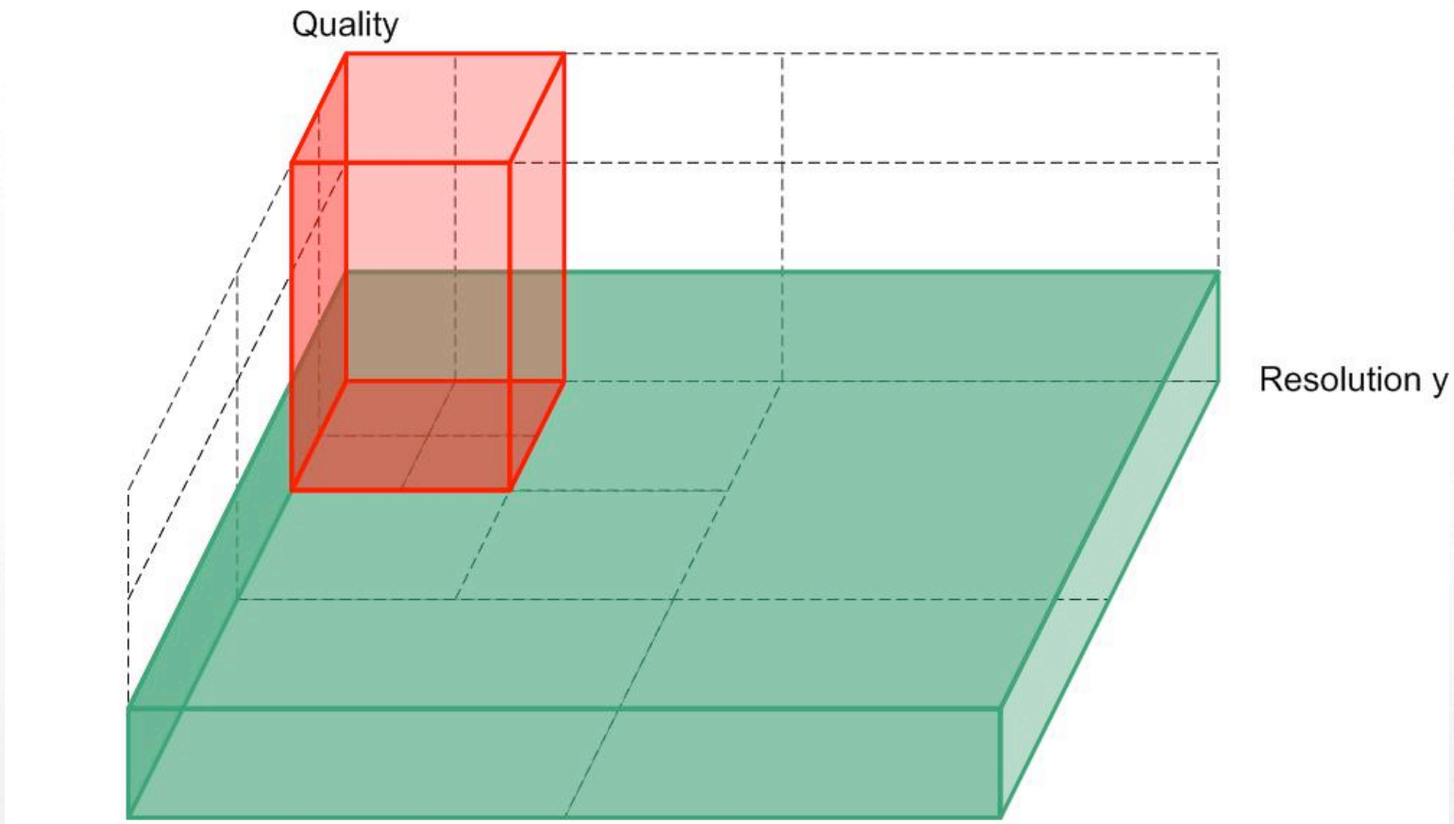
- Tile-ing & Padding
- Wavelet Transformation

