University of St.Gallen

School of Computer Science (SCS)
Artificial Intelligence & Machine Learning [AI:ML]

The AAAI 2021 KDF Workshop

"From insight to impact"

Leaking Sensitive Accounting Data in Plain Sight using Deep Autoencoder Neural Networks

February 9th, 2021

Marco Schreyer[1], Christian Schulze[2] and Damian Borth[1]
[1]University of St.Gallen (HSG), [2]German Research Center for Artificial Intelligence (DFKI)

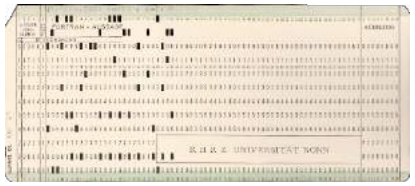
Introduction & Background

Artificial Intelligence and Machine Learning
University of St.Gallen

Evolution of Recording and Processing of Enterprise Resource Planning Data

1940

~1960



~1990

Data Volume

Towards the "Big Data" Driven Economy

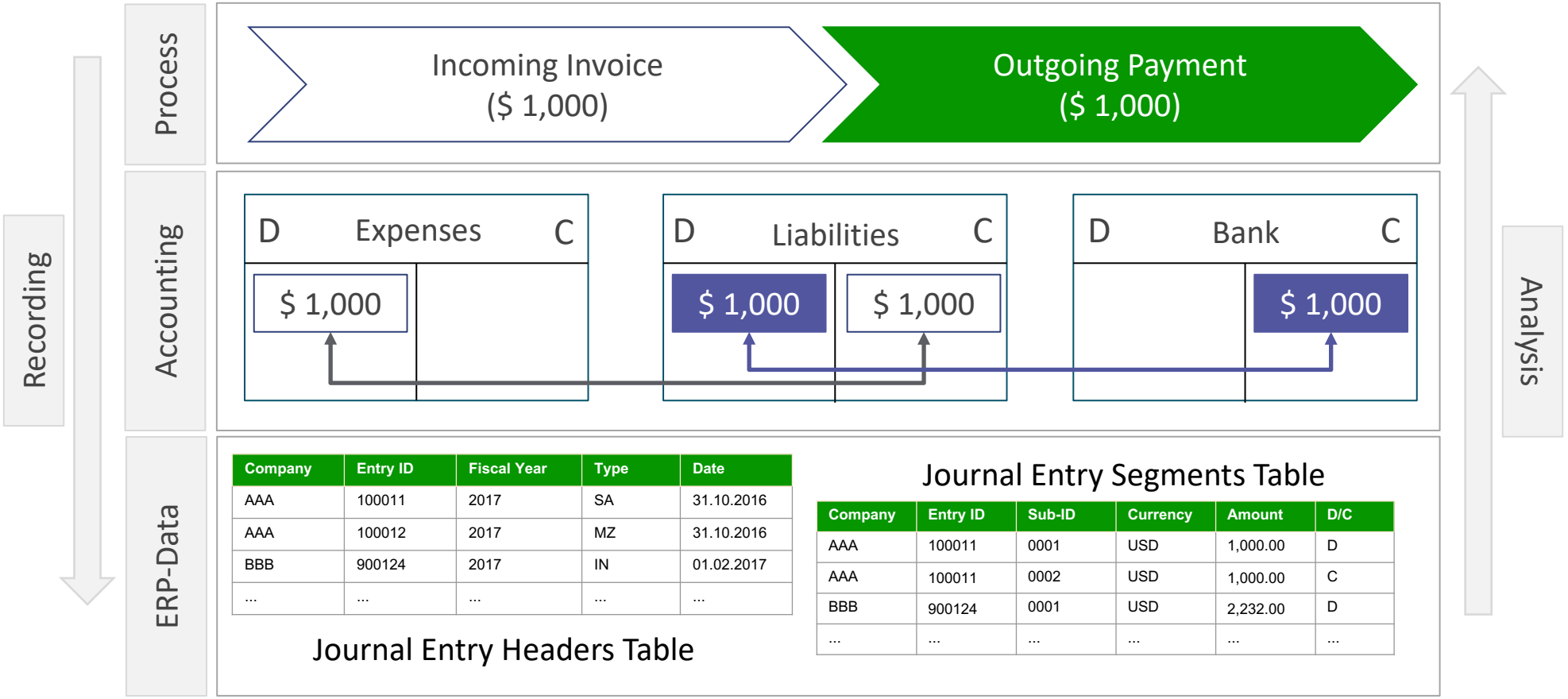
- Displacement of the non-digital processing of organizational activities
- Accumulation of exhaustive volumes of transactional and accounting data
- Almost every activity within an organization leaves **a digital trace** ... !

Following: Vasarhelyi, M. A., Kogan, A., Tuttle, B. M., "Big Data in Accounting: An Overview", Accounting Horizons, Vol. 29, No. 2, 2015
Warren Jr., J. D., Mofitt K. C., Byrnes, P., "How Big Data Will Change Accounting", Accounting Horizons, Vol. 29, No. 2, 2015
Brown-Liburd, H. and Vasarhelyi, M. A., "Big Data and Audit Evidence", Journal of Emerging Technologies in Accounting, Vol. 12, 2015

Introduction & Background

Artificial Intelligence and Machine Learning
University of St.Gallen

Evolution of Recording and Processing of Enterprise Resource Planning Data



Company	Entry ID	Fiscal Year	Type	Date
AAA	100011	2017	SA	31.10.2016
AAA	100012	2017	MZ	31.10.2016
BBB	900124	2017	IN	01.02.2017
...	...	...	...	...

Journal Entry Headers Table

Journal Entry Segments Table

Company	Entry ID	Sub-ID	Currency	Amount	D/C
AAA	100011	0001	USD	1,000.00	D
AAA	100011	0002	USD	1,000.00	C
BBB	900124	0001	USD	2,232.00	D
...	...	...	...	...	...

Introduction & Background

Artificial Intelligence and Machine Learning
University of St.Gallen

The Rise of Insider Threats

Deloitte.

”Approx. 59% of employees who leave an organization voluntarily or involuntary say they take sensitive data with them.”

Deloitte Global - “The Rise of Insider Threats Amid COVID-19”
Weekly high-level brief update, Issue 6, May 12, 2020

EUROPEAN UNION AGENCY FOR CYBERSECURITY

enisa

”The primary attack vector in information leakage is insiders.
This term is used to describe a person with an interest in ‘exfiltrating’ important inside information on behalf of a third party.”

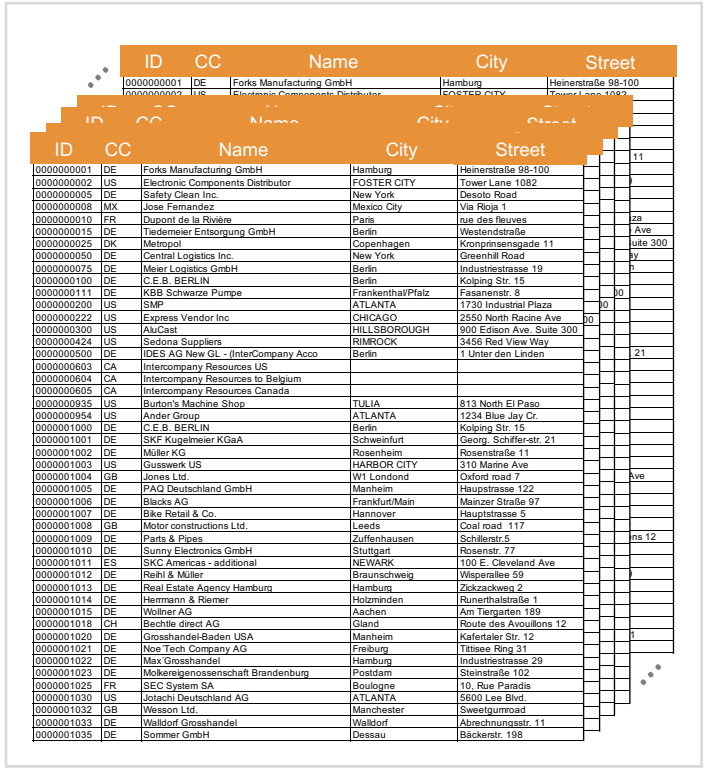
“Information Leakage - ENISA Threat Landscape 2019 – 2020”
The European Union Agency for Cybersecurity

