Robuste Hashes zur forensischen Bilderkennung

Dr. Martin Steinebach

Information Assurance (IAS)
Fraunhofer SIT
Rheinstrasse 75, 64295 Darmstadt

Telefon: 06151 869-349, Fax: 06151 869-224
E-mail: martin.steinebach@sit.fraunhofer.de
http://www.sit.fraunhofer.de

Inhalt

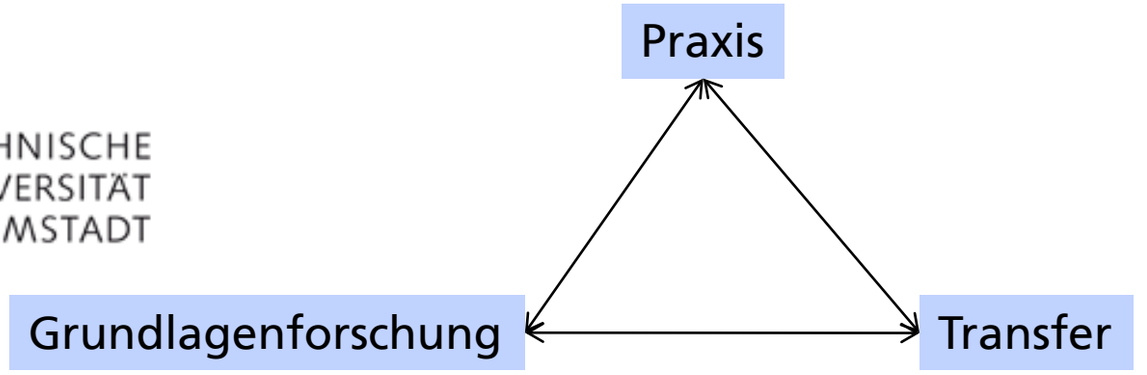
1. Projektszenario ForBild
2. Motivation: JPEG und Hashverfahren
3. Robuste Blockhashs
4. Ergebnisse zu robusten Hashverfahren
5. Ausblick

ForBild

- Forensische Bilderkennung
- Gefördertes Projekt mit starkem Anwendungsbezug
- LOEWE-Projekt aus CASED Umfeld über Hessen Agentur
- Integration von neuen Methoden zur Bilderkennung in produktives System
    - Robuste Hashverfahren
    - Verbindliche Sicherung der Beweismittel
    - Datenschutzkonformer Bildvergleich

