



HistoCrypt 2023

**6th International Conference
on Historical Cryptology**

20-22 June 2023, Munich

Proceedings of the 6th International Conference on Historical Cryptology HistoCrypt 2023

Editors

Carola Dahlke and Matthias Göggerle

Published by:

NEALT Proceedings Series No. 50

ISSN: 1736-8197 (print), 1736-6305 (online)

ISBN 978-91-8075-134-6 (PDF)

<https://doi.org/10.3384/ecp195>

Linköping Electronic Conference Proceedings No. 195

ISSN 1650-3686 (print), 1650-3740 (online)

NEALT Proceedings Series No. 50

ISSN 1736-8197 (print), 1736-6305 (online)

Contents

Preface.....	V
Eugen Antal, Pavol Marák, Pavol Zajak, Tünde Lengyelová and Diana Duchoňová..... <i>Encrypted Documents and Cipher Keys from the 18th and 19th Century in the Archives of Aristocratic Families in Slovakia</i>	1
Richard Bean, Corinna Gannon and Sarah Lang..... <i>The Cipher of Emperor Rudolf II's "Alchemical Hand Bell"</i>	13
Paolo Bonavoglia..... <i>Ottavian Medici and the decline of Venetian cryptography</i>	18
Carola Dahlke and Robert Jahn..... <i>The Making of Fritz Menzer – A Secret Life</i>	28
Jörgen Dinnissen and Hugo Araújo..... <i>A "Mirror for All Traitors". Captured Ciphertexts from a Portuguese Spy in Dutch Brazil (1646)</i>	36
Magnus Ekhall and Klaus Schmeh..... <i>A WW2 device for breaking the M-209 encryption machine</i>	55
Marek Grajek..... <i>Mysteries of P.C. Cadix and its evacuation in 1942/43</i>	63
Wolfgang Killmann..... <i>The History of the Development and the Analysis of the Cipher Machine T-310/50 and the Procedure ARGON by the ZCO</i>	73
Eunice Kim and Christian Millichap..... <i>Deciphering Secrets Throughout History: An Interdisciplinary Linguistics and Cryptology Course</i>	83
Sarah Lang..... <i>Situating ciphers among alchemical techniques of secrecy</i>	93
George Lasry..... <i>Armand de Bourbon's Poly-Homophonic Cipher – 1649</i>	105
Colin Layfield, René Zandbergen, Lisa Fagin Davis, John Abela, Claire Bower, Michael Rosner and Lonneke van der Plas..... <i>International Conference on the Voynich Manuscript 2022</i>	113

Beáta Megyesi, Justyna Sikora, Filip Fornmark, Michelle Waldispühl, Nils Kopal and Vasily Mikhalev.....	120
<i>Historical Language Models in Cryptanalysis: Case Studies on English and German</i>	
Vasily Mikhalev, Nils Kopal, Bernhard Esslinger, Michelle Waldispühl, Benedek Láng and Beáta Megyesi.....	130
<i>What is the Code for the Code? Historical Cryptology Terminology</i>	
Cosimo Palma.....	139
<i>Encrypted epigraphy - the case of a mysterious inscription in the Neapolitan church of Santa Maria La Nova</i>	
Cécile Pierrot, Camille Desenclos, Pierrick Gaudry and Paul Zimmermann.....	148
<i>Deciphering Charles Quint (A diplomatic letter from 1547)</i>	
Eveline Szarka.....	160
<i>On the Combination of Cryptography and Steganography in 17th Century Germany</i>	
Claus Taaks.....	170
<i>Scherbius and the Enigma: Political, Economic and Military Conditions 1917-1925</i>	
Fredrik Wallin.....	180
<i>“We just did it!” – Female employees in Swedish sigint during the Second World War</i>	
Sebastien Zimmermann.....	190
<i>Runic cryptography in early epigraphic period (200-700)</i>	
Poster Session.....	199

Encrypted Documents and Cipher Keys From the 18th and 19th Century in the Archives of Aristocratic Families in Slovakia

Eugen Antal, Pavol Marák,
Pavol Zajac

Slovak University of
Technology in Bratislava
Slovakia

<firstname.secondname>@stuba.sk

Tünde Lengyelová, Diana Duchoňová

Institute of History of
the Slovak Academy of Sciences
Slovakia

tunde.lengyelova@savba.sk,
histdidi@savba.sk

Abstract

In this article, we present encrypted documents and cipher keys from the 18th and 19th century, related to central-European aristocratic families Amade-Üchtritz, Esterházy, and Pálffy-Daun. In the first part of the article, we present an overview and analysis of the available documents from the archives with examples. We provide a short historical overview of the people related to the analyzed documents to provide a context for the research. In the second part of the article, we focus on the digital processing of these historical manuscripts. We developed new tools based on machine learning that can automate the transcription of encrypted parts of the documents, which contain only digits as cipher text alphabet. Our digit detection and segmentation are based on YOLOv7. YOLOv7 provided good detection precision and was able to cope with problems like noisy paper background and areas where digits collided with the text from the reverse side of the paper.

1 Introduction

Many historical encrypted documents and cipher keys have survived in various archives all over the world. Collecting materials from a particular time period or geographic location can bring insights into the cipher design from a specific time/location. A valuable collection of historical encrypted documents and cipher keys can be found in Austria (Láng, 2020), Germany (Antal and Mírka, 2022), etc. It is thus desirable to investigate and compare various collections from a wide time range and location (Megyesi et al., 2022), because it is essential for understanding how ciphering evolved in the past. The encrypted

documents and keys are easy to recognize but are difficult to locate in archives. This fact was already observed by Láng (2020) and other researchers in historical cryptography.

Systematic collection, annotation, and sharing of these materials among researchers are thus very important. For this reason, we bring to the reader's attention to two interesting projects that focus on such collections. The *DECRYPT*¹ project (Megyesi et al., 2020; Megyesi et al., 2022) contains 4360 records at the time of writing this paper. Perhaps the only disadvantage of this database is that most of the documents are not publicly available². The *HCPortal*³ project (Antal and Zajac, 2020; Antal and Zajac, 2021) contains at the time of the writing of this document 763 records. Every record is freely available to everyone. One of the data collections that is planned to be added to HCPortal in the near future is the content of this article.

