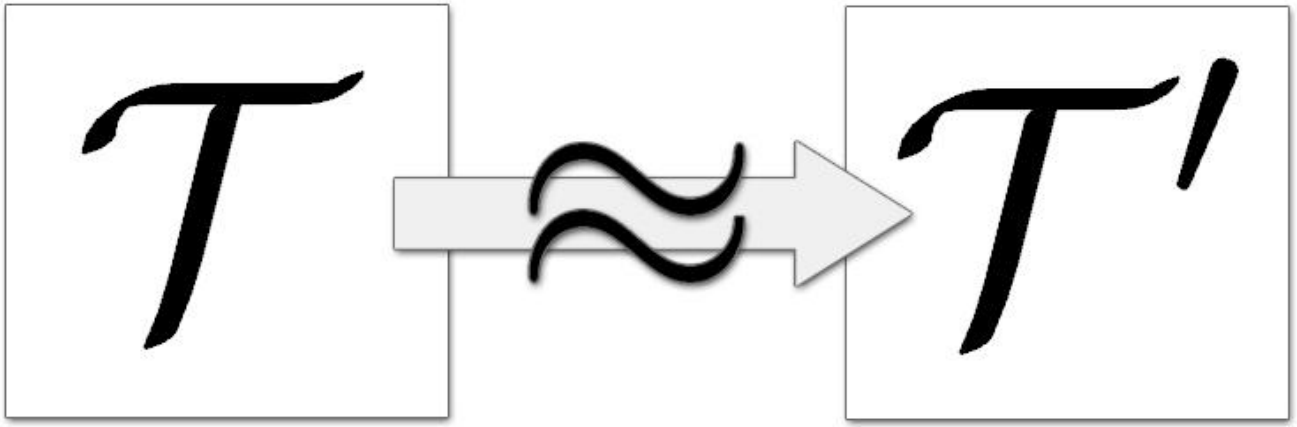
Natural Language Watermarking

Foundations of individual Text-Watermarking

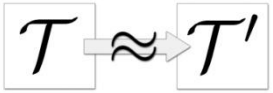
TECHNISCHE UNIVERSITÄT DARMSTADT



Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- Motivation
- Introduction: Natural Language Watermarking
- Examples of embedding methods
- Challenges in NLW
- References



What is NLW ?

TECHNISCHE UNIVERSITÄT DARMSTADT

- Imagine the following scenario:

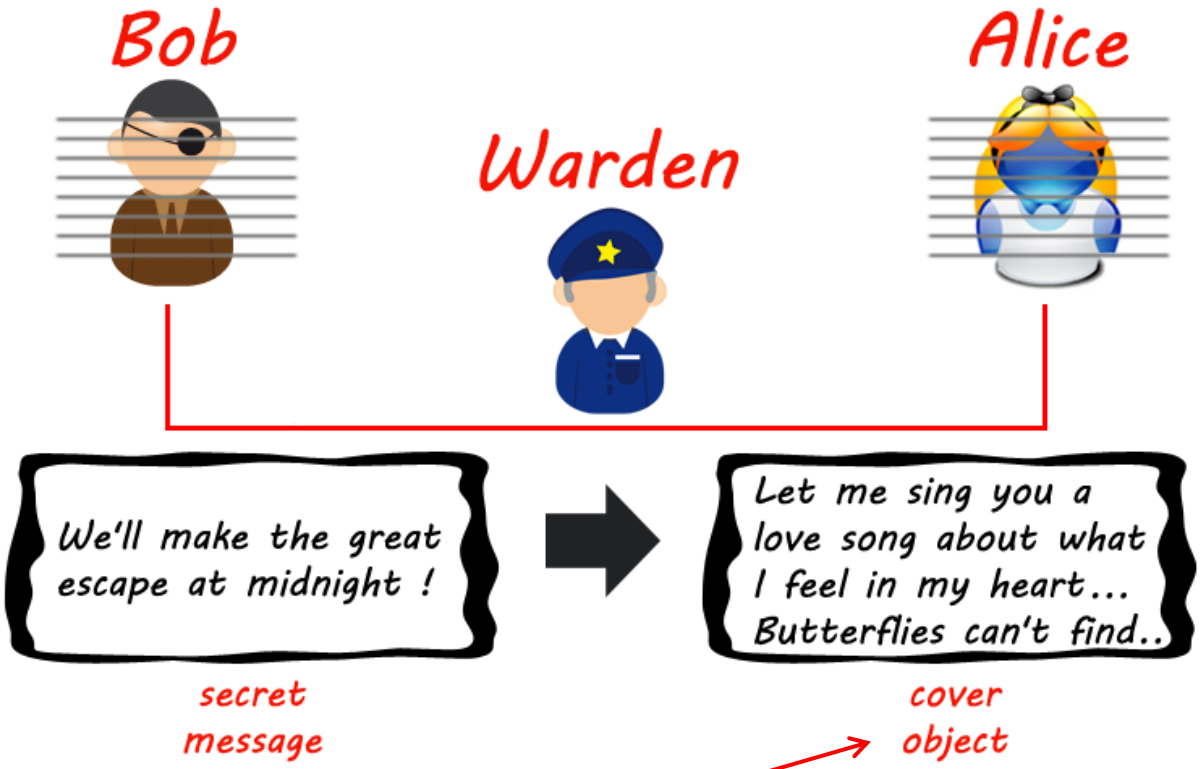
„Two prisoners (Alice and Bob) want to communicate and the only possibility they have, is sending eachother plaintext messages, which are delivered by the warden.

*The prisoners **cannot use encryption** because the warden wants to read all outgoing messages, otherwise he will **not deliver the message**…"*

This scenario is called:

"The Prisoners' Problem and the Subliminal Channel"

What is NLW ?



Note: the cover object remains the same !

What is NLW ?

TECHNISCHE UNIVERSITÄT DARMSTADT

The Prisoners' Problem is the fundamental idea behind “Information Hiding”

And “Information Hiding” is the superordinate concept of NLW…

$T \approx T'$

What is NLW ?

TECHNISCHE UNIVERSITÄT DARMSTADT

NLW = "embedding of information by modifying original data in a discreet manner, such that the modifications are imperceptible when watermarked data is consumed…"

- The information to embed is called "**watermark-message**" which can be e.g.
  - Serial / ID number of the document
  - Customer licence data (Purchase date, IP Address,…)
  - Meaningful text (short messages)
  - etc.

$T \approx T'$

Some characteristics of NLW

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Robust / Fragility**
  - Difficult to **remove** for an attacker, who would like to destroy it
  - Should be **resistent** against simple format conversions, that occour often in a workaday life, e.g. HTML → TXT, DOC → PDF, XLS → XML, etc.
  - Removal should cause degradation in the **quality** of the data
- **Readily Detectable**
  - Data owner should easily **detect** it
- **Unobtrusive**
  - **Invisible** enough not to degrade data quality and prevent attacker from finding and deleting it

$T \approx T'$

The link between NLP and NLW

TECHNISCHE UNIVERSITÄT DARMSTADT

- How does Natural Language Processing (NLP) relate to Natural Language Watermarking (NLW) ?