ForBild Partner

LSK

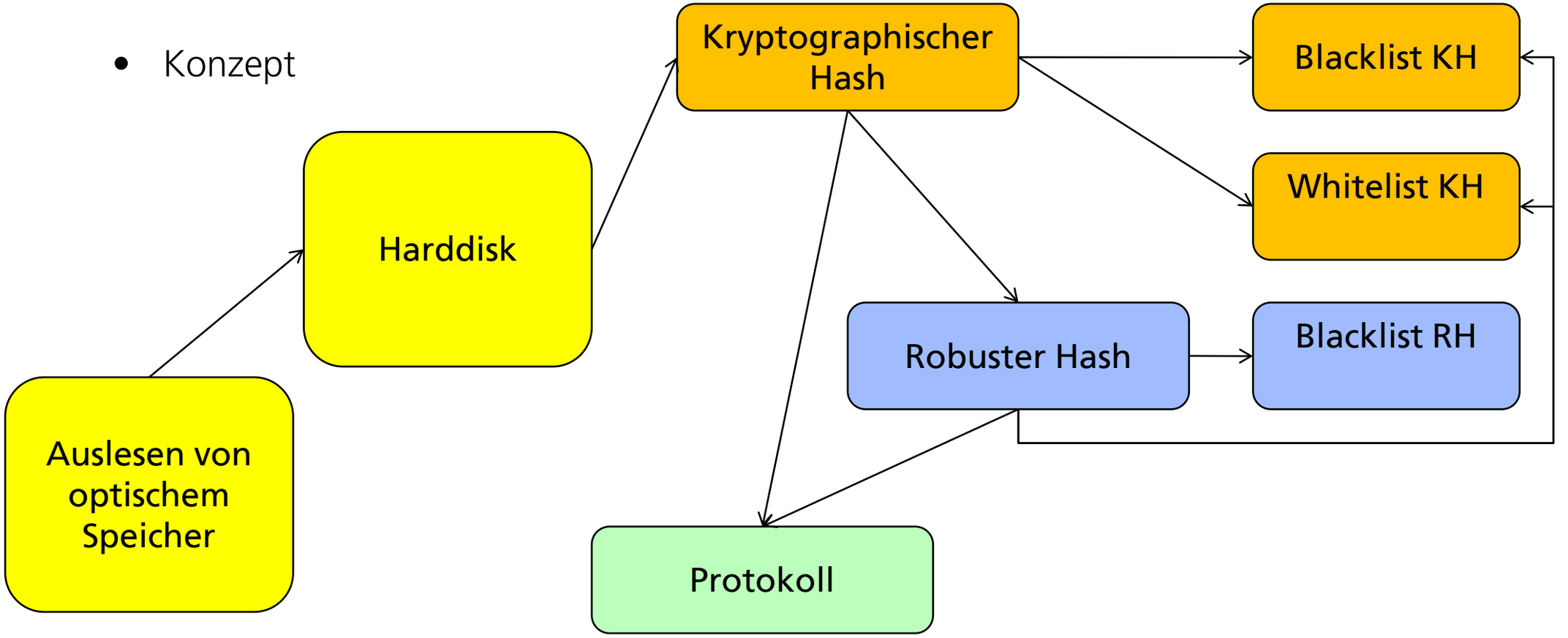


TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

ForBild

- Konzept



Motivation

- Herkömmliche Hashverfahren sind für digitale Medien nur eingeschränkt geeignet
- Nur identische Kopien werden erkannt
- Eine Verschleierung unerlaubter Inhalte ist daher einfach
- Viele Anforderungen an Hashverfahren gelten bei der Unterstützung zur Suche illegaler Inhalte nicht
  - Insbesondere Aspekte der Sicherheit

MD5 und JPEG

Test: JPEG mit Paint laden, wieder als JPEG speichern.

```
E:\Temp>md5 *.jpg
3B3FD01FD259BD9E215F76821C7FD4A1   SANY0178.JPG
FA54E4027DDCE7F315F78DEFE964B0ED   SANY0178_1.JPG
A6D7610ECBA10813394849775BB051CD   SANY0178_2.JPG
8ACB44D55693F3811D28A6AE398F9BB5   SANY0178_3.JPG
```

SSDeep und JPEG

```
SANY0178_1.JPG: 2PnL4ySsdX4Y37h8N9YzSWTaEvq2zmhpf1JhModDmEQbA8BUl:
                65SSIEhhah2zef1JpdmdPBUl
SANY0178_2.JPG: 9qAjnknYytozR63RErlfjQbHGuIWjkqcDG:9qAjtytom2lfW6i
```

Robuste Hashverfahren

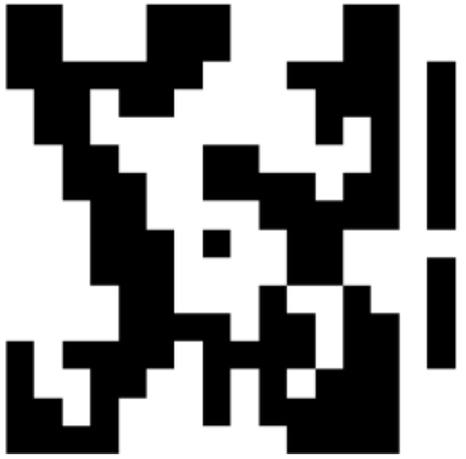
- Robuste Hashverfahren
  - sind aufwändiger als kryptographische Hashverfahren
    - Abhängig von Konzept und Implementierung kann schnell ein Zeitfaktor 1.000 erreicht werden
- sind weniger genau als kryptographische Hashverfahren
  - Fehlerraten (FAR/ FRR)
  - Robuste Hashs benötigen mehr Speicherplatz
- benötigen mehr Speicherplatz

