

Anthony P. Machado, Gaby G. Dagher, and Eddie C. Davis

Hiding Data in Cellular DNA: Contextualizing Diverse Encoding Schemes

Abstract: DNA, the macromolecule used by organisms to store and transmit genomic data, has attracted the attention of privacy researchers as a channel for secure data transfer. DNA's small size and abundance in nature makes it an ideal steganographic medium for hiding messages. Already, artificially synthesized DNA has been used to store text, audio, and images. Encoded cellular DNA is not far behind, with much research being done on ways to safely embed data without harming the cell.

In this survey we provide the first systematic comparison of cellular encoding schemes proposed in the literature. Different DNA regions in the cell have their own unique bio-restrictions that must be satisfied for DNA storage. Drawing from a wide array of schemes, we compare the novel techniques used to meet these bio-restrictions. This contextualization of the research creates a bigger picture that can help guide the design of future schemes. We also survey the compression methods and error detection techniques used by the encoding schemes, and their effect on error rate and bits-per-base density. Finally, we propose future directions for research in untapped cellular regions such as mitochondrial DNA and we offer novel insights into the potential for epigenetic encoding with methylation and histones.

Keywords: keywords, keywords

DOI Editor to enter DOI

Received ...; revised ...; accepted ...

1 Introduction

Biosteganography is an emerging field in privacy research that combines techniques from genetic engineering, bioinformatics, cryptography and forensics to secretly transfer data within a living cell's DNA [1]. Data ranging from simple text messages to audio recordings and color images can be inserted into cellular DNA. Because DNA is information dense and occurs abundantly in nature, it makes an ideal medium for sending

messages secretly. Basic steganographic principles dictate that if an attacker doesn't know where to find a confidential message in the first place, the message is far more secure [2].

Traditional digital storage systems such as hard drives and SD cards have detectable emanations, which makes them vulnerable to side attacks [3]. Modified DNA, however, has no measurable emanations. If an agent needed to carry a hidden message through a tight security checkpoint, any form of electronic storage could be easily detected, while physical recordings like paper or tape could be visibly located by the security guard. A DNA encoded message, however, located in the cells of the agent's thumb, or in bacteria under the agent's nail, could be brought through without detection. The receiver of the message would need to know how to decode the data, and have the lab equipment to amplify and sequence the DNA.

Inserting hidden data into DNA is also crucial for watermarking patented genes. Advances in gene editing technology has led to a rise in genetically modified organisms being developed in a variety of sectors such as agriculture, healthcare, and energy. For added security of these novel genomes, many companies have already begun embedding hidden watermarks in their DNA so that ownership can be established in the case of theft. For this purpose too, secrecy is essential. The watermark must be embedded in such a way that the thief cannot find it, else the thief would simply remove it. Thus, biosteganography is an overlapping goal both of individuals wanting to send data privately and companies wanting to watermark genetic inventions.

In this survey, -encoding overview - in this work

2 Background

2.1 DNA

Every living cell contains DNA molecules encoded with instructions for making the proteins necessary for the cell to function. DNA takes the form of a double helix made of two antiparallel strands. Each strand is composed of a sequence of 4 nucleotides: adenine (A), guanine (G), cytosine (C), and thymine (T). The purines adenine and guanine, and the pyrimidines cytosine and thymine hydrogen bond with each other across the double helix. Every three nucleotides forms a codon

Anthony P. Machado: Boise State University, E-mail: anthony-machado@u.boisestate.edu

Gaby G. Dagher: Boise State University, E-mail: gabydagher@boisestate.edu

that the cell reads and processes to create an amino acid, the building block of a protein [4].

There are only 20 amino acids, despite the fact that $4^3 = 64$ possible codon variations exist. This is because many amino acids have up to five redundant codons. Also, three codons are used specifically as stop signals to indicate the end of a protein chain. The redundancy in codon to amino acid mapping is called codon degeneracy [5]. Codon degeneracy gives an evolutionary advantage to the cell by allowing certain mutations to occur in a codon while preserving the codon's functionality.