Introduction & Background

Artificial Intelligence and Machine Learning
University of St.Gallen

The Sensitivity of Enterprise Resource Planning Data

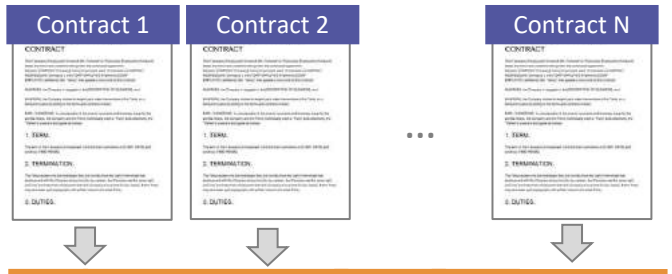
Customer Master Data



ID	CC	Name	City	Street
0000000001	DE	Forks Manufacturing GmbH	Hamburg	Heinerstraße 98-100
0000000002	US	Electronic Components Distributor	FOSTER CITY	Tower Lane 1082
0000000005	DE	Safety Clean Inc.	New York	Desoto Road
0000000008	MX	Jose Fernandez	Mexico City	Via Rioja 1
0000000010	FR	Dupont de la Rivière	Paris	rue des fleuves
0000000015	DE	Tiedemeier Entsorgung GmbH	Berlin	Westendstraße
0000000025	DK	Metropol	Copenhagen	Kronprinsengade 11
0000000050	DE	Central Logistics Inc.	New York	Greenhill Road
0000000075	DE	Meier Logistics GmbH	Berlin	Industriestrasse 19
0000000100	DE	C.E.B. BERLIN	Berlin	Kolping Str. 15
0000000111	DE	KBB Schwarze Pumpe	Frankenthal/Pfalz	Fasanenstr. 8
0000000200	US	SMP	ATLANTA	1730 Industrial Plaza
0000000222	US	Express Vendor Inc	CHICAGO	2550 North Racine Ave
0000000300	US	AluCast	HILLSBOROUGH	900 Edison Ave. Suite 300
0000000424	US	Sedona Suppliers	RIMROCK	3456 Red View Way
0000000500	DE	IDES AG New GL - (InterCompany Acco	Berlin	1 Unter den Linden
0000000603	CA	Intercompany Resources US		
0000000604	CA	Intercompany Resources to Belgium		
0000000605	CA	Intercompany Resources Canada		
0000000935	US	Burton's Machine Shop	TULIA	813 North El Paso
0000000954	US	Ander Group	ATLANTA	1234 Blue Jay Cr.
0000001000	DE	C.E.B. BERLIN	Berlin	Kolping Str. 15
0000001001	DE	SKF Kugelmeier KGaA	Schweinfurt	Georg. Schiffer-str. 21
0000001002	DE	Müller KG	Rosenheim	Rosenstraße 11
0000001003	US	Gusswerk US	HARBOR CITY	310 Marine Ave
0000001004	GB	Jones Ltd.	W1 Londond	Oxford road 7
0000001005	DE	PAQ Deutschland GmbH	Manheim	Hauptstrasse 122
0000001006	DE	Blacks AG	Frankfurt/Main	Mainzer Straße 97
0000001007	DE	Bike Retail & Co.	Hannover	Hauptstrasse 5
0000001008	GB	Motor constructions Ltd.	Leeds	Coal road 117
0000001009	DE	Parts & Pipes	Zuffenhausen	Schillerstr.5
0000001010	DE	Sunny Electronics GmbH	Stuttgart	Rosenstr. 77
0000001011	ES	SKC Americas - additional	NEWARK	100 E. Cleveland Ave
0000001012	DE	Reihl & Müller	Braunschweig	Wisperallee 59
0000001013	DE	Real Estate Agency Hamburg	Hamburg	Zickzackweg 2
0000001014	DE	Hermann & Riemer	Holzminden	Runerthalstraße 1
0000001015	DE	Wollner AG	Aachen	Am Tiergarten 189
0000001018	CH	Bechtle direct AG	Gland	Route des Avouillons 12
0000001020	DE	Grosshandel-Baden USA	Manheim	Kafertaler Str. 12
0000001021	DE	Noe Tech Company AG	Freiburg	Tittisee Ring 31
0000001022	DE	Max Grosshandel	Hamburg	Industriestrasse 29
0000001023	DE	Molkereigenossenschaft Brandenburg	Postdam	Steinstraße 102
0000001025	FR	SEC System SA	Boulogne	10, Rue Paradis
0000001030	US	Jotachi Deutschland AG	ATLANTA	5600 Lee Blvd.
0000001032	GB	Wesson Ltd.	Manchester	Sweetgumroad
0000001033	DE	Walldorf Grosshandel	Walldorf	Abrechnungsstr. 11
0000001035	DE	Sommer GmbH	Dessau	Bäckerstr. 198

e.g., SAP-Tables: KNA1, KNB1, KNBK, …

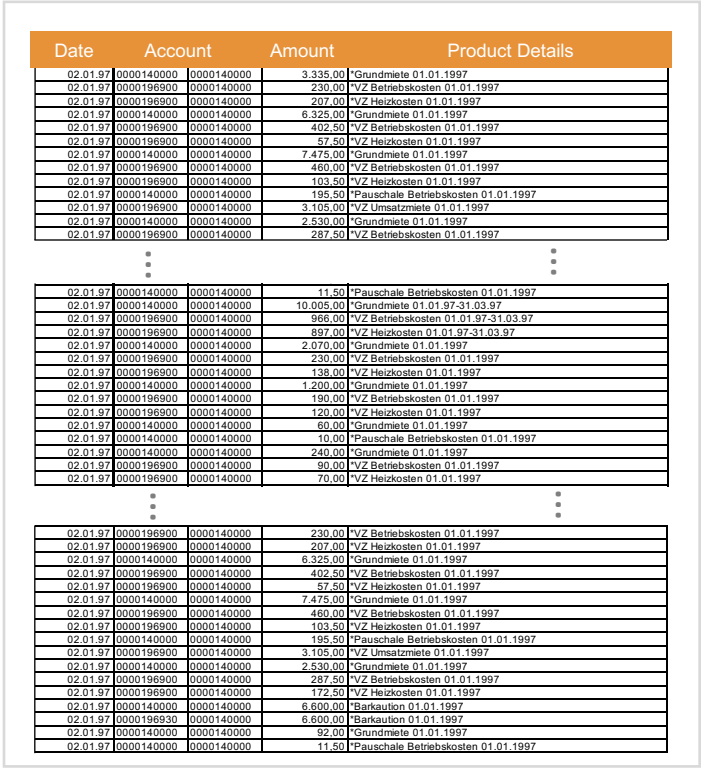
Vendor Contractual Data



ID	Product	Volume		Price	Unit	Price
3000000004	Desk Pads	ST	ST	27,95	1	27,95
3000000004	Mouse Pads	ST	ST	10,95	1	10,95
3000000005	IDES Consumer Products / IDES	ST	ST	27,95	1	27,95
3000000005	IDES Consumer Products / IDES	ST	ST	10,95	1	10,95
3000000006	Artgallery Multimedia	ST	ST	52,99	1	52,99
3000000006	Ides Text processing Professional, Windo	ST	ST	64,99	1	64,99
3000000006	Ides Text processing Standard, Windows 9	ST	ST	49,50	1	49,50
3000000007	High Speed Printer/Laser Printer	ST	ST	2.228,00	1	2.228,00
3000000007	Maxitec R 3200 personal computer	ST	ST	1.698,00	1	1.698,00
3000000007	PAQ Monitor, 21", Color	ST	ST	532,00	1	532,00
3000000008	Dishwasher Gel, Automatic	ST	ST	6,95	1	13,90
3000000008	Cleaner, Clear Vision Glass	ST	ST	9,95	1	29,85
3000000008	Cleaner, Concentrated Wood	ST	ST	19,95	1	99,75
3000000008	Cleaner, Tile & Grout	ST	ST	5,95	1	23,80
3000000008	Cleaner, Toilet Bowl	ST	ST	3,97	1	11,91
3000000008	Cleaner, Upholstery	ST	ST	3,06	1	15,30
3000000009	Shafting assembly	ST	ST	120,00	1	360,00
3000000009	Pressure cover	ST	ST	162,00	1	324,00
3000000009	Rubber Seal	ST	ST	1,00	1	7,00
3000000010	Pump Installation	STD	STD	50,00	1	300,00
3000000011	PAQ Monitor, 21", Color	ST	ST	532,00	1	532,00
3000000012	Desk Pads	ST	ST	27,95	1	83,85
3000000012	Mouse Pads	ST	ST	10,95	1	32,85
3000000012	Pencil, Marking, Refill Black	ST	ST	1,04	1	104,00
3000000013	Softwareset modern Office.jpg	ST	ST	52,99	1	52,99
3000000014	High Speed Printer/Laser Printer	ST	ST	2.228,00	1	2.228,00
3000000014	Maxitec R 3200 personal computer	ST	ST	1.698,00	1	1.698,00
3000000015	Mouse Pads	ST	ST	10,95	1	10,95
3000000015	Desk Pads	ST	ST	27,95	1	27,95
3000000016	High Speed Printer/Laser Printer	ST	ST	2.228,00	1	2.228,00
3000000016	Maxitec-R 3300 Professional PC	ST	ST	1.898,00	1	1.898,00
3000000016	PAQ Monitor, 21", Color	ST	ST	532,00	1	532,00