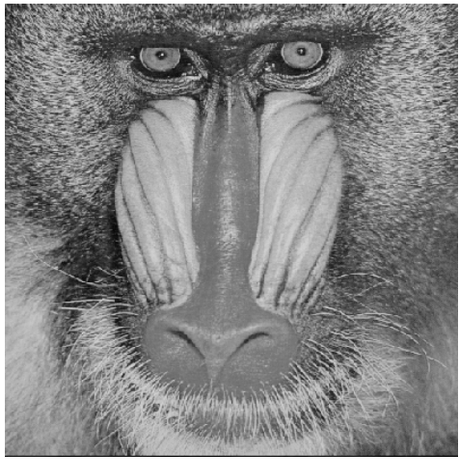
Robuste Hashverfahren

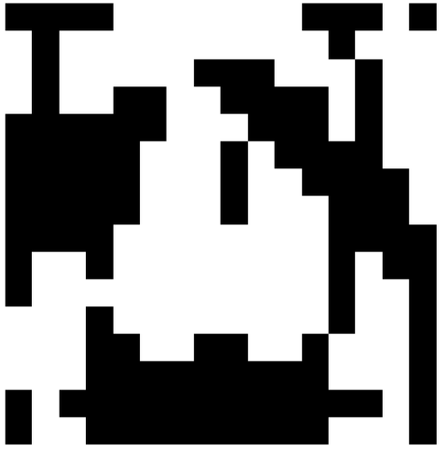
- Beispiele für bekannte robuste Hashverfahren

  - DCT (Spektrum des Bildes)
  - Marr-Hildreth Operator (Kantenerkennung)
  - Radiale Transformation (Projektion)
  - Blockdurschnitt (Helligkeit von Blöcken)

