<table>
<thead>
<tr>
<th>Title</th>
<th>A Modified Watermark Synchronisation Code for Robust Embedding of Data in DNA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authors(s)</td>
<td>Haughton, David; Balado, Félix</td>
</tr>
<tr>
<td>Publication date</td>
<td>2013-05-26</td>
</tr>
<tr>
<td>Publication information</td>
<td>2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) Proceedings</td>
</tr>
<tr>
<td>Conference details</td>
<td>Poster presentation at the 38th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2013), May 23-31, 2013, Vancouver, Canada</td>
</tr>
<tr>
<td>Publisher</td>
<td>IEEE</td>
</tr>
<tr>
<td>Item record/more information</td>
<td><a href="http://hdl.handle.net/10197/4371">http://hdl.handle.net/10197/4371</a></td>
</tr>
<tr>
<td>Publisher's statement</td>
<td>Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.</td>
</tr>
</tbody>
</table>
A MODIFIED WATERMARK SYNCHRONISATION CODE FOR ROBUST EMBEDDING OF DATA IN DNA

David Haughton and Félix Balado

School of Computer Science and Informatics
University College Dublin, Ireland

ABSTRACT

DNA data embedding is a newly emerging field aspiring to encode data in deoxyribonucleic acid (DNA). DNA is an inherently digital and noisy medium, undergoing substitution, insertion and deletion mutations. Hence, encoding information in DNA can be seen as a particular case of digital communications in which biological constraints must be observed. In this paper we propose a modification of Davey and MacKay’s watermark synchronisation code (unrelated to digital watermarking) to create an encoding procedure more biocompatible with the host organism than previous methods. In addition, when combined with a low density parity check (LDPC) code, the method provides near-optimum error correction. We also obtain the theoretical embedding capacity of DNA under substitution mutations for the increased biocompatibility constraint. This result, along with an existing bound on capacity for insertion and deletion mutations, is compared to the proposed algorithm’s performance by means of Monte Carlo simulations.

Index Terms— DNA data embedding, decoder performance, LDPC, watermark code, capacity

1. INTRODUCTION

Recent advances in technology have enabled the use of DNA in novel ways, such as highly parallel computing and data storage. Numerous applications of DNA data embedding have been proposed in the past decade, such as the tracking of organisms’ movements, the assertion of proprietary DNA sequences [1] and highly compact data storage [2]. One real world scenario, proposed in literature, where this field could directly apply is in determining the source of a biological containment following an outbreak [3]. A high profile instance of DNA data embedding was undertaken recently, the purpose of which was to encode, in vitro (using DNA in test tubes), an entire book in DNA sequences [4]. This method incorporated error correction in the form of repetition coding. While the experiment was not performed in vivo (using DNA within living organisms), the results are nonetheless very encouraging, as the information density (bits/mm³) attained is several orders of magnitude higher than flash memory, even surpassing the demonstrated density of quantum memory.

Encoding data in living organisms is more challenging because it is undesirable for encoded regions to alter the biological processes of the host organism. In vivo data embedding involves encoding information within genes (protein coding DNA, or pcDNA) or within the rest of the genome (noncoding DNA, or ncDNA). Here we will consider the ncDNA data embedding scenario only. Several groups have successfully performed in vivo ncDNA information embedding already, such as Wong et al. [5] and Yachie et al. [6] using wild bacteria, or the JCVI using an artificially engineered synthetic bacterium [7]. Nevertheless, unlike in the method that we will present here, some key biocompatibility constraints for embedding information in ncDNA are not strictly enforced by any of these previous methods.

Also, DNA in the cell is subject to substitution and indel (insertion and deletion) mutations. From the point of view of DNA data embedding these are equivalent to a probabilistic “mutation channel” inducing random errors. As such data embedding algorithms should incorporate error correction specific to the DNA mutation channel. However despite the proposal of many DNA data encoding methods in the last ten years, none make use of optimal error correction, although Yachie et al. [6] do use repetition coding and Heider and Barnekow [5] have applied basic error correction codes such as Hamming. One particularly challenging error control problem is that indel mutations create desynchronisation errors. Given the nature of the mutations channel, LDPC codes in conjunction with modified watermark synchronisation codes proposed by Davey and MacKay [9] are ideally suited to this task.