e.g., SAP-Tables: EKKO, EKPO, …

Detailed Payment Data



Date	Account	Amount	Product Details
02.01.97	0000140000	0000140000	3.335,00 *Grundmiete 01.01.1997
02.01.97	0000196900	0000140000	230,00 *VZ Betriebskosten 01.01.1997
02.01.97	0000196900	0000140000	207,00 *VZ Heizkosten 01.01.1997
02.01.97	0000140000	0000140000	6.325,00 *Grundmiete 01.01.1997
02.01.97	0000196900	0000140000	402,50 *VZ Betriebskosten 01.01.1997
02.01.97	0000196900	0000140000	57,50 *VZ Heizkosten 01.01.1997
02.01.97	0000140000	0000140000	7.475,00 *Grundmiete 01.01.1997
02.01.97	0000196900	0000140000	460,00 *VZ Betriebskosten 01.01.1997
02.01.97	0000196900	0000140000	103,50 *VZ Heizkosten 01.01.1997
02.01.97	0000140000	0000140000	195,50 *Pauschale Betriebskosten 01.01.1997
02.01.97	0000196900	0000140000	3.105,00 *VZ Umsatzmiete 01.01.1997
02.01.97	0000140000	0000140000	2.530,00 *Grundmiete 01.01.1997
02.01.97	0000196900	0000140000	287,50 *VZ Betriebskosten 01.01.1997
02.01.97	0000140000	0000140000	11,50 *Pauschale Betriebskosten 01.01.1997
02.01.97	0000140000	0000140000	10.005,00 *Grundmiete 01.01.97-31.03.97
02.01.97	0000196900	0000140000	966,00 *VZ Betriebskosten 01.01.97-31.03.97
02.01.97	0000196900	0000140000	897,00 *VZ Heizkosten 01.01.97-31.03.97
02.01.97	0000140000	0000140000	2.070,00 *Grundmiete 01.01.1997
02.01.97	0000196900	0000140000	230,00 *VZ Betriebskosten 01.01.1997
02.01.97	0000196900	0000140000	138,00 *VZ Heizkosten 01.01.1997
02.01.97	0000140000	0000140000	1.200,00 *Grundmiete 01.01.1997
02.01.97	0000196900	0000140000	190,00 *VZ Betriebskosten 01.01.1997
02.01.97	0000196900	0000140000	120,00 *VZ Heizkosten 01.01.1997
02.01.97	0000140000	0000140000	60,00 *Grundmiete 01.01.1997
02.01.97	0000140000	0000140000	10,00 *Pauschale Betriebskosten 01.01.1997
02.01.97	0000140000	0000140000	240,00 *Grundmiete 01.01.1997
02.01.97	0000196900	0000140000	90,00 *VZ Betriebskosten 01.01.1997
02.01.97	0000196900	0000140000	70,00 *VZ Heizkosten 01.01.1997
02.01.97	0000196900	0000140000	230,00 *VZ Betriebskosten 01.01.1997
02.01.97	0000196900	0000140000	207,00 *VZ Heizkosten 01.01.1997
02.01.97	0000140000	0000140000	6.325,00 *Grundmiete 01.01.1997
02.01.97	0000196900	0000140000	402,50 *VZ Betriebskosten 01.01.1997
02.01.97	0000196900	0000140000	57,50 *VZ Heizkosten 01.01.1997
02.01.97	0000140000	0000140000	7.475,00 *Grundmiete 01.01.1997
02.01.97	0000196900	0000140000	460,00 *VZ Betriebskosten 01.01.1997
02.01.97	0000196900	0000140000	103,50 *VZ Heizkosten 01.01.1997
02.01.97	0000140000	0000140000	195,50 *Pauschale Betriebskosten 01.01.1997
02.01.97	0000196900	0000140000	3.105,00 *VZ Umsatzmiete 01.01.1997
02.01.97	0000140000	0000140000	2.530,00 *Grundmiete 01.01.1997
02.01.97	0000196900	0000140000	287,50 *VZ Betriebskosten 01.01.1997
02.01.97	0000196900	0000140000	172,50 *VZ Heizkosten 01.01.1997
02.01.97	0000140000	0000140000	6.600,00 *Barkaution 01.01.1997
02.01.97	0000196930	0000140000	6.600,00 *Barkaution 01.01.1997
02.01.97	0000140000	0000140000	92,00 *Grundmiete 01.01.1997
02.01.97	0000140000	0000140000	11,50 *Pauschale Betriebskosten 01.01.1997

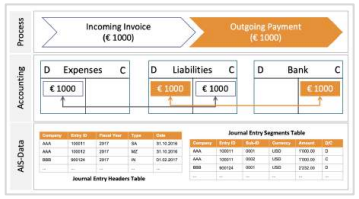
e.g., SAP-Tables: REGUH, REGUP, …

Insider Data Leakage Threat Model

Artificial Intelligence and Machine Learning
University of St.Gallen

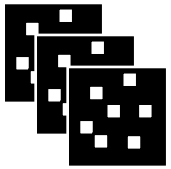
Leaking Sensitive Enterprise Resource Planning Data

Internal



ERP-System

(1) Regular Data Extract



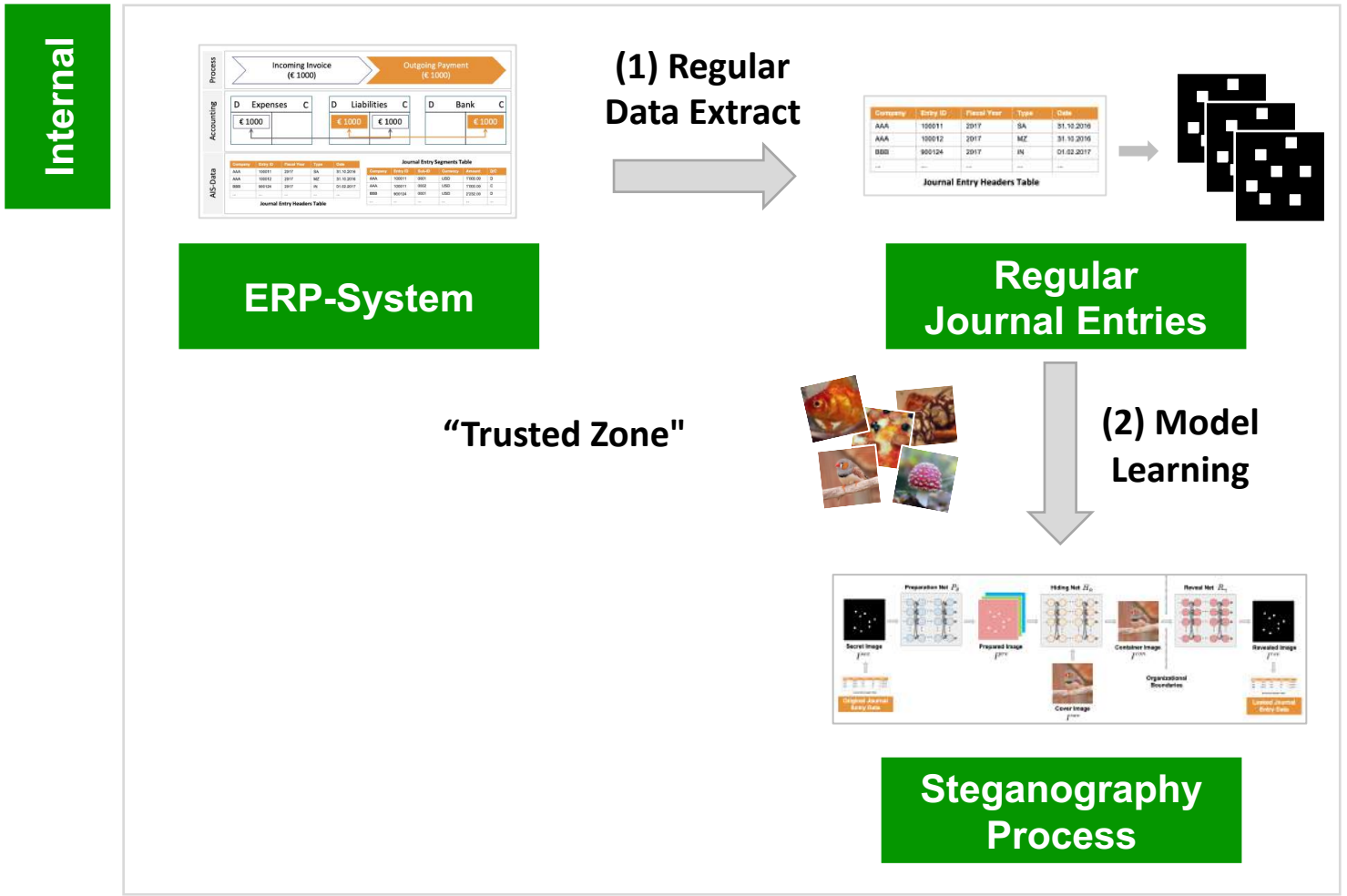
Regular Journal Entries

"Trusted Zone"

