# A CRYPTOGRAPHIC APPROACH TO LANGUAGE IDENTIFICATION: PPM 

Ebru Celikel<br>Ege University International Computer 35100 Bornova/Izmir, Turkey

Keywords: Language identification, Statistical modelling, PPM


#### Abstract

The problem of language discrimination may arise in situations when many texts belonging to different source languages are at hand but we are not sure to which language each belongs to. This might usually be the case during information retrieval via Internet. We propose a cryptographic solution to the language identification problem: Employing the Prediction by Partial Matching (PPM) model, we generate a language model and then use this model to discriminate languages. PPM is a cryptographic tool based on an adaptive statistical model. It yields compression rates (measured in bits per character -bpc) to far better levels than that of many other conventional lossless compression tools. Language identification experiment results obtained on sample texts from five different languages as English, French, Turkish, German and Spanish Corpora are given. The rate of success yielded that the performance of the system is highly dependent on the diversity, as well as the target text and training text file sizes. The results also indicate that the PPM model is highly sensitive to input language. In cryptographic aspect, if the training text itself is kept secret, our language identification system would provide security to promising degrees.


## 1 INTRODUCTION

With ongoing improvements in network facilities, the number of computers getting connected to Internet is increasing everyday. This widespread use of Internet makes diversity of languages available online. Hence, there should be a sound way of determining the correct language of a retrieved text. This would not only help discriminate texts belonging to different source languages, but also facilitate text categorization, natural language processing and information retrieval.

Of many techniques used to determine the correct language, exploiting the statistical characteristics of disputed languages is quite common. Frequency values for the alphabet size, average word length, statistics of vowel/consonants throughout the text might all be used to generate the characteristics of different languages (Ganesan and Sherman, 1998). Using the frequency of short word occurrences (Klukowski, 1991 and Ingle, 1991), the independent as well as joint probability of symbols (Rau, 1974), n-grams (Beesley 1988; Cavner and
Trenkle, 1994), n-graphs, i.e. group of n-words (Batchelder, 1992), diacritics and special characters (Newman, 1987) may all help extract the linguistic characteristics. Exploiting statistics might be
extended to incorporate syllable characteristics (Mustonen, 1965) and morphology and syntax (Ziegler, 1991) of texts under suspect. Being a statistical approach, Hidden Markov Model (HMM) is employed in language discrimination studies, too (Preez and Weber, 1996).

Another approach in language discrimination is to use artificial intelligence system with neural networks. In this way, the system can learn characteristics of a language and the language of unknown texts might be determined (Braum and Levkowitz, 1998).

Our approach towards language identification incorporates the Prediction by Partial Matching (PPM) algorithm. The premises of our study are cryptographic, as well as statistical: It is cryptographic in that, PPM is basically a lossless compression tool which is used to encode texts into formats that are hard to recover, as long as the algorithm itself is hidden. It is also statistical because, PPM extracts a statistical model out of a given text (called training text) and uses this model to decide whether the text in question belongs to the same language as that of the text from which the model was extracted. Teahan used PPM technique to discriminate the language of Bibles written in six
languages as English, French, German, Italian, Latin and Spanish (Teahan, 2000).

## 2 COMPONENTS

The scheme we designed and developed for language identification is made up of an adaptive statistical model PPM, followed by an encoder, Arithmetic Coding. In the following subsection, these components are introduced. We then give the details of Corpora we used during our implementation.

### 2.1 PPM Model

PPM is a compression technique, making use of a statistical model of the input text. It was first introduced by Cleary and Witten (Cleary and Witten, 1984), and was improved by Moffat (Moffat, 1990). The algorithm reads the upcoming symbol from the input text, assigns a probability to it and sends it to an adaptive encoder, i.e. the Arithmetic Coder. The probabilities assigned to each symbol are determined by blending together and adaptively updating the several fixed order context models (Nelson, 1991).

PPM is a bijective algorithm. By employing fixed input symbol sizes, it is capable of interpreting any collection of bytes as valid compressed input. This property has positive implications for compression efficiency and security: there is no way to distinguish random data from valid output (Nodeworks Encyclopedia URL).

PPM employs a context of length $k$ to predict and assign a probability to the up-coming symbol. If the upcoming symbol is a new one that has never occurred so far, then the length-k context cannot predict it. In this case, an escape symbol is issued and the model is transferred to a lower level, i.e. length $\mathrm{k}-1$ context. This reduction may continue until a non-first-time symbol is reached. When the upcoming symbol is determined successfully, Arithmetic Coder is then used to encode it (Teahan, 1998).