To conclude, although the general limits of information embedding in noncoding DNA strands are known for some particular mutation channels [10], this is not the case when special constraints for increased biocompatibility, such as the ones considered here, are enforced. Consequently no practical method has been proposed to achieve these limits either. Here we also provide the Shannon capacity analysis for methods operating under this constraint.

2. NOTATION AND FRAMEWORK

This section outlines the biological framework, in conjunction with the channel model and principle coding components. Throughout the paper random variables are represented by upper case italicised letters. Vectors are denoted by bold lower case letters and upper case calligraphic letters denote sets. The fundamental units in DNA are nucleotide bases, and the set of DNA bases is given by \( \mathcal{X} \triangleq \{A,C,T,G\} \). A DNA molecule may be represented as an \( n \) length vector \( \mathbf{x} = \{x_1, x_2, \cdots, x_n\} \), \( x_i \in \mathcal{X} \). A DNA molecule is double-stranded, that is, composed by two sequences of identical length. One strand is completely determined by the other through the so-called Watson-Crick pairings C–G and A–T.

As already mentioned, there are two types of regions in the DNA of living organisms: protein coding DNA (pcDNA) and noncoding DNA (ncDNA). Although we are only concerned with data embedding in ncDNA it is necessary to review some facts about pcDNA in order to explain the increased biocompatibility constraint. pcDNA encodes genes as sequences of codons. Codons are base triplets,
each of which codes for an amino acid according to the genetic code \([11]\). Start codons are special codons which signal the genetic machinery to begin the translation of a gene into a protein (amino acid sequence). The standard set of start codons is \([11]\)

\[
S = \{\text{ATG, CTG, TTG, CAT, CAG, CAA}\}. \tag{1}
\]

A start codon can be found at any locus in a DNA molecule’s two strands, and hence, there are six possible amino acid translation frames. It is also important to note that the strand complementary to \(x\) is read in the opposite direction, and thus termed antiparallel.

2.1. Encoding and Channel Models

In this section we outline the proposed DNA data embedding method, as summarised by Figure 1. Details of the individual components will be elucidated in Section 5. A binary message vector \(m\) to be encoded, is mapped to a quaternary vector, \(b\) using any trivial mapping \([00, 01, 10, 11] \mapsto X\). Since \(|X| = 4\), all error correction methods discussed here operate over the finite field GF(4). Next, an LDPC encoder generates the encoded vector \(c\) from \(b\). A biocompatible watermark encoder is then applied to enable the correction of indel mutations while simultaneously ensuring the biocompatibility of the encoded information. The output of this is \(y\), to be embedded in an organism in specific ncDNA sites known to have no biological function, as we will discuss in Section 5.

Next the organism (including \(y\)) undergoes a probabilistic error channel which is modelled by a substitution mutation channel concatenated with an indel mutation channel. We will assume that all mutation events are mutually independent. The base substitution mutation model used here is called the Kimura model of molecular evolution \([12]\), which reflects that DNA bases belong to one of two chemically distinct groups: purines, \(R = \{A, G\}\) or pyrimidines \(Y = \{C, T\}\). Mutations within each of these two groups are more likely than mutations to the opposite group; these are known as transitions and transversions, respectively. For one generation of an organism, the transition probability matrix \(\Pi = [p(Y|X)]\), with \(X, Y \in X\), of Kimura’s model is

\[
\Pi = \begin{bmatrix}
1 - q & \gamma q & \gamma q & (1 - 2\gamma)q \\
\gamma q & 1 - q & (1 - \frac{3\gamma}{2})q & \gamma q \\
(1 - \frac{2\gamma}{3})q & \gamma q & 1 - q & \frac{3}{4}q \\
(1 - \frac{2\gamma}{3})q & \gamma q & \frac{3}{4}q & 1 - q
\end{bmatrix}
\]

The two parameters of the model are \(q\), the base substitution mutation rate per generation, and \(\gamma\), which is obtained from the transitions/transversions rate \(\epsilon\) as \(\gamma = 3/(2(\epsilon + 1))\). The well known Jukes-Cantor model is a particular case of the Kimura model where \(\gamma = 1\). The Kimura transition probability matrix after \(p\) generations is given by \(\Pi^p\). Finally the rate of base indel mutations per generation and site is denoted by \(\rho\).

