Some Interactive Tools for Examining Renaissance Ciphers

Alexander Boxer
AXOLOTL Science Outreach
2475 Virginia Ave. NW, Washington, DC 20037, USA
alexander.boxer@gmail.com

Abstract

This paper describes interactive tools for exploring the ciphers in Johannes Trithemius' *Steganographia* (1500). These tools have been implemented on the website *Trithemius Redivivus* (`http://trithemius.com`) and provide capabilities to (1) apply Trithemius' cryptographic techniques on any text, (2) display letter-frequency histograms of the output, and (3) rank the outputs according to their relative entropy, computed with respect to a reference text.

Introduction: The *Steganographia* of Johannes Trithemius

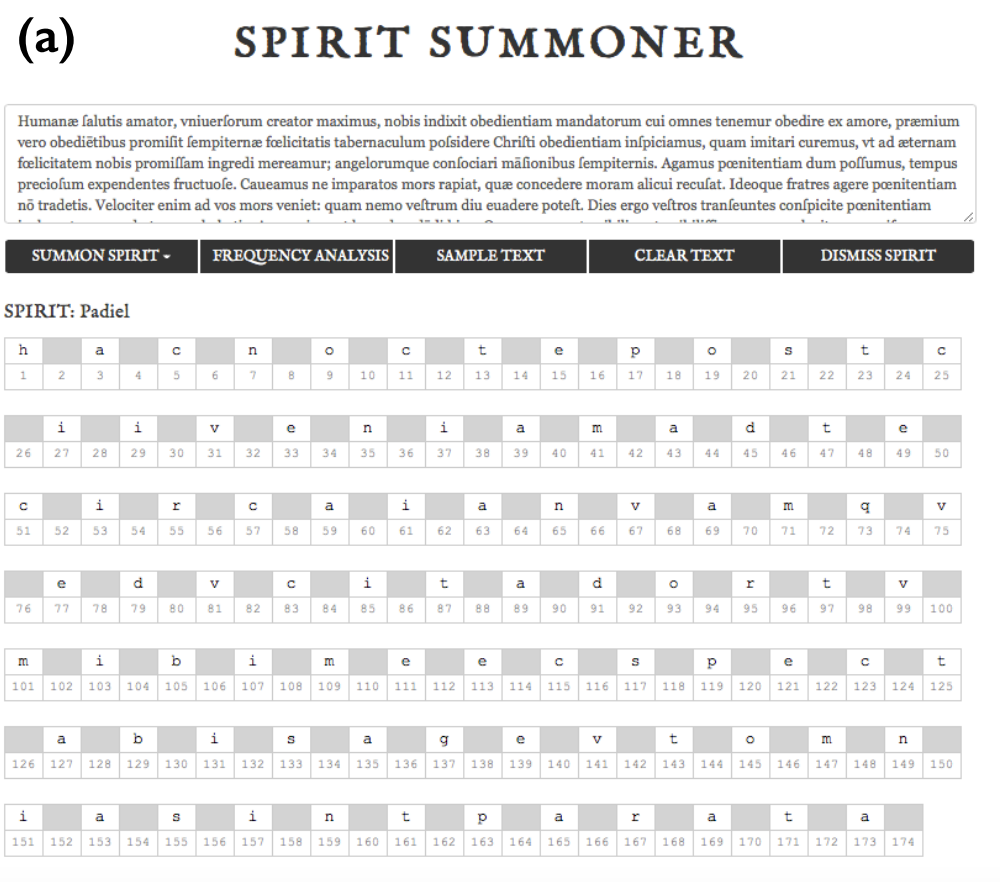
The *Steganographia* purports to be a manual on how to transmit secret messages by enlisting the aid of aerial spirits with names like Pamersiel, Padiel, Camuel, and so on. It was composed as a manuscript in the year 1500 by Johannes Trithemius, the abbot of a Benedictine monastery in Sponheim, Germany. No copies of the original manuscript survive, but the first printed edition of the work, dated 1606, included a "key" revealing that the incantations used to summon the spirits were, in fact, coded instructions for how to implement various cryptographic ciphers [1]. More precisely, this 1606 key pertained to the first two books of the *Steganographia*; it was not until 1996-7 that Thomas Ernst and Jim Reeds, working independently, discovered the key to the third and final book [2], [3]. As these keys disclose, each chapter of the *Steganographia* demonstrates a different technique for concealing a plaintext message within a larger cover-text. Indeed, the term devised by Trithemius to name his art, "steganography," comes from the Greek $\sigma\tau\acute{\epsilon}\gamma\omega$ (stego) = cover, and $\gamma\rho\acute{\alpha}\varphi\omega$ (grapho) = write. Trithemius' *Steganographia* is, therefore, both a manual and an example of steganography.