- NLW combines many tools and methods provided by NLP in order to embedd watermarks at a "natural language" level, e.g.:

  ✓ (Intelligent) Tokenization / Pattern Matching

  ✓ POS-Tagging

  ✓ Parsing

  ✓ Text simplification / text paraphrasing

  ✓ Word sense disambiguation

  ✓ Anaphora resolution

  ✓ …and many more

$T \approx T'$

NLW Applications

TECHNISCHE UNIVERSITÄT DARMSTADT

Ownership Assertion

- Alice generates watermark and embedds it into her document
- Alice makes watermarked document publicly available
- Bob downloads document and claims he's the owner of copyrighted content
- Alice produces the unmarked original and establishes the presence of her embedded watermark → Result: **Bob is not the owner !**

Fingerprinting

- Used to avoid unauthorized duplication / distribution
- A distinct watermark (fingerprint) is embedded in each copy of the data
- If unauthorized copies are found, the original copy can be traced back by retrieving the fingerprint

$T \approx T'$

NLW Applications

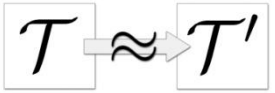
TECHNISCHE UNIVERSITÄT DARMSTADT

Content Protection

- Content owner wants to publish his content (for free), but in a "**read-only**" manner
- Content owner wants to publish individual copies of his content, (that means each copy is marked in a "**unique**" manner)

Content labeling

- Bits embedded in the data, comprise an annotation, giving some more information about the data



Embedding process

TECHNISCHE UNIVERSITÄT DARMSTADT

- Embedding a watermark-message into natural language text requires a systematic method for transforming (modifying) text…
- **Claim:** Transformations should **preserve grammaticality** of sentences
- **Ideally: differences** in sentence meaning caused by transformations should **not be noticeable**
- Generally there are three types of transformations:
  - Synonym substitution
  - Syntactic transformations
  - Semantic transformations

$T \approx T'$

Embedding process: Notation

TECHNISCHE UNIVERSITÄT DARMSTADT

- Following symbols will be used as abbreviations:

$\mathcal{T}$	The original document
$\mathcal{T}'$	The watermarked document
$\mathcal{W}$	The watermark message, e.g. "10001" → formaly: $\mathcal{W} \in \bigcup_{i \in \mathbb{N}}^{n} \{0,1\}^i$
$\mathcal{W}_{bit}$	One single watermark bit, e.g.
$\mathcal{T} =_{sem} \mathcal{T}'$	Semantical equality (both documents have the same sense)
$\mathcal{T} =_{syn} \mathcal{T}'$	Syntactical equality (both documents have „somehow" same syntactical structure)

$\mathcal{T} \approx \mathcal{T}'$

Embedding process: Steps

TECHNISCHE UNIVERSITÄT DARMSTADT

1) Annotate $\mathcal{T}$ with POS-Tags for each word

2) Apply regular expressions to extract patterns to match the rules of the embedding methods

Note: A pattern equals to one $\mathcal{W}_{bit}$

3) Apply methods to embedd $\mathcal{W}$ into $\mathcal{T}$

4) If a method **A** couldn't embedd $\mathcal{W}$ by itself, some other methods **B**, **C**, **D**, **...** will try to help (collaborative NLW)

5) During the process of applying transformations, embedding-methods must "ensure" that the sense of $\mathcal{T}$ is preserved

   To handle this some methods call a semantic query module, which tries to lookup in a giant corpus for phrases that are somehow similar to the transformations

$\mathcal{T} \approx \mathcal{T}'$

Embedding process: Conclusion

TECHNISCHE UNIVERSITÄT DARMSTADT

- What do we know so far ?

- We know **what** Natural Language Watermarking is
- We know for **which purpose** we use this disciplin
- We know (some) **characteristics** of NLW
- We know (a part) of the commonly used **notation**

- Guess what's missing?

$T \approx T'$

Embedding process: Conclusion

TECHNISCHE UNIVERSITÄT DARMSTADT

- What do we know so far ?

- We know **what** Natural Language Watermarking is
- We know for **which purpose** we use this disciplin
- We know (some) **characteristics** of NLW
- We know (a part) of the commonly used **notation**

- Guess what's missing?

The **methods** to embed the watermarks ("the core")

$T \approx T'$

Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- Conjunction Modulation
- Enumeration Modulation
- Center Permutation
- Hyponym & Troponym Truncation
- Synonym Substitution

Focus in this presentation…

- Hyphen Split
- Subordinate Clause Swap
- Prefix Elimination
- ……
- ……
- ……
- …

Note: since the implemented framework was focused on a local language, the following examples are in **german**…

$T \approx T'$

Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

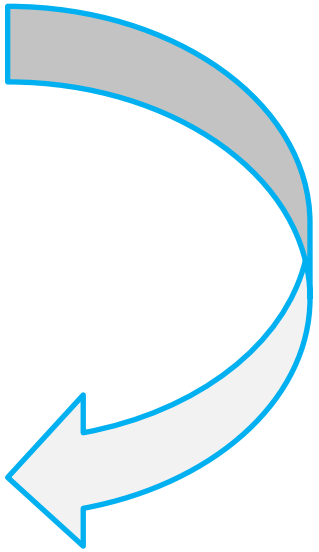
- **Conjunction Modulation**

Idea: Swap open-class words, which are connected by conjunctions…

$\mathcal{T}_1$ = "*…bei den **Wahlmännern** und **Wahlfrauen** der Union…*"

$\mathcal{T}_2$ = "*…hätte die Linke **Gauck** oder **Wulff** gewählt…*"

$\mathcal{T}_3$ = "*…es war weder **gelb** noch **grün**…*"



$\mathcal{T}'_1$ = "*…bei den **Wahlfrauen** und **Wahlmännern** der Union…*"

$\mathcal{T}'_2$ = "*…hätte die Linke **Wulff** oder **Gauck** gewählt…*"

$\mathcal{T}'_3$ = "*…es war weder **grün** noch **gelb**…*"

$\mathcal{T} \approx \mathcal{T}'$

Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Conjunction Modulation:** What's behind it?

```
patternList.add("NN APPR NN KON NN ADJD VVINF"); // Bsp. "Hochschulen in Forschung und Lehre erheblich beitragen"
patternList.add("NN APPR NN KON NN ADV ADJA"); // Bsp. "Verwaltungsportalen für Wirtschaft und Bürger auch neue"
patternList.add("NN APPR NN KON NN APPR ADJA"); // Bsp. "Informationstechnologie für Gesellschaft und Staat von hoher"
patternList.add("NN APPR NN KON NN APPR ART"); // Bsp. "Förderung von Wissenschaft und Forschung auf dem"
patternList.add("NN APPR NN KON NN APPRART NN"); // Bsp. "Experten aus Wirtschaft und Forschung beim CAST"
patternList.add("NN APPR NN KON NN KON ART"); // Bsp. "Daten auf Tauschbörsen oder Internetplattformen und ein"
patternList.add("NN APPR NN KON NN KON PIS"); // Bsp. "Vernetzung zwischen Forschung und Praxis und einer"
patternList.add("NN APPR NN KON NN PTKVZ"); // Bsp. "Fragestellungen für Forschung und Entwicklung ab"
patternList.add("NN APPR NN KON NN PTKZU VVINF"); // Bsp. "-Anschaffungskosten in Praxen und Kliniken zu vermeiden"
patternList.add("NN APPR NN KON NN VAFIN PDS"); // Bsp. "Gewährleistung von Sicherheit und Vertrauenswürdigkeit sind die"
patternList.add("NN APPR NN KON NN VMFIN NN"); // Bsp. "Informationen zwischen Unternehmen und Verwaltung können Informationen"
patternList.add("NN APPR NN KON NN VMFIN PIAT"); // Bsp. "Vereinheitlichung von Schnittstellen und Protokollen kann solche"
patternList.add("NN APPR NN KON NN VVFIN ADV"); // Bsp. "Einsatz in Krankenhäusern und Praxen existiert bereits"
patternList.add("NN APPR NN KON NN VVFIN PRF"); // Bsp. "Prozessen zwischen Staat und Industrie verbergen sich"
patternList.add("NN APPR NN KON NN VVFIN PTKVZ"); // Bsp. "SIT für Hörbücher und Musikstücke basiert auf"
patternList.add("NN APPR NN KON NN VVFIN"); // Bsp. "Beziehung zwischen Original und Fälschung zeigt"
patternList.add("NN APPR NN KON NN VVINF"); // Bsp. "Preisgeld für Forschung und Entwicklung einsetzen"
patternList.add("NN APPR NN KON NN VVPP PRELS"); // Bsp. "Bundesministerium für Wirtschaft und Technologie unterstützt die"
patternList.add("NN APPR NN KON NN VVPP VAINF"); // Bsp. "Allianz zwischen IT-Sicherheit und Forschung verstärkt werden"
patternList.add("NN APPRART ADJA KON ADJA NN VVPP"); // Bsp. "Internetplattformen zur privaten und geschäftlichen Kontaktpflege untersucht"
patternList.add("NN APPRART NN KON NN APPR ADJA"); // Bsp. "Erfahrung beim Implementieren und Betreiben von sicheren"
patternList.add("NN APPRART NN KON NN APPR NN"); // Bsp. "Verfahren zur Verteilung und Überprüfung von kryptografischen"
patternList.add("NN APPRART NN KON NN PTKZU VVINF"); // Bsp. "Verfahren zur Authentisierung und Verschlüsselung zu entwickeln"
patternList.add("NN ART ADJA KON ADJA NN ART"); // Bsp. "Durchführung einer umfassenden und detaillierten Sicherheitsanalyse der"
patternList.add("NN ART ADJA KON ADJA NN KON"); // Bsp. "Technik eine schnellere und bessere Warenverfolgung und"
patternList.add("NN ART ADJA KON ADJA NN VVPP"); // Bsp. "Hydra eine kontextsensitive und sichere Middleware entwickelt"
patternList.add("NN ART NN KON ART NN ADJA"); // Bsp. "Veröffentlichung eines Spielfilms oder eines Musikstücks illegale"
patternList.add("NN ART NN KON ART NN ADV"); // Bsp. "Kenntnis des Einbettungsalgorithmus und des Wasserzeichencodes auch"
patternList.add("NN ART NN KON NN VAFIN ART"); // Bsp. "Wohle der Wirtschaft und Gesellschaft sind ein"
patternList.add("NN ART NN KON NN"); // Bsp. "Fragen der Autorschaft und Authentizität."
patternList.add("NN KOKOM NE KON NN APPR NE"); // Bsp. "Geräte wie Handy oder PDA auf Java"
patternList.add("NN KOKOM NN KON NN VVFIN PTKVZ"); // Bsp. "Geheimnisse wie Passwörter oder PINs verschlüsselt auf"
```