  (Hoch- / Tiefpass)
- Quantisierung
- Codierung

Codestream Aufbau



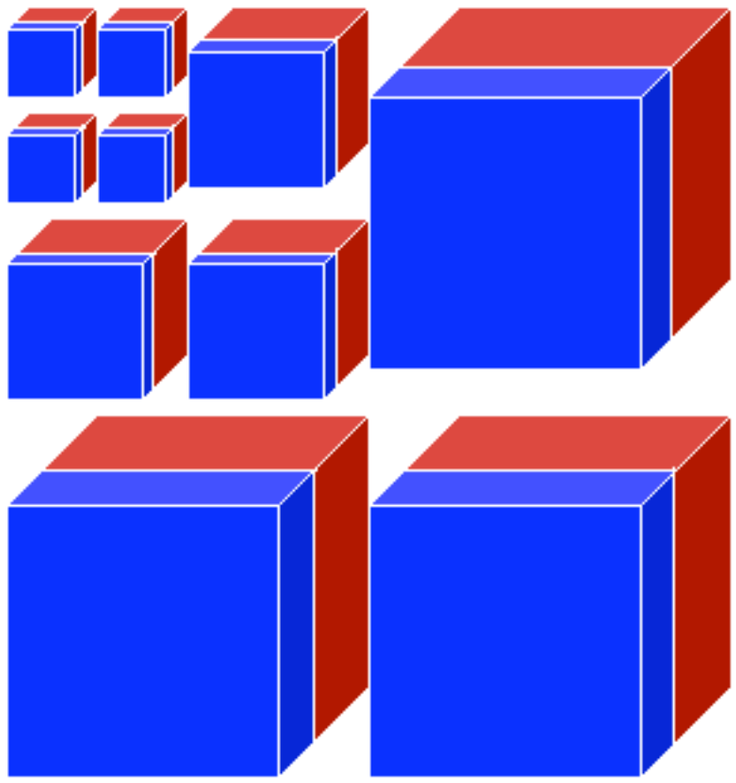
Codestream - Progression



RLCP – wachsende Auflösung

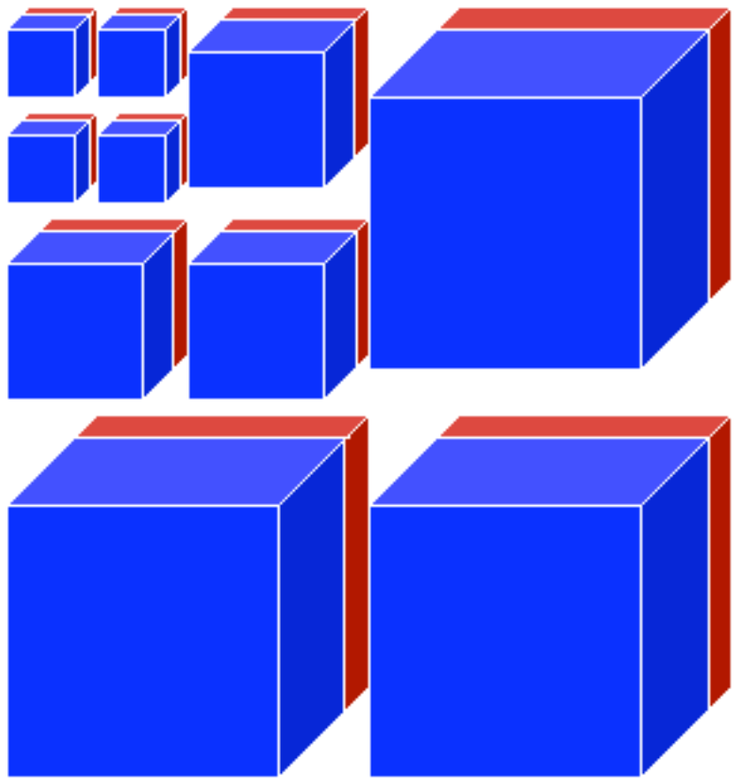
LRCP – steigende Qualität

Codestream LRCP



Quelle: http:/JJ2000.epfl.ch

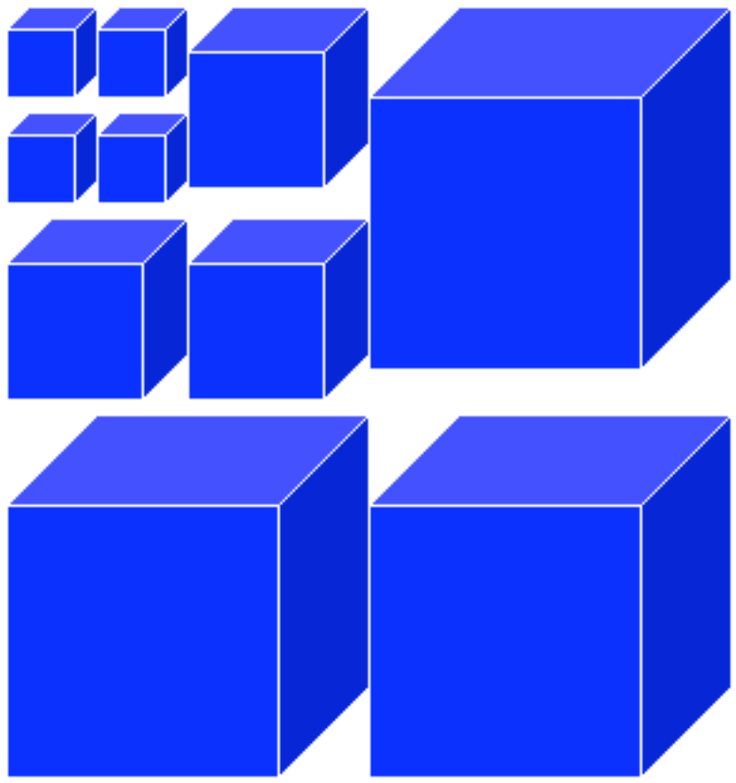
Codestream LRCP



Quelle: http:/JJ2000.epfl.ch

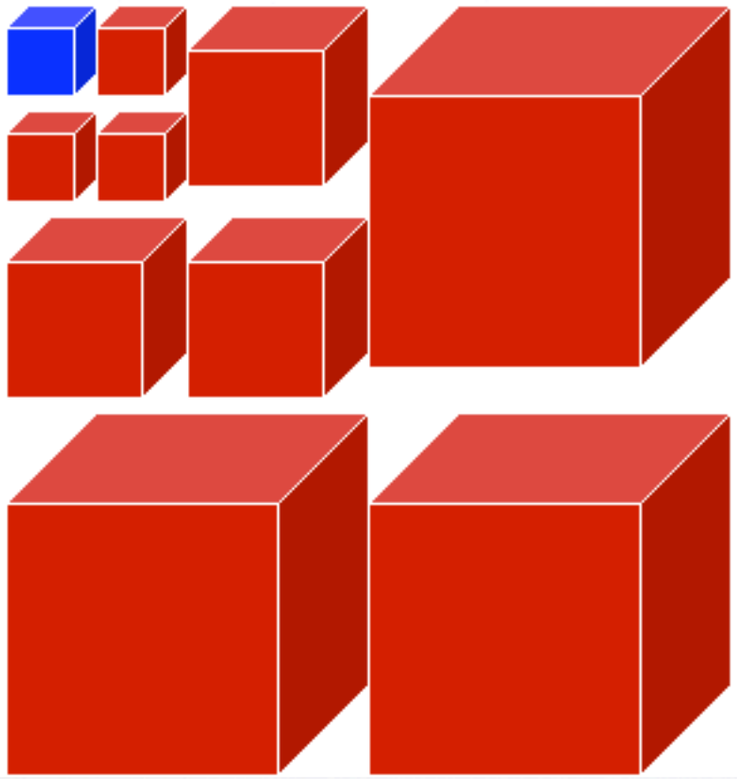
Jpeg2000

Codestream LRCP



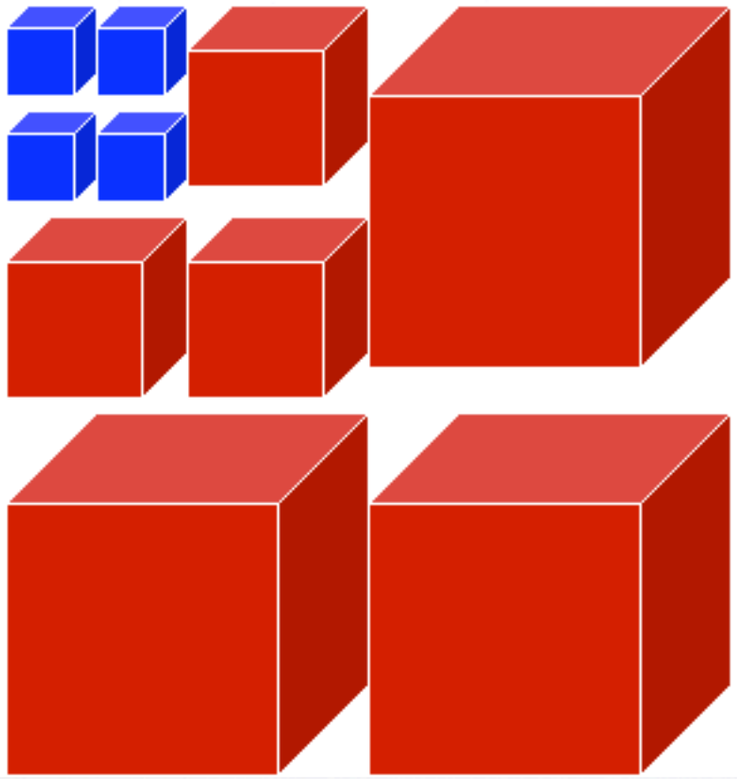
Quelle: http:/JJ2000.epfl.ch

Codestream RLCP



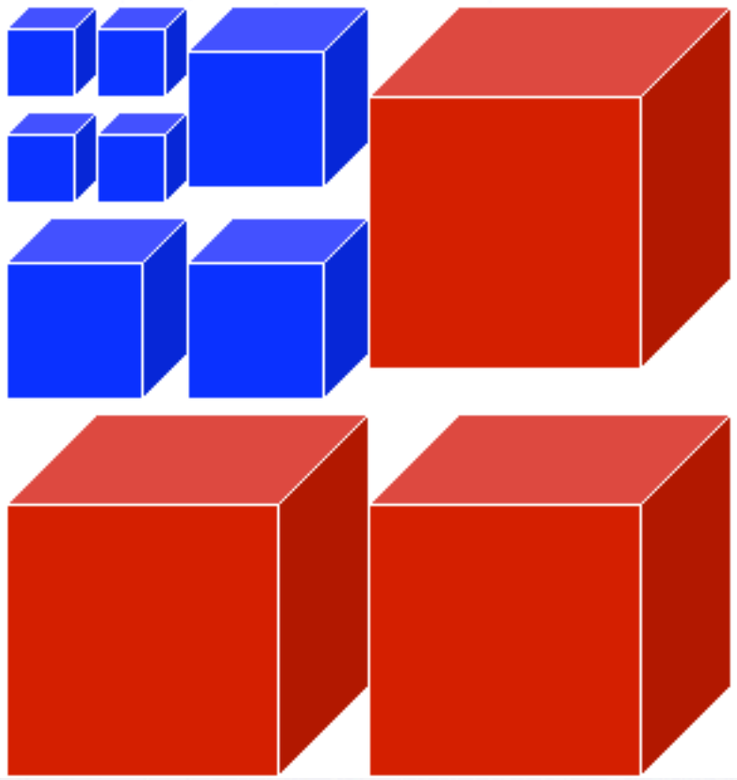
Quelle: http:/JJ2000.epfl.ch

Codestream RLCP



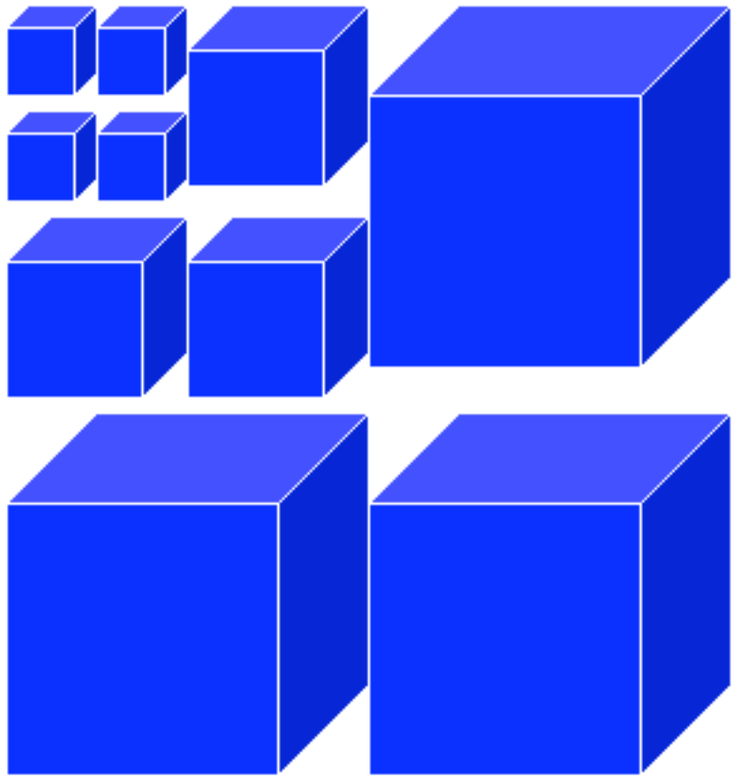
Quelle: http:/JJ2000.epfl.ch

Codestream RLCP



Quelle: http:/JJ2000.epfl.ch

Codestream RLCP



Quelle: http:/JJ2000.epfl.ch

NIST Fingerprint Matching Suite

- FBI: 60k Fingerprint Anfragen / Tag
