

Secure Methodology for Data Encryption with DNA Steganography and vein Patterns

H. Ramyya¹, Samerender N.H² and W.M. Lekha³

¹Computer Science Engineering Panimalar Institute of Technology, Chennai, India.

²Bio Engineering Sastra University, Thanjavur, India

³Electricals and Sri Sai Ram Institute Chennai, India.

Abstract

The transfer of data in a secure way can be implemented using Biometric technology to authenticate. Thanjavur, India.

We identify and use invariant and unique biometric features to embed data. The mechanism consists of a two level encryption system using certain algorithms. The vein pattern of a user is obtained and his DNA sequence is retrieved from the database. The first level of encryption involves mapping ASCII characters to parameters relative to the vein topology followed by encrypting vein topology parameters to certain locations in the DNA sequences where we shall embed encrypted data. The decryption process will require the vein pattern as a key. DNA and Vein patterns are unique and can't be replicated as they are internal hence making the system more secure and resilient with very small margin for error. The entire processing requires capabilities to the likes of a supercomputer in the place of which we could make use of a compact supercomputer that is both compact and economic comparatively. It helps provide security to the biometric data with the help of digital signatures. Pressure sensors and heat sensors are also present to prevent duplication of results. This can be successfully used even in household security system.

1. Introduction

The vein patterns of human hand is obtained from the Charged Coupled Device, which is commonly shared between the sender and receiver for authentication using the Hansdorf algorithm. We use Hansdorf algorithm to estimate the relative distances of

veins from the largest vein. These distances are encrypted along with the ASCII characters which is further processed for secondary level encryption. The DNA strands are taken and base pairs identified are used for second level encryption of the output from the previous stage. The encrypted data received is decoded using the vein pattern as a key.

2. DNA Pattern

Every cell in our body contains DNA. DNA is a set of instructions which instructs our cells on building of proteins. These instructions are in a language that was discovered recently. A DNA strand resembles a ladder. The rungs of this ladder is composed of bases. Each rung is a pair of two bases that are bonded together in the middle. The four bases used in DNA are Cytosine, Guanine, Adenine, and Thymine. These bases are paired in a specific way: Adenine with Thymine, and Guanine with Cytosine. The protein that is built is based upon the order that these base pairs occur. Protein is made up of amino acids. It is the order of the DNA bases that tell cells the order to place amino acids. Three DNA bases pair for one amino acid. This series of three bases is called a codon because it codes for which type of amino acid to be used.

2.1 Cytosine

It is a pyrimidine derivative, with a heterocyclic aromatic ring and two substituents attached (an amine group at position 4 and a keto group at position 2). The nucleoside of cytosine is cytidine. In Watson-Crick base pairing, it forms three hydrogen bonds with guanine.

2.2 Guanine

With the formula $C_5H_5N_5O$, guanine is a derivative of purine, consisting of a fused pyrimidine-imidazole ring system with conjugated double bonds. Being unsaturated, the bicyclic molecule is planar. The guanine nucleoside is called guanosine.

2.3 Thymine

Thymine may be derived by methylation of uracil at the 5th carbon. In RNA, thymine is replaced with uracil in most cases. In DNA, thymine (T) binds to adenine (A) via two hydrogen bonds, thus stabilizing the nucleic acid structures..

2.4 Adinine

Adinine is a nucleobase (a purine derivative) with a variety of roles in biochemistry including cellular respiration, in the form of both the energy-rich adenosine triphosphate (ATP) and the cofactors nicotinamide adenine dinucleotide (NAD) and flavin adenine dinucleotide (FAD), and protein synthesis, as a chemical component of DNA and RNA.[2] The shape of adenine is complementary to either thymine in DNA or uracil in RNA.