The aim of this paper is to provide the first detailed description of encrypted documents and cipher keys from the 18th and 19th century, related to central-European aristocratic families that lived in the territory of modern Slovakia. The investigated collection is deposited in the Slovak National Archive in Bratislava. During the initial research phase, we found documents related to historical cryptology in the fonds of three different aristocratic families:

- Amade-Üchtritz,
- Esterházy,
- Pálffy-Daun.

In these fonds, we identified a total of 13 card-

¹<https://de-crypt.org/>

²The probable reason is the problem with granting permissions from archives.

³<https://hcportal.eu>

board boxes containing 96 encrypted documents⁴ and 9 cipher keys.

The encrypted documents are from the 18th and 19th century. The earliest document is from 1711, and the latest is from 1834. The most commonly used encryption system from this time period is called *nomenclator*. Several publications have already described this cipher system in detail, including its large variety. For more information about this encryption system see (Antal and Mírka, 2022; Megyesi et al., 2022) or other publications published in the proceedings of the HistoCrypt⁵ conference.

2 Analysis of Available Materials

The used symbol set (cipher text alphabet) of the investigated collection, both in encrypted documents and cipher keys consist of only numbers (e.g. on Figures 1, 3), and markups of numbers (Figure 2). It also confirms that using digits became more common/standard in the 17th/18th centuries as stated in (Megyesi et al., 2022). A nomenclator system can be used with and without separators based on its design. Separators are mostly required to clearly distinguish/split the cipher text units (Antal and Mírka, 2022). In total, 37 encrypted documents contain cipher text with a separator, and 59 are without a separator character.

Some documents consist of cipher text only, some contain the corresponding (decrypted) plain text. In 8 cases, only the cipher text is preserved. Plain text is written above/under the encrypted lines of the text in 16 documents. In 58 cases, the plain text is available in a separate document. Finally, in 14 cases we were unable to verify whether the plain text is preserved.

Encrypted documents were preserved in all three fonds, however, cipher keys were only found in two of them. An interesting fact about this collection is that the preserved encryption keys do not match⁶ the preserved cipher texts. We also investigated some (possibly related) cipher keys from Austria (Haus-, Hof- und Staatsarchiv of Vienna) and from Hungary, however, these keys also did not match our encrypted documents.

A more detailed description of the available encrypted documents and cipher keys are present in

⁴The documents consist of nearly 300 pages containing encrypted text.

⁵<https://histocrypt.org>

⁶Except for one key matching the encrypted diary of Emil Üchritz, see Section 2.1.

the following subsections.

2.1 Encrypted Manuscripts

The Esterházy⁷ family archive contains most of the encrypted documents (fifty-eight), spread in four boxes. In cardbox no. 631 there is (only) one document related to cryptography, a four-page-long encrypted letter from 1744 written in the German language. The most promising materials⁸ are deposited in cardbox no. 634, which contains an extensive communication between Count Nicolaus Esterházy and Wenzel Anton Prince of Kaunitz-Rietberg from the years 1756 and 1757. The whole communication is in the German language. Interestingly, they used at least two different encryption keys in the communication - one where the cipher text units are separated with a separator char (Figure 1) and one without a separator (Figure 3). Moreover, the cipher texts with a separator contain special digit markups (Figure 2). There are two additional documents sent to Count Nicolaus Esterházy in this box, one sent by Graf Colloredo and one by Empress Maria Theresa. For most of the encrypted documents in this box, the plain text is also available in separate documents.

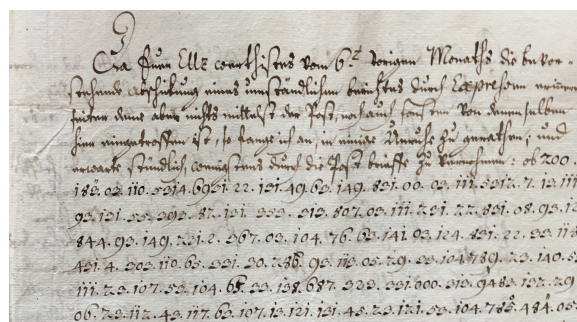


Figure 1: Cipher text example with separator chars (Slovak National Archives, fond Esterházy - čeklíska vetva, box n. 634)

Cardbox no. 635 contains letter concepts from the years 1741 and 1744 with encrypted parts in nine of them. It should be noted, however, that only small parts of these letter concepts are encrypted. These encrypted parts are mainly written below the corresponding plain text parts (Figure 4), or inserted next to the non-encrypted text parts (Figure 5). Again, the text is written in the German language.

⁷Čeklís family branch.

⁸Forty one documents with encrypted content.

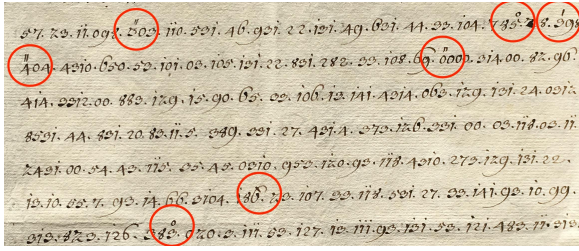


Figure 2: Special digit markups (Slovak National Archives, fond Esterházi - čeklíska vetva, box n. 634)

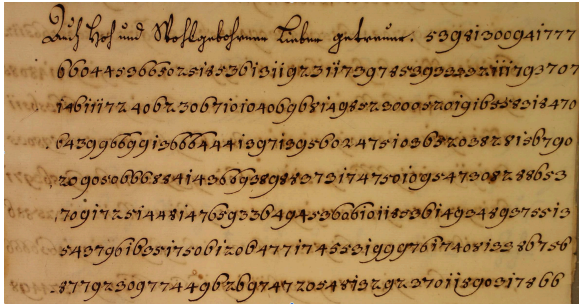


Figure 3: Cipher text example without separator chars (Slovak National Archives, fond Esterházi - čeklíska vetva, box n. 634)

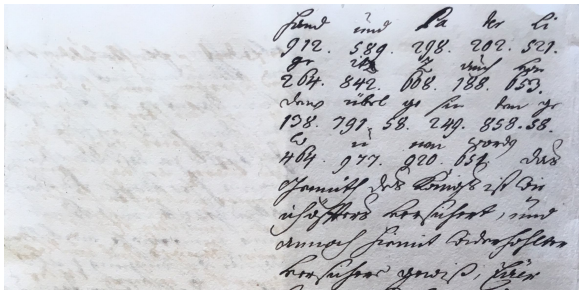


Figure 4: Message concept with encrypted part (Slovak National Archives, fond Esterházi - čeklíska vetva, box n. 635)