$T \approx T'$

Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Conjunction Modulation:** What's behind it?

lassen	sich	Manipulationen	und	Systemausfälle	verhindern
VVFIN	PRF	NN	KON	NN	VVINF

- Both nouns (NN) are connected through the "und" conjunction (KON)
- They're both independent from all the other words in the sentence, (more formaly, they are **constituents** !)
- **Grammer rule:** "*Only for constituents it is permitted to be swapped* ***closed*** *inside a sentence…*"
- How does a machine recognizes constituents? → Chunker (e.g. Stanford Parser)

Embedding methods: Overview

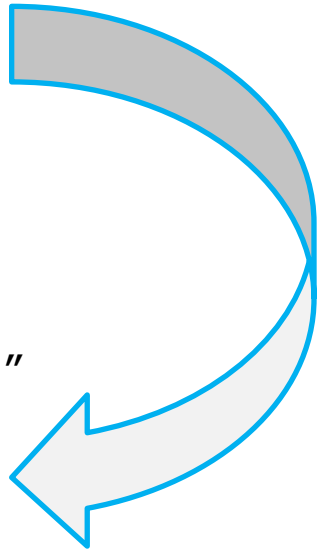
TECHNISCHE UNIVERSITÄT DARMSTADT

- **Enumeration Modulation**

Idea: slightly different than the Conjunction Modulation method
Swap open-class words, which are separated by comma…

$\mathcal{T}_1$ = "*…Fertigprodukte wie **Pizza**, **Cornflakes** oder Limonade…*"

$\mathcal{T}_2$ = "*…der **teuren**, **serviceaufwändigen** und kunden-unfreundlichen Technik…*"



$\mathcal{T}_1'$ = "*…Fertigprodukte wie **Cornflakes, Pizza** oder Limonade…*"

$\mathcal{T}_2'$ = "*…der **serviceaufwändigen, teuren** und kunden-unfreundlichen Technik…*"

$\mathcal{T} \approx \mathcal{T}'$

Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Center Permutation**

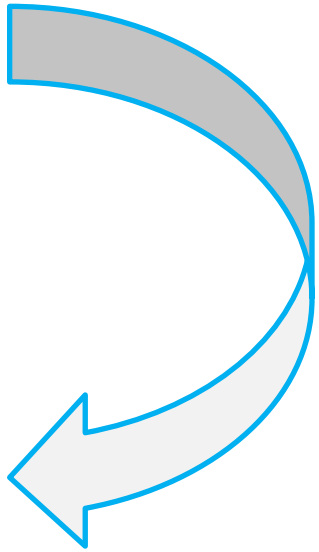
  Idea: Swap independent constituents in the middle field of a sentence…

  $\mathcal{T}_1$ = "…*Opa Rainer hat* ***seinem Enkel das Buch gestern*** *geschenkt…*"

  $\mathcal{T}'_1$ = "…*Opa Rainer hat* ***das Buch seinem Enkel*** *gestern geschenkt…*"

  = "…*Opa Rainer hat* ***gestern das Buch*** *seinem Enkel geschenkt…*"

  = "…*Opa Rainer hat* ***gestern seinem Enkel*** *das Buch geschenkt…*"



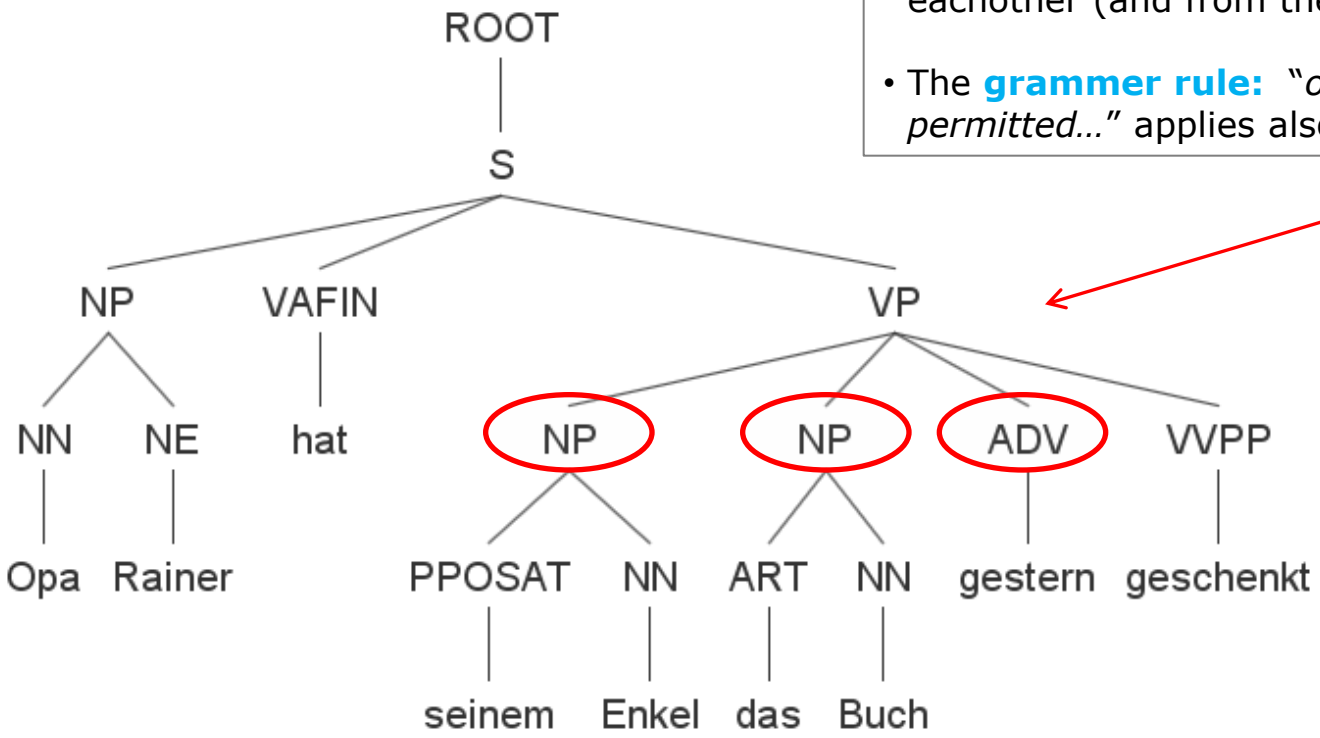
$\mathcal{T} \approx \mathcal{T}'$

Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Center Permutation:** How does it work?