Ernst and Reeds' relatively recent discovery of the key to the final book of the *Steganographia* highlights a long-running question: Given that we know at least one occult text (the *Steganographia*) was actually an elaborate ruse for conveying hidden messages, do any of the the similar occult texts from that time period also contain hidden messages concealed using the same techniques? This is not a new idea. As early as the 17^{th} century, Robert Hooke (of Hooke's Law fame) proposed that John Dee's infamous angel diaries were not transcripts of his crystal ball sances, but rather secret intelligence reports encrypted with Trithemian steganography for dispatch to his sovereign, Queen Elizabeth I [4]. Could such a wild claim be true? This paper will describe approaches to address this and similar questions in a systematic and quantitative way.

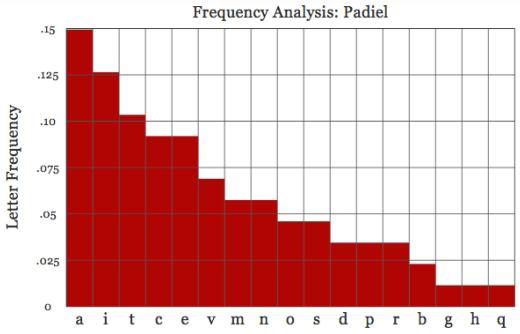
Tools to Apply and Analyze Trithemius' Steganographical Techniques

The first step in ascertaining the presence or absence of a Trithemian cipher in a text is to understand the form of the ciphers themselves. Each chapter of the *Steganographia* corresponds to one spirit and one cipher. Book 1 contains 32 chapters and treats ciphers based on increasingly elaborate patterns of nulls in the sequence of initial letters of the words of the covertext. For example, the cipher corresponding to the spirit Aseliel takes as significant only the initial letters of words 3, 4, 7, 8, 11, 12, and so forth. Book 2 contains 25 chapters and treats primarily alphabet-shift ciphers, again using only the sequence of initial letters. Book 3, although

(a)



(b)



(c)

SPIRIT: Pandemonium (A Relative-Entropy Analysis of Every Spirit)

Spirit	Relative-Entropy (Reference Text: *Genesis* - Latin)
1.2 Padiel	0.186
1.1 Pamersiel	0.259
1.4 Aseliel	0.295
1.6 Gediel	0.405

Figure 1 : *Views of the* "Spirit Summoner" *at* Trithemius Redivivus. (a) *The covertext input and candidate plaintext output.* (b) *Letter-frequency histogram of the output.* (c) *Table sortable by the relative entropies of the outputs.*

containing only one full chapter, provides a template for concealing messages in tables of numbers such as an astrological almanac.

The website *Trithemius Redivivus* (`http://trithemius.com`) has been created to facilitate an exploration of these ciphers. The site features an ability to view the text of the *Steganographia* in either Latin, English, or side-by-side mode; dynamic navigation menus; and intertextual key-icons that reveal the key to the relevant section of text when pressed. The site also contains a "Spirit Summoner" that allows one to quickly apply and analyze the steganographical techniques described by Trithemius. The Spirit Summoner has three basic functionalities that we can illustrate with one of Trithemius' own examples.

1. The first functionality is to apply Trithemius' steganographical techniques on any text of interest. Consider a prayer that begins, "*Humanæ salutis amator, vniuersorum creator maximus, nobis indixit obedientiam mandatorum cui omnes tenemur obedire ex amore...*" Following Trithemius' instructions, we can "summon" the spirit named Padiel. Padiel is the codeword directing the recipient to keep only the first letters of every other word in the covertext. This yields a plaintext message that begins, "*hac nocte...*", which is Latin for "tonight," and which in the example continues on as a perfectly intelligible message.

2. Given the multitude of named spirits and the corresponding multitude of ways devised by Trithemius to conceal a text within a text, it is generally very difficult to search for a message encrypted using one of his ciphers. Even in Trithemius' examples, where the correct spirit is known in advance, the plaintext is often difficult to recognize due to the absence of word-breaks, Trithemius' use of odd spellings, and the fact that the languages involved are 16^{th} century Latin and German. A letter-frequency histogram of the output of an operation provides a further check on whether that operation has produced an intelligible message or gibberish. In Western languages like Latin, German, and English, letters like 'E' are very common whereas letters like 'X' much less so; consequently, a letter-frequency histogram is a quick way to determine if the output looks natural or unnatural. For example, we can confidently dismiss the possibility that an author has concealed a message with a particular cipher if that cipher returns a plaintext where 'X' and 'Z' are the most frequent letters.