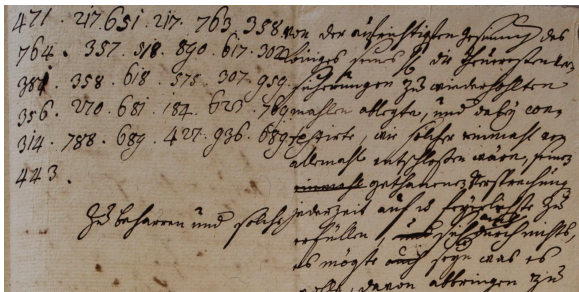


Figure 5: Message concept with encrypted part (Slovak National Archives, fond Esterházi - čeklíska vetva, box n. 635)

Cardbox no. 636 contains six encrypted documents: one fully encrypted concept and five letters, of which there are five documents written in French (Figure 6), and one in the German language. All of the documents are dated to 1744. One encrypted letter was sent by Empress Maria Theresa to Count Nicolaus Esterházy. In the remaining documents, we do not recognize the participants of the communication. The corresponding plain text parts are not available for these documents.

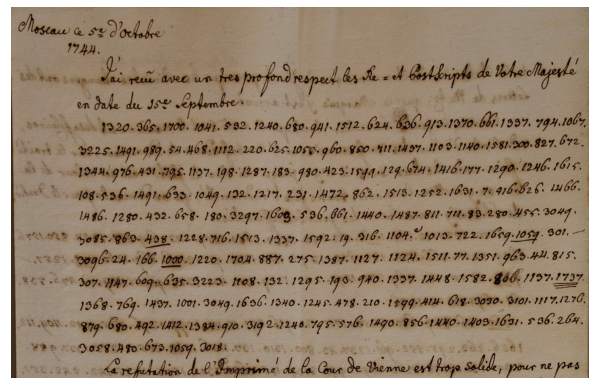


Figure 6: Cipher text example (Slovak National Archives, fond Esterházi - čeklíska vetva, box n. 636)

In the **Amade-Üchtritz** family archive, we have found thirty-seven encrypted documents. Most of the documents are from the beginning of the 19th century and are related to Emil Üchtritz in the diplomatic service of the King of Saxony and to various Saxon envoys. Cardbox n. 136 contains five encrypted messages from 1814-1834, written in German and French. Three documents were sent by Detlev Graf von Einsiedel, and two by Minckwitz, Saxon Minister for Foreign Affairs. Four documents contain the corresponding plain text parts written above/below the cipher text. In one case, only the cipher text is preserved (Figure 7).

Cardbox n. 139 contains six encrypted French messages from 1806, correspondence of Senfft von Pilsach, Saxon envoy in Paris. In all cases, the corresponding plain text is written above the cipher text (Figure 8).

Cardbox n. 140 contains twenty-one documents written in French and German languages dated between 1816-1823. These messages are communication of Detlev Graf von Einsiedel with Schulenburg, the Saxon envoy in Vienna, and to Griesinger, the Saxon Legation Counsellor in Vi-

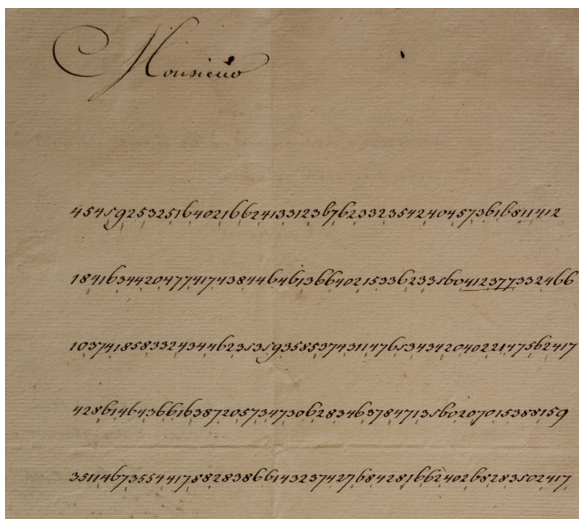


Figure 7: Cipher text example (Slovak National Archives, fond Amade-Üchtritz, box n. 136)

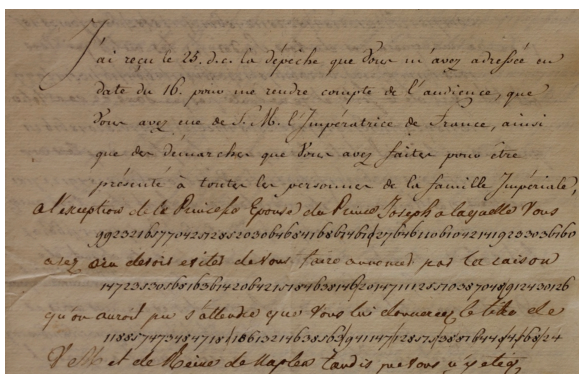


Figure 8: Cipher text example (Slovak National Archives, fond Amade-Üchtritz, box n. 139)

enna. One message was sent by Minckwitz to Schulenburg. At least two different cipher keys were used. In all cases, the corresponding plain text is available. Cardbox n. 141 contains four encrypted documents written in German and French languages sent to Fleming, the Polish-Saxon envoy in Vienna (Figure 9). These documents are from 1758, and the corresponding plain text is written above the cipher text in all cases.

Very interesting materials are located in cardbox n. 150, which contains the diary of Emil Üchtritz from October 1804 to August 1805 written mainly in the German language. The diary has 123 pages, containing encrypted entries on 27 pages (Figure 10). Analysis and detailed description of the diary will be the content of a future publication.