Insider Data Leakage Threat Model

Artificial Intelligence and Machine Learning
University of St.Gallen

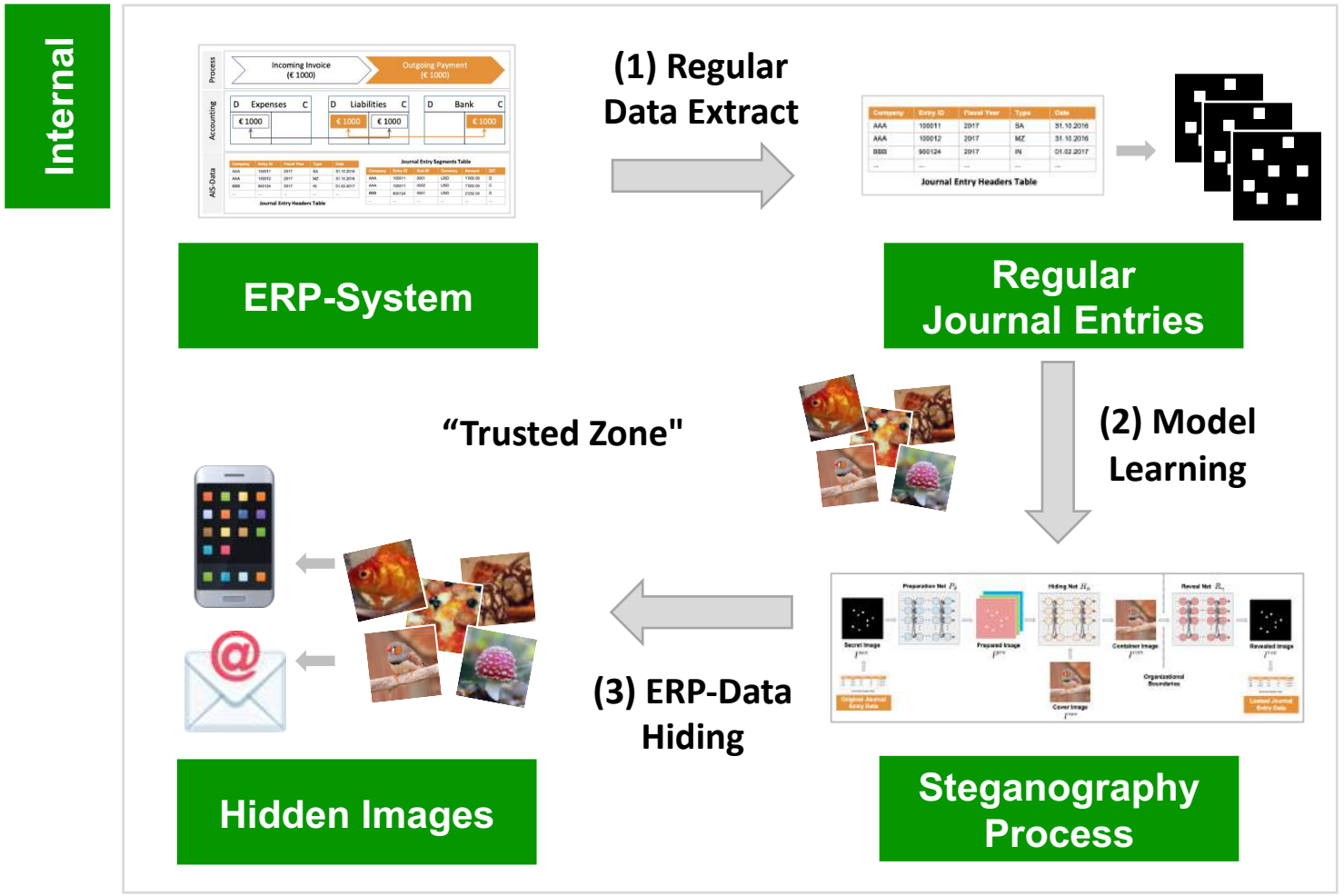
Leaking Sensitive Enterprise Resource Planning Data



Insider Data Leakage Threat Model

Artificial Intelligence and Machine Learning
University of St.Gallen

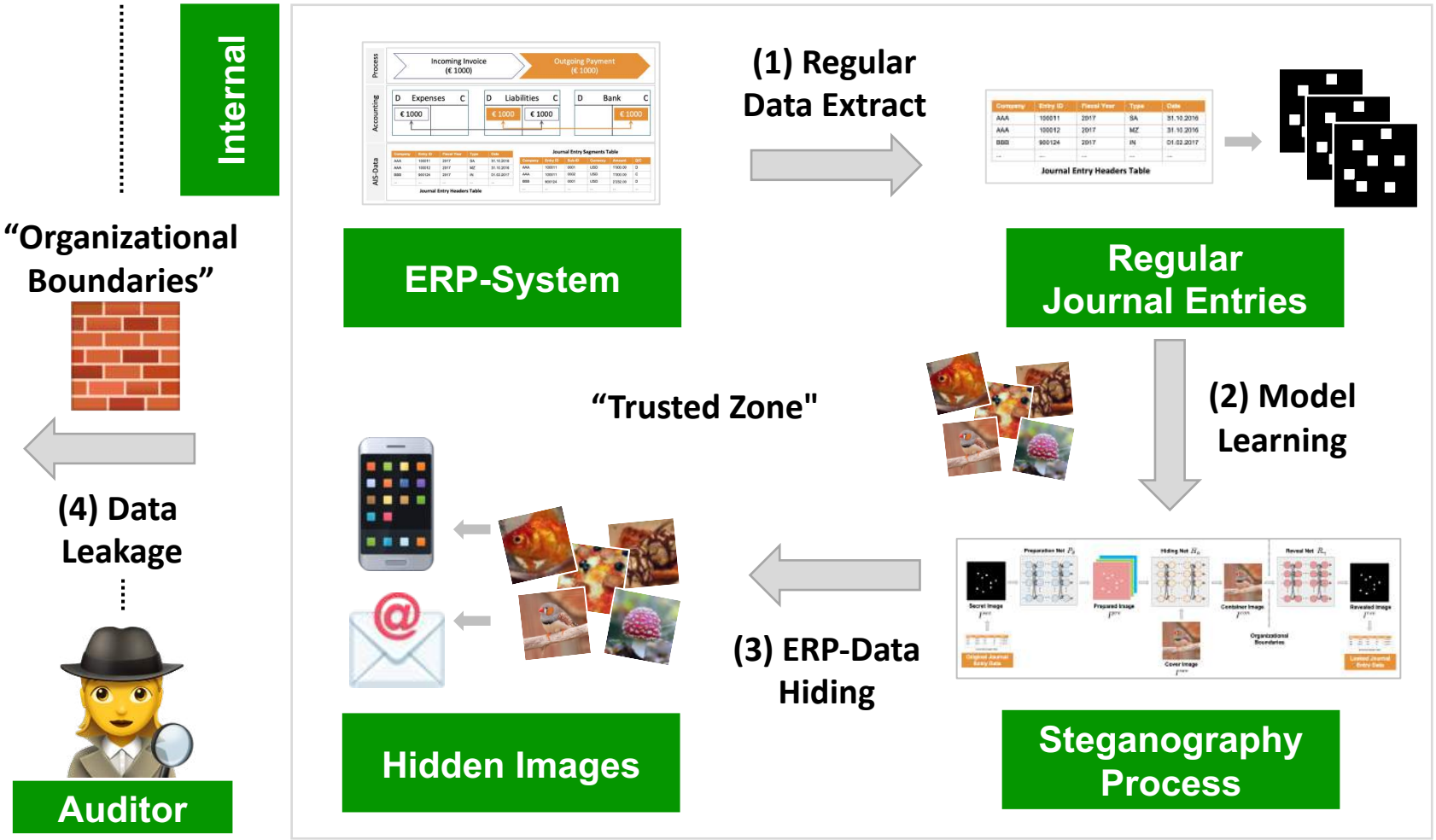
Leaking Sensitive Enterprise Resource Planning Data



Insider Data Leakage Threat Model

Artificial Intelligence and Machine Learning
University of St.Gallen

Leaking Sensitive Enterprise Resource Planning Data



Insider Data Leakage Threat Model

Artificial Intelligence and Machine Learning
University of St.Gallen

Leaking Sensitive Enterprise Resource Planning Data

External

Internal

(5) Data Extraction

"Organizational Boundaries"

(4) Data Leakage

Auditor

(1) Regular Data Extract

ERP-System

Regular Journal Entries

(2) Model Learning

"Trusted Zone"

(3) ERP-Data Hiding

Hidden Images

Steganography Process

Insider Data Leakage Threat Model

Artificial Intelligence and Machine Learning
University of St.Gallen

Leaking Sensitive Enterprise Resource Planning Data

External

Internal

(1) Regular Data Extract

(2) Model Learning

(3) ERP-Data Hiding

(4) Data Leakage

(5) Data Extraction

(6) Data Revealing

"Organizational Boundaries"

"Trusted Zone"