Blockhash



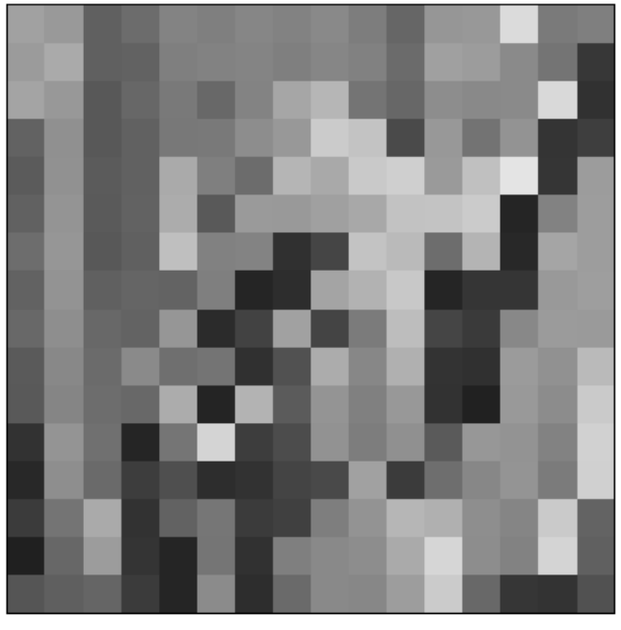




- Jeweils Bild und zugehöriger robuster Hash

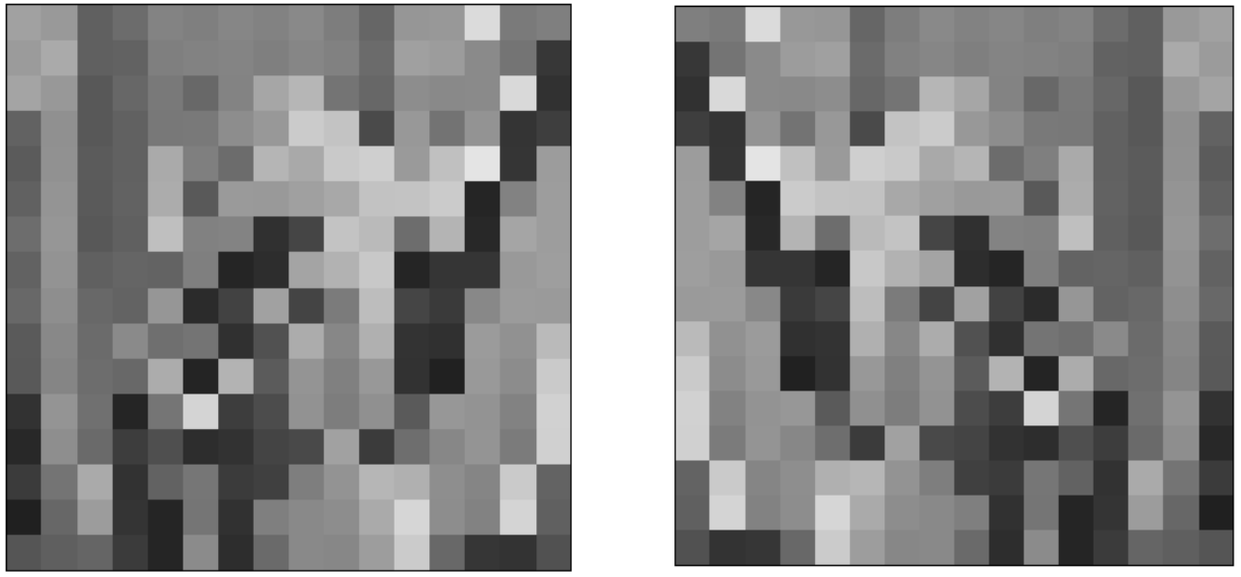
Blockhash

- Schritt 1:
  - Graustufen
  - Skalieren auf 16 x 16 Pixel



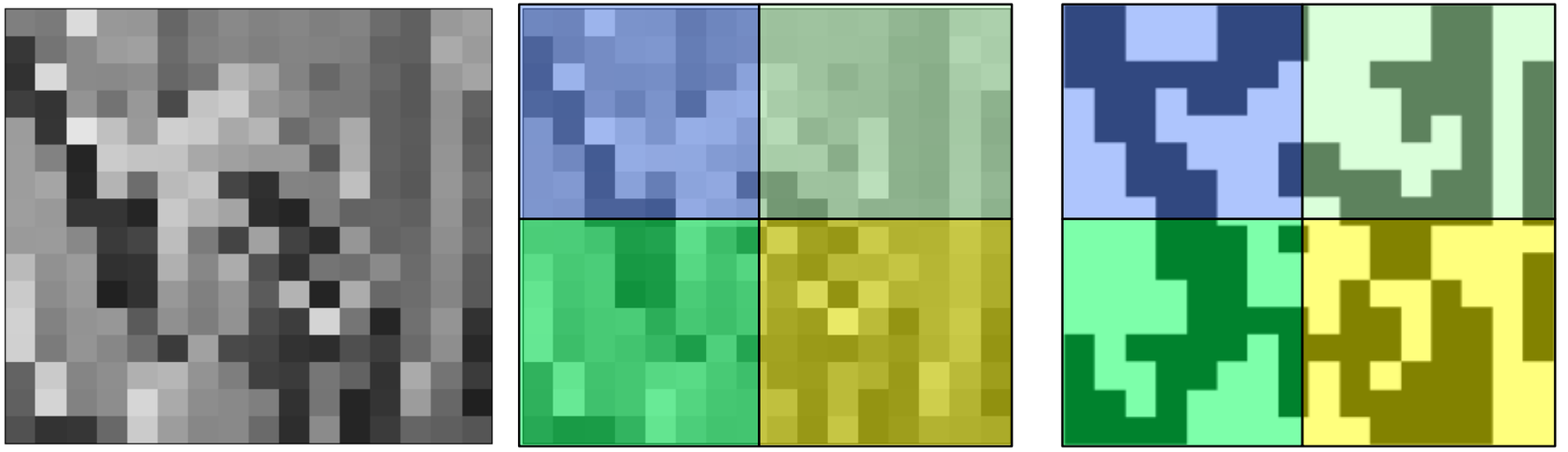
Blockhash

- Schritt 2:
  - Automatische Spiegelung
  - Quadrant mit hellsten Punkten oben links



Blockhash

- Schritt 3:
  - Pro Quadrant von 8x8 Pixeln Berechnung des Medians
  - Hashentscheidung: Pixel < oder >= Median