In the fonds of the **Pálffy-Daun** family, we

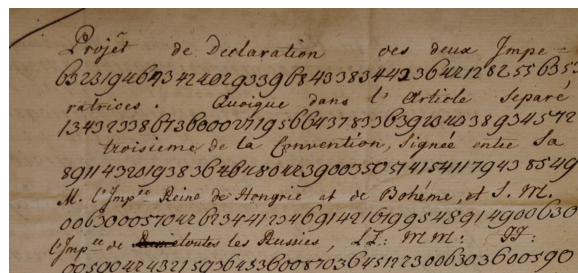


Figure 9: Cipher text example (Slovak National Archives, fond Amade-Üchtritz, box n. 141)

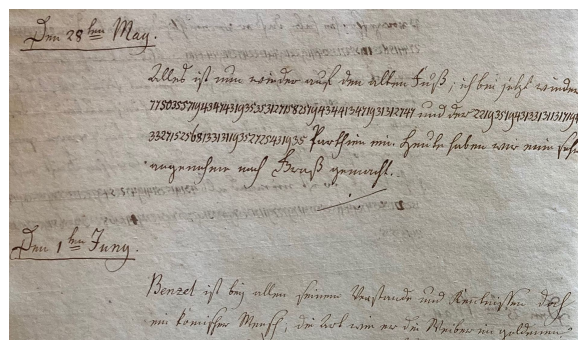


Figure 10: Encrypted diary parts (Slovak National Archives, fond Amade-Üchtritz, box n. 150)

found only one encrypted document written in the French language sent by Emperor Charles VI to Wirich Filip von Daun. The message contains only a few lines of encrypted text, where the corresponding plain text is written above the cipher text.

2.2 Cipher Keys

The examined fonds contain nine cipher keys. Seven cipher keys in the **Pálffy-Daun** family archive are (probably) related to the War of Spanish Succession. These (Spanish and Italian) cipher keys were used by Wirich Daun to communicate with several Counts and Marquises. The structure of these keys is very similar and copies the structure of a classical nomenclator system (Figure 15), each key is drawn on a large paper sheet and consists of simple/homophonic substitution⁹, bigram (and trigram) substitution, codes, and nulls. The individual sub-encryption systems are graphically separated in a table.

There are two cipher keys in the **Amade-Üchtritz** family archive. One cipher key is for a small (German) nomenclator system, containing letter substitution and a few codes, which was used

⁹Homophones were commonly used only for vowels in these cipher keys.

itself as an ally of Napoleon among the defeated countries, and through its envoys sought to regain lost positions, especially the revision of territorial losses.

Detlev Graf von Einsiedel (1773-1861) was a Saxon businessman, minister, and confidant of the Saxon kings Frederick Augustus I and his successor Anton. In foreign policy, he advocated a close alliance with Austria, seeking to strengthen Saxony's sovereignty by brokering new dynastic alliances with European ruling families. (Wetzel, 2014) In this he was supported by his brother-in-law *Emil von Üchtritz* (1783-1841), a long-time Saxon envoy to the Viennese court. He stood in the service of King Frederick Augustus of Saxony, especially during his captivity after the Battle of Leipzig in 1813, and worked for the restoration of the Saxon kingdom. He then served as an envoy to France and, from 1830 to Vienna. His son Emil was an officer, married into the Hungarian **Amade** family. (Wurzbach, 1883)

4 Digital Processing of Historical Manuscripts

Our valuable collection of historical manuscripts was converted into a digital form so it can be processed by modern computer algorithms to analyse statistical properties and even solve the documents encrypted by nomenclator. The image resolution of the original images is 4160×6240 pixels. Documents vary in quality and readability. Some of the documents contain encrypted and non-encrypted parts on a single page. The portion of the collection contains documents with digits formed in groups delimited by separators. Automated image processing needs to take all these factors into consideration.

Antal and Marák (2022) proposed an automated software system for historical handwritten digit detection, recognition, and transcription based on deep learning. This way, a large number of historical documents can be analyzed and solved in an automated manner. They provided a detailed description of a digit detector based on Mask R-CNN (He, 2017) method along with technical details related to the dataset, manually created annotations, training, inference, and transcription algorithm. Their Mask R-CNN based detector works well in general, however, it has some limitations which need to be addressed.

Limitations of the digit detector proposed in

(Antal and Marák, 2022):

- Mask R-CNN detector along with ResNet as its backbone network require a large amount of GPU memory which led to unavoidable optimizations. They needed to resize their original images to a smaller resolution to be able to fit data into memory and run training.
- Handwritten digit detection is a challenging task where small and densely grouped objects (digits) are located in a large document. Most detectors, where Mask R-CNN is no exception, fail to reliably detect such objects. For this reason, they had to employ a strategy of dividing an input image into smaller 128×128 blocks. Training Mask R-CNN on the image blocks led to significant improvement in digit detection. Unluckily, it has introduced a serious downside. The image division may lead to splitting of a single digit into two different image blocks. As a result, this solution misses digits positioned near the border of each image block.
- Mask R-CNN was introduced in 2017 and is no longer considered as state-of-the-art detector. According to the benchmark (Papers with code, 2023), there are new families of modern multi-class object detectors achieving average precision approximately 25 % higher than Mask R-CNN. Moreover, modern detector architectures make detection of small objects possible without having to split the image into small blocks.

These problems motivated us to design, train, and test a new digit detector based on YOLOv7 (Wang et al., 2022), which is a faster and more accurate deep learning model than Mask R-CNN. Furthermore, YOLOv7 can easily be configured to detect small objects using its auto-anchor algorithm. Its official implementation and documentation can be found at (YOLOv7 GitHub, 2023). In its essence, YOLOv7 is an object detector producing rectangular bounding boxes for object instances. However, it has a special architectural tweak which allows it to run in instance segmentation mode to produce high precision polygonal masks for detected objects.

Handwritten digit transcription based on YOLOv7 is a procedure consisting of several steps:

1. Preparing the software environment and dependencies for YOLOv7.
2. Obtaining the YOLOv7 model pretrained on COCO dataset (Tsung-Yi Lin et al., 2014).
3. Preparing the training, validation and testing dataset.
4. Converting digit annotations from COCO format to YOLOv7 PyTorch format.
5. Configuring the model and setting hyperparameters.
6. Training the model using transfer learning.
7. Testing the model.
8. Digit transcription.