2.2 Artificial DNA Encoding

DNA was first encoded with a secret message in 1999 by Clelland et al [6]. Inspired by the tiny, concealed “microdot” messages used in World War II, artificial DNA strands were constructed using a simple substitution cipher, then mixed with human DNA and pipetted onto a printed period on filter paper. The encoded DNA was later recovered from the dot and sequenced to successfully read the secret message: “JUNE 6 INVASION: NORMANDY”.

3 Bio-Restrictions

Cellular DNA encoding must not harm the carrier organism, either by removing cellular functionality or adding mutative behavior. To avoid this, encoding schemes must ensure that modified DNA strands remain biologically equivalent to their wild-type form. This section defines the bio-restrictions that exist for two distinct areas of cellular DNA, protein coding DNA (pcDNA) and noncoding DNA (ncDNA). As our knowledge of genetics continues to expand, more particular restrictions may become known.

3.1 pcDNA Constraints

The protein coding region of DNA contains the codons that are translated to amino acids, which are then concatenated into proteins. Any data insertions in this area must meet the following constraints.

Protein Preservation The structure of the protein coded by the region must remain unchanged.

Codon Bias Preservation

3.2 ncDNA Constraints

The noncoding region of DNA is often called “junk DNA” for its apparent lack of use in the cell. Because these regions appear to be non-functional, data can be embedded into these regions if the following constraints are met.

Truly nonfunctional region. When ncDNA was first discovered it was assumed to have no role in cell functionality, but recent studies have shown that up to 80% of ncDNA may have biochemical functions in the cell, despite not coding for proteins [7]. Therefore, it is first imperative that the individual who wishes to insert a message into ncDNA verify that they are encoding their message in the 20% that has no biochemical use.

No start codons. When a cell's genetic machinery locates a start codon, it can begin the transcription process. To prevent unwanted transcription from happening in ncDNA with embedded data, it is important to make sure the encoded nucleotides do not create a start codon. When a DNA string is being transcribed, three-nucleotide codons can be read in six different reading frames. Therefore, there should not be a start codon in any of the six frames. The most common start codon is AUG, though some alternative start codons can also exist, particularly in bacteria [8]. If a cell contains alternative start codons, the encoding scheme should avoid all of them.

No homopolymers. A DNA homopolymer is a region where the same nucleotide is repeated multiple times. Too many repeats can cause errors during DNA replication through polymerase slippage [9]. These replication errors could quickly distort the inserted message and possibly damage the cell after a few generations. For this reason any ncDNA encoding scheme should not include homopolymers greater than length 3.

4 Encoding Schemes

Encoding schemes for cellular DNA can involve several components:

1. Encryption algorithm
2. Mapping table
3. Compression
4. Error correction
5. Fake data embedding

The following encoding schemes use some or all of these elements in their design.

4.1 pcDNA Encoding

Shimanovsky et al [10] were the first to propose using codon degeneracy to encode data in pcDNA. By switching codons between their redundant forms with the modification of one nucleotide, data could be inserted without altering protein translation. Arita and Ohashi [11] were the first to implement this scheme in a living cell. They did this using site-directed mutagenesis of wobble codons in the *ftsZ* gene of *Bacillus subtilis*. The university name "KEIO" was inserted by modifying the redundant nucleotides of the codons downstream of the *ftsZ* start codon. An unmodified codon represented value 0 while a codon with a wobble nucleotide changed to any of its non-wild type redundant forms represented value 1. Messages were translated using a 6-bit mapping table, with the first 5 bits corresponding to an English alphabet letter or basic punctuation, and the last used as a parity bit for error correction.

	U	C	A	G
U	6	87837	787	
C	7	78	5415	
A	545	778	7507	
G	545	18744	7560	
5	88	788	6344	

4.2 ncDNA Encoding

4.3 Plasmid Encoding

5 Compression and Error Correction

Smith et al [10] were the first to suggest a data compression technique in DNA encoding, specifically the Huffman Code. The Huffman Code is a form of lossless data compression that forms a symbol table using fewer bits to encode more common characters [12]. Smith et al created a Huffman Code table mapping letters of the alphabet to nucleotide strings, where the most common English letter 'e' was mapped to the nucleotide string "T", and the least common english letter 'z' was mapped to a longer nucleotide string "CCCTG". This achieved an average encoding length of 2.2 bases per letter. The mapping is unambiguous, making only one possible interpretation of each message.