Arithmetic Coding is an encoding technique providing compression rates close to the language entropy. Arithmetic Coding is considered to be optimal because, on the average, it is not possible to encode better than the entropy rate (Witten, Moffat and Bell, 1999). The algorithm for Arithmetic Coding is as follows:

```
procedure ArithmeticCoding()
set low to 0.0 and high to 1.0
while there is more input symbol do
```

```
    get an input symbol
    code_range = high - low
    high=low + range * high_range(symbol)
    low = low + range * low_range(symbol)
end of while
output low
end procedure
```

Arithmetic Coding is achieved by representing a stream of input symbols as a floating point number between 0 and 1, instead of replacing an input symbol with a new symbol. As the text is encoded, this interval narrows as much as the frequency of the symbols in the source text. Source message symbols with high frequency narrows the interval less as compared to the low frequency source message symbols. In this manner, high frequency source message symbols require less number of bits in the output sequence.

### 2.2 Language Identification System

The language identification system we designed and developed is made up of two components as a statistical model generator and an encoder (Fig. 1). There are two inputs to the system: One being the text whose language is already known and the other is the text in question (the disputed text), i.e. whose language is to be determined. Within the system, the former is called the training text and is fed into the PPM model, and the latter is called the plaintext and is fed into the encoder itself.


Figure 1: The Language identification system
During implementation, we incorporated the PPM algorithm as follows: We used training text to gather symbol frequencies and out of these frequencies, we com-pressed different texts whose languages are of question. When the languages of the training text and disputed text are the same, the compression performance of PPM is expected to be better. But there are some effects as linguistic characteristics, type and length of texts, etc. that might affect the performance of our system.

In order to evaluate our scheme's rate of success in determining the right language, we employed the cross-entropy. The cross-entropy $\mathrm{H}(\mathrm{L}, \mathrm{M})$ is defined as an upper bound to the actual entropy $\mathrm{H}(\mathrm{L})$ of a
language by using a probability model M . We need the cross-entropy because, the exact probability distribution of a language is never certain. Hence, $\mathrm{H}(\mathrm{L})$ is just a theoretical value. The cross-entropy of a language L calculated using a model M is formulated in Eq. 1. The entropy and cross-entropy are both measured in bits per character - bpc.
$H(L, M)=-\sum p_{M}\left(x_{1}, x_{2}, \ldots, x_{m}\right) \log p_{M}\left(x_{1}, x_{2}, \ldots, x_{m}\right)$
In Eq. 1, the entropy of a language L, i.e. $\mathrm{H}(\mathrm{L})$ is calculated as follows (Eq. 2):

$$
\begin{equation*}
H(L)=\underset{m \rightarrow \infty}{\lim -\frac{1}{m}} \sum p\left(x_{1}, x_{2}, \ldots, x_{m}\right) \log p\left(x_{1}, x_{2}, \ldots, x_{m}\right) \tag{2}
\end{equation*}
$$

Entropy H in Eq. 1 is the average number of bits per symbol needed to encode a message (Shannon, 1948).

$$
\begin{equation*}
H(P)=-\sum_{i=1}^{k} p\left(x_{i}\right) \log p\left(x_{i}\right) \tag{3}
\end{equation*}
$$

Assuming that the probabilities summing to 1 are independent and the k possible symbols have a probability distribution $\mathrm{P}=\mathrm{p}\left(\mathrm{x}_{1}\right), \mathrm{p}\left(\mathrm{x}_{2}\right), \ldots, \mathrm{p}\left(\mathrm{x}_{\mathrm{k}}\right)$, the entropy can be calculated as below (Eq. 3):

For this study, we incorporated Corpora from five European languages as English, French, Turkish, German and Spanish. These languages differ from each other to varying degrees. For example, while English, French and Spanish are more alike, Turkish is totally different from these languages and German has some common linguistic characteristics with the above mentioned group of three. The alphabet size for these languages are 26 letters for English and French, 29 letters for Turkish and 30 letters for both German and Spanish.

All languages of concern in this study are analytical, agglutinative and fusional (having affixes). Analytical languages either does not combine concepts into single words at all (like in Chinese) or does so economically as is the case in English and French. The sentence itself is of primary concern in analytical languages, while the word is of minor interest. Turkish is synthetic and a free constituent order language, morphologically extendible with the its rich set of derivational and inflectional suffixes. In a synthetic language, the concepts cluster more thickly, the words are more richly chambered, but there is a tendency to keep the range of concrete significance in the single word down to a moderate compass (Sapir, 1921). German has extensive use of inflectional endings and compound words are quite common (German Linguistic URL). Spanish has quite the same linguistic characteristics as French, with higher average word length.