4.1 Preparation Stage

All the experiments were carried out on a computer with the following specification: AMD Ryzen 9 5900HX, GeForce RTX 3080 16 GB, 32GB DDR4 3200MHz. In order to have a robust detector and minimize training time, we employed a transfer learning technique. We obtained a pretrained model on the COCO dataset. The pretrained model accepts images of size 1280×1280 , so we needed to downscale our original images. Our image dataset has 18 images and was split into training (12 images), validation (3 images) and testing (3 images) sets. We collected more than twelve thousand¹⁰ polygonal annotations of digits 0-9 which are stored in well-known COCO format. More details about the annotations can be found in (Antal and Marák, 2022). Since our YOLOv7 performs digit detection on the entire image rather than on image blocks, we needed to transform geometric properties of annotations so they correspond to images of size 1280×1280 . The annotations were converted from COCO format to YOLOv7 PyTorch format using Roboflow framework (Roboflow, 2023).

4.2 Model Configuration, Hyperparameters and Training

The training took 300 epochs and the batch size was set to 1 due to GPU memory limitations. The learning rate was set to 0.0025 using a stochastic gradient descent optimizer. We also performed

¹⁰12,433

slight image augmentation to enhance the variability of our dataset. Namely, we generated augmented images by modifying hue, saturation, and brightness. Geometric transformations were omitted. Table 1 shows the values of standard performance indicators measured on the test dataset for the best model after 300 epochs of training.

Masks are polygons produced by the detector which determine the area of the object. Bounding boxes are rectangular areas defining the object location. Compared to masks, bounding boxes are less accurate estimations of object location when the object has an irregular shape. $mAP@.50$ and $mAP@.50:.95$ indicators represent mean average precision which is a common metric to evaluate the performance of the object detector. mAP indicator quantifies the detection accuracy measured for different IoU (Intersection over Union) values. IoU measures the degree of overlap between the predicted bounding box/mask and the ground truth box/mask. mAP is the average of AP (Average Precision) values where AP corresponds to the area under the precision-recall curve. The precision is calculated as the ratio of correctly predicted positive examples divided by the total number of positive examples that were predicted. The recall is a metric that quantifies the number of correct positive predictions made out of all positive predictions that could have been made.

Mask accuracy			
$mAP@.50$	$mAP@.50:.95$	Precision	Recall
91.3 %	60.9 %	88.2 %	91.0 %
Bounding box accuracy			
$mAP@.50$	$mAP@.50:.95$	Precision	Recall
91.6 %	66.8 %	88.6 %	91.1 %

Table 1: YOLOv7 digit detection performance on the test dataset after 300 training epochs

4.3 Testing

We evaluated the model inference using the confidence threshold of 50 % (i.e. only digits with at least 50% confidence are included in the final set of detections). We experimented with standard quality images to judge the general performance. The detector turned out to have only minor problems with missed out or misclassified digits. Figure 12 shows the detected bounding boxes and masks in a sample document.

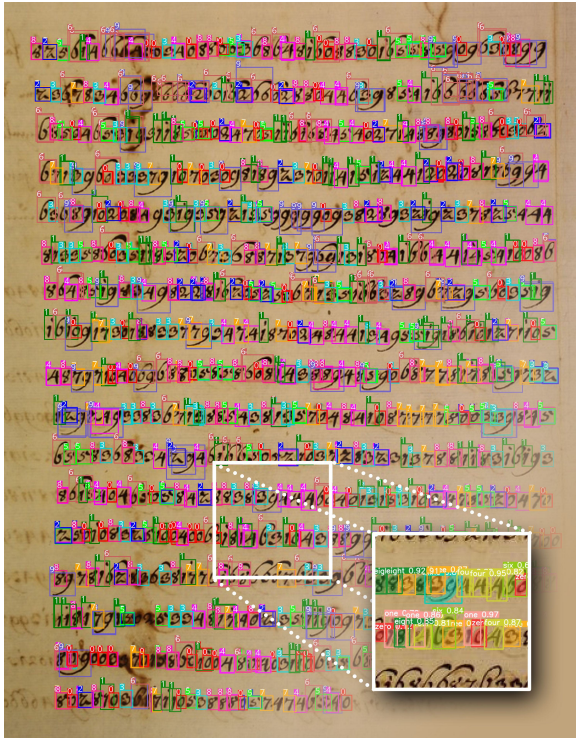


Figure 12: Result of digit detection and segmentation

Since our solution currently does not perform any image preprocessing, we also investigated the detection performance on images of lower quality. YOLOv7 was able to cope with problems like noisy paper background and areas where digits collided with the text from the reverse side of the paper. There are documents with encrypted and non-encrypted parts on a single page. In such situations we need to avoid false digit detections in non-encrypted parts. As we can see in Figure 13, this is where YOLOv7 performed quite well producing only minimum detections in areas outside the encrypted regions.

Last but not least, we sometimes encounter digit separators (dots) which are placed in digit sequences. We investigated the impact of the separators on detection performance. We found that separators do not have adverse effects on detection accuracy. Sample output from the aforementioned testing scenario is depicted in Figure 14.

4.4 Transcription

Once digits are detected by YOLOv7, all bounding boxes and their corresponding class labels are passed to the automated transcription algorithm presented in (Antal and Marák, 2022) which detects lines and extracts the digits. Digits are then

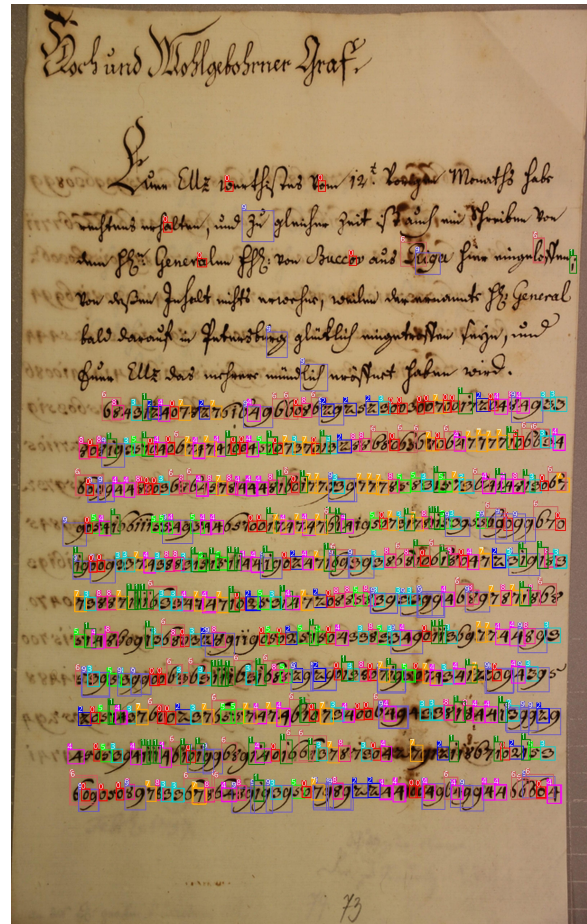


Figure 13: Digit detection performance in a document combining encrypted (at the bottom) and non-encrypted parts (at the top)