- Zusammenarbeit mit
  National Institute of Standards and Technology (NIST)
- nach 911 besonderes Augenmerk (Patriot Act)
- NFIS2

Applikationen

- Preprocessing:

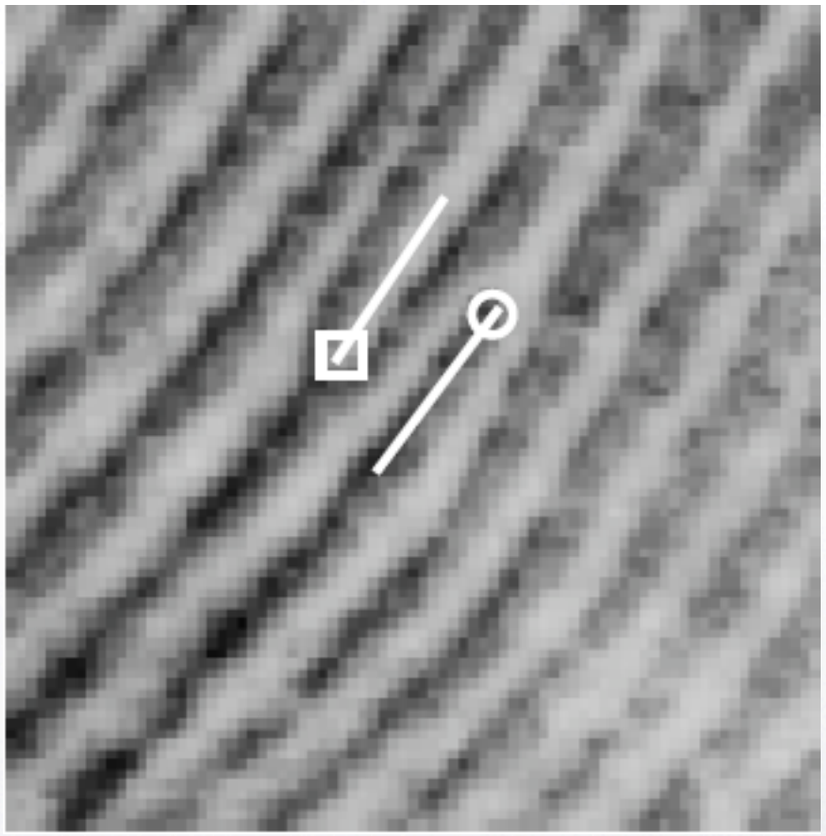
  - cjpgl
  - nfiq
  - mindtct

- Matching:

  - bozorth3

NFIS2

Fingerprints



Quelle: NFIS2 Documentation (S11, S12)

mindtct - Ablauf

- Generating Image Maps:

  - Direction Maps
  - Low contrast Maps
  - Low flow Maps
  - High Curve Maps
  - Quality Maps

mindtct - Ablauf

- Umwandlung in binäres S/W-Bild
  Direction-Map

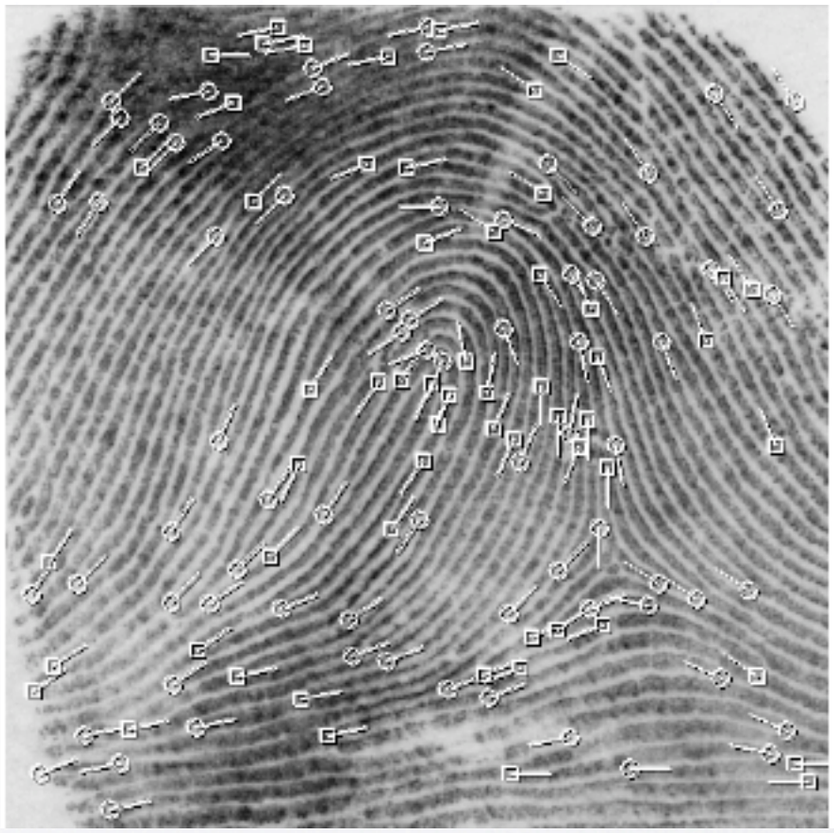
- Minutien Erkennen
  Vordefinierte Patterns

- Falsche Minutien entfernen
  Inseln, Löcher, Ausbuchtungen, Haken

mindtct - Ausgabe

x	y	°	q
147	119	225	6
188	134	157	8
197	175	169	18
202	203	180	21

~100 Zeilen pro Finger



Quelle: NFIS2 Documentation (S.77)