ERP-System

Regular Journal Entries

Steganography Process

Hidden Images

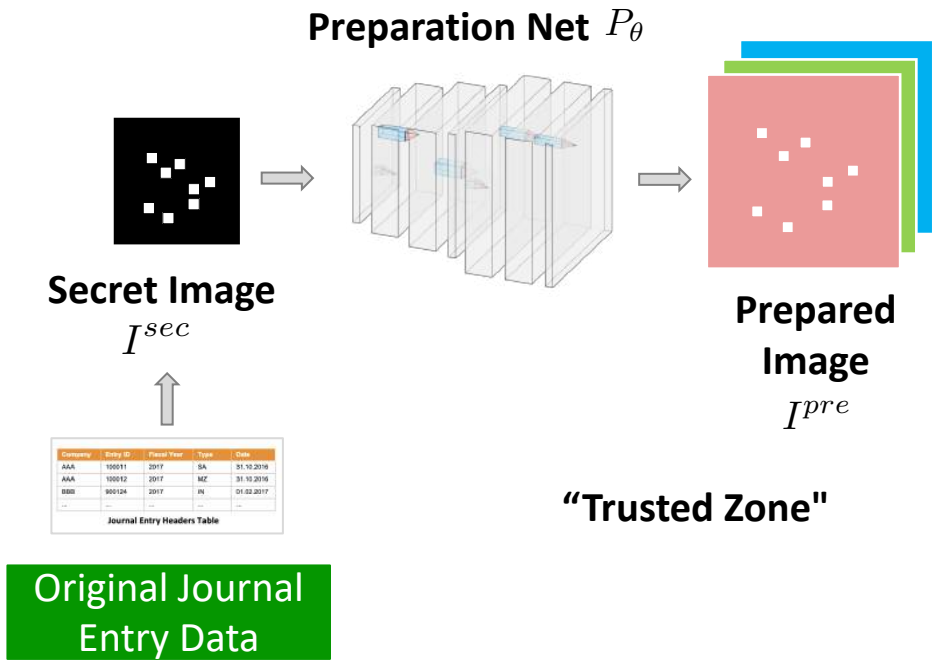
Leaked Journal Entries

Auditor

Data Leakage Process

Artificial Intelligence and Machine Learning
University of St.Gallen

Steganographic Process to Leak Sensitive Enterprise Resource Planning Data

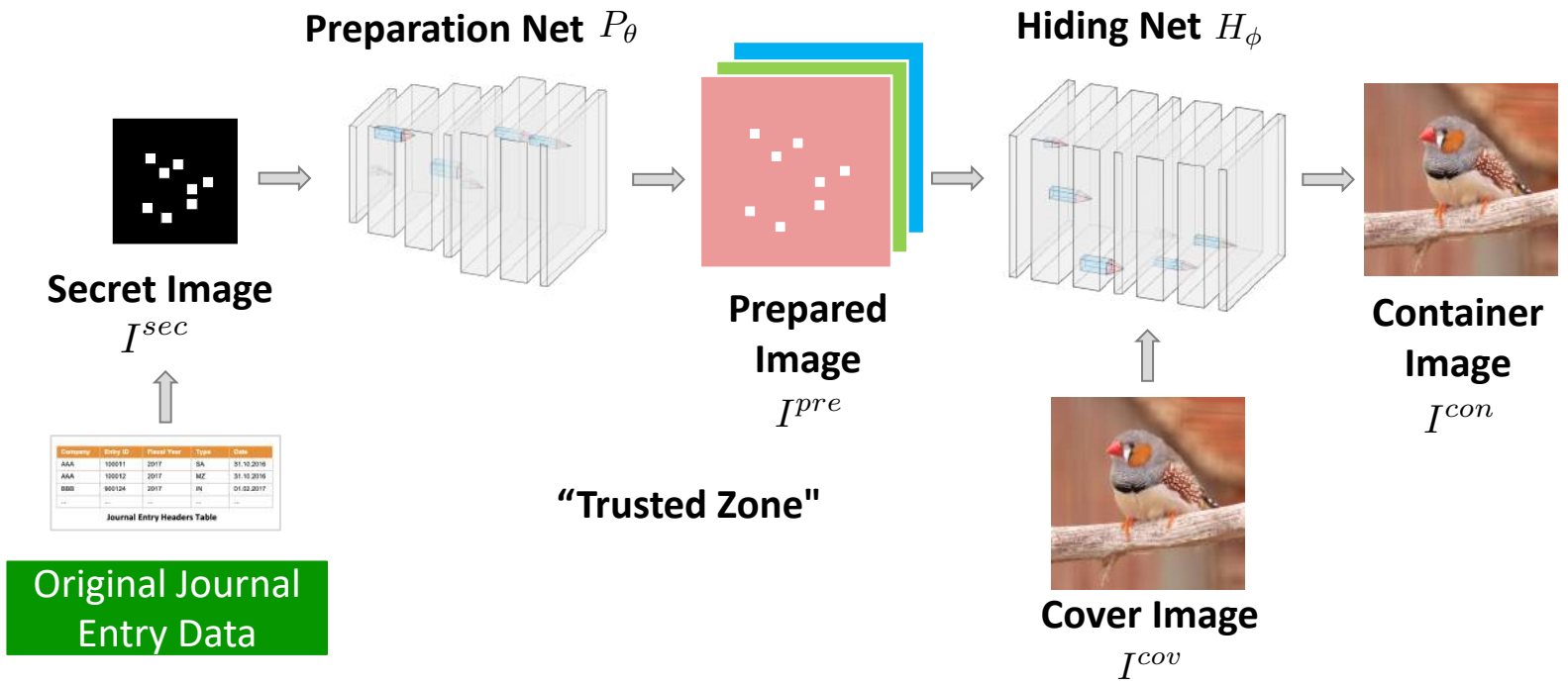


Following: Baluja, S. 2017. Hiding Images in Plain Sight: Deep Steganography. In Advances in Neural Information Processing Systems, 2069–2079.

Data Leakage Process

Artificial Intelligence and Machine Learning
University of St.Gallen

Steganographic Process to Leak Sensitive Enterprise Resource Planning Data

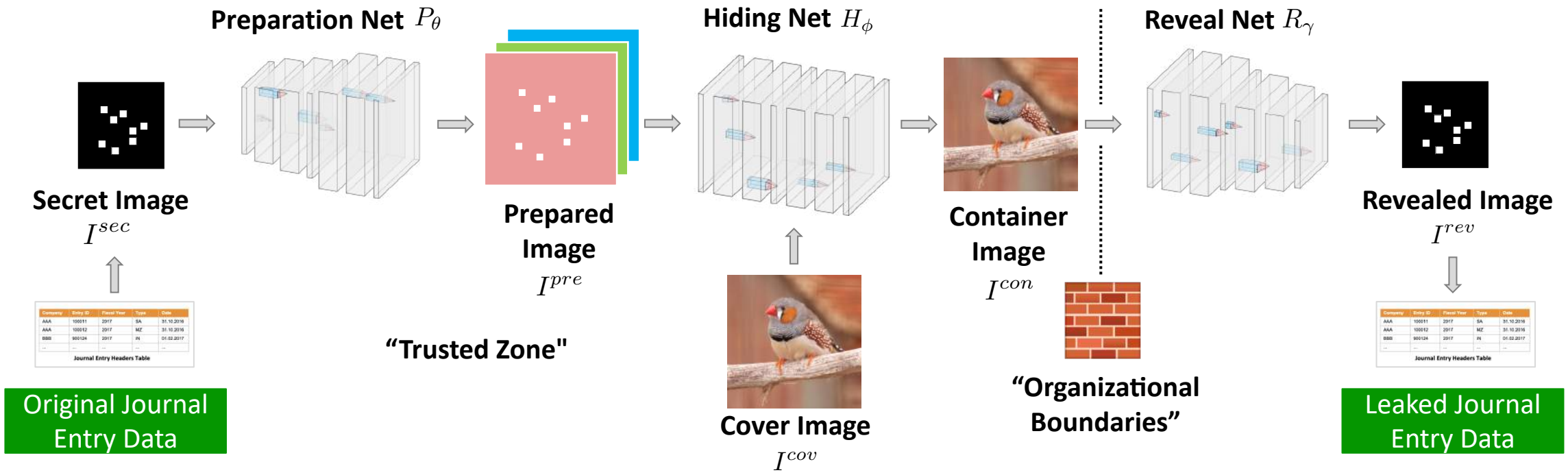


Following: Baluja, S. 2017. Hiding Images in Plain Sight: Deep Steganography. In Advances in Neural Information Processing Systems, 2069–2079.