The decoder receives a mutated version of \(y\), denoted \(z\), from a descendant of the original host organism. Between \(y\) and \(z\), \(p\) generations have elapsed. The watermark decoder resynchronises \(z\), which in effect means identifying indels, removing insertions and insertions a base for deletions. It also produces a maximum likelihood estimate of the substitution mutation channel parameters, \(\hat{\gamma}\) and \(\hat{\epsilon}\). These parameters are passed to the LDPC decoder, which decodes the output of the watermark decoder \(\hat{c}\) to produce \(\hat{b}\). The quaternary decoder then performs the reverse mapping of the quaternary encoder, mapping bases to information bits.

3. CONSTRAINTS OF ncDNA EMBEDDING

When encoding data in ncDNA it is essential that the host’s biological functionality remains unaffected. Although ncDNA has in the past been labelled as “junk DNA” due to its supposed lack of purpose when compared to gene-encoding pcDNA, recent research spearheaded by the ENCODE consortium \([13]\) has demonstrated that up to 80% of ncDNA may be involved in regulatory functions of gene activity. However it is safe to assume that the remaining 20% of the ncDNA of a genome can be appended, inserted or overwritten without ill effects, as proven by Wong et al. \([5]\), Yachie et al. \([6]\) and Gibson et al. \([15]\), who have successfully embedded information in suitable regions of the ncDNA of living organisms. In truly redundant ncDNA regions, a further constraint to increase biocompatibility is that they must not be mistaken as protein coding regions by the cell’s machinery. To enforce this, start codons must not appear in \(y\) or in its complementary antiparallel strand. The problem becomes increasingly difficult when we consider that the appearance of start codons must be prevented in each of the three reading frames, for both sequences. There are four dinucleotides, composed of the first two bases of each codon in \(S\), which indicate that a start codon may appear. This set is given by

\[
B = \{\text{AT, CT, TT, CA}\}. \tag{2}
\]

A data embedding algorithm called BioCode ncDNA will now be presented. This method was previously proposed by us to ensure that start codons do not appear in an encoded sequence \([16]\). At the encoder, base \(y_i\) will be encoded at position \(i\) with reference to the trailing two bases already encoded, denoted by \(d = [y_{i-2}, y_{i-1}]\). It is only when \(d \in B\) that the possible values of \(y_i\) must be restricted to a particular subset of \(X\). This subset contains all the bases for which a start codon will not appear both in the strand being encoded and in its antiparallel complimentary strand; otherwise any \(y_i \in X\) can be chosen by the encoder. During encoding, \(d\) can be monitored, and using a lookup of Table 1, bits from \(m\) can be encoded in such a way that start codons never appear. This procedure will be exploited in Section 5 to enforce the no-start-codons constraint.
Combining these considerations, the average rate at step $i$ is

$$R_i = \sum_{x} R_i(x)p(x) \text{ bits/base},$$

where $p(x)$ is the probability mass function (pmf) of the trailing two bases, $x$. For the first step ($i = 3$) we may assume uniformity, that is, $p(y_1, y_2) = 1/16$. After that, using the 16 conditioned pmf's $p(y_1|y_{i-2}, y_{i-1})$ that yield the maximum rates at step $i$, we can compute $p(y_{i-1}, y_i) = \sum_{y_{i-2} \in X} p(y_{i-2}, y_{i-1})p(y_{i-1}, y_i)$, which can be used to obtain $R_{i+1}$ as in (4). The overall average rate is obtained in the limit as

$$\bar{R} = \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} R_i \text{ bits/base.} \quad (5)$$

5. ENCODING AND DECODING ALGORITHMS

Optimal coding strategies are needed to reach capacity. Such methods exist in digital communications for the equivalent of the substitution mutation channel, but have not yet been applied to the DNA data embedding problem. As for the indel mutation channel, whose capacity is unknown, one of the most effective resynchronisation error correction codes to date is the watermark code, proposed by Davey and MacKay over ten years ago [9]. These authors also proposed using an LDPC code concatenated with the watermark code to correct substitution mutations. Since LDPC codes are near-optimal under substitution channels, this combination is ideally suited to DNA data embedding, provided the biological constraints discussed in Section 3 are observed. This will be achieved by modifying the watermark code.