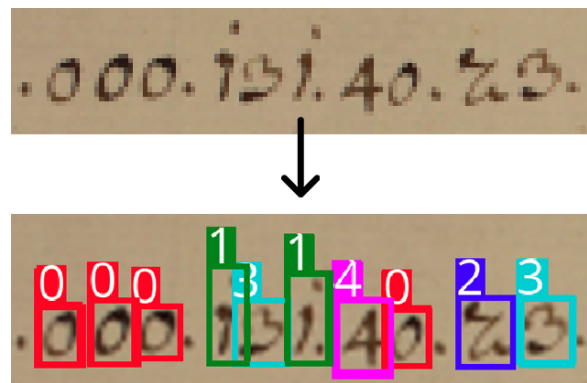


Figure 14: Digit detection performance in a document containing digit separators

stored in a text file. Figure 16 shows the intermediate steps of automated transcription of the encrypted document.

4.5 Future Work

In this paper we have presented our YOLOv7 based handwritten digit detector which is able to detect and classify large number of digits on a paper with acceptable performance. In addition, besides standard bounding boxes, it also supports polygonal masks for even higher precision. We have also eliminated the problem of Mask R-CNN detector where input images must be divided into small blocks leaving digits at the borders undetected. YOLOv7 solves this using its auto-anchor algorithm and detects digits in the entire document.

We plan to further improve our digit detection algorithm by extending the training dataset and incorporating geometric augmentations. It is crucial to train the detector on digits written using different writing styles and images of various quality. Currently, we deal with more research problems including segmentation of handwritten text area within the document, detection of special digit markups and glyphs. It is equally important to apply deep learning methods to segmentation and extraction of structured information from nomenclator keys.

5 Conclusions

During our research of historical encrypted documents in the Slovak National Archive in Bratislava we found several encrypted documents and keys in the archives of the aristocratic families Amade-Üchtritz, Esterházy, and Pálffy-Daun. Some of the documents are still encrypted, without known decryption or preserved corresponding key. To facilitate the potential decryption of these documents we focus on different tasks:

- systematic collection and examination of the materials, trying to match the documents with keys, or at least with similar documents with known decryption;
- historical study of the related time period, persons, and their relations, to provide insight on potential location of keys and potential key words for decryption attempts;
- and finally providing a supporting automation, mainly in the transcription of documents.

We believe that only with proper computer automation the researchers would be able to prop-

erly examine the large number of historical documents contained in the archives. As presented, new machine learning methods have promising results with good precision. However, the automated transcription of documents with machine learning does always lead to some detection and transcription errors (FAR, FRR). Unlike in plain text documents, such errors are difficult to detect and correct, because the ciphertext is seemingly a random sequence of characters. The ultimate goal of automatic decryption would require a further research in decryption methods that can tolerate some amount of transcription failures.

Acknowledgments

This work was supported by grant VEGA 2/0072/20: *Modern processing methods of encrypted archival documents*, and grant APVV-21-0371: *The glamour and fall of nobility. Strategies of noble representation in the History of Slovakia*.

We thank Jakub Mírka for his help, and Benedek Láng for providing materials from Austria and Hungary.

References

- Eugen Antal and Pavol Zajac. 2020. HCPortal Overview. In *Proceedings of the 3rd International Conference on Historical Cryptology, HistoCrypt 2020*, pages 18 - 20. Linköping University Electronic Press.
- Eugen Antal and Pavol Zajac. 2021. HCPortal Modules for Teaching and Promoting Cryptology. In *Proceedings of the 4th International Conference on Historical Cryptology, HistoCrypt 2021*, pages 1 - 11. Linköping University Electronic Press.
- Eugen Antal and Pavol Marák. 2022. Automated transcription of historical encrypted manuscripts. In *Tatra Mountains Mathematical Publications*, 82 (2022), pages 65 - 86. Slovak Academy of Sciences.
- Eugen Antal and Jakub Mírka. 2022. Wrong Design of Cipher Keys: Analysis of Historical Cipher Keys From the Hessisches Staatsarchiv Marburg Used in the Thirty Years' War. In *Proceedings of the 5th International Conference on Historical Cryptology, HistoCrypt 2022*, pages 1 - 11. Linköping University Electronic Press.
- Encyclopaedia Beliana. 2017. Kaunitz, Wenzel Anton. Available online: <https://beliana.sav.sk/heslo/kaunitz-wenzel-anton>. ISBN 978-80-89524-30-3.
- Kaiming He et al.. 2017. Mask R-CNN. In *IEEE International Conference on Computer Vi-*