Data Leakage Process

Artificial Intelligence and Machine Learning
University of St.Gallen

Steganographic Process to Leak Sensitive Enterprise Resource Planning Data

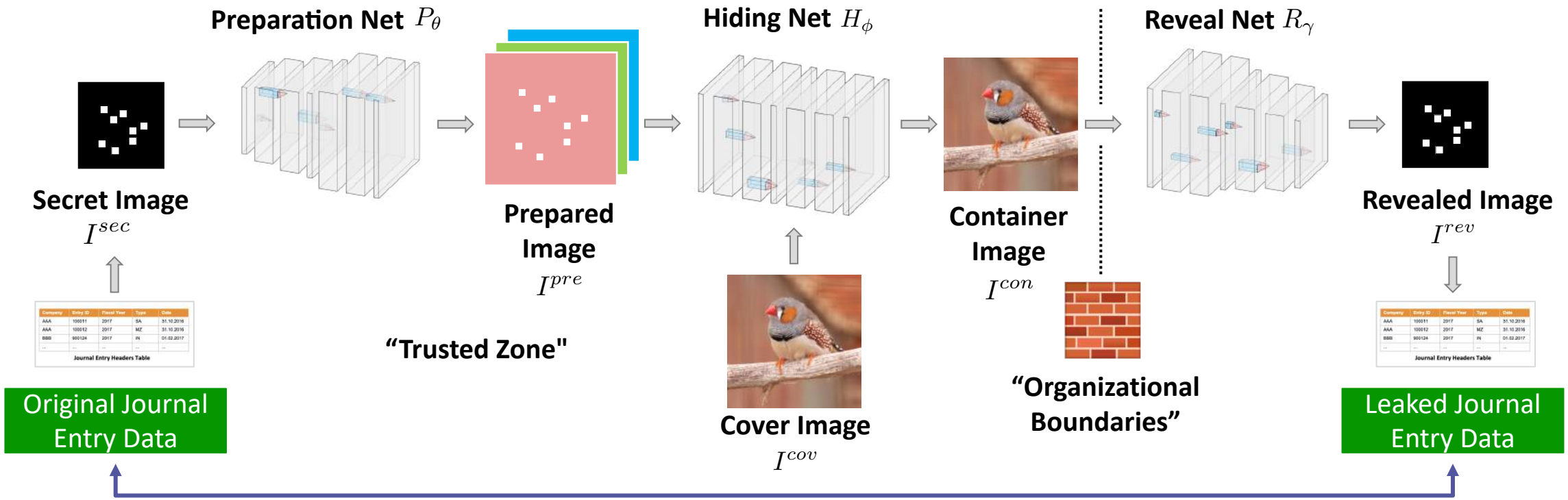


Following: Baluja, S. 2017. Hiding Images in Plain Sight: Deep Steganography. In Advances in Neural Information Processing Systems, 2069–2079.

Data Leakage Process

Artificial Intelligence and Machine Learning
University of St.Gallen

Steganographic Process to Leak Sensitive Enterprise Resource Planning Data



BCE Secret loss

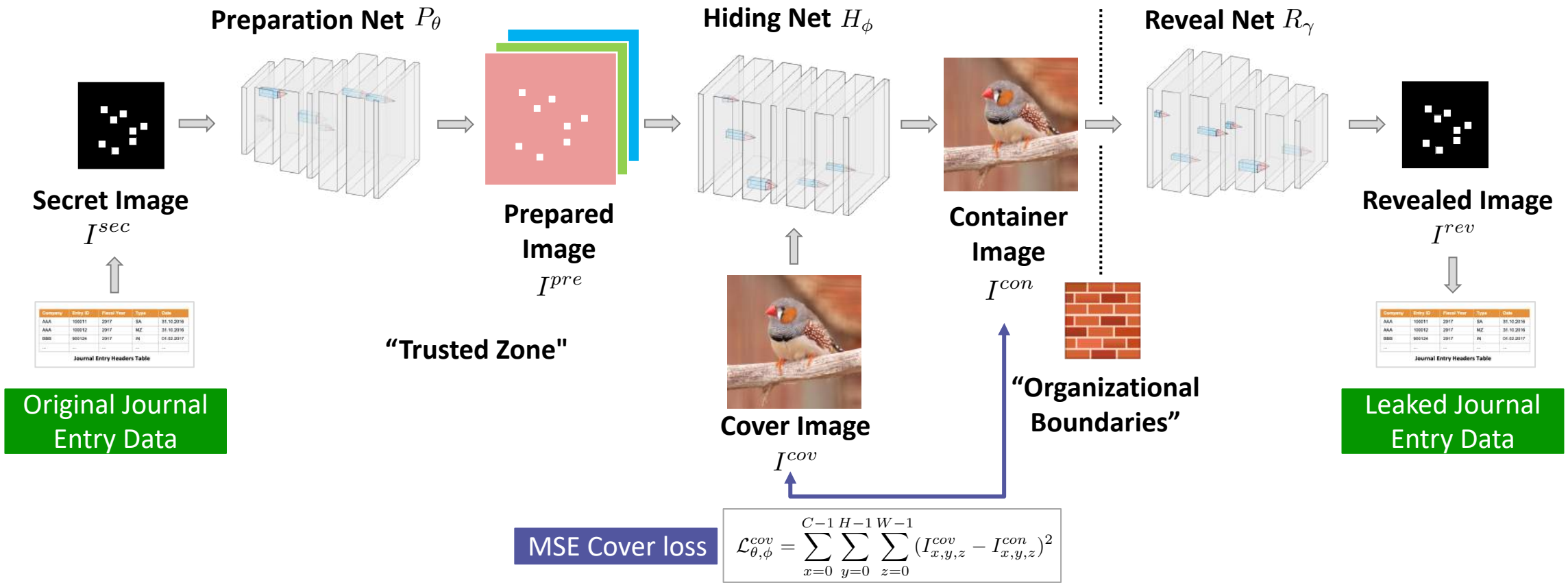
$$\mathcal{L}^{sec}_{\theta,\phi,\gamma} = \sum_{x=0}^{H-1}\sum_{y=0}^{W-1} I^{sec}_{x,y}\log I^{rev}_{x,y} + (1 - I^{sec}_{x,y})\log(1 - I^{rev}_{x,y})$$

Following: Baluja, S. 2017. Hiding Images in Plain Sight: Deep Steganography. In Advances in Neural Information Processing Systems, 2069–2079.

Data Leakage Process

Artificial Intelligence and Machine Learning
University of St.Gallen

Steganographic Process to Leak Sensitive Enterprise Resource Planning Data



Following: Baluja, S. 2017. Hiding Images in Plain Sight: Deep Steganography. In Advances in Neural Information Processing Systems, 2069–2079.

Experimental Setup

Artificial Intelligence and Machine Learning
University of St.Gallen

Utilized “Secret” Datasets of City Payment Data

Dataset: Philadelphia “City Payments”

- $4.2 billion city payments of the fiscal year 2017
- 60 offices, departments, boards and committees
- N=238,894 payments: 10 categorical, 1 numerical attribute
- 8,565 ‘one-hot’ encoded dimensions: $x^i \in \mathcal{R}^{8,565}$

City of Philadelphia

check_date	document_no	dept	department_title	char_	character_title	sub_obj	sub_obj_title
2016-11-25T00:00:00Z	CHEK17063379	1	01 CITY COUNCIL	3	03 MATERIALS AND SUPPLIES	325	PRINTING 0325
2017-01-26T00:00:00Z	CHEK17087297	1	01 CITY COUNCIL	2	02 PURCHASE OF SERVICES	240	ADVERTISING/PROMOTIONAL ACTIVITIES
2016-08-04T00:00:00Z	CHEK17012548	1	01 CITY COUNCIL	2	02 PURCHASE OF SERVICES	240	ADVERTISING/PROMOTIONAL ACTIVITIES
2016-08-26T00:00:00Z	ACHD17028318	1	01 CITY COUNCIL	2	02 PURCHASE OF SERVICES	210	POSTAGE 0210
2017-06-30T00:00:00Z	ACHD17192218	1	01 CITY COUNCIL	3	03 MATERIALS AND SUPPLIES	309	CORDAGE AND FIBERS 0309
2017-06-08T00:00:00Z	CHEK17141080	1	01 CITY COUNCIL	3	03 MATERIALS AND SUPPLIES	325	PRINTING 0325
2017-04-12T00:00:00Z	CHEK17117562	1	01 CITY COUNCIL	2	02 PURCHASE OF SERVICES	255	DUES 0255
2017-04-13T00:00:00Z	ACHD17151640	1	01 CITY COUNCIL	3	03 MATERIALS AND SUPPLIES	304	BOOKS AND OTHER PUBLICATIONS 0304

Source: https://www.phila.gov/2019-03-29-philadelphias-initial-release-of-city-payments-data/

Dataset: Chicago “Vendor Payments”

- $5.3 billion vendor payments of the fiscal years 2009-2019
- 30 departments, 928 contracts
- N=72,814 payments: 7 categorical, 1 numerical attribute
- 2,354 ‘one-hot’ encoded dimensions: $x^i \in \mathcal{R}^{2,354}$

CHICAGO DATA PORTAL

VOUCHER NUMBER	AMOUNT	CHECK DATE	DEPARTMENT NAME	CONTRACT NUMBER	VENDOR NAME	CASHED
CV5419500322	94.80	07/01/2019	DEPT OF COMMUNITY DEV...	50236	18TH STREET, DEVELOPME...	Yes
CVIP174102790	-6.56	04/30/2019	DEPARTMENT OF HEALTH	64612	RESPIRATORY HEALTH ASS...	No
CVIP175004687	1,380.00	01/02/2019	DEPT OF FAMILY AND SUPP...	33322	FEATHERFIST	Yes
CVIP182500015	2,686.10	01/08/2019		82037	PHALANX FAMILY SERVICES	Yes
CVIP182500016	12,831.19	01/09/2019		82037	PHALANX FAMILY SERVICES	Yes
CVIP182500017	48,589.00	01/25/2019		87489	CHICAGO CITYWIDE LITERA...	Yes
CVIP182500021	115.47	04/29/2019		89573	CATHOLIC CHARITIES OF T...	Yes
CVIP182500022	963.03	04/29/2019		89573	CATHOLIC CHARITIES OF T...	Yes

Source: https://data.cityofchicago.org/Administration-Finance/Payments/s4vu-giwb/

