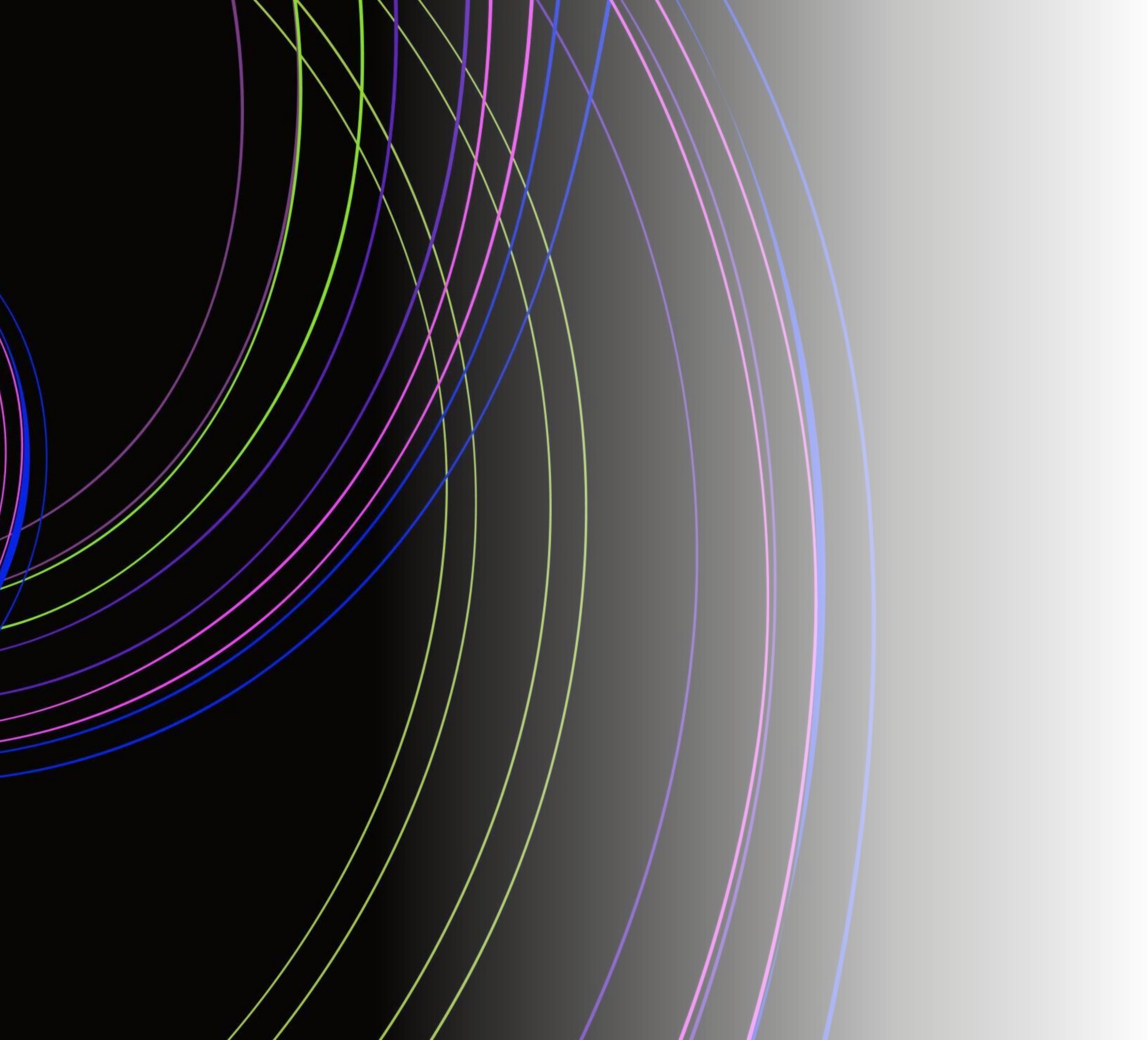


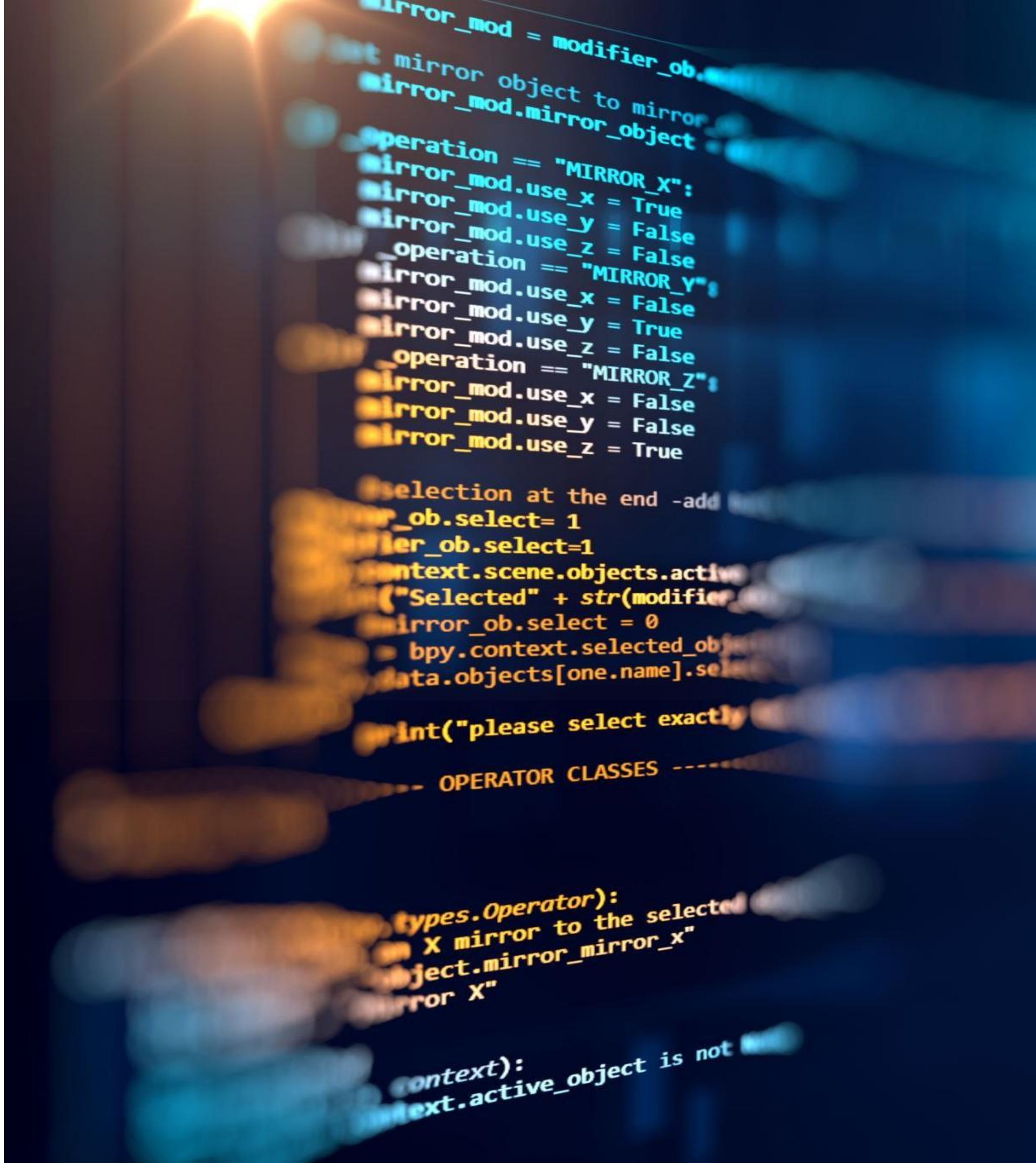
STUDENT DETAILS

- NAME: B NIKHIL
- ROLL NO: 22ME1A4609
- EMAIL:bnn2039v@gmail.com
- BRANCH: CYBER SECURITY
- COLLEGE:
RAMACHANDRA COLLEGE OF ENIGNEERING

STEGANOGRAPHY

1. Steganography is the practice of concealing information within another message or physical object or hiding methods to avoid detection. Steganography can be used to hide virtually any type of digital content, including text, image, video, or audio content. That hidden data is then extracted at its destination.