3. DNA Code

Amino Acid	DNA Base Triplets	M-RNA Codons	T-RNA Anticodons
alanine	CGA, CGG, CGT, CGC	GCU, GCC, GCA, GCG	CGA, CGG, CGU, CGC
arginine	GCA, GCG, GCT, GCC TCT, TCC	CGU, CGC, CGA, CGG AGA, AGG	GCA, GCG, GCU, GCC UCU, UCC
asparagine	TTA, TTG	AAU, AAC	UUA, UUG
aspartate	CTA, CTG	GAU, GAC	CUA, CUG
cysteine	ACA, ACG	UGU, UGC	ACA, ACG
glutamate	CTT, CTC	GAA, GAG	CUU, CUC
glutamine	GTT, GTC	CAA, CAG	GUU, GUC
glycine	CCA, CCG, CCT, CCC	GGU, GGC, GGA, GGG	CCA, CCG, CCU, CCC
histidine	GTA, GTG	CAU, CAC	GUA, GUG
isoleucine	TAA, TAG, TAT	AUU, AUC, AUA	UAA, UAG, UAU
leucine	AAT, AAC, GAA, GAG GAT, GAC	UUA, UUG, CUU, CUC CUA, CUG	AAU, AAC, GAA, GAG GAU, GAC
lysine	TTT, TTC	AAA, AAG	UUU, UUC
methionine	TAC	AUG	UAC
phenylalanine	AAA, AAG	UUU, UUC	AAA, AAG
proline	GGA, GGG, GGT, GGC	CCU, CCC, CCA, CCG	GGA, GGG, GGU, GGC
serine	AGA, AGG, AGT, AGC TCA, TCG	UCU, UCC, UCA, UCG AGU, AGC	AGA, AGG, AGU, AGC UCA, UCG
stop	ATG, ATT, ACT	UAA, UAG, UGA	AUG, AUU, ACU
threonine	TGA, TGG, TGT, TGC	ACU, ACC, ACA, ACG	UGA, UGG, UGU, UGC
tryptophan	ACC	UGG	ACC
tyrosine	ATA, ATG	UAU, UAC	AUA, AUG
valine	CAA, CAG, CAT, CAC	GUU, GUC, GUA, GUG	CAA, CAG, CAU, CAC

Tabulation of DNA Base Triplets , M-RNA codons and T-RNA codons that form twenty different types of amino acids.

4. Algorithm

Method:

1. Mechanism of dual encryption
2. Let us consider base vein as P (largest L vein)
3. Calculate distances of P from all other veins

4. Assign veins to characters based on ascending distance
5. if number of veins greater than 128: assign to first 128
6. veins to respective characters .Else : assign in cyclic order

We take three dna base pairs and encode them to the 128 identified veins .Now the data is encrypted using the above algorithm and introduced into the dna sequence. The vein pattern is sent as private key and this authenticates both the receiver and the sender and this becomes the receivers decryption key We identify from the entire dna sequence of the person sets of basepairs and translate them onto the veins At the receiver's end we decrypt the encoded sequence and extract the original data.

The characteristics of the proposed method are that no prior knowledge about the objects is necessary and the parameters can be set automatically. A CCD is adopted as the input device to capture the pattern of the palm-dorsa. In the proposed approach, two of the finger webs are automatically selected as the datum points to define the region of interest on the thermal images. Within each region of interest, feature points of the vein patterns are extracted by modifying the basic tool of watershed transformation based on the properties of thermal images. According to the heat conduction law (the Fourier law), multiple features can be extracted from each FPVP for verification. Multiresolution representations of images with FPVPs are obtained using multiple multiresolution filters (MRFs) that extract the dominant points by filtering miscellaneous features for each FPVP. A hierarchical integrating function is then applied to integrate multiple features and multiresolution representations. The former is integrated by an inter-to-intra personal variation ratio and the latter is integrated by a positive Boolean function. We also introduce a logical and reasonable method to select a trained threshold for verification. Experiments were conducted using the thermal images of palm-dorsas and the results are satisfactory with an acceptable accuracy rate (FRR:2.3% and FAR:2.3%). The experimental results demonstrate that our proposed approach is valid and effective for vein-pattern verification.

5. Conclusion

Existing systems propose dna steganography but extraction of data is cumbersome. Introducing vein patterns as an advanced layer of encryption makes decoding of data simpler.

This technique reduces processing time and gives results of high accuracy. As the proposed method is based on dna and vein patterns which are invariant it assures confidentiality of sensitive information while accessing .

References

- [1] Finger Vein Recognition Based on Local Directional Code Sensors (Basel). 2012; 12(11): 14937–14952. Published online 2012 November 5. doi: 10.3390/s121114937.
- [2] Portal vein reconstruction based on topology. Zahlten C, Jürgens H, Evertsz CJ, Leppek R, Peitgen HO, Klose KJ.] *Eur J Radiol.* 1995 Jan;19(2):96-100. Department of Mathematics, University of Bremen, Germany.
- [3] Biometric verification using thermal images of palm-dorsa vein patterns. Chih-Lung Lin ; Inst. of Comput. Sci. & Inf. Eng., Nat. Central Univ., Chung-li, Taiwan ; Kuo-Chin Fan.
- [4] <http://waynesword.palomar.edu/codons.htm>