Experimental Setup

Artificial Intelligence and Machine Learning
University of St.Gallen

Utilized “Cover” Dataset of Unobtrusive Data-to-Day Images

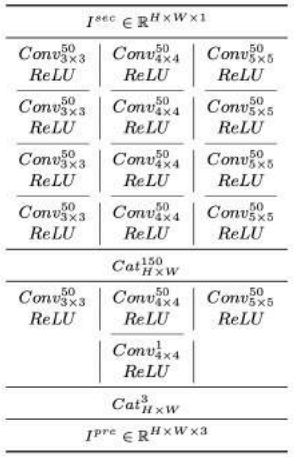
Dataset: “Tiny ImageNet” Images

- Contains 100,000 images utilized as ”cover” images
- Each image shows an individual objects at low resolution
- Each image is of size 3 x 224 x 244 (C x H x W) pixels
- Grayscale images are reduced to 1 x 224 x 244 pixels

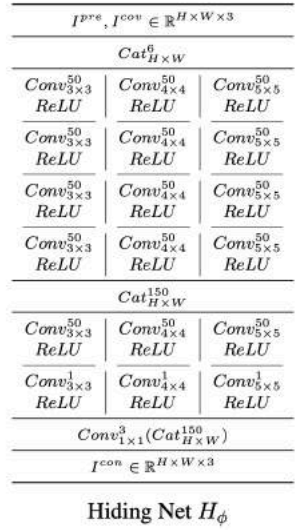
(Source: https://www.researchgate.net/figure/Examples-in-the-ImageNet-dataset_fig7_314646236)

Network Architectural Details

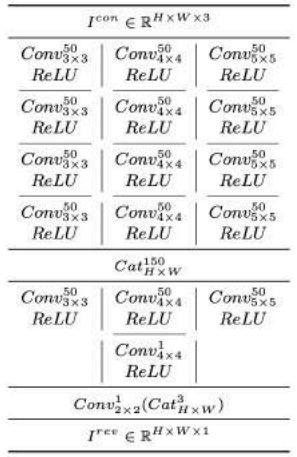
- Each network applies three distinct series of 2D convolutions of different spatial filter sizes.
- Each convolutional layer is followed by a non-linear Rectified Linear Unit (ReLU) activation function.



Preparation Net P_θ



Hiding Net H_ϕ



Reveal Net R_γ

Experimental Setup

Artificial Intelligence and Machine Learning
University of St.Gallen

Experimental Quality Measures

Peak Signal-to-Noise Ratio (PSNR)

- Defines the ratio between the power of image fidelity and the power of corrupting noise.

  ⇨ The “technical” container image quality.

$$\mathrm{PSNR} = 10 \cdot \log_{10} \frac{\max |I^{cov}|}{\mathcal{L}^{cov}_{\theta,\phi}(I^{cov}, I^{con})}$$

Structural Similarity Index Measure (SSIM)

- Defines a perception-based model considering image degradation as perceived change in structural information.

  ⇨ The “perceived” container image quality.

$$\mathrm{SSIM} = \frac{(2\mu_{cov}\mu_{con} + c_1)(2\sigma_{cov,con} + c_2)}{(\mu^2_{cov} + \mu^2_{con} + c_1)(\sigma^2_{cov} + \sigma^2_{con} + c_2)}$$

Bit Accuracy (BACC)

- Defines the fraction of identical active bits between the secret image and the revealed image.

  ⇨ The revealed data accuracy.

$$\mathrm{BACC} = 1 - \frac{\sum_{x=0}^{H-1} \sum_{y=0}^{W-1} \mathbb{1}_{[\|I^{sec}_{x,y} - M \circ I^{rev}_{x,y}\| \leq \delta]}}{\sum_{x=0}^{H-1} \sum_{y=0}^{W-1} \mathbb{1}_{[I^{sec}_{x,y} > 0]}}$$

Experimental Results

Artificial Intelligence and Machine Learning
University of St.Gallen

Quantitative Experimental Results

RGB Cover

	Dataset	BPP	α	β	$\mathcal{L}^{ALL}_{\theta,\phi,\gamma}$	$\mathcal{L}^{cov}_{\theta,\phi}$	$\mathcal{L}^{sec}_{\theta,\phi,\gamma}$	PSNR (Cover Quality)	SSIM (Cover Quality)	BACC (Accuracy)
Philadelphia:	A	0.0436	0.2	1.0	0.63 ± 0.01	0.43 ± 0.06	0.54 ± 0.01	43.91 ± 0.64	0.997 ± 0.001	0.999 ± 0.001
			0.5	1.0	0.74 ± 0.03	0.40 ± 0.04	0.54 ± 0.04	44.23 ± 0.50	0.997 ± 0.001	0.998 ± 0.003
			0.8	1.0	0.81 ± 0.03	0.34 ± 0.03	0.55 ± 0.01	44.97 ± 0.43	0.998 ± 0.001	0.999 ± 0.001
			1.0	1.0	0.92 ± 0.06	0.38 ± 0.05	0.54 ± 0.02	44.42 ± 0.65	0.997 ± 0.001	0.998 ± 0.002
Chicago:	B	0.0120	0.2	1.0	0.67 ± 0.07	0.79 ± 0.03	0.51 ± 0.00	41.38 ± 0.32	0.998 ± 0.002	0.999 ± 0.001
			0.5	1.0	0.77 ± 0.01	0.52 ± 0.02	0.51 ± 0.01	42.94 ± 0.23	0.996 ± 0.001	0.998 ± 0.001
			0.8	1.0	0.87 ± 0.05	0.46 ± 0.07	0.51 ± 0.00	43.51 ± 0.65	0.995 ± 0.003	0.998 ± 0.002
			1.0	1.0	0.99 ± 0.04	0.47 ± 0.04	0.52 ± 0.01	43.35 ± 0.37	0.997 ± 0.001	0.997 ± 0.003

Variances originate from parameter initialization using four distinct random seeds.

Grayscale Cover

	Dataset	BPP	α	β	$\mathcal{L}^{ALL}_{\theta,\phi,\gamma}$	$\mathcal{L}^{cov}_{\theta,\phi}$	$\mathcal{L}^{sec}_{\theta,\phi,\gamma}$	PSNR	SSIM	BACC
Philadelphia:	A	0.1307	0.2	1.0	0.11 ± 0.01	0.01 ± 0.00	0.54 ± 0.01	64.84 ± 0.49	0.999 ± 0.001	0.997 ± 0.003
			0.5	1.0	0.29 ± 0.00	0.01 ± 0.00	0.54 ± 0.01	60.93 ± 1.58	0.999 ± 0.001	0.997 ± 0.002
			0.8	1.0	0.44 ± 0.00	0.01 ± 0.00	0.54 ± 0.00	60.98 ± 0.13	0.999 ± 0.001	0.999 ± 0.006
			1.0	1.0	0.55 ± 0.01	0.01 ± 0.00	0.54 ± 0.01	60.15 ± 1.79	0.999 ± 0.001	0.999 ± 0.004
Chicago:	B	0.0359	0.2	1.0	0.75 ± 0.02	0.82 ± 0.08	0.53 ± 0.01	39.98 ± 0.33	0.985 ± 0.001	0.983 ± 0.003
			0.5	1.0	0.87 ± 0.04	0.64 ± 0.07	0.55 ± 0.02	42.27 ± 0.49	0.989 ± 0.001	0.977 ± 0.002
			0.8	1.0	0.98 ± 0.05	0.52 ± 0.06	0.58 ± 0.01	43.19 ± 0.53	0.990 ± 0.001	0.967 ± 0.006
			1.0	1.0	0.99 ± 0.13	0.41 ± 0.14	0.58 ± 0.01	44.28 ± 1.34	0.991 ± 0.001	0.966 ± 0.005

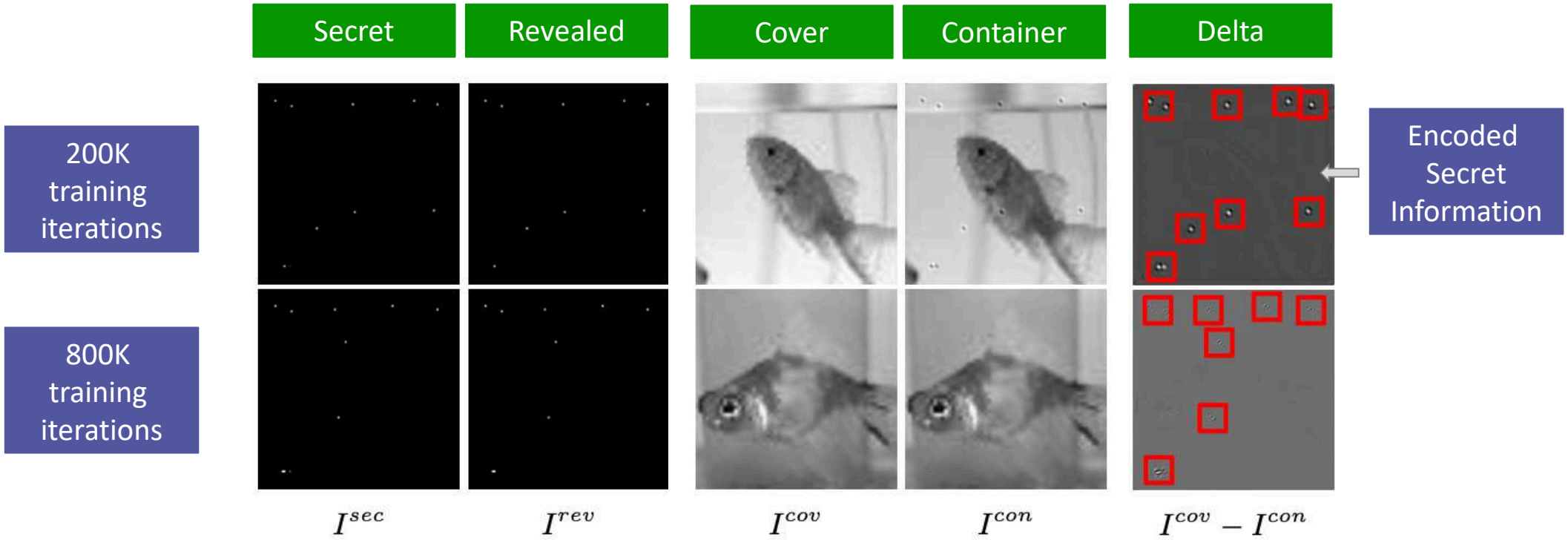
Variances originate from parameter initialization using four distinct random seeds.