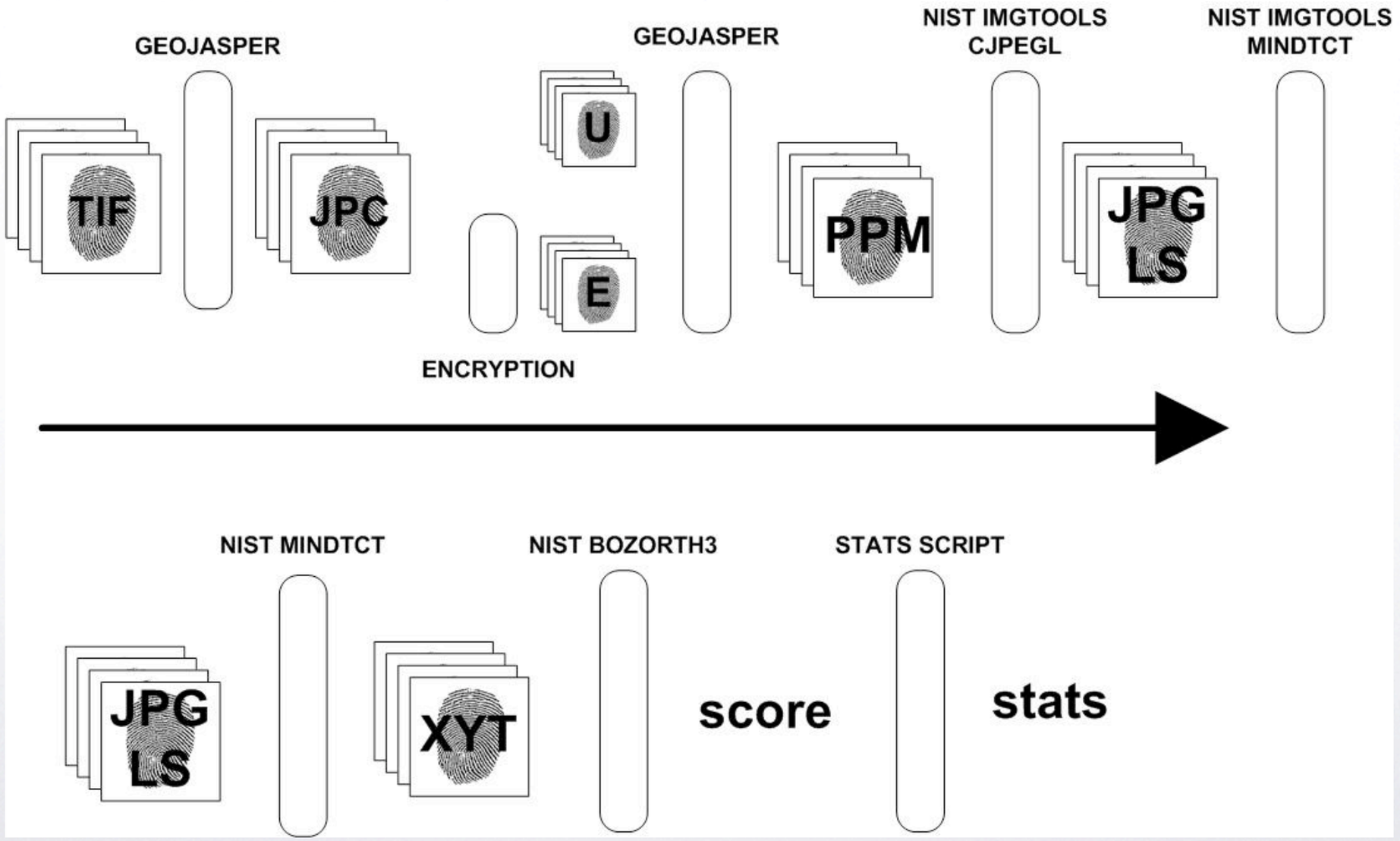
bozorth3

- 1:1 und 1:n Vergleiche

- Schlüsselwerte:
  - Koordinaten und Winkel
  - Unabhänging von Bilddrehung, Skalierung

- Berechnung:
  - 2 Tabellen zur Berechnung
  - Vergleichen und Bilden einer Kompatibilitätstabelle
  - Bereinigen und Finden von gleichen Clustern

Workflow und Ergebnisse



Segmentation Symbols

no segsym

with segsym

Testbed

- Hardware:
  - Server: HP-DL380G5, 4x2GHz CPU, 9GB RAM,
  - Storage: IBM DS4700 SAN, 4GBit/s Fibre Channel Connect.
  - OS: Debian Stable, Kernel 2.4.27-SMP, Installation auf VMWare ESX 3
  - Zugriff über SSH
- Verwendung aller 4 CPUs beim Matching

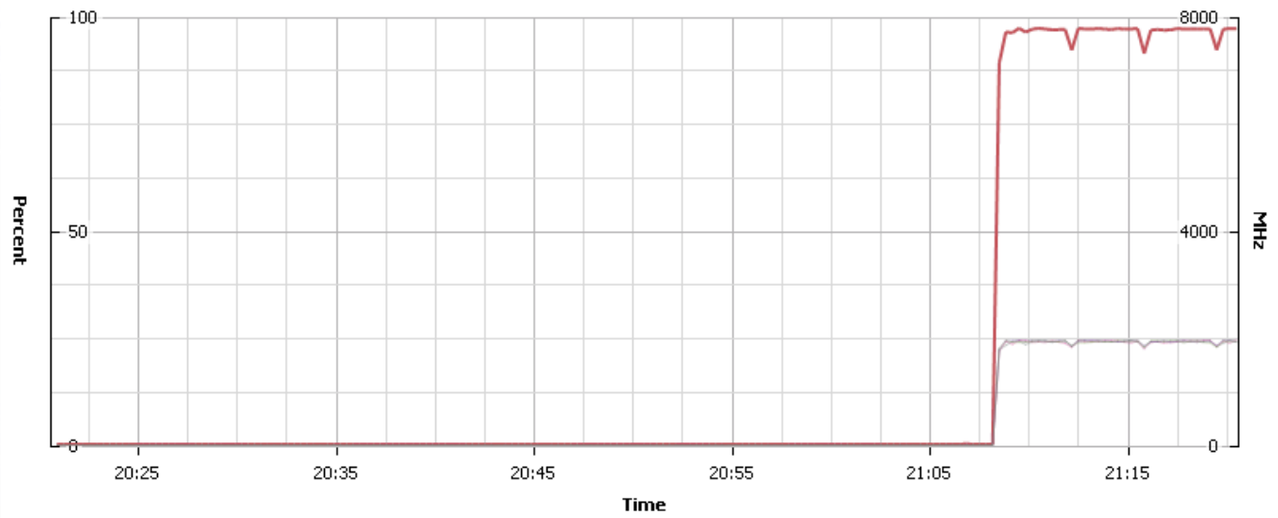
Testdurchführung

- Entwicklung der Matching Tools auf Parallelisierung
- ~50GB an Bilddaten
- ~5h Matching Durchlaufzeit
- 100 Fingerprint Sets á 8 Files

2 Encoding Modi (LRCP, RLCP)

20 Encryption Levels

= 32.000 Files (~240k Matches)

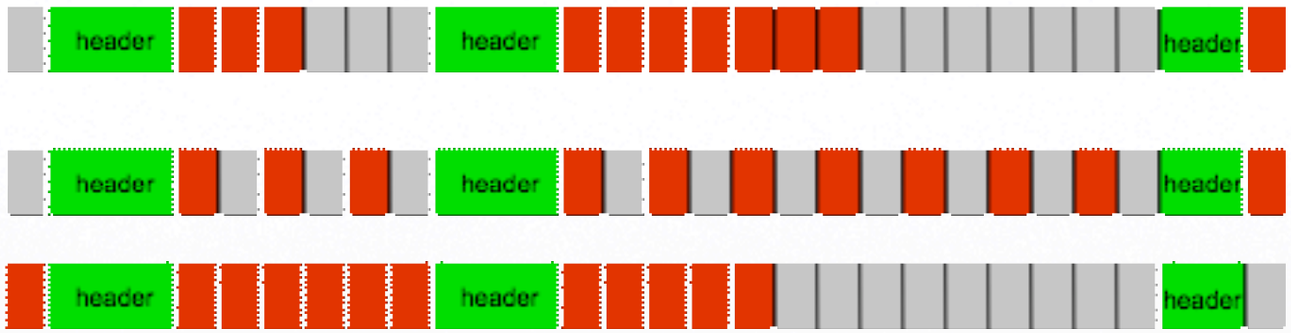


Performance Chart Legend

Key	Object	Measurement	Units	Latest	Maximum	Minimum	Average
	(Perfler) Debian...	CPU Usage (Average/Rate)	Percent	97,53	97,64	0,24	20,09
	(Perfler) Debian...	CPU Usage in MHz (Average/Rate)	MHz	7802	7811	19	1607,39
	0	CPU Usage in MHz (Average/Rate)	MHz	1974	1974	7	402,55
	1	CPU Usage in MHz (Average/Rate)	MHz	1952	1969	2	399,85
	2	CPU Usage in MHz (Average/Rate)	MHz	1933	1970	2	400,97
	3	CPU Usage in MHz (Average/Rate)	MHz	1938	1959	2	399,49