- The three constituents are all **independent** from eachother (and from the rest of the sentence)
- The **grammer rule:** *"only for constituents it is permitted…"* applies also here !

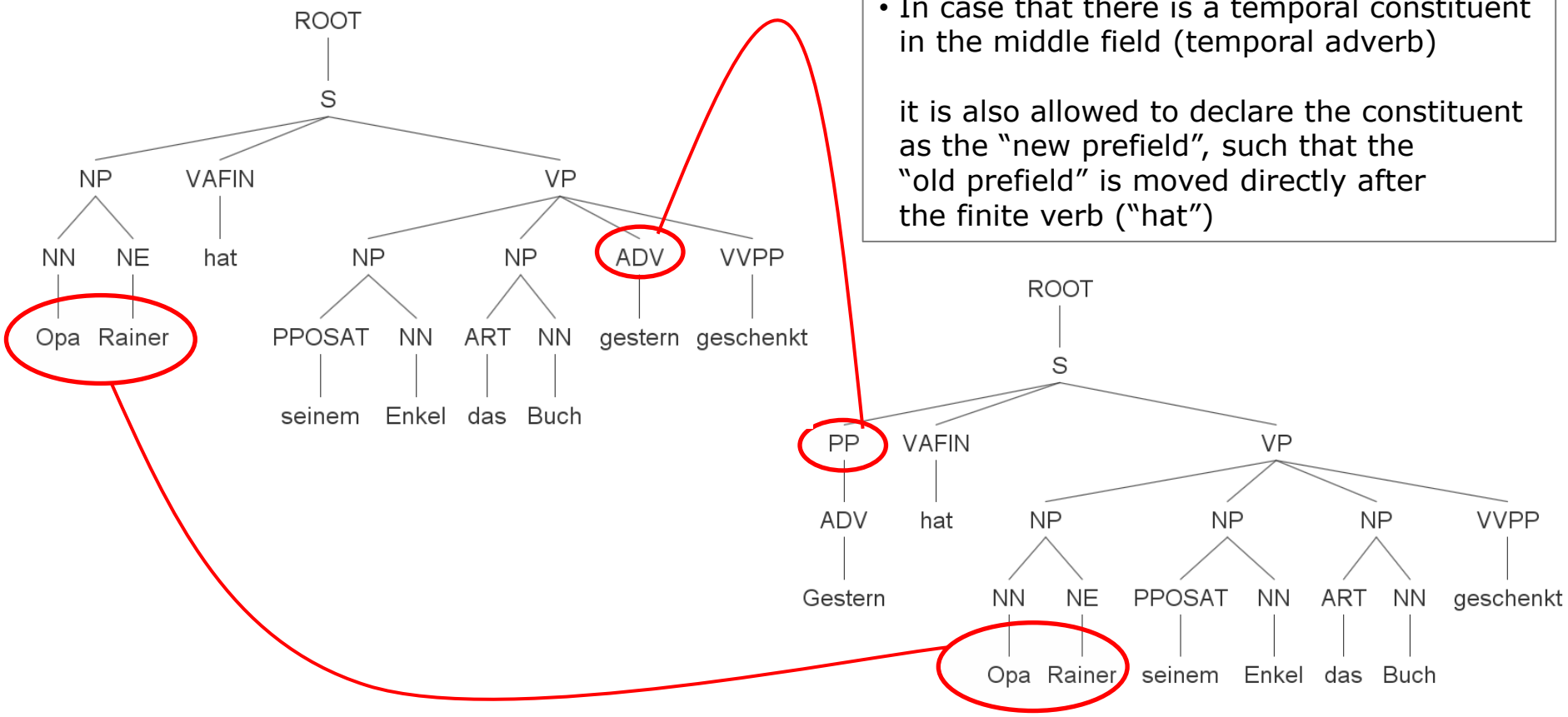


$T \approx T'$

Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Center Permutation:** How does it work?



- In case that there is a temporal constituent in the middle field (temporal adverb)

  it is also allowed to declare the constituent as the "new prefield", such that the "old prefield" is moved directly after the finite verb ("hat")

Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Hyponym & Troponym Truncation**

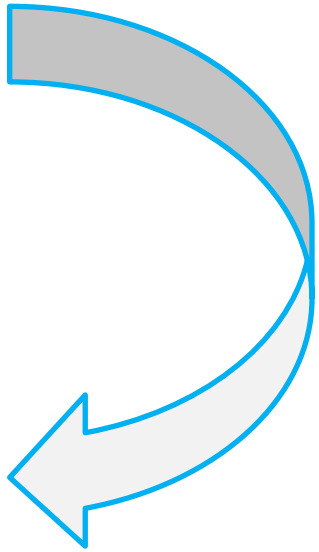
  Idea: Replace noun/verb by it's direct Hyponym…

  $\mathcal{T}_1$ = "*…gestern wurde unser Nachbar von einem* ***Bullterrier*** *gebissen…*"

  $\mathcal{T}_2$ = "*…Zum Öffnen des Gehäuses wird ein* ***Kreuz-schraubenzieher*** *benötigt…*"

  $\mathcal{T}'_1$ = "*…gestern wurde unser Nachbar von einem* ***Terrier*** *gebissen…*"

  $\mathcal{T}'_2$ = "*…Zum Öffnen des Gehäuses wird ein* ***Schraubenzieher*** *benötigt…*"



$\mathcal{T} \approx \mathcal{T}'$

Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Hyponym & Troponym Truncation**

  How does it work?

- Pickup a word from a sentence, e.g. “Perserkatze”

- Build a hyponym-chain (at least 3 hyponyms)

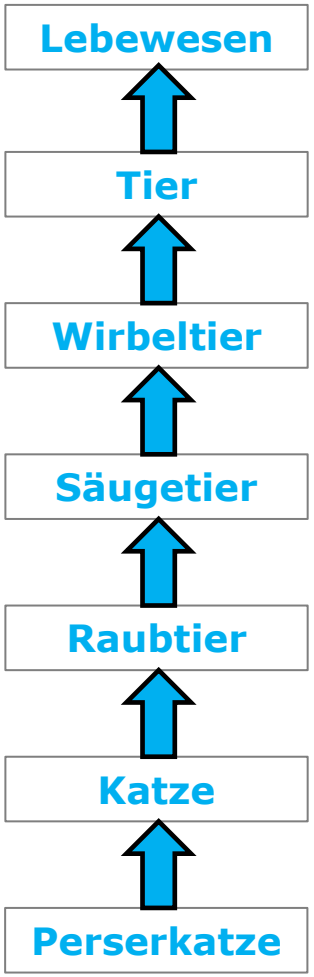
Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Hyponym & Troponym Truncation**

  How does it work?