5.1. Encoding Algorithm

The LDPC code used in our experiments was created with reference to LDPC codes designed for wireless communications [19]. Parity check matrices were constructed randomly, with the condition that short cycles in the corresponding Tanner graph not be present. The resynchronisation method used here to correct indel mutations is a variant of the original watermark encoding algorithm [9]. While the watermark facilitates resynchronisation, it serves two other important functions for this encoding scheme: 1) to produce an estimate of the substitution mutation channel parameters; and 2) to prevent start codons from appearing.

Firstly a no-start-codon watermark $w$ known to the encoder and decoder is created. To create $w$ a pseudorandom binary vector is generated and then encoded in DNA using the BioCode ncDNA method in Section 3. The algorithm then iterates through $w$ and identifies positions at which any base can be safely substituted in without creating a start codon. It is at these locations that $c$ will be inserted. Given the base $w_i$, it is useful to define all possible codon offsets which this base is part of,

$$\mathcal{W}_i = \{[w_i, w_{i-1}, w_{i-2}], [w_{i-1}, w_i, w_{i+1}], [w_i, w_{i+1}, w_{i+2}]\}.$$  

It is determined that base $w_i$ is suitable for embedding only if $\mathcal{W}_i \not\subseteq S$. Otherwise $w_i$ has the potential to create a start codon if it is replaced by the wrong base. $w$ may then be trimmed such that it only specifies enough embeddable positions to exactly contain $c$. If this is done the position of substitutions does not have to be explicitly stated: the decoder can determine these positions by finding all possible locations that are suitable for embedding.

In the original watermark code proposal the forward-backward algorithm is used to infer indel sites. Our decoding algorithm, first proposed in [16], instead aligns $x$ with $w$ using the edit distance. This process of resynchronisation is suboptimal but still effective and more practical, since it uses hard decision decoding and thus does not require estimates of the indel rate. Two important factors

<table>
<thead>
<tr>
<th>$d$</th>
<th>AT</th>
<th>CT</th>
<th>TT</th>
<th>CA</th>
<th>$X^2 \setminus B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO-START-CODONS CONSTRAINT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$S_d$</th>
<th>A</th>
<th>A</th>
<th>A</th>
<th>C</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Given the dinucleotide sequence $d$ the next message base to be encoded is one belonging to the set $S_d$. Each bit message found in $M_d$ corresponds to a base in $S_d$.

4. CAPACITY OF ncDNA EMBEDDING WITH NO-START-CODONS CONSTRAINT

One way to determine the performance of a practical ncDNA method is to assess its distance from channel capacity, which is the upper bound on the maximum information rate that can be asymptotically transmitted without errors. In this section we establish the capacity of ncDNA with the no-start-codons constraint discussed in Section 3.

In our computation only the substitution channel will be considered. The rationale behind this is that if the watermark code works perfectly this allows the LDPC decoder to “see” a substitution mutation channel. It must be remarked that the exact capacity for even the simplest indel channel remains unknown [17]. In any case, the approach proposed here still yields an upper bound to capacity when indels are present.