Bilddatenverschlüsselung

- Verschlüsselungsvarianten
  - Sequential
  - Distributed
  - Absolute

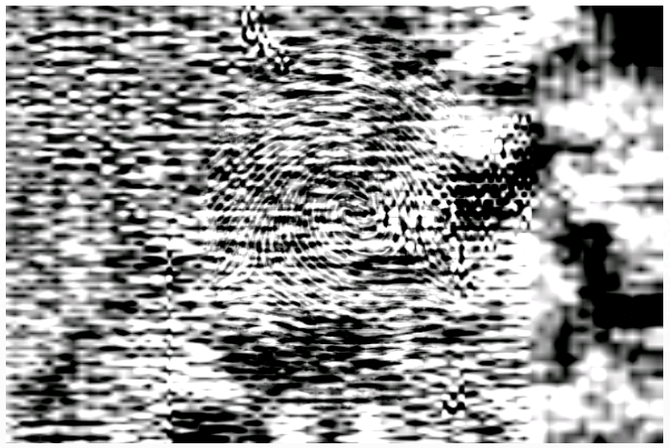


- Warum Absolute Encryption ?
  - Absolute Encryption erlaubt einfachere (schnellere) Verschlüsselung
  - Annahme: Begrenzte Ressourcen (CPU, Speicher) auf Fingerprint Reader

Workflow

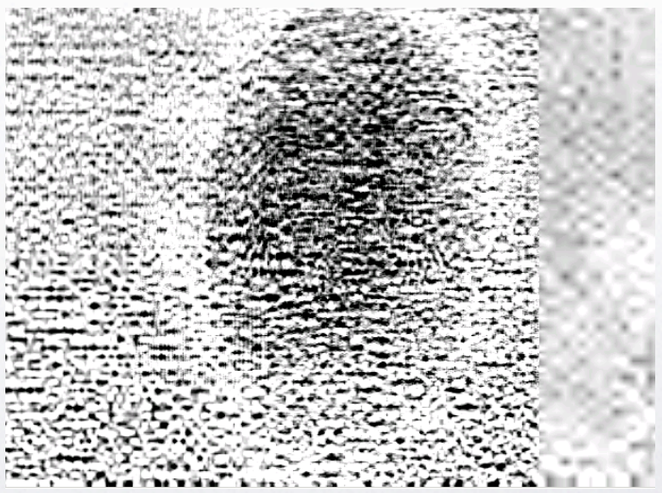
Visueller Vergleich

Unencrypted Fingerprint



Absolute Encryption 2%

Sequential Encryption 2%



Distributed Encryption 2%

Analysierte Werte

- Match Score:
  - Ab 40 wird üblicherweise der Fingerprint als erkannt gewertet.
  - Durchschnittlicher Match Score von (unverschl.) Bildern eines Fingerprint Sets: 56 (Standardabweichung: 44)
  - Mittelwert der Match Scores für jede Verschlüsselungsstufe
  - Standardabweichung der Match Scores für jede Verschlüsselungsstufe
  - Interpretation
    - Günstig: Hoher Match Score bei niedriger Standardabweichung

Analysierte Werte

- Qualität der verschlüsselten Bilder

  Frage: In welchem Ausmaß sinkt die Bildqualität mit der Verschlüsselung?

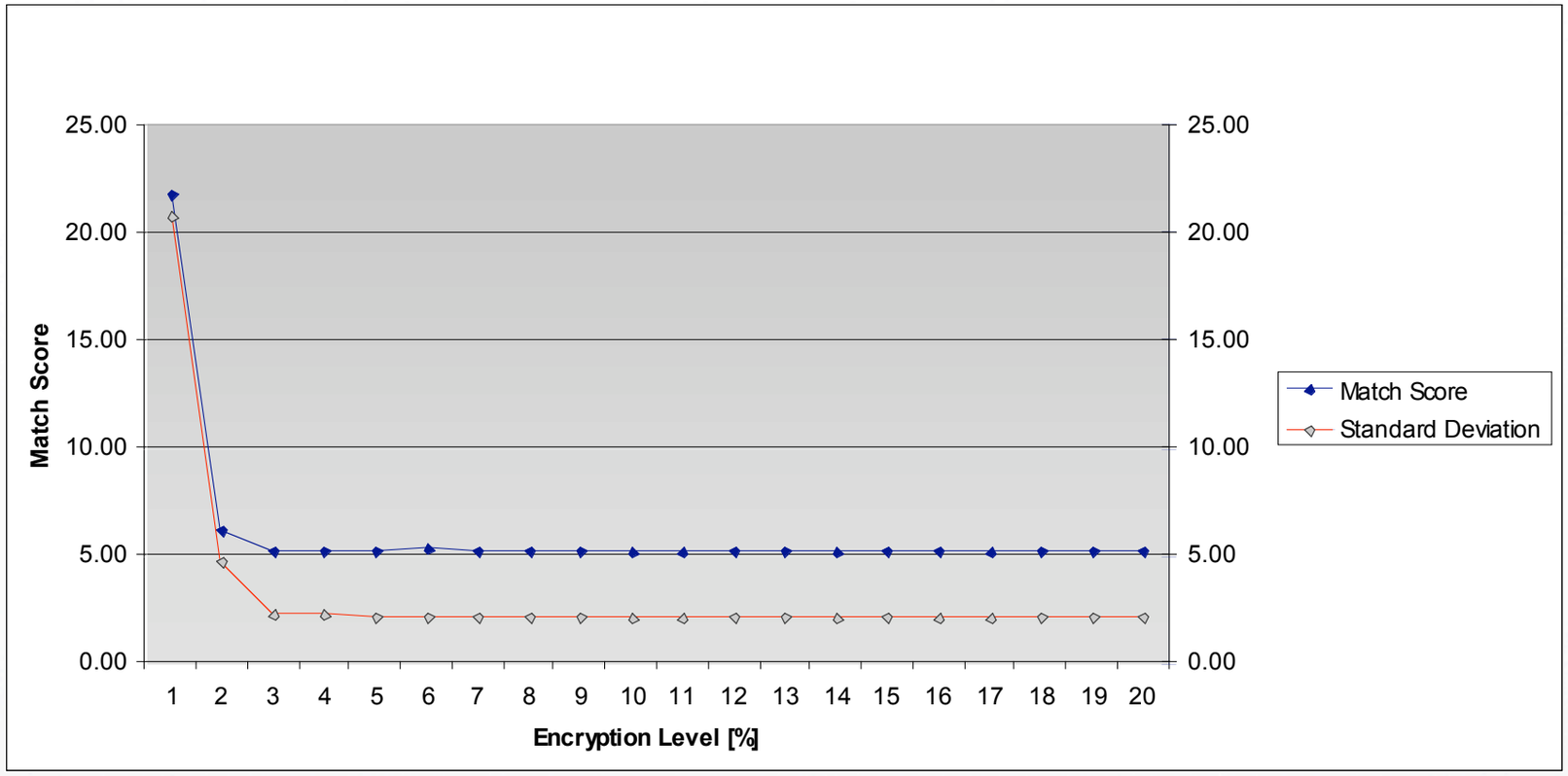
- Qualität der unverschlüsselten Ausgangsbilder

  Frage: Inwiefern beeinflusst die Ausgangsqualität das Matching
  Ist es vorteilhaft, Bilder ab einer bestimmten Qualität nicht weiterzu verwerten?

- Ziel: Schlechte Fingerprints nicht zu akzeptieren
  Stabilere Ergebnisse ?