- Pickup a word from a sentence, e.g. “Perserkatze”
- Build a hyponym-chain (at least 3 hyponyms)



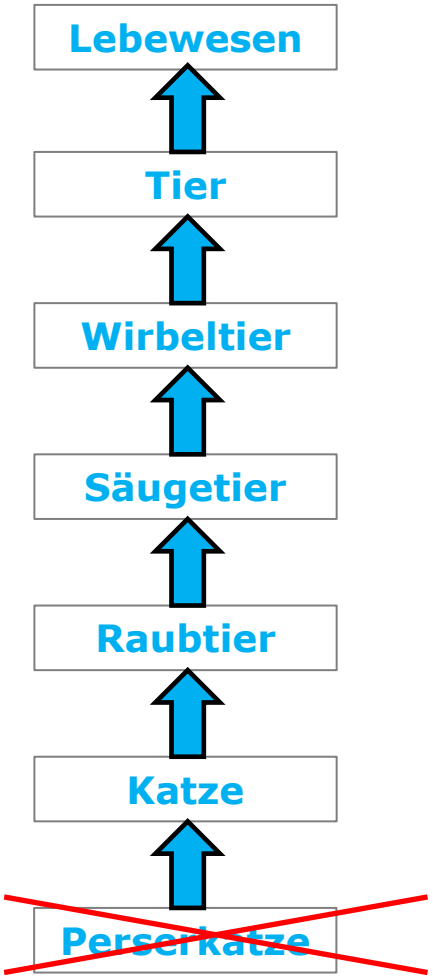
Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Hyponym & Troponym Truncation**

  How does it work?

- Pickup a word from a sentence, e.g. “Perserkatze”
- Build a hyponym-chain (at least 3 hyponyms)
- Truncate chain at the hyponym next to last and replace old word by it‘s direct hyponym…



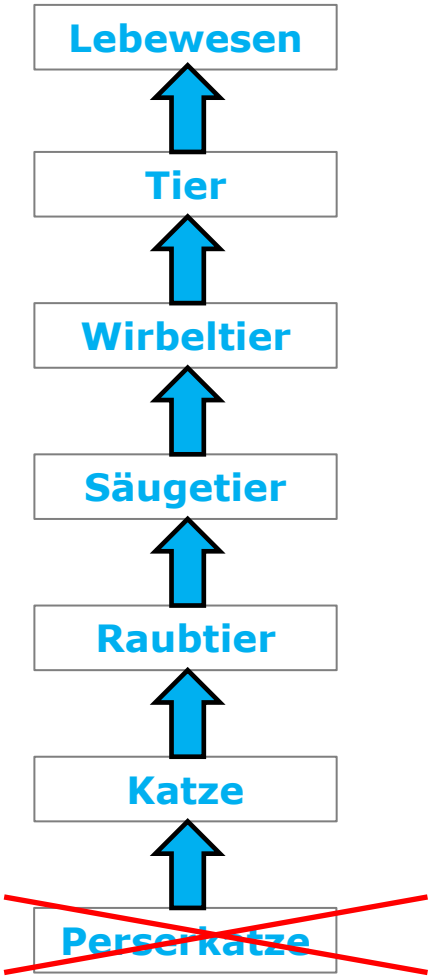
Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Hyponym & Troponym Truncation**

  How does it work?

- Pickup a word from a sentence, e.g. “Perserkatze”
- Build a hyponym-chain (at least 3 hyponyms)
- Truncate chain at the hyponym next to last and replace old word by it‘s direct hyponym…
- May loose information on details level…
  BUT sense will always remain the same!
- **Note:** good results, if hyponym appears as a substring of the old word (Katze / Perserkatze)



Embedding methods: Overview

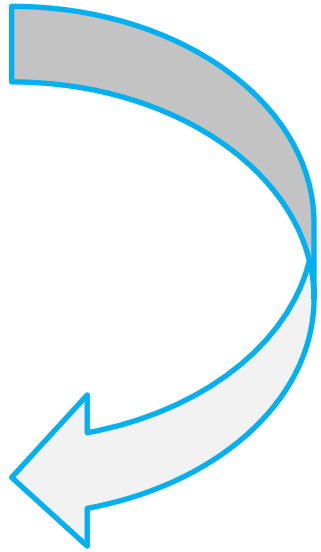
TECHNISCHE UNIVERSITÄT DARMSTADT

- **Synonym Substitution**

Idea: Replace a word (mostly adverbs/adjectives) with a similar synonym…

$\mathcal{T}_1$ = "*…könnte nach BP-Angaben deutlich mehr Öl austreten, als **bislang** angenommen…*"

$\mathcal{T}_2$ = "*…im zweiten Wahlgang ist für Komorowski daher **optimistischer** als…*"



$\mathcal{T}'_1$ = "*…könnte nach BP-Angaben deutlich mehr Öl austreten, als **bisher** angenommen…*"

$\mathcal{T}'_2$ = "*…im zweiten Wahlgang ist für Komorowski daher **zuversichtlicher** als…*"

$\mathcal{T} \approx \mathcal{T}'$

Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Synonym Substitution:** How does it work?

Before words can be replaced, it's necessary to have a synonym database

118	angeschlossen	einig	zugehörig	angegliedert	verbunden	
119	angeschwollen	wulstig	dick	bauschig	gebauscht	geschwollen
120	angespannt	nervös	gespannt			
121	angestellt	beschäftigt	tätig			
122	angrenzend	nahe	anliegend	daneben	bei	benachbart
123	angriffslustig	streitlustig	offensiv	aggressiv		
124	ängstlich	mutlos	feige	schüchtern		
125	anheimelnd	gemütlich	lauschig			
126	änigmatisch	rätselhaft	enigmatisch			
127	anlässlich	aus Anlass				
128	anliegend	anbei	beiliegend	beigefügt	beigelegt	als Anlage
129	anmaßend	breitspurig	hochmütig	vermessen	stolz	hybrid
130	annähernd	so gut wie	gerade noch	beinahe	nahezu	um ein Haar
131	annehmbar	in Ordnung	ganz recht	gut so		
132	annual	alljährlich	per annum	jährlich	pro Jahr	jedes Jahr
133	annualisiert	auf ein Jahr gerechnet				
134	anonym	namenlos	unnennbar	ungenannt		
135	anscheinend	augenscheinlich	scheinbar			
136	anschließend	danach	nachfolgend	anknüpfend	nachkommend	im Folgenden
137	anspornend	motivierend	animierend	ermutigend	aufputschend	antreibend
138	anstandslos	sicherlich	gern	gerne	freudig	freilich

Database can be either **local** or **external** (e.g. Uni-Leipzig knowledge base)

$T \approx T'$

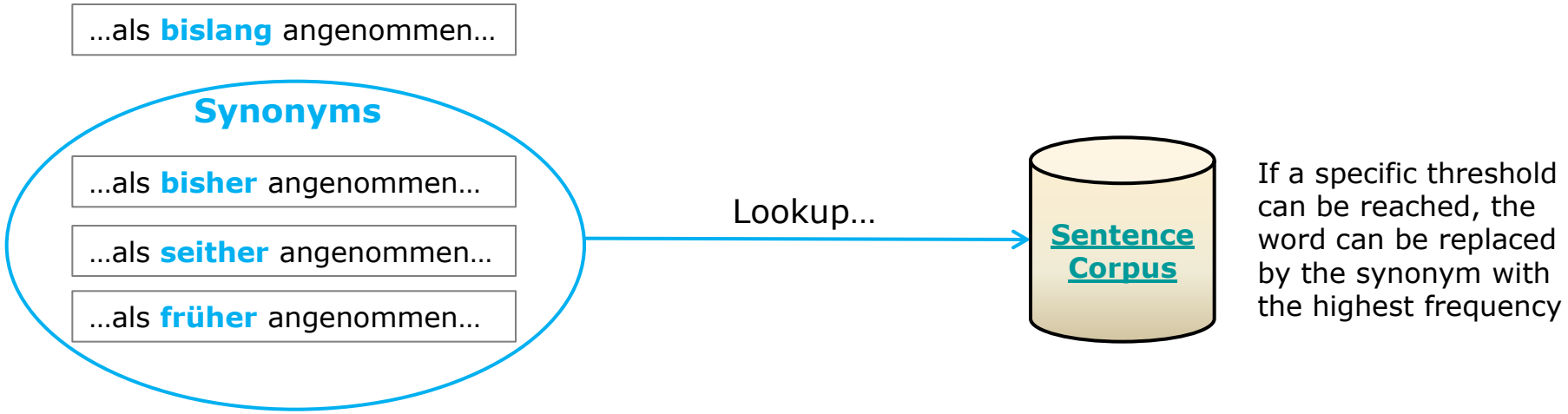
Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Synonym Substitution:** How does it work?

