Introduction

DNA cryptography is a cutting-edge field that leverages the principles of biological DNA (Deoxyribonucleic Acid) to enhance data security. Inspired by the complex encoding of genetic information in DNA sequences, this approach transforms data into sequences resembling DNA strands, which consist of four nucleotides: adenine (A), thymine (T), cytosine (C), and guanine (G). Its strength lies in the immense storage capacity and randomness of DNA sequences, which are challenging to decipher without precise keys. DNA cryptography combines biological concepts with computational techniques to create robust encryption systems, making it an intriguing avenue for safeguarding sensitive data in modern cryptographic applications.

DNA cryptography and image cryptography can be integrated to create an innovative hybrid encryption system that combines the strengths of both approaches. The intricate encoding mechanisms of DNA cryptography can be applied to encrypt pixel data from images, transforming visual information into DNA-like sequences. By leveraging the high randomness and complex representation of DNA sequences, this integration enhances the security of image encryption, making it resistant to unauthorized decoding. In this process, the DNA-encoded pixel data can be further manipulated using image cryptographic techniques, ensuring that the resulting encrypted image remains secure and visually distinct. The synergy of DNA and image cryptography opens up exciting possibilities for robust data protection, especially in scenarios where secure transmission and storage of multimedia data are critical.

Objective

To design and implement an innovative encryption mechanism that merges DNA cryptographic concepts with image cryptographic techniques. The goal is to explore the interplay between biological data encoding and multimedia security, creating a system that transforms visual information into an encoded format inspired by DNA sequences. This system aims to achieve enhanced data security, visual encryption integrity, and novel cryptographic methods to address modern multimedia protection challenges.

Theory

- **Nucleotide Bases** :Adenine, guanine, thymine, and cytosine are the four nitrogenous bases that make up the building blocks of DNA. They are abbreviated as A, G, T, and C, respectively. These bases are crucial for storing and transmitting genetic information.

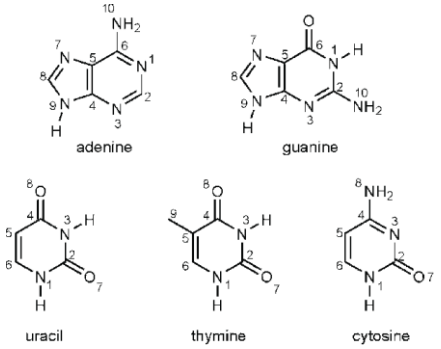

Fig 1 Neuclotide Bases

Another important concept for understanding the project is **Complementary Bases**.

- **Complementary Bases**:Complementary base pairing refers to the specific way nucleotides with different nitrogenous bases pair up in DNA and RNA molecules. In DNA, adenine (A) always pairs with thymine (T), and guanine (G) always pairs with cytosine (C). In RNA, uracil (U) replaces thymine, so adenine pairs with uracil. These pairs are held together by hydrogen bonds

These come in use in our project for the swapping function.
Next, we need an understanding for a vital process in our key generation process, Codone

- **Codon:** Codons are sequences of three nucleotide bases (adenine [A], thymine [T], cytosine [C], and guanine [G]) in DNA or RNA that correspond to specific amino acids or signal instructions during protein synthesis. In the genetic code, each codon acts like a "word" that tells the cell which amino acid to add to a growing protein chain.
  Codons are fundamental to translating genetic information into functional proteins, making them a key component of how living organisms function and grow. They're like nature's biological programming language.

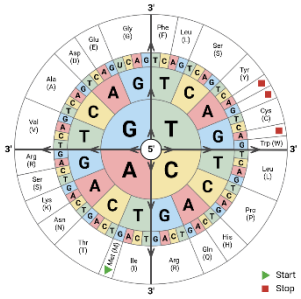

Fig 2. DNA Codon wheel

METHODOLOGY

The workflow for the program can be broken down into 3 parts: Key Generation, Encryption and Decryption.

1. Key Generation : A 64 bit random key is generated using the **Secrets** module from Python. The generated bit string is then split into 4 16-bit blocks. These blocks are then individually further broken down into groups of 4. The first of these 4 groups in linked to codon a , second to codon g , third to codon c and the last to codon t. The 4-bit binary digit is converted to decimal and they are then replaced by the nucleotide link indexed at the decimal value within their respective codon groups.

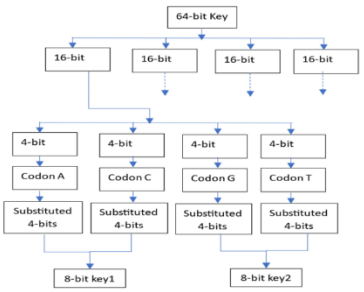

Fig 3. Key Generation Process

Molecule	Substitution
A	C
C	G
T	A
G	T

Fig 4. Nucleotide Substitutions

Now the new stored strings are substituted using the substitution table shown in Fig 4.
The newly generated string is then searched for within the all 4 Second Base codon groups, when

a match is found , the index is noted down and converted to binary . This is the final modification done to the 4 bit word . The bits are now concatenated back to 16 bit string Finally , the 4 16-bit strings are XORed together to form the final encryption key **Skey**

	T		C		A		G		
T	TTT	phe	TCT	ser	TAT	tyr	TGT	cys	T
	TTC		TCC		TAC		TGC		C
	TTA	leu	TCA		TAA	stop	TGA	stop	A
	TTG		TCG		TAG		TGG	try	G
C	CTT	leu	CCT	pro	CAT	his	CGT	arg	T
	CTC		CCC		CAC		CGC		C
	CTA		CCA		CAA	gln	CGA		A
	CTG		CCG		CAG		CGG		G
A	ATT	ile	ACT	thr	AAT	asp	AGT	ser	T
	ATC		ACC		AAC		AGC		C
	ATA	ile	ACA		AAA	lys	AGA	arg	A
	ATG	met	ACG		AAG		AGG		G
G	GTT	val	GCT	ala	GAT	asp	GGT	gly	T
	GTC		GCC		GAC		GGC		C
	GTA		GCA		GAA	glu	GGA		A
	GTG		GCG		GAG		GGG		G

Fig.5 Standard Codon Table

2. Encryption :

 Bitplane Encryption:

- The image is split into its Red, Green, and Blue (RGB) color channels.
- Each color channel is further decomposed into 8 bitplanes, separating each bit position across all pixels.
- Based on the key, a specific bitplane is selected and XORed with a pattern (like alternating 0s and 1s) to introduce controlled randomness while preserving reversibility.