Ergebnisse

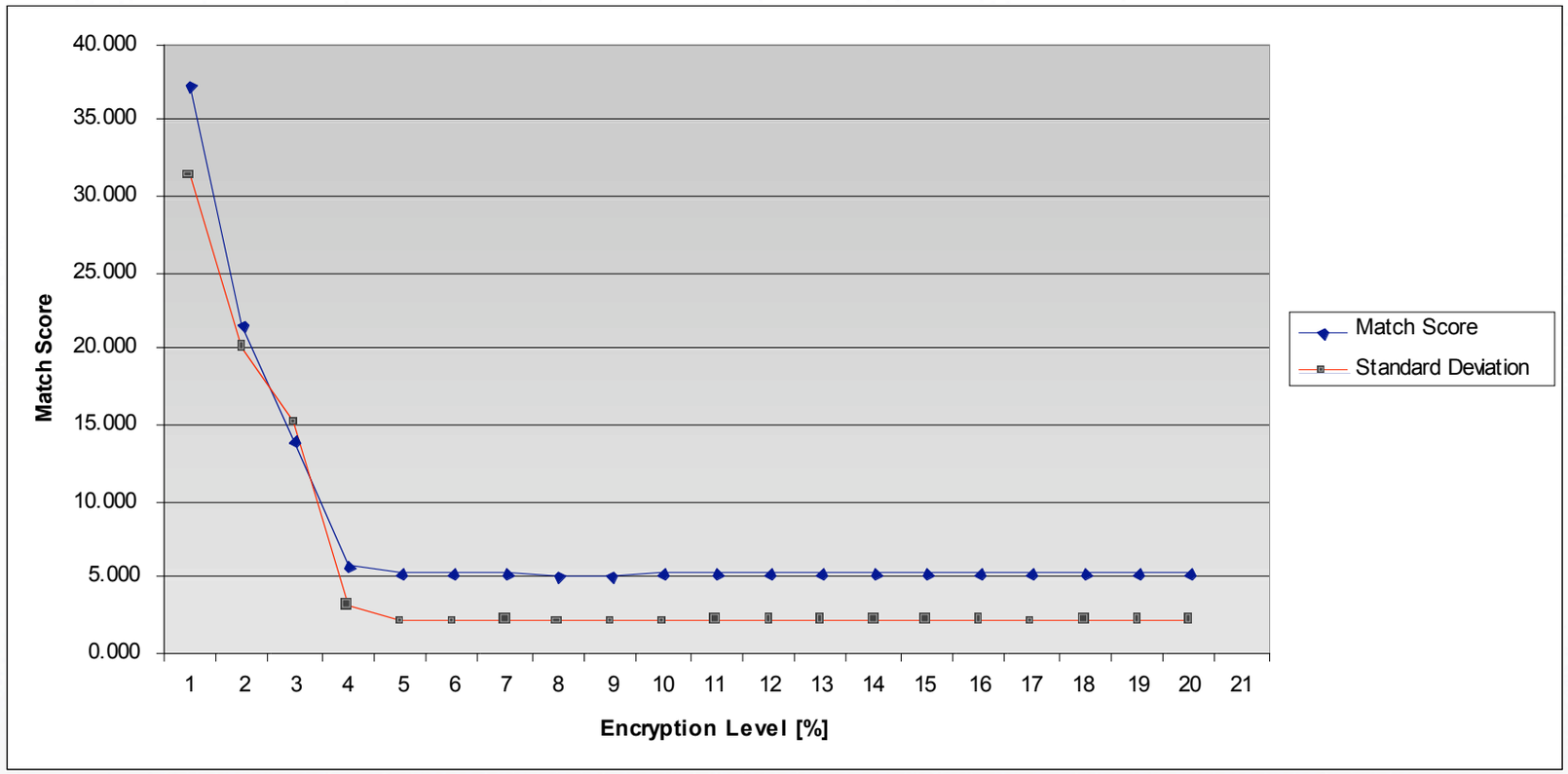
Matching - LRCP



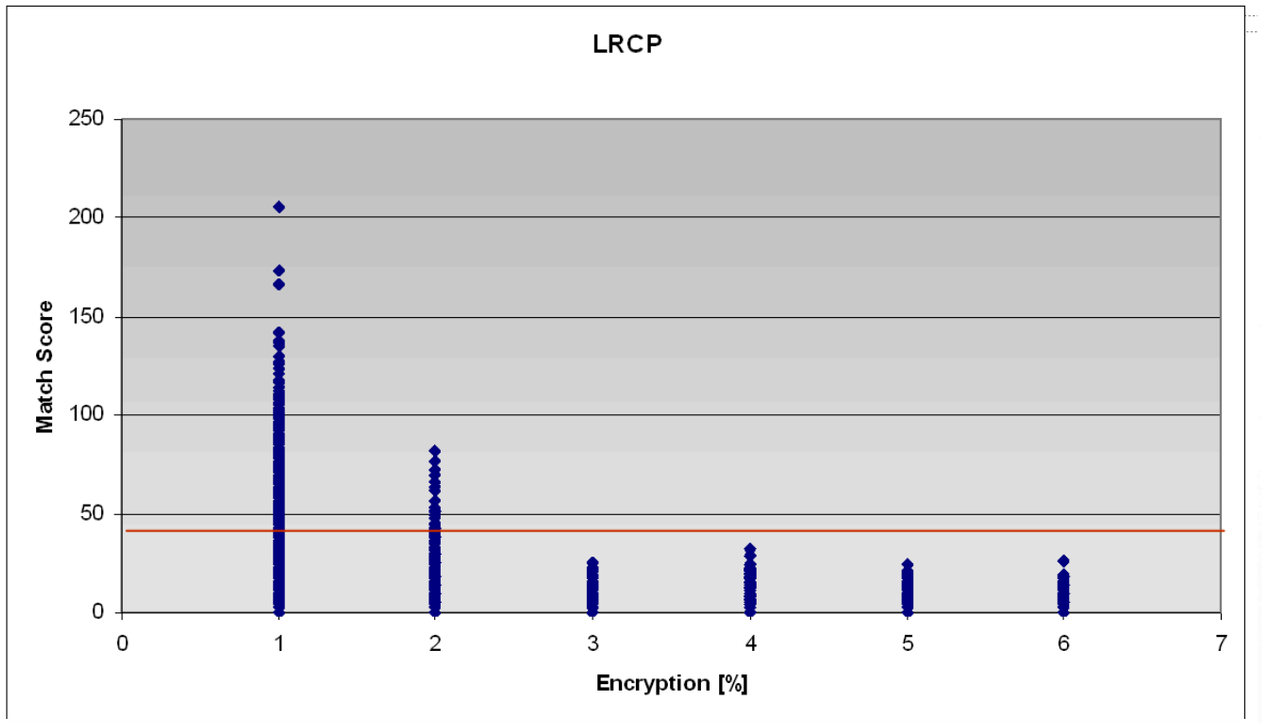
- Match Score fällt schon bei 1-3% Verschlüsselung sehr stark ab
- Stabilisierung der Werte (Match Score und Standardabweichung ab ca. 3%)
- Standardabweichung im Bereich von 1-2% Verschlüsselung fast gleich dem Match Score
- Die hohe Standardabweichung lässt keine klare Grenze definieren
- Der Bereich von 1-3% Verschlüsselung sollte besser aufgelöst werden