- Once a synonym is chosen, it must be sure that it's somehow replaceable with the original word (preserve meaning…)

- Idea: Lookup in a concordancer for occurance of original and marked word, use a context-window with a minimum of <u>two</u> surrounding neigbours…



$T \approx T'$

Embedding methods: Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Synonym Substitution:** ***alternative approach…***

No matter which tricks you try to apply – this method is a challenge !

But there are quite other alternative approaches, e.g. Phrase Substitution

$\mathcal{T}_1$ = "***Ich begreife nicht was Sie meinen …***"

$\mathcal{T}'_1$ = "***Ich kann Ihnen nicht folgen…***"

Problem: requires (several) phrase corpora (e.g. Wiki-Phrases)

$\mathcal{T} \approx \mathcal{T}'$

Challenges in NLW

TECHNISCHE UNIVERSITÄT DARMSTADT

- Nor of the presented methods is 100% "bulletproof" ☹
- Most expensive part of NLW is: **evaluation of the result**…

Only **humans** are able to judge if a transformation is 100% justified !

- Embedding usefull watermarking-messages (> 32bit) requires larger texts, ≈ 10KBytes is a quite good start…
- Embedding methods usually work together, but sometimes they can block eachother, such that the whole embedding process fails…

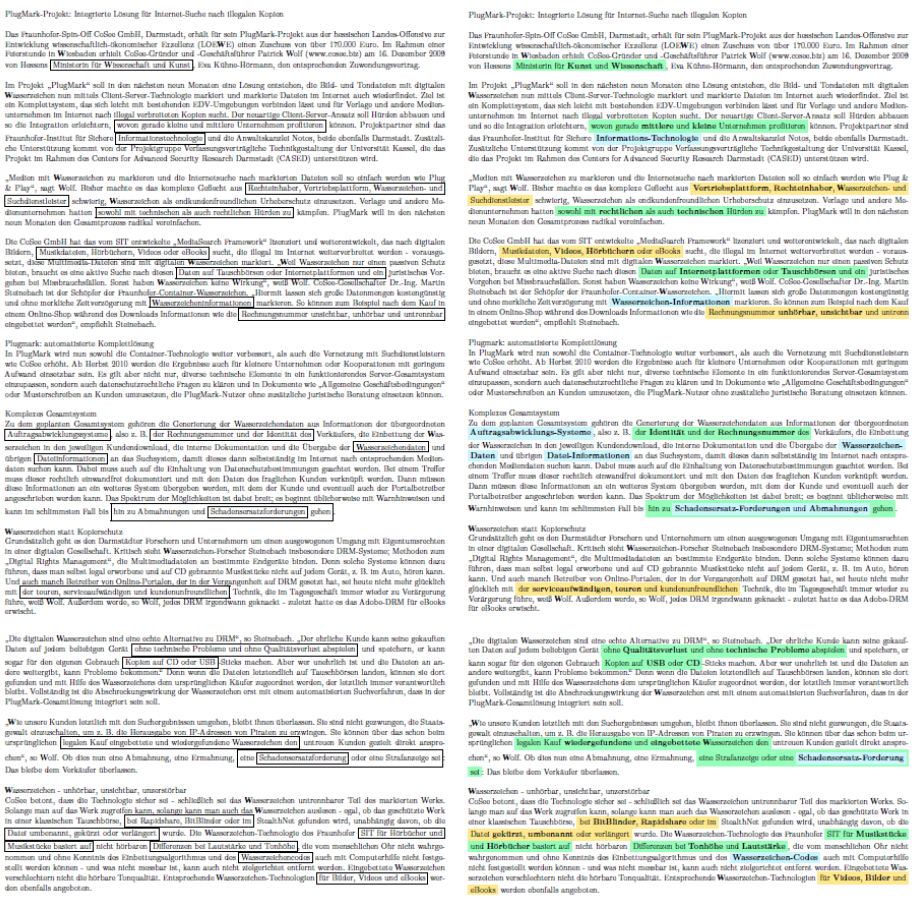
$T \approx T'$

Challenges in NLW

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Example**

T T'



PlugMark-Projekt: Integrierte Lösung für Internet-Suche nach illegalen Kopien

Das Fraunhofer-Spin-Off CoSeo GmbH, Darmstadt, erhält für sein PlugMark-Projekt aus der hessischen Landes-Offensive zur Entwicklung wissenschaftlich-ökonomischer Exzellenz (LOEWE) einen Zuschuss von über 170.000 Euro. Im Rahmen einer Feierstunde in Wiesbaden erhielt CoSeo-Gründer und -Geschäftsführer Patrick Wolf (www.coseo.biz) am 16. Dezember 2009 von Hessens Ministerin für Wissenschaft und Kunst, Eva Kühne-Hörmann, den entsprechenden Zuwendungsvertrag.

Im Projekt „PlugMark" soll in den nächsten neun Monaten eine Lösung entstehen, die Bild- und Tondateien mit digitalen Wasserzeichen nun mittels Client-Server-Technologie markiert und markierte Dateien im Internet auch wiederfindet. Ziel ist ein Komplettsystem, das sich leicht mit bestehenden EDV-Umgebungen verbinden lässt und für Verlage und andere Medienunternehmen im Internet nach illegal verbreiteten Kopien sucht. Der neuartige Client-Server-Ansatz soll Hürden abbauen und so die Integration erleichtern, wovon gerade kleine und mittlere Unternehmen profitieren können. Projektpartner sind das Fraunhofer-Institut für Sichere Informationstechnologie und die Anwaltskanzlei Notos, beide ebenfalls Darmstadt. Zusätzliche Unterstützung kommt von der Projektgruppe Verfassungsverträgliche Technikgestaltung der Universität Kassel, die das Projekt im Rahmen des Centers for Advanced Security Research Darmstadt (CASED) unterstützen wird.

„Medien mit Wasserzeichen zu markieren und die Internetsuche nach markierten Dateien soll so einfach werden wie Plug & Play", sagt Wolf. Bisher machte es das komplexe Gefecht aus Rechtsinhaber, Vertriebsplattform, Wasserzeichen- und Suchdienstleister schwierig, Wasserzeichen als endkundenfreundlichen Urheberschutz einzusetzen. Verlage und andere Medienunternehmen hatten sowohl mit technischen als auch rechtlichen Hürden zu kämpfen. PlugMark will in den nächsten neun Monaten den Gesamtprozess radikal vereinfachen.

Die CoSeo GmbH hat das vom SIT entwickelte „MediaSearch Framework" lizenziert und weiterentwickelt, das nach digitalen Bildern, Musikdateien, Hörbüchern, Videos oder eBooks sucht, die illegal im Internet weiterverbreitet werden - vorausgesetzt, diese Multimedia-Dateien sind mit digitalen Wasserzeichen markiert. „Weil Wasserzeichen nur einen passiven Schutz bieten, braucht es eine aktive Suche nach diesen Dateien auf Tauschbörsen oder Internetplattformen und ein juristisches Vorgehen bei Missbrauchsfällen. Sonst haben Wasserzeichen keine Wirkung", weiß Wolf. CoSeo-Gesellschafter Dr.-Ing. Martin Steinebach ist der Schöpfer der Fraunhofer-Container-Wasserzeichen. „Hiermit lassen sich große Datenmengen kostengünstig und ohne merkliche Zeitverzögerung mit Wasserzeicheninformationen markieren. So können zum Beispiel nach dem Kauf in einem Online-Shop während des Downloads Informationen wie die Rechnungsnummer unsichtbar, unhörbar und untrennbar eingebettet werden", empfiehlt Steinebach.