- sion (ICCV), 2017, pages 2980-2988. DOI: 10.1109/ICCV.2017.322.
- Olga Khavanova. 2016. Farewell to Sent-Petersburg: count Nicolas Esterházy leaves the Russian capital (orig. Búcsú Szentpétervártól: Gróf Esterházy Miklós elhagyja az orosz fővárost). In *Aetas* 31 / 4, pages 188 - 199.
- Olga Khavanova. 2017. The career of count Nicolas Esterházy Ambassador of St. Petersburg (orig. Gróf Esterházy Miklós szentpéteri nagykövet karrierje). In *Az Esterházyak fraknoi ifjabb ága.*, pages 60 - 75. Mesto Senec.
- Olga Khavanova. 2019. From Madrid To St. Petersburg. Count Miklós Esterházy, the first Hungarian Career Diplomat of Maria Theresa (orig. Madridtől Szentpétervárig. Gróf Esterházy Miklós, Mária Terézia első magyar karrierdiplomatája). In *Századok* 153/6, pages 1123 - 1128.
- Jiří Kubeš et al. 2018. On behalf of the Emperor. Czech and Moravian aristocracy in Habsburg diplomacy 1640-1740 (orig. V zastoupení císaře. Česká a moravská aristokracie v habsburské diplomacii 1640–1740). ISBN: 9788074225741 Praha : NLN.
- Benedek Láng. 2020. Was it a Sudden Shift in Professionalization? Austrian Cryptology and a Description of the Staatskanzlei Key Collection in the Haus-, Hof- und Staatsarchiv of Vienna. In *Proceedings of the 3rd International Conference on Historical Cryptology, HistoCrypt 2020*, pages 87 - 95. Linköping University Electronic Press.
- Beáta Megyesi, Bernhard Esslinger, Alicia Fornés, Nils Kopal, Benedek Láng, George Lasry, Karl de Leeuw, Eva Pettersson, Arno Wacker and Michelle Waldispühl. 2020. Decryption of historical manuscripts: the DECRYPT project. In *Cryptologia*, volume 44, number 6, pages 545-559. Taylor & Francis.
- Beáta Megyesi, Crina Tudor, Benedek Láng and Anna Lehofer. 2021. Key Design in the Early Modern Era in Europe. In *Proceedings of the 4th International Conference on Historical Cryptology, HistoCrypt 2021*, pages 121 - 130. Linköping University Electronic Press.
- Beáta Megyesi, Crina Tudor, Benedek Láng, Anna Lehofer, Nils Kopal, Karl de Leeuw and Michelle Waldispühl. 2022. Keys with nomenclatures in the early modern Europe. In *Cryptologia*, DOI: 10.1080/01611194.2022.2113185. Taylor & Francis.
- Papers with code. 2023. Object Detection on COCO test-dev. <https://paperswithcode.com/sota/object-detection-on-coco>.
- Roboflow. 2023. Roboflow. <https://roboflow.com/>.
- Lothar Schilling. 1994. Kaunitz und das renversement des alliances. Studien zur außenpolitischen Konzeption Wenzel Antons von Kaunitz. In *Historische Forschungen*, volume 50. Berlin : Duncker & Humblot.
- Antonio Schmidt-Brentano. 2006. Kaiserliche und k.k. Generale (1618-1815) Österreichisches Staatsarchiv/A. Schmidt-Brentano.
- Tsung-Yi Lin et al.. 2014. Microsoft COCO: Common Objects in Context. In *CoRR*, abs/1405.0312 <http://arxiv.org/abs/1405.0312> Dataset URL: <https://cocodataset.org/#home>
- Wang Chien-Yao, Bochkovskiy Alexey, Liao Hong-Yuan Mark. 2022. YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors. In *ArXiv*, pages 2980-2988. DOI: 10.48550/ARXIV.2207.02696 <https://arxiv.org/abs/2207.02696>.
- Michael Wetzel. 2014. Detlev Graf von Einsiedel. Available online: [https://saebi.isgv.de/biografie/Detlev_Graf_von_Einsiedel_\(1773-1861\)](https://saebi.isgv.de/biografie/Detlev_Graf_von_Einsiedel_(1773-1861)).
- Constant von Wurzbach. 1883. Üchtritz, Emil von. In *Biographisches Lexikon des Kaiserthums Oesterreich Trzetzewinsky-Ullepitsch*, Band 48. Verlag der Universitäts-Buchdruckerei von L. C. Zamarski. Wien.
- YOLOv7 GitHub. 2023. Official YOLOv7 GitHub repository. <https://github.com/WongKinYiu/yolov7>.

Appendices

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	W	X	Y	Z	Trattamento
56	58	60	62	64	65	69	71	73	75	76	77	78	79	66	68	70	72	74	57	59	61	63	65	Da 45 sin'a. 50
51			52					53					54						55					Nulle 30586
Da. be. bi. bo. bu 5-6-7-8-9	Ca. ce. ci. co. cu 10-11-12-13-14	Da. de. di. do. du 15-16-17-18-19	La. fe. fi. fo. fu 20-21-22-23-24	Ga. ge. gi. go. gu 25-26-27-28-29	Ha. he. hi. ho. hu 30-31-32-33-34	La. le. li. lo. lu 35-36-37-38-39																		
Ma. me. mi. mo. mu 40-41-42-43-44	Na. ne. ni. no. nu 80-81-82-83-84	Pa. pe. pi. po. pu 85-86-87-88-89	Qua. que. qui. qua 90-91-92-93	Ta. te. ti. to. tu 95-96-97-98-99	Ua. ue. ui. ua. ua 100-101-102-103-104	Ja. te. ti. to. tu 105-106-107-108-109																		
Va. ve. vi. vo. vu 110-111-112-113-114	Za. ze. zi. zo. zu 115-116-117-118-119	Ab. eb. ib. ob. ub 120-121-122-123-124	Ac. ec. ic. oc. uc 125-126-127-128-129	Ad. ed. id. od. ud 130-131-132-133-134	Af. ef. if. of. uf 135-136-137-138-139	Aq. eq. iq. oq. uq 140-141-142-143-144																		
Al. el. il. ol. ul 145-146-147-148-149	Am. em. im. om. um 150-151-152-153-154	An. en. in. on. un 155-156-157-158-159	Ap. ep. ip. op. up 160-161-162-163-164	Ar. er. ir. or. ur 165-166-167-168-169	As. es. is. os. us 170-171-172-173-174	At. et. it. ot. ut 175-176-177-178-179																		
M. Ma. 180	Cancellier 195	Esercito 213	Caeta 231	Mazzaccara 249	Puffia 267	Foscana 285																		
M. Aleman 181	Catalana 196	Brendazu 214	Herole 232	Miro 250	De 268	Partana 286																		
M. Ambasciat. 182	Collateral 197	Eugenia 215	Raya 233	Maoleon 251	Regina 269	Tursis 287																		
M. Ammirante 183	Consiglio 198	Dicelaffatic 216	Imperat. 234	Modignani 252	Regublia 270	Turin 288																		
M. Artiglieria 184	Consignier 199	Florenza 217	Imperial 235	Mason 253	Roma 271	Trasporto 289																		
M. Arcivescovo 185	Cardinal 200	Fiandra 218	Inghilterra 236	Madrid 254	Vienna 272	Turchi 290																		
M. Aparado 186	Conca 201	Francia 219	Italia 237	Malta 255	Ravennari 273	Vienna 291																		
M. Aquirre 187	Conte 202	Francia 220	Legotenora 238	Napole 256	Regano 274	Venezia 292																		
M. Argente 188	Camera 203	Poncalada 221	Londra 239	Nuntio 257	Regente 275	Vicere 293																		
M. Argento 189	Calabria 204	Perrara 222	Livorno 240	Nanda 258	Regio 276	Vicere 294																		
M. Barcelona 190	Castell 205	Poggia 223	Levante 241	Nanda 259	Regio 277	Vicere 295																		
M. Bolano 191	Casare 206	Spinale 224	Milano 242	Dupa 260	Regio 278	Vicere 296																		
M. Beleredi 192	Duca 207	General 225	Mantova 243	Dyniupe 261	Regio 279	Vicere 297																		
M. Baron 193	Deput. 208	Genova 226	Marche 244	Dionte 262	Regio 280	Vicere 298																		
M. Baya 194	Darsena 210	Gallasio 227	Madana 245	Dionte 263	Regio 281	Vicere 299																		
	Doppie 211	Spiera 228	Messina 246	Dionte 264	Regio 282	Vicere 300																		
	Dulcino 212	Gran 229	Montesano 247	Dionte 265	Regio 283	Vicere 301																		
		Evernator 230	Misoria 248	Dionte 266	Regio 284	Vicere 302																		