Blockhash

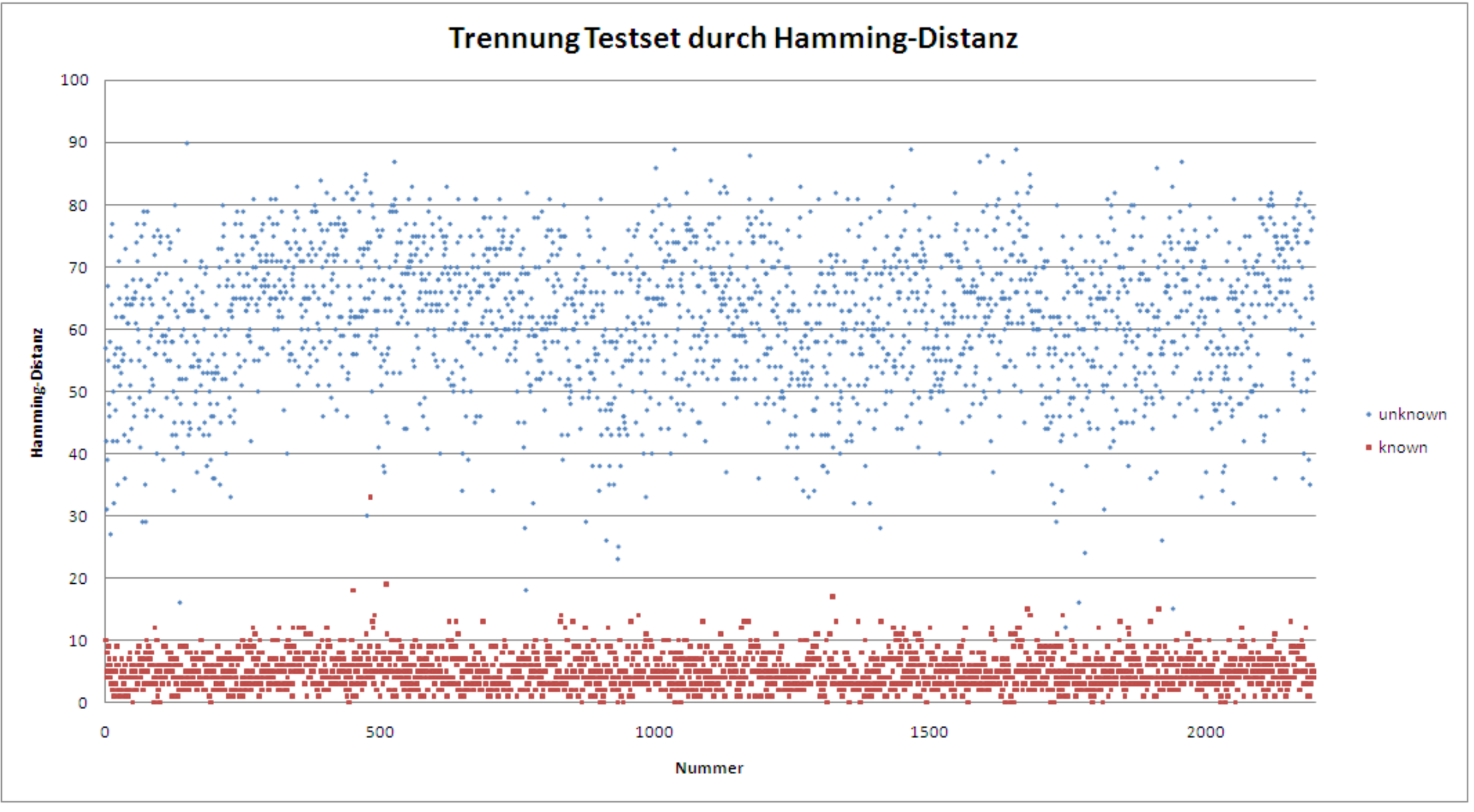
- Hashgröße
  - 8 x 8 = 64 Pixel pro Quadrant
  - Mindestens 32 Pixel pro Quadrant weiß, weil bei mindestens 32 Pixel Helligkeit >= Median
  - $\left[\binom{64}{32}+\binom{64}{33}+\cdots+\binom{64}{64}\right]^4 \approx 1{,}057\times10^{76}$ mögliche robuste Hashs
  - Geschätzte Anzahl von Atomen im Universum: 10^78
  - Bilder, die zufällig den geleichen Hash haben, sind also unwahrscheinlich
  - Wahrscheinlichkeit ist aber höher als oben berechnet, da Bilder wiederkehrende Strukturen haben, die sich in ähnlichen Hashsequenzen niederschlagen

Blockhash

- Beispiel Robustheit
  - Starke JPEG Kompression
  - Spiegelung
  - Nur ein Bit Differenz

Blockhash

- Entscheidung, ob ein Hash zu einem bekannten Bild in der Datenbank gehört, wird über Hamming-Distanz gefällt
  - Anzahl der Bits, die sich zwischen Bildhash und Hash in Datenbank unterscheiden
- Im Gegensatz zu herkömmlichen kryptographischen Hashs wird nach ähnlichen Hashs gesucht, nicht nach identischen
- Beispiel:
  - Hashgröße 256 Bit
  - Bild wird erkannt, wenn es eine Hammingdistanz <=32 zu einem Bild in der Datenbank hat