Our Corpora consists of these five different languages and each language has a group of seven texts. The texts within each language have been deliberately selected from different essay categories to reflect the changes of the style into our language discrimination implementation. These categories are novel, technical document, poetry, manual, theatre text, Holy book (Bible or Qoran) and a dictionary/encyclopedia. We first based our Corpora construction on text files from the standard English Cor-pus Canterbury (Canterbury Corpus). Modeling after the Canterbury Corpus, we then compiled Corpora from the other four source languages as French, Turkish, German and Spanish. The texts in Turkish Corpus are from Celikel (Celikel, 2004), and the rest of the texts in other languages are all from Internet. The sizes and contents of each Corpus are listed in Tables 1 through Table 5:

Table 1: English Corpus


Table 2: French Corpus.


Table 3: Turkish Corpus
Table 4: German Corpus


Table 5: Spanish Corpus


## 3 RESULTS

To discriminate among languages, we applied the PPM model on texts from each Corpus. During implementation, we repeated the language identification experiments on each text file. Within each language set, we employed each of seven text files as the training text to PPM to compress the texts of the whole Corpora. Since there are five different languages, it makes $7 \times 5=35$ runs for each text; since there are seven texts within each language set, it makes $7 \times 5 \times 7=245$ runs for each language; and since there are five different languages, it makes $245 \times 5=1,225$ runs in total.

In order to evaluate the performance of our language discriminator, we used the accuracy rate measure (Eq. 4). In this formula, the successes are the cases when both the training text and the
disputed text belong to the same language. All other cases are considered to be as failure.

$$
\begin{equation*}
\text { Accuracy rate }=\frac{\# \text { of successes }}{\text { total } \# \text { of experiments }} \tag{4}
\end{equation*}
$$

In Table 6 below, language determination experiment results with training texts as-signed from the English Corpus are given. The rows having the lowest bpe rates for English at each row are depicted as success cases. If so, we conclude that the text in question is in English, as well. Unfortunately, this is not the case all the time: There are some rows in Table 6, where the lowest compression rates with PPM are obtained with training texts in other languages than English. These cases are called as fails and are depicted as bold cells. The reason why the language identifier fails might be caused by the insufficient size of the training text or the compressed text (Table 6). According to Table 6, there are 18 failures and 31 successes, yielding the accuracy rate of $63.27 \%$. This is the accuracy rate performed by the PPM model on English.

Repeating the language identification experiments on French texts, we obtained the results in Table 7. Here, the effect of training text size on the performance of the iden-tification scheme is obvious: In cases when the training text size is small (files 2, 4, 5 and 7) the number of failures are greater, while with larger training text (file 6), the system has only two failures. Moreover, when the compressed text is not in French but its size is relatively large, the language identifier system incorrectly decides that it was written in French. This is the effect of compressed text size on the overall system performance. The accuracy rate is $46.94 \%$ for French with 23 successes and 26 failures.

Applying our scheme with training texts in Turkish this time, we obtained the bpc values in Table 8. The number of failures for Turkish is 39 while the number of suc-cesses is only 10 out of 49 experiments. Hence, the accuracy rate of our model on Turkish is only $20.41 \%$. This performance degradation in the identification scheme is probably due to the different linguistic characteristics of Turkish.

Table 6: Language identification experiments with training text from English Corpus


Table 7: Language identification experiments with training text from French Corpus


For German, we repeated the experiments and gathered the figures in Table 9. Whenever the training texts are in German, the performance of the PPM model in discriminating the languages of texts are not quite good. It has 36 failures and only 13 successes, yielding an accuracy rate of $26.53 \%$.

Lastly, we run our language discriminator with training texts assigned from the Spanish language set and recorded the results on Table 10. According to the values in Table 10, our scheme yielded 34 failures versus 15 successes. So, the accuracy rate indicated by our system for Spanish is $30.61 \%$.

To observe the overall success rate of our scheme on the five languages of concern, we have plotted the accuracy rate vs. language chart in Fig. 2.


Figure 2: Accuracy rate of the language identification system for different languages.