The quantitative results demonstrate the steganographic capabilities of the trained models.

Experimental Results

Artificial Intelligence and Machine Learning
University of St.Gallen

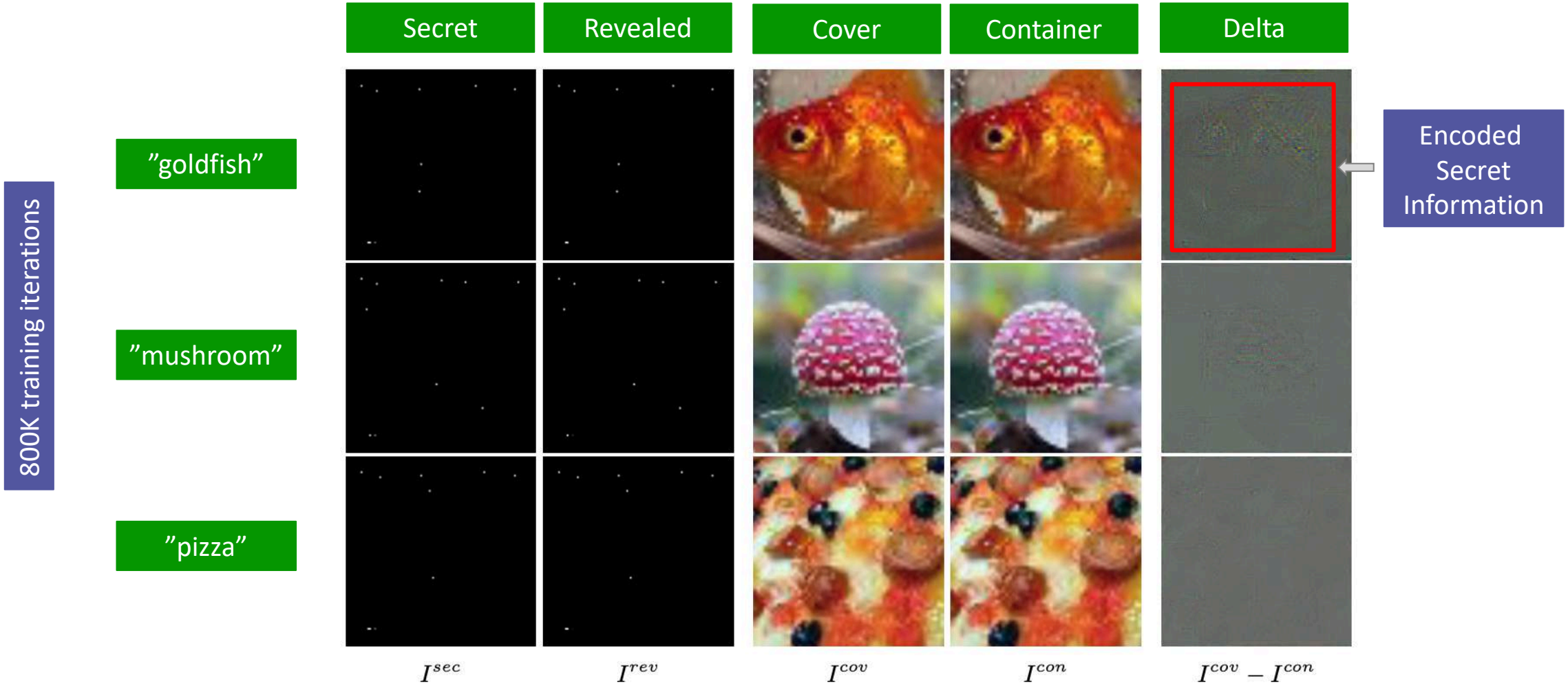
Qualitative Experimental Results (single Journal Entry, single Grayscale Cover Images)



Experimental Results

Artificial Intelligence and Machine Learning
University of St.Gallen

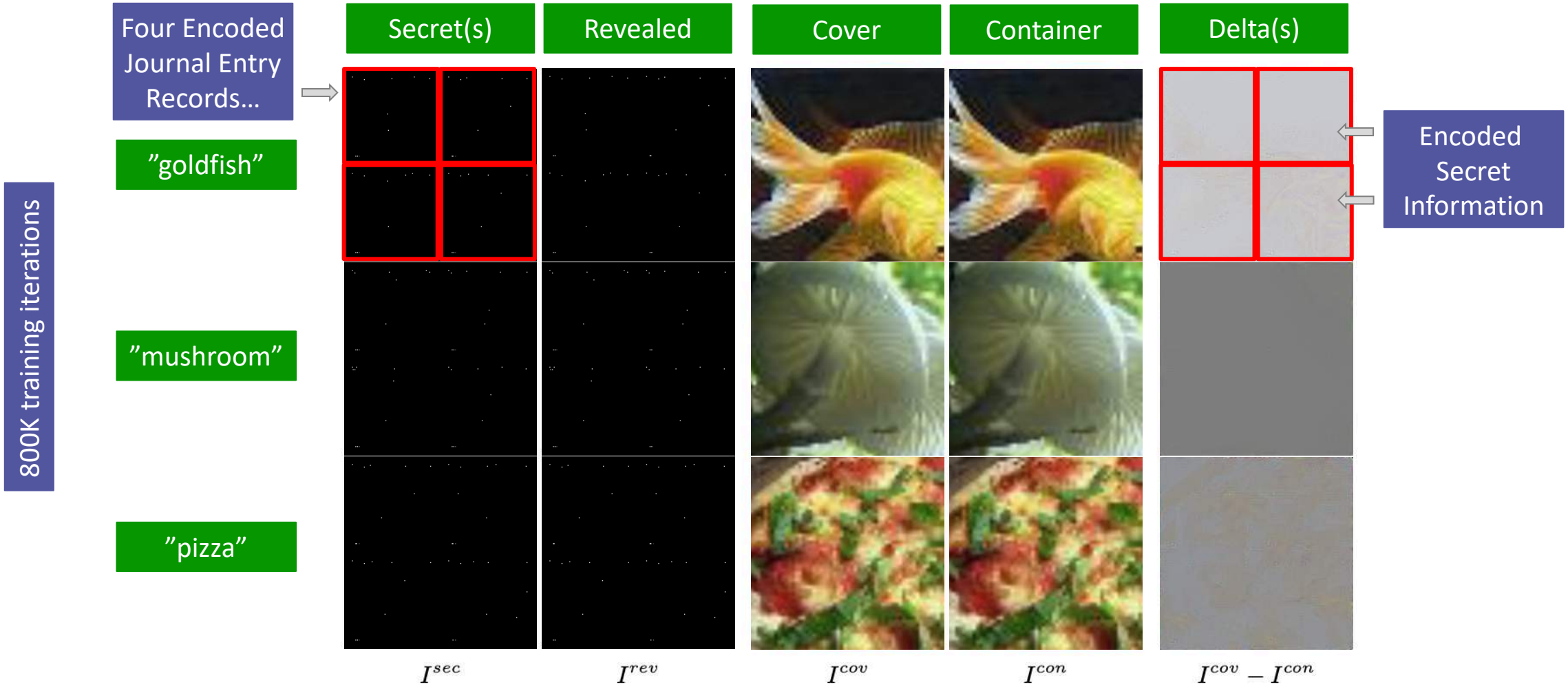
Qualitative Experimental Results (single Journal Entry, single RGB Cover Images)



Experimental Outlook

Artificial Intelligence and Machine Learning
University of St.Gallen

Qualitative Experimental Results (four Journal Entries, single RGB Cover Images)



Thank you 🤓

University of St.Gallen

Contact: **Marco Schreyer**
Artificial Intelligence & Machine Learning
University of St.Gallen (HSG)
marco.schreyer@unisg.ch

Paper:

Paper available via:
https://aaai-kdf.github.io/kdf2021/