To begin, the capacity the Kimura channel without the no-start-codons constraint is

$$C_{nc} = 2 - H(Z_{(n)}|Y) \text{ bits/base,} \quad (3)$$

where $Y$ models a base at a given ncDNA site and $Z_{(n)}$ its mutated version after $p$ generations of the host organism. This is just the capacity of a symmetric 4-ary channel, which is attained for uniform $Y$. The conditional entropy in (3) is easily computed using any row of $\Pi^n$. The case with the no-start-codons constraint, which we address next, is more complicated because a single-letter characterisation of the channel cannot be used (i.e. a base-by-base analysis). Firstly let us determine the achievable rate conditioned to $d = [y_{i-2}, y_{i-1}]$, which we denote $R_i(d)$. If $d \notin B$, then there are no constraints on $y_i$, and the rate is then given by Equation 3. When $d \in B$ we have to consider two cases:

1. $d = [C, A]$; observing Table 1 the rate in this case is 0, since only one base may be used to prevent a start codon.
2. Otherwise, the channel becomes nonsymmetric, with input belonging to $\{A, T, C\}$ and output belonging to $\{X\}$. In this case the maximising input distribution and maximum rate may be numerically obtained using the Blahut-Arimoto algorithm [13].

Combining these considerations, the average rate at step $i$ is

$$R_i = \sum_{x \in X^2} R_i(x)p(x) \text{ bits/base,} \quad (4)$$

where $p(x)$ is the probability mass function (pmf) of the trailing two bases, $x$. For the first step ($i = 3$) we may assume uniformity, that is, $p(y_1, y_2) = 1/16$. After that, using the 16 conditioned pmf’s $p(y_1|y_{i-2}, y_{i-1})$ that yield the maximum rates at step $i$, we can compute $p(y_{i-1}, y_i) = \sum_{y_{i-2} \in X} p(y_{i-2}, y_{i-1})p(y_{i-1}, y_i)$, which can be used to obtain $R_{i+1}$ as in (4). The overall average rate is obtained in the limit as

$$\bar{R} = \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} R_i \text{ bits/base.} \quad (5)$$

5. ENCODING AND DECODING ALGORITHMS

Optimal coding strategies are needed to reach capacity. Such methods exist in digital communications for the equivalent of the substitution mutation channel, but have not yet been applied to the DNA data embedding problem. As for the indel mutation channel, whose capacity is unknown, one of the most effective resynchronisation error correction codes to date is the watermark code, proposed by Davey and MacKay over ten years ago [9]. These authors also proposed using an LDPC code concatenated with the watermark code to correct substitution mutations. Since LDPC codes are near-optimal under substitution channels, this combination is ideally suited to DNA data embedding, provided the biological constraints discussed in Section 3 are observed. This will be achieved by modifying the watermark code.

5.1. Encoding Algorithm

The LDPC code used in our experiments was created with reference to LDPC codes designed for wireless communications [19]. Parity check matrices were constructed randomly, with the condition that short cycles in the corresponding Tanner graph not be present. The resynchronisation method used here to correct indel mutations is a variant of the original watermark encoding algorithm [9]. While the watermark facilitates resynchronisation, it serves two other important functions for this encoding scheme: 1) to produce an estimate of the substitution mutation channel parameters; and 2) to prevent start codons from appearing.

Firstly a no-start-codon watermark $w$ known to the encoder and decoder is created. To create $w$ a pseudorandom binary vector is generated and then encoded in DNA using the BioCode ncDNA method in Section 3. The algorithm then iterates through $w$ and identifies positions at which any base can be safely substituted in without creating a start codon. It is at these locations that $c$ will be inserted. Given the base $w_i$, it is useful to define all possible codon offsets which this base is part of,

$$\mathcal{W}_i = \{[w_i, w_{i-1}, w_{i-2}], [w_{i-1}, w_i, w_{i+1}], [w_i, w_{i+1}, w_{i+2}]\}.$$  

It is determined that base $w_i$ is suitable for embedding only if $\mathcal{W}_i \not\subseteq S$. Otherwise $w_i$ has the potential to create a start codon if it is replaced by the wrong base. $w$ may then be trimmed such that it only specifies enough embeddable positions to exactly contain $c$. If this is done the position of substitutions does not have to be explicitly stated: the decoder can determine these positions by finding all possible locations that are suitable for embedding.