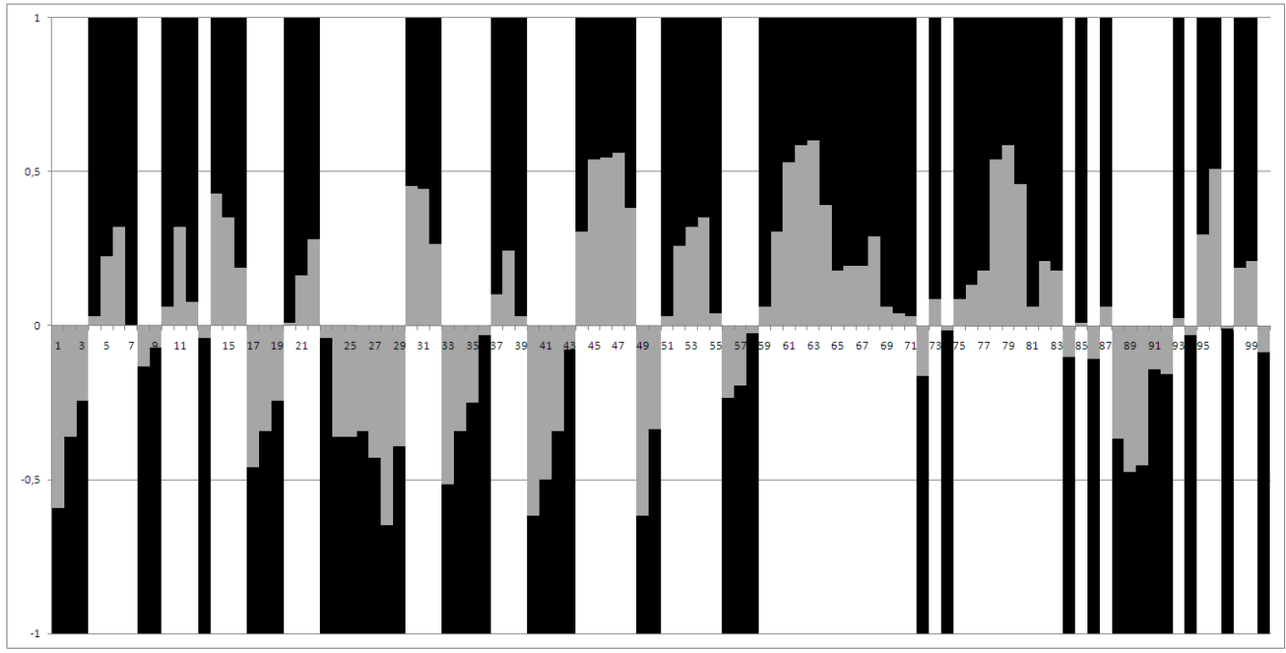
LOEWE – Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz

CASED

Fraunhofer SIT

Blockhash

- Nicht jedes Hashbit ist gleich
  - Nicht gleich robust gegen Änderungen
  - Nicht gleich vertrauenswürdig
- Daraus resultiert das Konzept des Quanten-Hashes
  - Die Hamming-Distanz wird zusätzlich bewertet, indem betrachtet wird, ob die nicht übereinstimmenden Bits stark ausgeprägt waren oder nicht
    - Stark ausgeprägt: Unterschiedliches Bild
    - Schwach ausgeprägt: Auswirkung von Kompression o.ä.