Plugmark: automatisierte Komplettlösung

In PlugMark wird nun sowohl die Container-Technologie weiter verbessert, als auch die Vernetzung mit Suchdienstleistern wie CoSeo erhöht. Ab Herbst 2010 werden die Ergebnisse auch für kleinere Unternehmen oder Kooperationen mit geringem Aufwand einsetzbar sein. Es gilt aber nicht nur, diverse technische Elemente in ein funktionierendes Server-Gesamtsystem einzupassen, sondern auch datenschutzrechtliche Fragen zu klären und in Dokumente wie „Allgemeine Geschäftsbedingungen" oder Musterschreiben an Kunden umzusetzen, die PlugMark-Nutzer ohne zusätzliche juristische Beratung einsetzen können.

Komplexes Gesamtsystem

Zu dem geplanten Gesamtsystem gehören die Generierung der Wasserzeichendaten aus Informationen der übergeordneten Auftragsabwicklungssysteme, also z. B. der Rechnungsnummer und der Identität des Verkäufers, die Einbettung der Wasserzeichen in den jeweiligen Kundendownload, die interne Dokumentation und die Übergabe der Wasserzeichendaten und übrigen Dateiinformationen an das Suchsystem, damit dieses dann selbstständig im Internet nach entsprechenden Mediendaten suchen kann. Dabei muss auch auf die Einhaltung von Datenschutzbestimmungen geachtet werden. Bei einem Treffer muss dieser rechtlich einwandfrei dokumentiert und mit den Daten des fraglichen Kunden verknüpft werden. Dann müssen diese Informationen an ein weiteres System übergeben werden, mit dem der Kunde und eventuell auch der Portalbetreiber angeschrieben werden kann. Das Spektrum der Möglichkeiten ist dabei breit; es beginnt üblicherweise mit Warnhinweisen und kann im schlimmsten Fall bis hin zu Abmahnungen und Schadensersatzforderungen gehen.

Wasserzeichen statt Kopierschutz

Grundsätzlich geht es den Darmstädter Forschern und Unternehmern um einen ausgewogenen Umgang mit Eigentumsrechten in einer digitalen Gesellschaft. Kritisch sieht Wasserzeichen-Forscher Steinebach insbesondere DRM-Systeme; Methoden zum „Digital Rights Management", die Multimediadaten an bestimmte Endgeräte binden. Denn solche Systeme können dazu führen, dass man selbst legal erworbene und auf CD gebrannte Musikstücke nicht auf jedem Gerät, z. B. im Auto, hören kann. Und auch manch Betreiber von Online-Portalen, der in der Vergangenheit auf DRM gesetzt hat, sei heute nicht mehr glücklich mit der servicunfreundlichen, touren und kundenunfreundlichen Technik, die im Tagesgeschäft immer wieder zu Vertärgerung führe, weiß Wolf. Außerdem werde, so Wolf, jedes DRM irgendwann geknackt - zuletzt hatte es das Adobe-DRM für eBooks erwischt.

„Die digitalen Wasserzeichen sind eine echte Alternative zu DRM", so Steinebach. „Der ehrliche Kunde kann seine gekauften Daten auf jedem beliebigen Gerät ohne technische Probleme und ohne Qualitätsverlust abspielen und speichern, er kann sogar für den eigenen Gebrauch Kopien auf CD oder USB-Sticks machen. Aber wer unehrlich ist und die Daten an andere weitergibt, kann Probleme bekommen." Denn wenn die Daten letztendlich auf Tauschbörsen landen, können sie dort gefunden und mit Hilfe des Wasserzeichens dem ursprünglichen Käufer zugeordnet werden, der letztlich immer verantwortlich bleibt. Vollständig ist die Abschreckungswirkung der Wasserzeichen erst mit einem automatisierten Suchverfahren, dass in der PlugMark-Gesamtlösung integriert sein soll.

„Wo unsere Kunden lokalisiert mit den Suchergebnissen umgehen, bleibt ihnen überlassen. Sie sind nicht gezwungen, die Staatsgewalt einzuschalten, um z. B. die Herausgabe von IP-Adressen von Piraten zu erzwingen. Sie können über das schon beim ursprünglichen legalen Kauf eingebettete und wiedergefundene Wasserzeichen den unreuen Kunden gezielt direkt ansprechen", so Wolf. Ob dies nun eine Abmahnung, eine Ermahnung, eine Schadensersatzforderung oder eine Strafanzeige sei: Das bleibe dem Verkäufer überlassen.

Wasserzeichen - unhörbar, unsichtbar, unzerstörbar

CoSeo betont, dass die Technologie sicher sei - schließlich sei das Wasserzeichen untrennbarer Teil des markierten Werks. Solange man auf das Werk zugreifen kann, solange kann man auch das Wasserzeichen auslesen - egal, ob das geschützte Werk in einer klassischen Tauschbörse, bei Rapidshare, BitBlinder oder im StealthNet gefunden wird, unabhängig davon, ob die Datei umbenannt, gekürzt oder verlängert wurde. Die Wasserzeichen-Technologie des Fraunhofer SIT für Hörbücher und Musikstücke basiert auf nicht hörbaren Differenzen bei Lautstärke und Tonhöhe, die vom menschlichen Ohr nicht wahrgenommen und ohne Kenntnis des Einbettungsalgorithmus und des Wasserzeichencodes auch mit Computerhilfe nicht festgestellt werden können - und was nicht messbar ist, kann auch nicht zielgerichtet entfernt werden. Eingebettete Wasserzeichen verschlechtern nicht die hörbare Tonqualität. Entsprechende Wasserzeichen-Technologien für Bilder, Videos und eBooks werden ebenfalls angeboten.

PlugMark-Projekt: Integrierte Lösung für Internet-Suche nach illegalen Kopien

Das Fraunhofer-Spin-Off CoSeo GmbH, Darmstadt, erhält für sein PlugMark-Projekt aus der hessischen Landes-Offensive zur Entwicklung wissenschaftlich-ökonomischer Exzellenz (LOEWE) einen Zuschuss von über 170.000 Euro. Im Rahmen einer Feierstunde in Wiesbaden erhielt CoSeo-Gründer und -Geschäftsführer Patrick Wolf (www.coseo.biz) am 16. Dezember 2009 von Hessens Ministerin für Kunst und Wissenschaft, Eva Kühne-Hörmann, den entsprechenden Zuwendungsvertrag.

Im Projekt „PlugMark" soll in den nächsten neun Monaten eine Lösung entstehen, die Bild- und Tondateien mit digitalen Wasserzeichen nun mittels Client-Server-Technologie markiert und markierte Dateien im Internet auch wiederfindet. Ziel ist ein Komplettsystem, das sich leicht mit bestehenden EDV-Umgebungen verbinden lässt und für Verlage und andere Medienunternehmen im Internet nach illegal verbreiteten Kopien sucht. Der neuartige Client-Server-Ansatz soll Hürden abbauen und so die Integration erleichtern, wovon gerade mittlere und kleine Unternehmen profitieren können. Projektpartner sind das Fraunhofer-Institut für Sichere Informations-Technologie und die Anwaltskanzlei Notos, beide ebenfalls Darmstadt. Zusätzliche Unterstützung kommt von der Projektgruppe Verfassungsverträgliche Technikgestaltung der Universität Kassel, die das Projekt im Rahmen des Centers for Advanced Security Research Darmstadt (CASED) unterstützen wird.