According to Fig. 2, the language identifier employing the PPM model achieves the best accuracy rate with training texts in English (with 63.27\%). The system indicates accuracy rates of $46.94 \%$ with French, $30.61 \%$ with Spanish, $26.53 \%$ with German and the worst performance as $20.41 \%$ with Turkish. The difference in performance levels might probably occur due to the characteristics of source languages, as well as the category, i.e. the type, together with the different time span each text belongs to.

Table 8: Language identification experiments with training text from Turkish Corpus


Table 10: Language identification experiments with training text from Spanish Corpus


## 4 CONCLUSION AND FUTURE WORK

We have designed and implemented a scheme incorporating the Prediction by Partial Matching (PPM) model. We applied this scheme which is both a cryptographic and statistical tool, in language identification problem. We have implemented our system on texts from five different languages as English, French, Turkish, German and Span-ish. Results revelaed that, the cryptographic tool we introduced achieves accuracy rates of $63.27 \%$, $46.94 \%, 20.41 \%, 26.53 \%$ and $30.61 \%$ for English, French, Turkish, German and Spanish, respectively. Experiments with the scheme can be extended with equally sized training as well as disputed text sizes to eliminate the size effect. Implementations further be carried on with more languages belonging to various language families. The performance of our system can be compared with that of the existing automatic language identification methods by running the algorithms on the same data set.

## REFERENCES

Batchelder, E.O., 1992. A learning experience: Training an artificial neural network to discriminate languages. Technical report.
Beesley, K.R., 1988. Language identifier: A computer program for automatic natural-language identification on on-line Text. In proceedings of the $29^{\text {th }}$ annual conference of the American translators association, 47-54.
Braum, J., Levkowitz, H., 1998. Automatic language identification with perceptually guided training and recurrent neural networks. In Int'l conf. on spoken language processing (ICSLP 98), Sydney, Australia.

Canterbury Corpus http://www.Corpus.canterbury.ac.nz
Cavner, W.B., Trenkle J. M., 1994. N-gram based text categorization. In proceedings of the $3^{\text {rd }}$ annual symposium on document analysis and information retrieval, 261-269.
Celikel, E., 2004. The compression and modelling of turkish texts, PhD Thesis, Ege University, International Computer Institute, Izmir/Turkey.
Cleary, J.G., Witten, I.H., 1984. Data compression using adaptive coding and partial string matching. In IEEE transactions on communications. 32(4), 396-402.
Ganesan R., Sherman A. T., 1988. Statistical techniques for language recognition: An introduction and guide for cryptanalyst. Cryptologia XVII:4, 321-366
German Linguistic URL: http://www.infoplease.com/ce6/society/A0858390.htm 1.

Ingle, N. C., 1991. A language Identification Table. In The Incorporated Linguist, Vol. 15(4), 98-101.
Kulikowski, S., 1991: Using short words: A language identification algorithm. Unpublished Technical Report.
Moffat, A., 1990. Implementing the PPM data compression scheme. In IEEE transactions on communications, 38(11), 1917-1921.
Mustonen, S., 1965. Multiple discriminant analysis in linguistic problems. In statistical methods in linguistics, no: 4, Skriptor Fack, Stockholm.
Newman, P., 1987. Foreign language identification: First step in the translation process. In Proceedings of the $28^{\text {th }}$ annual conference of the American translators association, 509-516.
Nelson, M., 1991. Arithmetic coding + statistical modeling $=$ data compression part $1-$ arithmetic coding. Dr.Dobb's Journal.
Nodeworks Encyclopedia URL: http://pedia.nodeworks.com/P/PP/PPM/PPM_compres sion_algorithm/
Preez, J., Weber, D., 1996. Automatic language recognition using high-order HMMs, In Inter-national
conference on spoken language processing (ICSLP), Sydney, Australia.
Rau, M.D., 1974. Language identification by statistical analysis. Master's thesis, Naval post-graduate school.
Sapir, E., 1921. Language: An introduction to the study of speech.
Shannon, C.E., 1948. A mathematical theory of communication. In Bell system technical journal. vol. 27, 623-656.
Teahan, W.J., 1998. Modeling English text. PhD Thesis, Univ. of Waikato, NZ.
Teahan, W.J., 2000. Text classification and segmentation using minimum cross-entropy. In proceedings of RIAO'2000. Vol. 2, Paris, France, 943-961.
Witten, I., Moffat, A. and Bell, T.C., 1999. Managing Gigabytes Compressing \& Indexing Documents and Images, 2nd ed., Morgan Kauffman Pub., CA, USA.
Ziegler, D.V., 1991 The Identification of Languages Using Linguistic Recognition Signals. PhD thesis, SUNY Buffalo.