6 Future Directions

7 Conclusions

References

- [1] T. Brunet, "Aims and methods of biosteganography," *Journal of Biotechnology*, vol. 226, pp. 56–64, 2016.
- [2] D. Artz, "Digital steganography: hiding data within data," *IEEE Internet Computing*, vol. 5(3), pp. 75–80, 2001.
- [3] H. Tanaka, "Evaluation of information leakage via electromagnetic emanation and effectiveness of tempest," *IEICE Transactions on Information and Systems*, vol. 91(5), pp. 1439–1446, 2008.
- [4] J. Watson and F. Crick, "Molecular structure of nucleic acids: a structure for deoxyribose nucleic acid," *Nature*, vol. 171 (4356), pp. 737–738, 1953.
- [5] J. Watson, T. Baker, S. Bell, A. Gann, M. Levine, and R. Losich, *Molecular Biology of the Gene, 6th Edition*. Pearson, 2008.
- [6] C. Clelland, V. Risca, and C. Bancroft, "Hiding messages in DNA microdots," *Nature*, vol. 399, pp. 533–534, 1999.
- [7] E. P. Consortium et al., "An integrated encyclopedia of dna elements in the human genome," *Nature*, vol. 489(7414), pp. 57–74, 2012.
- [8] F. e. a. Blattner, "The complete genome sequence of escherichia coli k-12," *Science*, vol. 277:5331, pp. 1453–1462, 1997.
- [9] E. Viguera, D. Conceill, and S. Ehrlich, "Replication slippage involves dna polymerase pausing and dissociation," *The Embo Journal*, vol. 20(10), pp. 2587–2595, 2001.
- [10] G. Smith, C. Fiddles, J. Hawkins, and J. Cox, "Some possible codes for encrypting data in DNA, volume = 25, pages = 1125-1130, year = 2003," *Biotechnology Letters*.
- [11] M. Arita and O. Yoshiaki, "Secret signatures inside genomic dna," *Biotechnology Progress*, vol. 20, pp. 1605–1607, 2004.
- [12] D. Huffman, "A method for the construction of minimum-redundancy codes," *Proceedings of the IRE*, vol. 40(9), pp. 1098–1101, 1952.

Table 1. Comparative evaluation of encoding schemes

Approach	Data Type		Privacy-Preserving Domain				Hosting Environment				Security		
	Set-Valued	Other	Non-Interactive		Interactive		Single	Two		Multiple		Threat Model †	Public Verifiability
			Differential Privacy	Syntactic Privacy	Differential Privacy	Syntactic Privacy		Horiz.	Vert.	Horiz.	Vert.		
Terrovitis <i>et al.</i> , He and Naughton	●			●			●						
Chen <i>et al.</i>	●		●				●						
Jiang and Clifton		●		●					●			○	
Jurczyk and Xiong		●		●						●		○	
Alhadidi <i>et al.</i>		●	●					●				○	
Mohammed <i>et al.</i> (DistDiffGen)		●	●						●			○	
Mohammed <i>et al.</i> (TIPS)		●		●					●			●	
Bhaskar <i>et al.</i> , Li <i>et al.</i>	●				●		●						
Wong <i>et al.</i>	●						●					○	
Giannotti <i>et al.</i>	●					●	●					○	
Kantarcioglu and Clifton	●									●		○	
Zhang <i>et al.</i>	●							●				○	
Wahab <i>et al.</i>	●				●			●		●		○	
Dwork <i>et al.</i>		●			●					●		●	
Narayan and Haeberlen		●			●			●		●		○	
Our proposed solution	●		●					●	●	●	●	●	●

† In this column, ○ denotes semi-honest threat model whereas ● denotes malicious threat model.