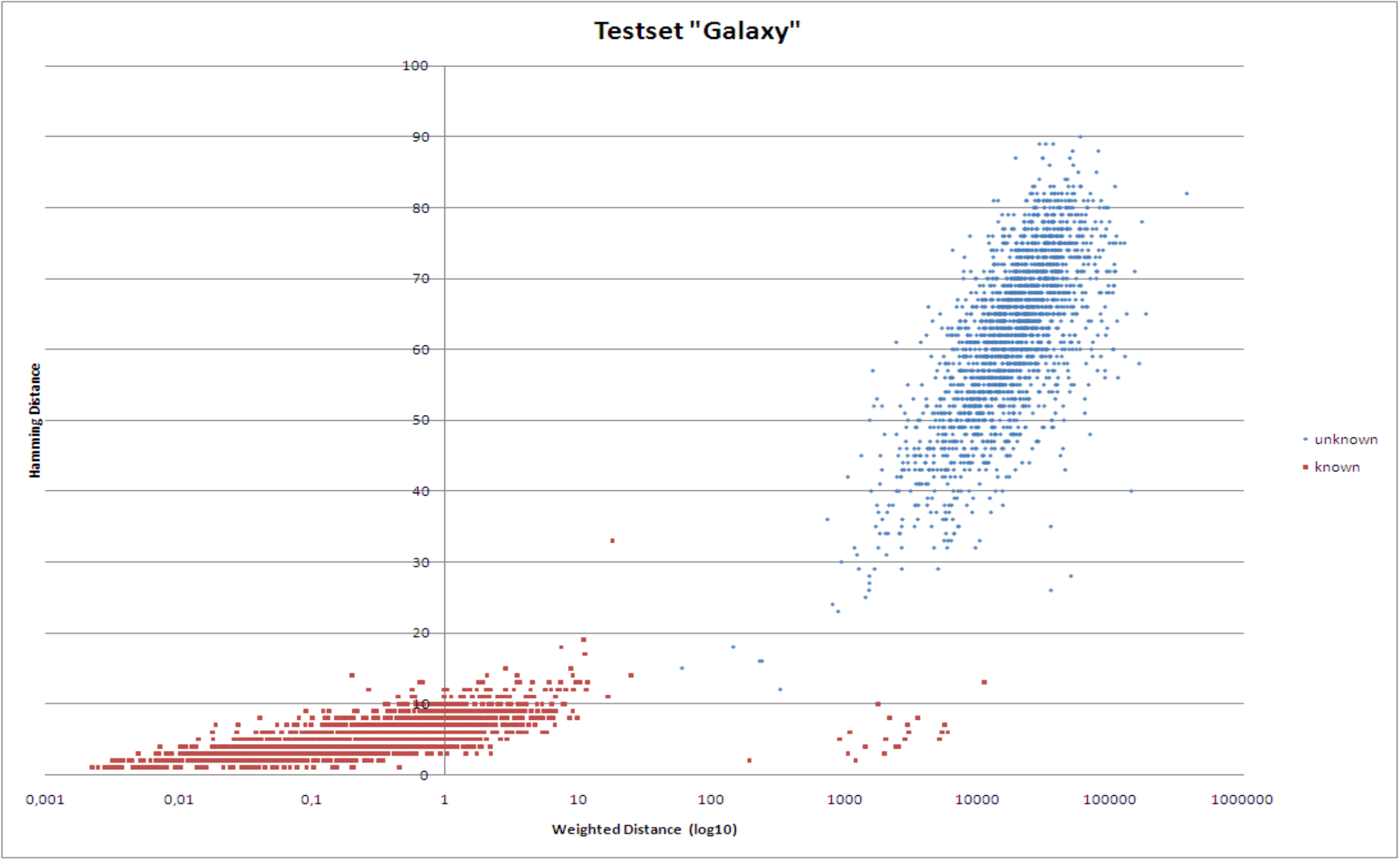


Blockhash

- Berechnung des Quantenhashes „gewichtete Hammingdistanz“

$$\frac{\text{Varianz(Abstände unterschiedlicher Hashbits zum Median der Blockhelligkeit)}}{\text{Varianz(Abstände gleicher Hashbits zum Median der Blockhelligkeit)}} * \text{Hammingdistanz} * 1000$$