3. A letter-frequency histogram treats only one steganographical operation, or "spirit", at at time. Ideally we would like to examine all of the operations at once in order to determine which ciphers, if any, warrant additional investigation. One way to do this is to rank each cipher according to the naturalness or unnaturalness of its output message. The Relative Entropy, or Kullback-Liebler (KL) distance, is a standard quantity from the field of Information Theory that measures how similar one distribution is to a reference distribution [5]. It is especially well-suited to discrete, alphabet-style distributions. Given a discrete probability distributions $p(x)$, and a reference distribution $q(x)$, the relative entropy is defined as:

$$D(p||q) = \sum_x p(x) \log \frac{p(x)}{q(x)}. \tag{1}$$

For our Spirit Summoner, we have generated a reference letter-frequency distribution $q(x)$ from the 133,889 letters in the Latin Vulgate version of *Genesis* [6]. Therefore, for any letter-frequency distribution $p(x)$ — for example, the letter frequency distribution of the output message of a Trithemian cipher operation — the relative entropy $D(p||q)$ provides a quantitative measure of how similar $p(x)$ is to $q(x)$, that is, how closely the output message resembles Latin. Smaller values indicate a greater similarity with zero representing a perfect match.

Intuitively, the relative entropy can be thought of as the labor expended by a typesetter who stores his cases of letters in different rooms along the corridor of his workshop, such that each room contains only one letter-type. In order to minimize the amount of time he must spend walking up and down the corridor to fetch letters, the typesetter could, prior to each job, arrange which letters are stored in which room according to his expectation of what the text will be. If the typesetter expects he will be setting a Latin text, he will achieve

maximum efficiency by placing the cases of ‘A’s’, ‘I’s’ and ‘E’s’ closest to him, and the cases of ‘X’s’, ‘Y’s’, and ‘Z’s’ furthest away. If instead the typesetter is handed a work not in Latin but in Polish, where the letters ‘Y’ and ‘Z’ are significantly more common, his mistaken expectation will result in more time spent walking to the very end of the corridor to fetch ‘Z’s’ . In this analogy, the relative entropy represents the difference in time required to typeset the Polish document versus a document in the expected Latin.

A relative entropy test is far too simplistic to determine whether a message belongs to the same alphabet as the reference. A more sophisticated test might compare the frequency of digraphs and trigraph combinations. However, the simple relative entropy test is quite effective for establishing that a message *does not* belong to the reference alphabet, which of course is the default case when looking for steganographically concealed messages. In this way, the relative entropy calculator of the Spirit Summoner can assist in the hunt for Trithemian ciphers by identifying which “spirits” warrant a closer look, and which do not.

Future Work

Trithemius Redivivus is a long-term project that is just getting started. In particular, I have translated just the first few chapters of the *Steganographia* out of more than sixty total. Likewise, I intend to add more features to the Spirit Summoner, most obviously by including options for other reference languages, such as German or English, to the relative entropy calculator. All the same, I hope that these efforts, although preliminary, will be of interest to those who enjoy seeing how modern, interactive tools can be used to explore fascinating historical texts.

References

[1] Trithemius, Johannes. *Steganographia*. Frankfurt: Matthias Becker, 1606. A digitized photographic reproduction of the complete text can be downloaded from, amongst other sites, that of the Bayerische StaatsBibliothek.

[2] Ernst, Thomas. “Schwarzweisse Magie. Der Schlussel zum dritten Buch der Steganographia des Trithemius.” *Daphnis* 25 (1996): Heft 1.

[3] Reeds, James A. Solved: The Ciphers in Book III of Trithemiuss Steganographia. *Cryptologia* 22 (October, 1998): 291-313.

[4] Hooke, Robert. Of Dr. Dees Book of Spirits, in *The Posthumous Works of Robert Hooke*. London: Richard Waller, 1705, 203-9.

[5] Cover, Thomas M., and Thomas, Joy A. *Elements of Information Theory*, 2nd Edition. Hoboken, New Jersey: Wiley and Sons, 2006.

[6] *Biblia Sacra Vulgata* (Stuttgartensia) `https://la.wikisource.org/wiki/Biblia_Sacra_Vulgata_(Stuttgartensia)/Genesis`