Figure 15: Cipher key example (Slovak National Archives, fond Pálffy-Daun, Klasse XXXIII - Wierich Daun, box n. 38, fasc. 22)

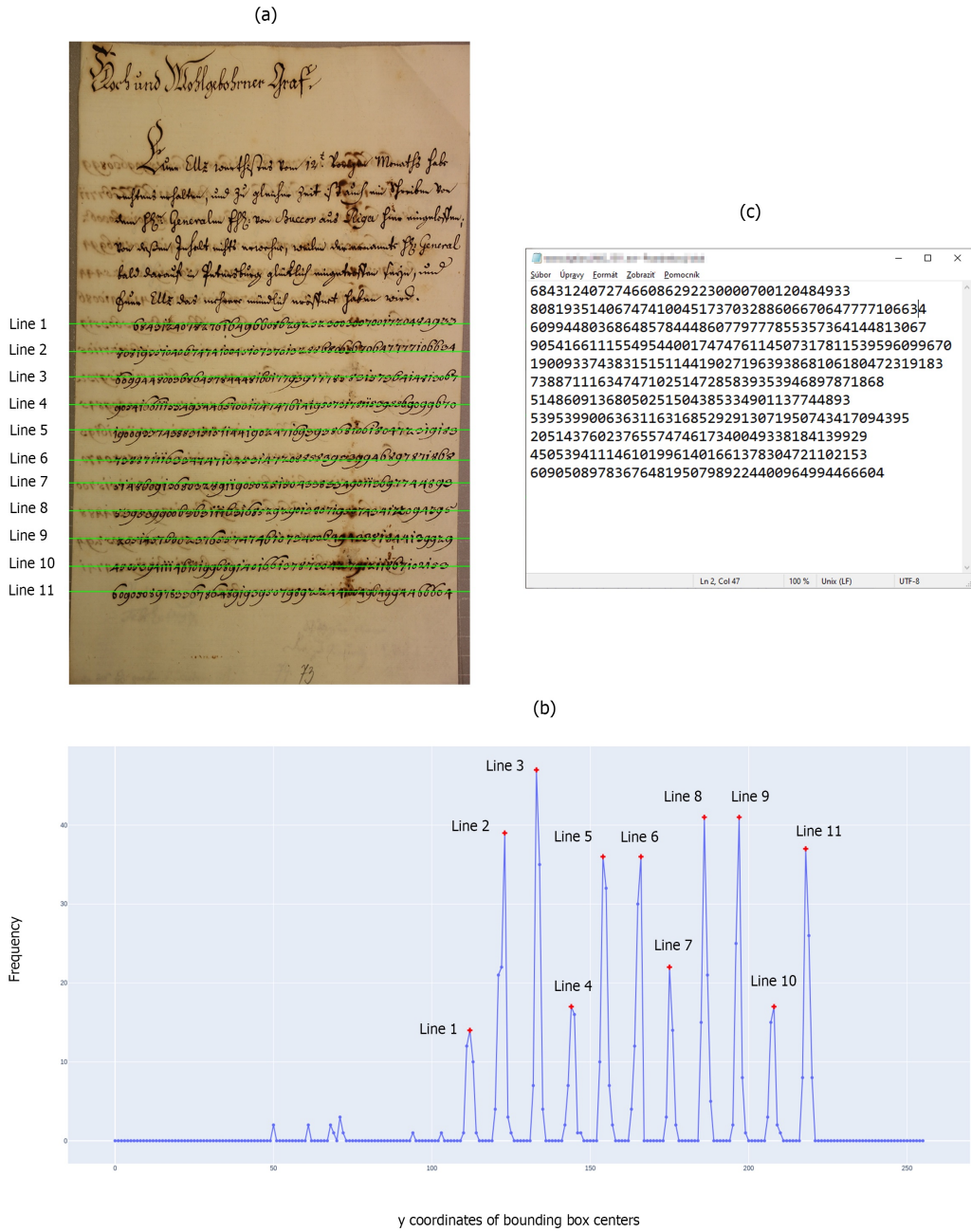


Figure 16: Intermediate results of our automated handwritten document transcription: (a) original document with highlighted positions of detected lines, (b) histogram of y coordinates of bounding box centers (peaks indicate line positions), (c) text file containing the transcribed digits



Published by:

NEALT Proceedings Series No. 50

ISSN: 1736-8197 (print), 1736-6305 (online)

ISBN 978-91-8075-134-6 (PDF)

<https://doi.org/10.3384/ecp195>

Linköping Electronic Conference Proceedings No. 195

ISSN 1650-3686 (print), 1650-3740 (online)

NEALT Proceedings Series No. 50

ISSN 1736-8197 (print), 1736-6305 (online)

**Cover images: Fritz Menzer - A Secret Life &
3D-Cipher, Deutsches Museum**