In the original watermark code proposal the forward-backward algorithm is used to infer indel sites. Our decoding algorithm, first proposed in [16], instead aligns $x$ with $w$ using the edit distance. This process of resynchronisation is suboptimal but still effective and more practical, since it uses hard decision decoding and thus does not require estimates of the indel rate. Two important factors
Using the transition probability matrix we have these estimates we undertake maximum likelihood estimation.

ties in the Kimura model, taking the natural logarithm we obtain an additional purpose: the estimation of the parameters $z$ once

5.2. Estimation of Channel Parameters

Once $z$ has been resynchronised, the received watermark $\hat{w}$ serves an additional purpose: the estimation of the parameters $\gamma$ and $q$ required for optimum decoding of the LDPC code. To obtain these estimates we undertake maximum likelihood estimation. Using the transition probability matrix we have $p(z|y; \gamma, q) = \prod_{i=1}^{n} p(z_i|y_i; \gamma, q)$. Since there are only three different probabilities in the Kimura model, taking the natural logarithm we obtain

$$
\log p(z|y; \gamma, q) = n_{tv} \log \left( \frac{\gamma}{3} \right) + n_{tr} \log \left( 1 - \frac{2\gamma}{3} \right) + (n_{tv} + n_{tr}) \log \frac{q}{1-q} + n \log(1-q),
$$

where $n_{tv}$ and $n_{tr}$ are the number of transversions and transitions that occur between $w$ and $\hat{w}$, and the watermark is of length $n$. Differentiating with respect to $\gamma$ and $q$ and equating to zero, we respectively obtain

$$
\hat{\gamma} = \frac{3}{2(1 + \hat{\epsilon})}, \quad \hat{q} = \frac{n_{tv} + n_{tr}}{n} \tag{6}
$$

where $\hat{\epsilon} = n_{tv}/n_{tr}$ is the empirical transitions/transversions ratio. It is also possible to obtain an estimate of $p$; however this is not trivial and $\Pi^p$ can be accurately approximated as $\hat{\Pi}$ using $\hat{q}$ and $\hat{\gamma}$ alone.

6. RESULTS

Evaluation of the watermark code with LDPC was undertaken by means of Monte Carlo simulations, with the following parameters: $q = 10^{-5}$, $\gamma = 0.1$ and $p = 10^{-6}$. The value of $p$ is considerably more extreme than estimated in literature [21], $(p = \frac{1}{10})$ was used over $p \approx \frac{1}{300}$. This was done purposefully to show how the watermark code performed under strenuous conditions.

Shown in Figure 2 is the probability of bit error ($P_e$) against the number of generations ($p$) of a host organism. The perfectly synchronised decoder has the position of indels revealed. The repetition code used BioCode ncDNA first to create a quaternary vector which was then repeated three times. Resynchronisation was performed using the heuristic multiple sequence alignment algorithm MUSCLE, followed by majority decoding on the aligned sequences. This resynchronisation procedure was previously proposed by us [22], however unlike here, it did not operate under the no-start-codon constraint. Figure 3 shows the mutual information of the watermark codes in addition to the bound presented in Section 4 for substitution mutation compared to perfectly synchronised versions (red, purple). Also shown is the bound presented in Section 7 for substitution mutation only (yellow). A capacity bound, proposed in literature [20], for the Jukes-Cantor model ($\gamma = 1$) with deletions (black) is also given.

7. RELATION TO PRIOR WORK

The work presented here proposes a practical application of Davey and MacKay’s watermark codes [9]. To the authors’ knowledge, there only exists one other practical application for watermark codes [23]. The only previous DNA data embedding method capable of counteracting indels was proposed by Yachie et al. [6]. However their solution is based on repetition coding plus realignment, which is suboptimal with respect to the use of watermark codes and LDPC. Furthermore, the watermark code was modified in order ensure biocompatibility with the host organism by precluding the appearance of start codons in the encoding. The only previous DNA data embedding method that approximately implements this important constraint is the one by JCVI [7], but it just minimises the probability of start codons appearing without avoiding them altogether, and without using optimum error correction coding. In fact, we believe that ours is the first application of near-optimum error correction to the problem of DNA data embedding.
8. REFERENCES