Ergebnisse

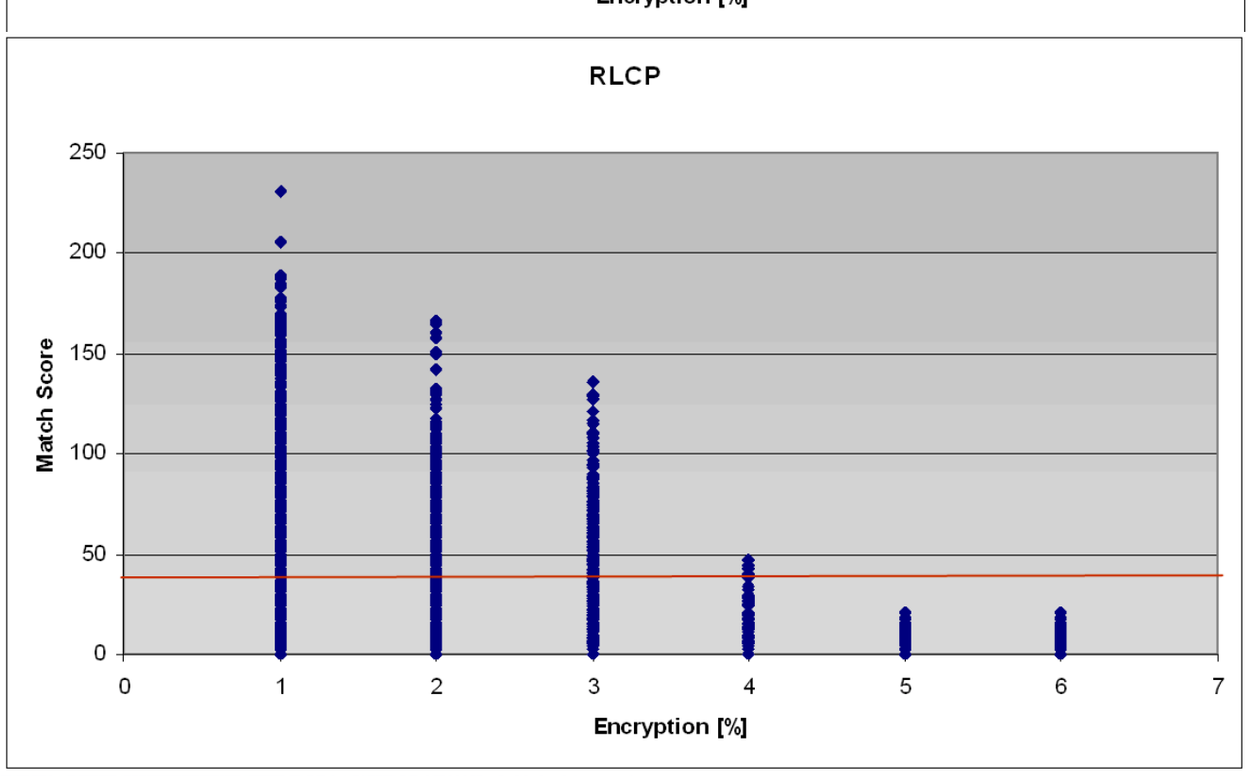
Matching - RLCP



- Match Score fällt langsamer ab im Vergleich zu LRCP
- Standardabweichung bei geringer Verschlüsselung fast ident zu Match Score
- Stabilisierung der Resultate ab ca 4% Verschlüsselung
- Die hohe Standardabweichung lässt keine klare Grenze definieren
- Das Liniendiagramm bietet zu wenig Informationen um eine Grenze zu definieren



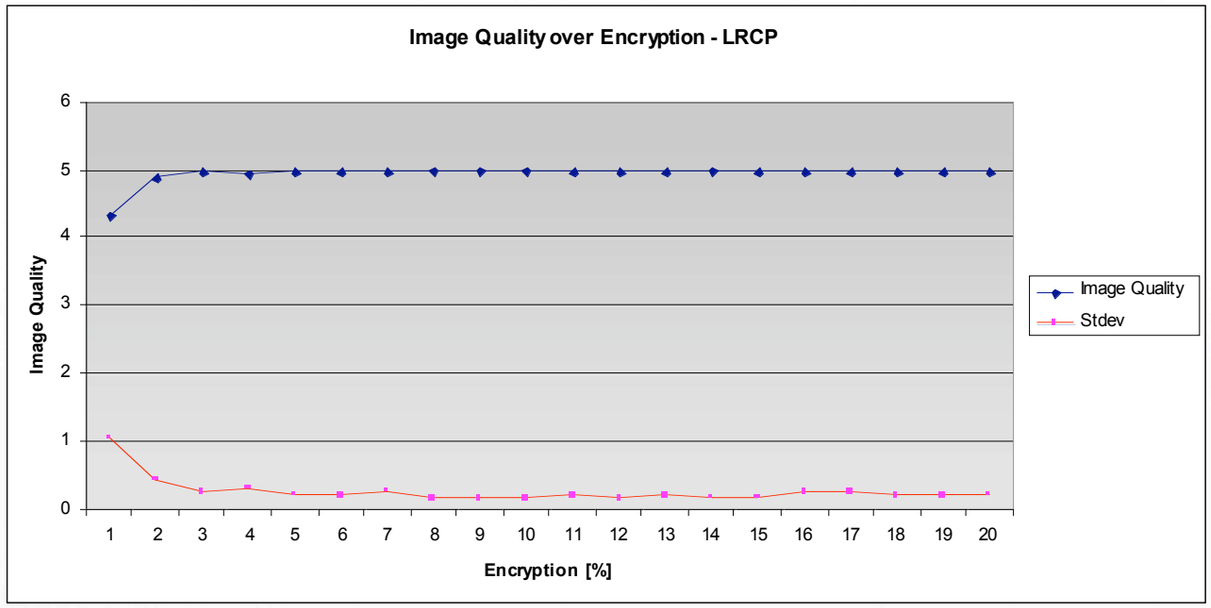
- Mit dem Scatterplot lässt sich die Verteilung sehr gut erkennen
- Bei LRCP treten ab 3% Verschlüsselung keine Match Score Werte über 40 auf