„Medien mit Wasserzeichen zu markieren und die Internetsuche nach markierten Dateien soll so einfach werden wie Plug & Play", sagt Wolf. Bisher machte es das komplexe Gefecht aus Vertriebsplattform, Rechtsinhaber, Wasserzeichen- und Suchdienstleister schwierig, Wasserzeichen als endkundenfreundlichen Urheberschutz einzusetzen. Verlage und andere Medienunternehmen hatten sowohl mit rechtlichen als auch technischen Hürden zu kämpfen. PlugMark will in den nächsten neun Monaten den Gesamtprozess radikal vereinfachen.

Die CoSeo GmbH hat das vom SIT entwickelte „MediaSearch Framework" lizenziert und weiterentwickelt, das nach digitalen Bildern, Musikdateien, Videos, Hörbüchern oder eBooks sucht, die illegal im Internet weiterverbreitet werden - vorausgesetzt, diese Multimedia-Dateien sind mit digitalen Wasserzeichen markiert. „Weil Wasserzeichen nur einen passiven Schutz bieten, braucht es eine aktive Suche nach diesen Dateien auf Internetplattformen oder Tauschbörsen und ein juristisches Vorgehen bei Missbrauchsfällen. Sonst haben Wasserzeichen keine Wirkung", weiß Wolf. CoSeo-Gesellschafter Dr.-Ing. Martin Steinebach ist der Schöpfer der Fraunhofer-Container-Wasserzeichen. „Hiermit lassen sich große Datenmengen kostengünstig und ohne merkliche Zeitverzögerung mit Wasserzeichen-Informationen markieren. So können zum Beispiel nach dem Kauf in einem Online-Shop während des Downloads Informationen wie die Rechnungsnummer unlöschbar, unsichtbar und untrennbar eingebettet werden", empfiehlt Steinebach.

Plugmark: automatisierte Komplettlösung

In PlugMark wird nun sowohl die Container-Technologie weiter verbessert, als auch die Vernetzung mit Suchdienstleistern wie CoSeo erhöht. Ab Herbst 2010 werden die Ergebnisse auch für kleinere Unternehmen oder Kooperationen mit geringem Aufwand einsetzbar sein. Es gilt aber nicht nur, diverse technische Elemente in ein funktionierendes Server-Gesamtsystem einzupassen, sondern auch datenschutzrechtliche Fragen zu klären und in Dokumente wie „Allgemeine Geschäftsbedingungen" oder Musterschreiben an Kunden umzusetzen, die PlugMark-Nutzer ohne zusätzliche juristische Beratung einsetzen können.

Komplexes Gesamtsystem

Zu dem geplanten Gesamtsystem gehören die Generierung der Wasserzeichendaten aus Informationen der übergeordneten Auftragsabwicklungs-Systeme, also z. B. der Identität und der Rechnungsnummer des Verkäufers, die Einbettung der Wasserzeichen in den jeweiligen Kundendownload, die interne Dokumentation und die Übergabe der Wasserzeichen-Daten und übrigen Datei-Informationen an das Suchsystem, damit dieses dann selbstständig im Internet nach entsprechenden Mediendaten suchen kann. Dabei muss auch auf die Einhaltung von Datenschutzbestimmungen geachtet werden. Bei einem Treffer muss dieser rechtlich einwandfrei dokumentiert und mit den Daten des fraglichen Kunden verknüpft werden. Dann müssen diese Informationen an ein weiteres System übergeben werden, mit dem der Kunde und eventuell auch der Portalbetreiber angeschrieben werden kann. Das Spektrum der Möglichkeiten ist dabei breit; es beginnt üblicherweise mit Warnhinweisen und kann im schlimmsten Fall bis hin zu Schadensersatz-Forderungen und Abmahnungen gehen.

Wasserzeichen statt Kopierschutz

Grundsätzlich geht es den Darmstädter Forschern und Unternehmern um einen ausgewogenen Umgang mit Eigentumsrechten in einer digitalen Gesellschaft. Kritisch sieht Wasserzeichen-Forscher Steinebach insbesondere DRM-Systeme; Methoden zum „Digital Rights Management", die Multimediadaten an bestimmte Endgeräte binden. Denn solche Systeme können dazu führen, dass man selbst legal erworbene und auf CD gebrannte Musikstücke nicht auf jedem Gerät, z. B. im Auto, hören kann. Und auch manch Betreiber von Online-Portalen, der in der Vergangenheit auf DRM gesetzt hat, sei heute nicht mehr glücklich mit der servicunfreundlichen, touren und kundenunfreundlichen Technik, die im Tagesgeschäft immer wieder zu Vertärgerung führe, weiß Wolf. Außerdem werde, so Wolf, jedes DRM irgendwann geknackt - zuletzt hatte es das Adobe-DRM für eBooks erwischt.

„Die digitalen Wasserzeichen sind eine echte Alternative zu DRM", so Steinebach. „Der ehrliche Kunde kann seine gekauften Daten auf jedem beliebigen Gerät ohne Qualitätsverlust und ohne technische Probleme abspielen und speichern, er kann sogar für den eigenen Gebrauch Kopien auf USB oder CD-Sticks machen. Aber wer unehrlich ist und die Daten an andere weitergibt, kann Probleme bekommen." Denn wenn die Daten letztendlich auf Tauschbörsen landen, können sie dort gefunden und mit Hilfe des Wasserzeichens dem ursprünglichen Käufer zugeordnet werden, der letztlich immer verantwortlich bleibt. Vollständig ist die Abschreckungswirkung der Wasserzeichen erst mit einem automatisierten Suchverfahren, dass in der PlugMark-Gesamtlösung integriert sein soll.

„Wo unsere Kunden lokalisiert mit den Suchergebnissen umgehen, bleibt ihnen überlassen. Sie sind nicht gezwungen, die Staatsgewalt einzuschalten, um z. B. die Herausgabe von IP-Adressen von Piraten zu erzwingen. Sie können über das schon beim ursprünglichen legalen Kauf wiedergefundene und eingebettete Wasserzeichen den unreuen Kunden gezielt direkt ansprechen", so Wolf. Ob dies nun eine Abmahnung, eine Ermahnung, eine Strafanzeige oder eine Schadensersatz-Forderung sei: Das bleibe dem Verkäufer überlassen.

Wasserzeichen - unhörbar, unsichtbar, unzerstörbar

CoSeo betont, dass die Technologie sicher sei - schließlich sei das Wasserzeichen untrennbarer Teil des markierten Werks. Solange man auf das Werk zugreifen kann, solange kann man auch das Wasserzeichen auslesen - egal, ob das geschützte Werk in einer klassischen Tauschbörse, bei BitBlinder, Rapidshare oder im StealthNet gefunden wird, unabhängig davon, ob die Datei gekürzt, umbenannt oder verlängert wurde. Die Wasserzeichen-Technologie des Fraunhofer SIT für Musikstücke und Hörbücher basiert auf nicht hörbaren Differenzen bei Tonhöhe und Lautstärke, die vom menschlichen Ohr nicht wahrgenommen und ohne Kenntnis des Einbettungsalgorithmus und des Wasserzeichen-Codes auch mit Computerhilfe nicht festgestellt werden können - und was nicht messbar ist, kann auch nicht zielgerichtet entfernt werden. Eingebettete Wasserzeichen verschlechtern nicht die hörbare Tonqualität. Entsprechende Wasserzeichen-Technologien für Videos, Bilder und eBooks werden ebenfalls angeboten.

$T \approx T'$

TECHNISCHE UNIVERSITÄT DARMSTADT

Questions?

TECHNISCHE UNIVERSITÄT DARMSTADT

Thanks for your attention…

References

- "**Foundations of individual Text-Watermarking**",

  O. Halvani, Bachelor thesis, 2010.

- "**The Prisoners' Problem and the Subliminal Channel**",

  http://www.cs.nccu.edu.tw/~raylin/UndergraduateCourse/ComtenporaryCryptography/Spring2009/ThePrisonerProblem.pdf