 Color Plane Rotation:

- The RGB channels are cyclically rotated. For example, Red becomes Green, Green becomes Blue, and Blue becomes Red.
- The number of rotations is derived from the key, ensuring that without the correct key, the original color composition cannot be reconstructed.

 Final XOR Encryption:

- Each pixel of the modified image is XORed with a fixed binary pattern (like 170, which is 0b10101010) to further scramble the pixel values.
- This adds another layer of confusion, strengthening the encryption.

 Encrypted Image Storage:

- The encrypted image is reconstructed from the modified channels and saved securely

Result:

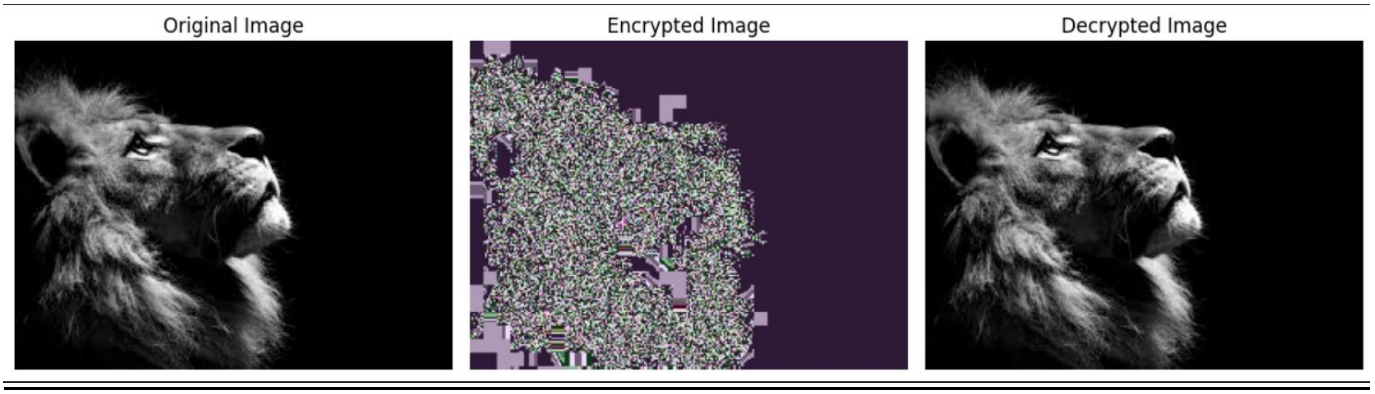

Fig. 6 Image comparsion of a greyscale Lion

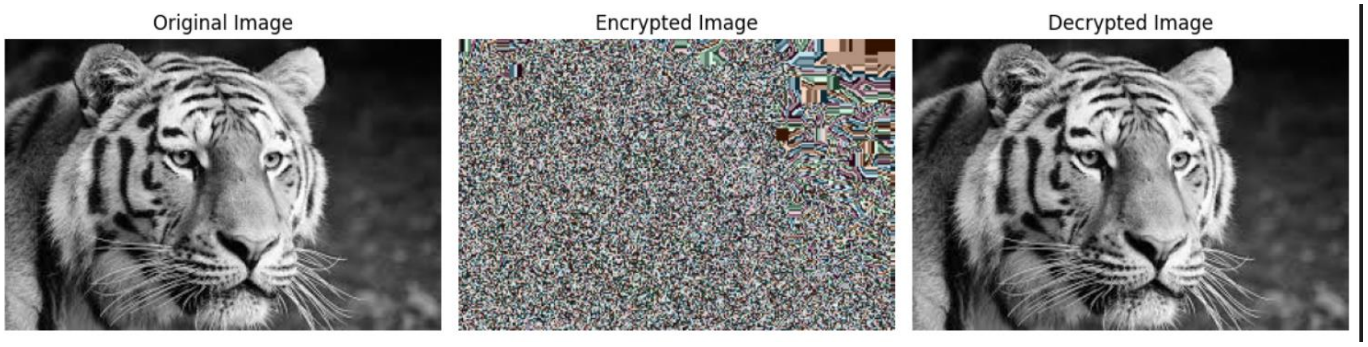

Fig 7 Image encryption of a grescale Tiger

Inference:

The integration of DNA cryptography and image cryptography has the potential to create a robust and innovative hybrid encryption framework. By combining the complex encoding mechanisms of DNA sequences with secure image processing techniques, the project demonstrates how interdisciplinary approaches can address modern challenges in data protection

References:

[1] Nadhan, A. S., & Jacob I, J. (2023). A Secure Lightweight Cryptographic Algorithm for the Internet of Things (IoT) Based on Deoxyribonucleic Acid (DNA) Sequences. *Engineering Proceedings*, *59*(1), 31.

[2] Akiwate, B., & Parthiban, L. (2021). A DNA cryptographic solution for secured image and text encryption. *International Journal of Advanced Computer Science and Applications*, *12*(2).