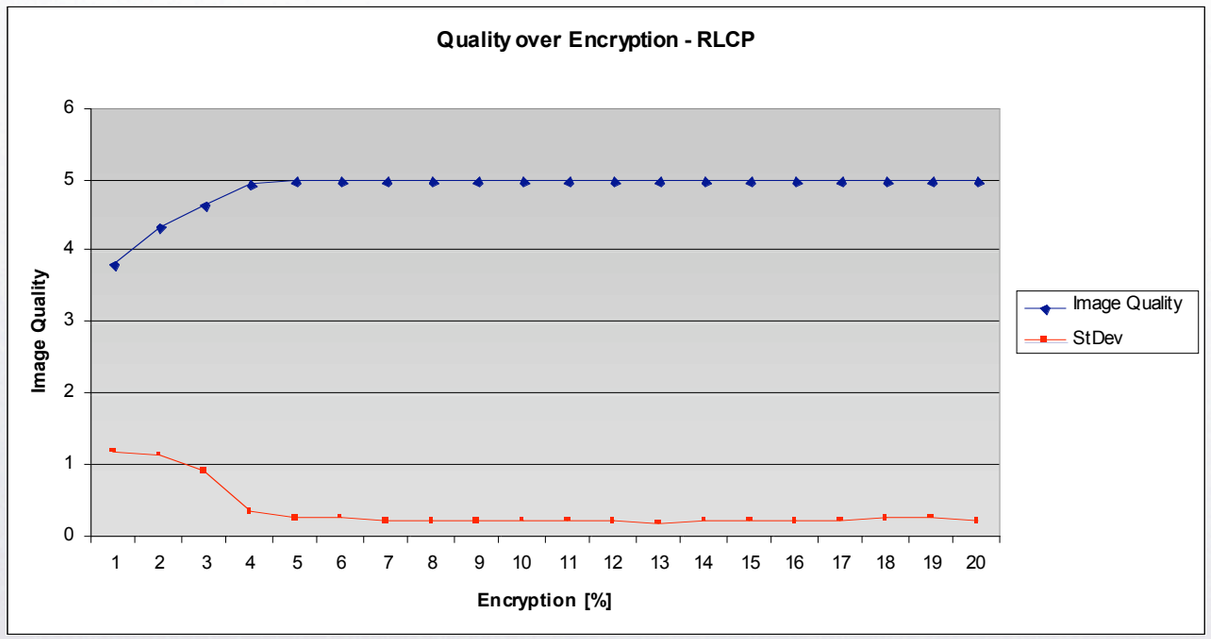


- Bei RLCP liegt der notwendige Verschlüsselungsgrad bei 5%

Ergebnisse

Bildqualität



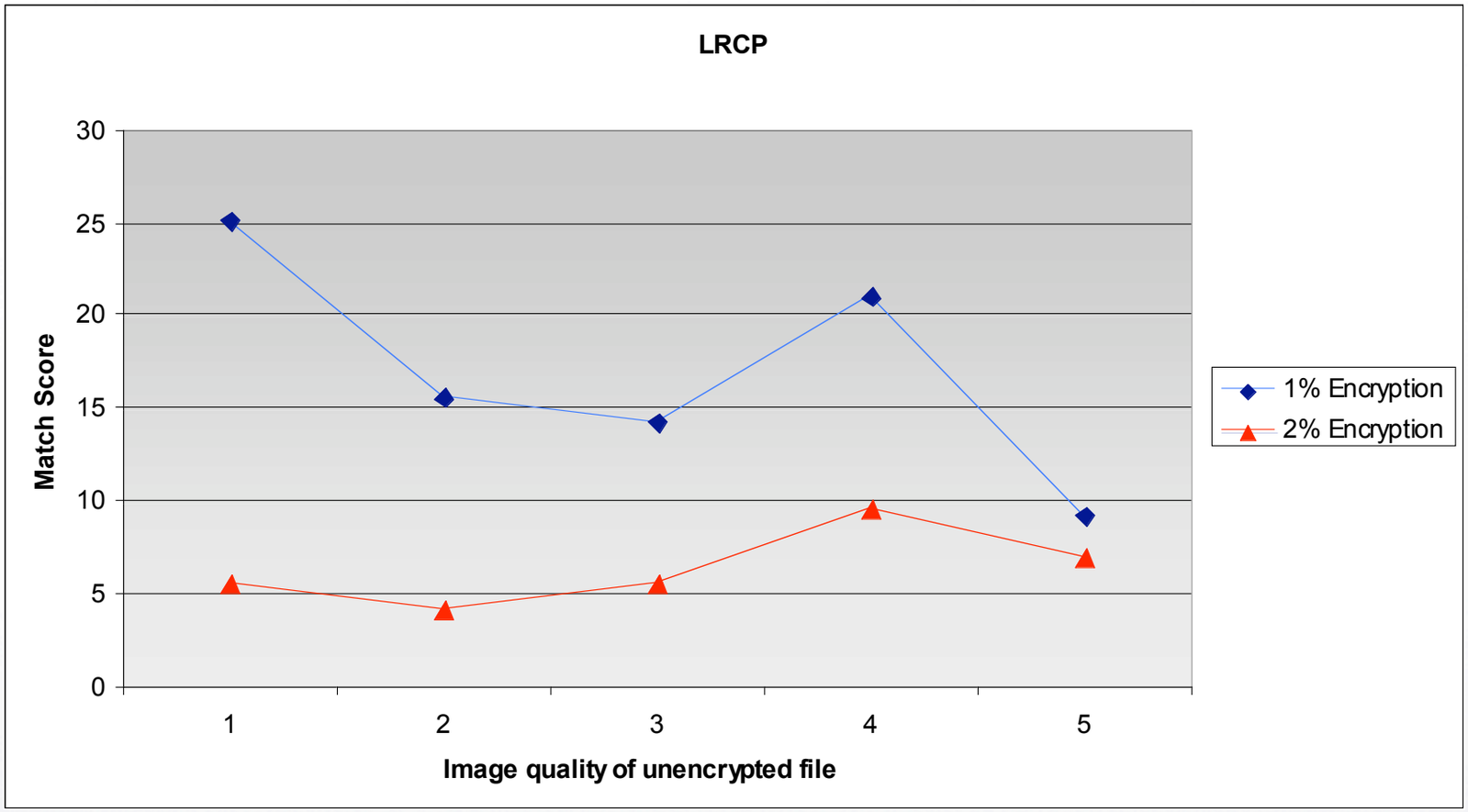


- Ergebnis sehr ähnlich dem Matching score

- Bildqualität 5 resultiert sehr wahrscheindlich in keinem Match

Ergebnisse

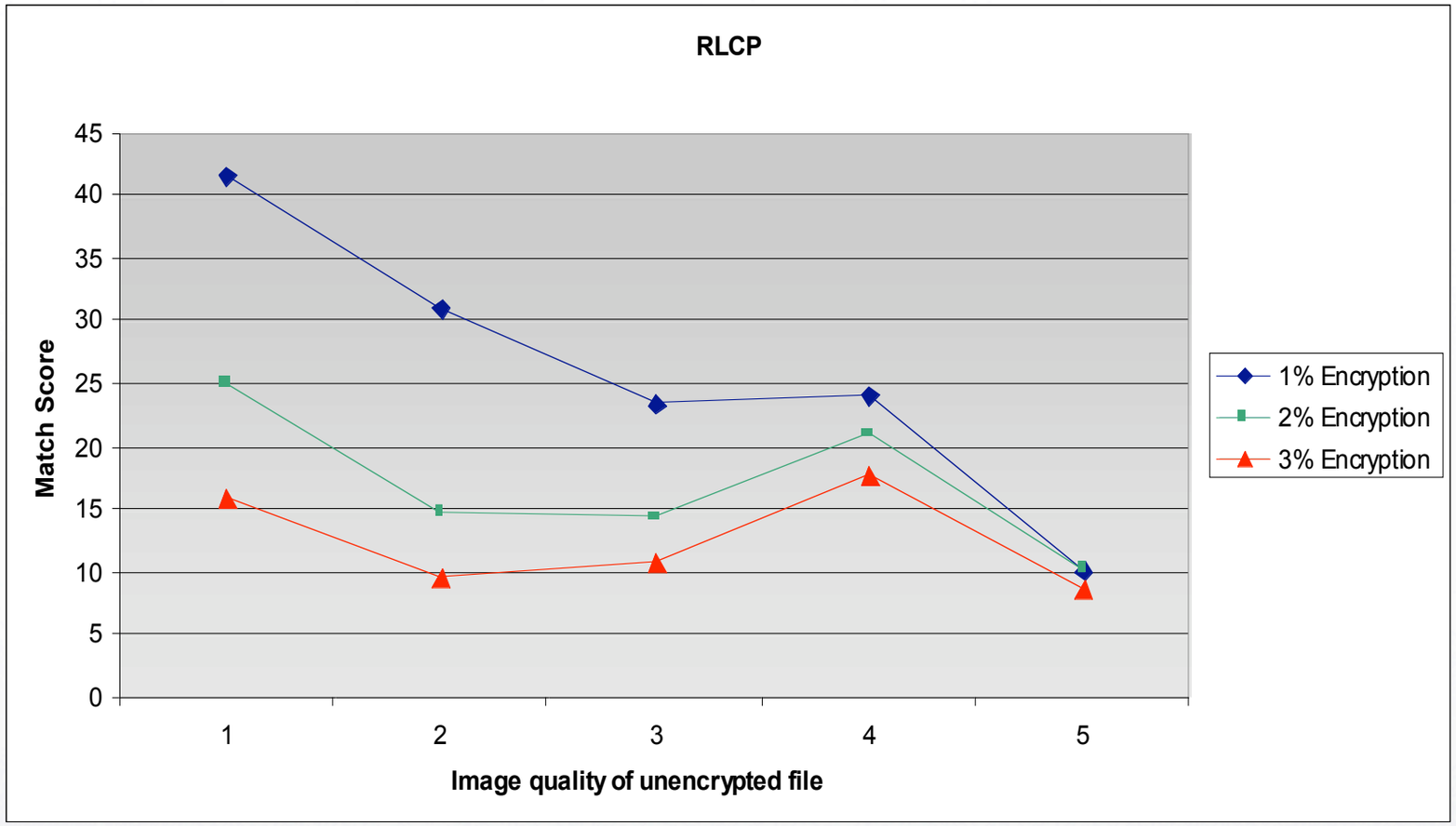
Bildqualität - Score - LRCP



- Beste Qualität im Ausgangsmaterial liefert auch die besten Match Scores
- Der Match Score bei einer Ausgangsqualität von 4 ist unerwartet hoch
- Bei geringer Verschlüsselung macht es ev. Sinn Ausgangsmaterial mit Qualität = 5 zu verwerfen

Ergebnisse

Bildqualität - Score - RLCP



Schlussfolgerungen

- Empfehlung für minimalen Verschlüsselungslevel:
  - LRCP: 3% des Bytestreams
  - RLCP: 5% des Bytestreams
- Nicht berücksichtigt wurde der visuelle Eindruck des verschlüsselteten Fingerprints (Rekonstruktion durch Imaging Software)

Ausblick

- Behandlung von False Positives
- Vergleich der Verschlüsselungsvarianten (insbesondere Distributed Encryption)
- Optimierung der Ergebnisse unter Berücksichtigung der Bildqualität (Ziel höhere Stabilität der Ergebnisse)

Ausblick

- Behandlung von False Positives
- Vergleich der Verschlüsselungsvarianten (insbesondere Distributed Encryption)
- Optimierung der Ergebnisse unter Berücksichtigung der Bildqualität (Ziel höhere Stabilität der Ergebnisse)