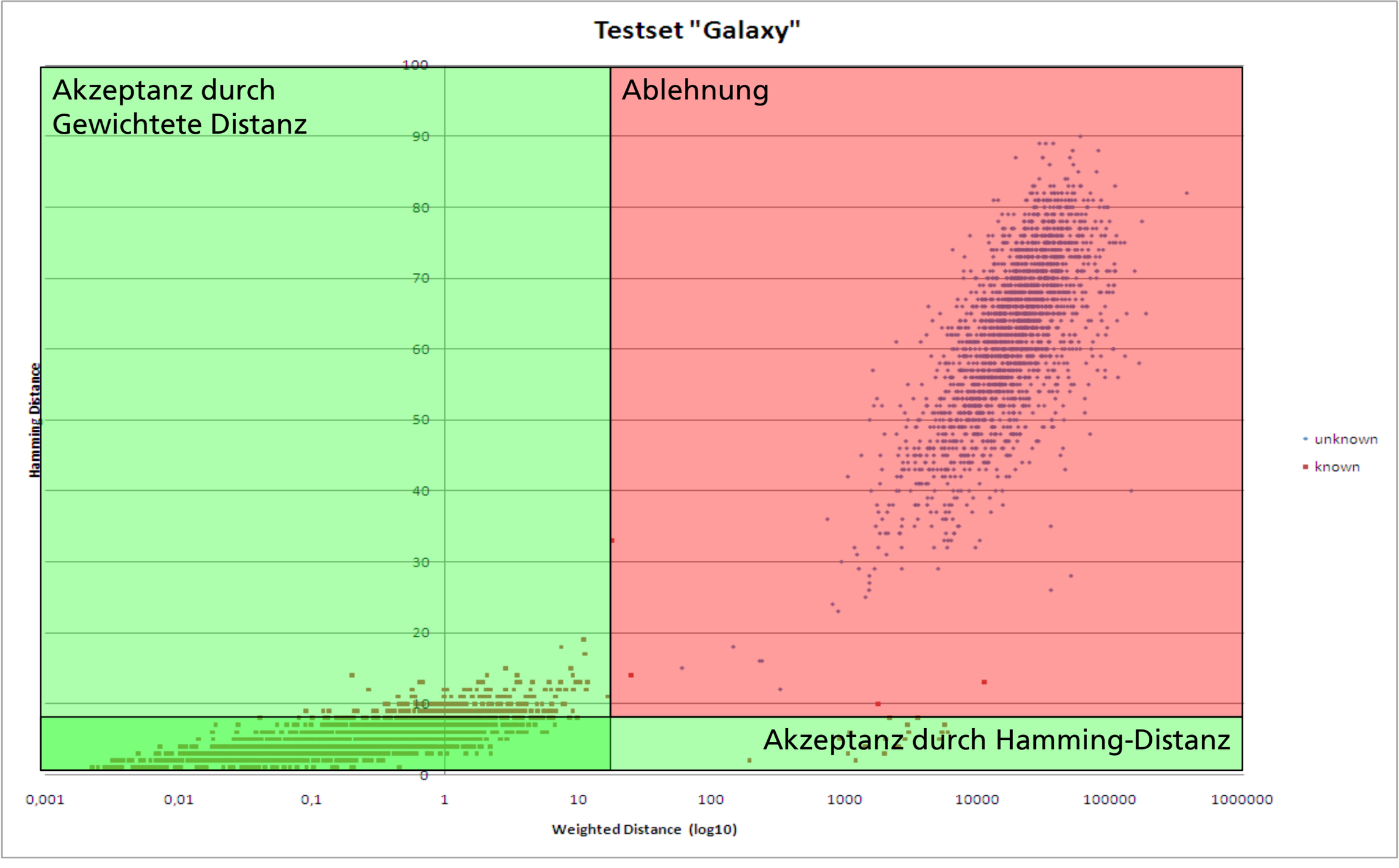
- Beispiel folgende Seite:
  - X-Achse = Quantenhash
  - Y-Achse= Hammingdistanz



LOEWE – Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz
CASED
Fraunhofer SIT

Blockhash

- Sehr gute FRR/FAR bei Kombination aus Hamming-Distanz und gewichteter Distanz
  - Alle Bilder mit Hamming-Distanz <= 32 werden betrachtet
  - Bilder mit Hamming-Distanz <=8 oder gewichteter Distanz <=16 werden akzeptiert
- Testszenario
  - Testset mit 4.394 Bildern
  - Hashbibliothek mit > 80.000 Bildern
  - Hälfte der Bilder in Bibliothek aufgenommen (known)
  - Andere Hälfte nicht aufgenommen (unknown)
- Ergebnisse
  - FAR = 0, FRR = 5
  - Fehlerrate also 1,1 Promille



LOEWE – Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz

CASED

Fraunhofer SIT

Ausblick

- Integration von Verfahren zum Erkennung von Bildteilen
  - Gesichtserkennung
  - Bildsegmentierung
- Betrachtung von Video

Ende

- Vielen Dank für Ihre Aufmerksamkeit