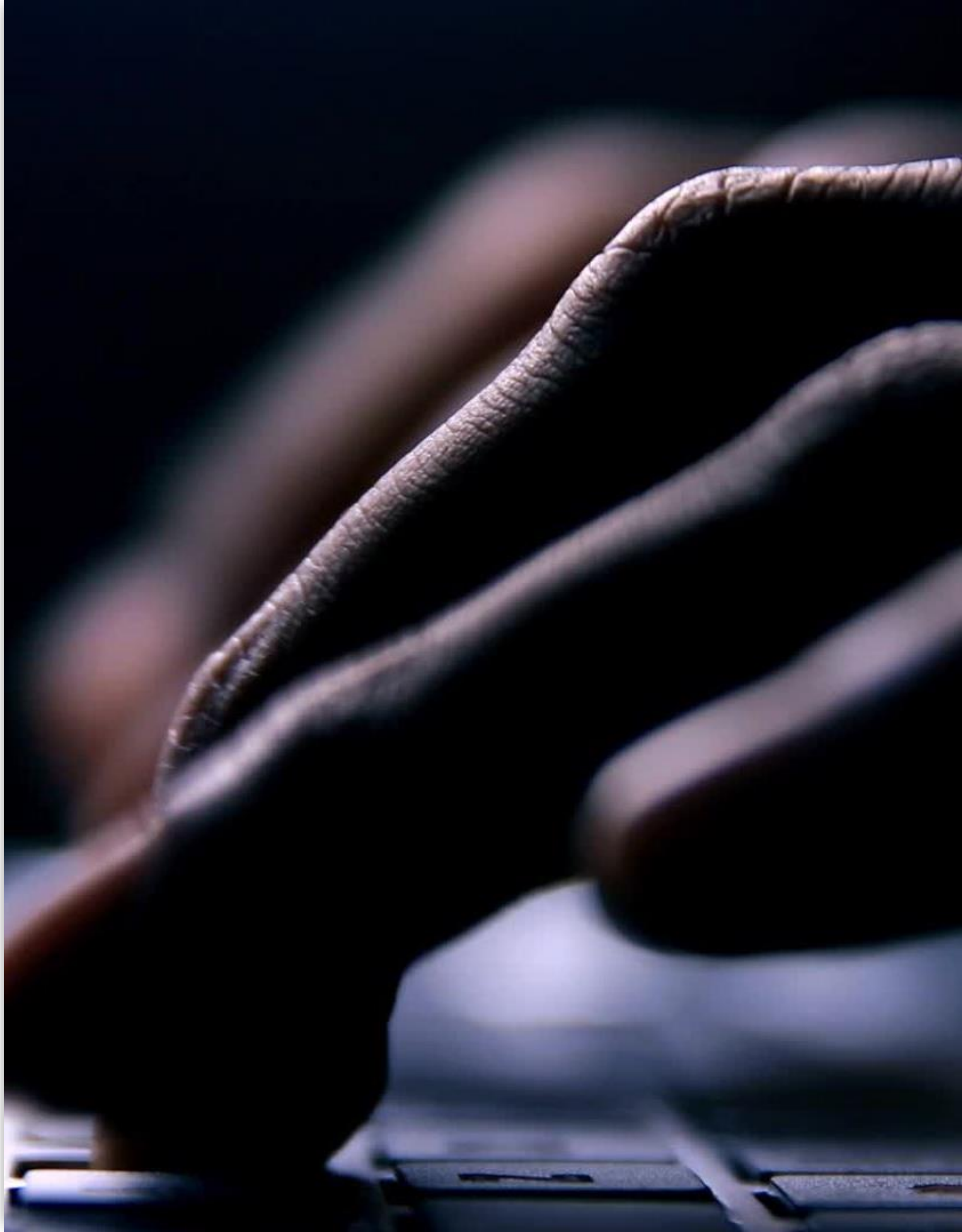
2. Text steganography involves hiding information inside text files. This includes changing the format of existing text, changing words within a text, using context-free grammars to generate readable texts, or generating random character sequences.



```
irror_mod = modifier_ob.
mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

selection at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.active
("Selected" + str(modifier
irror_ob.select = 0
 bpy.context.selected_ob
ata.objects[one.name].se

int("please select exactly

- OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
rror X"

ontext):
ext.active_object is not
```

STEGANOGRAPHY AGENDA

- Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing both the fact that a secret message is being sent and its contents. Steganography includes the concealment of information within computer files.
- Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program, or protocol.
- Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixels to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change



PROJECT OVERVIEW

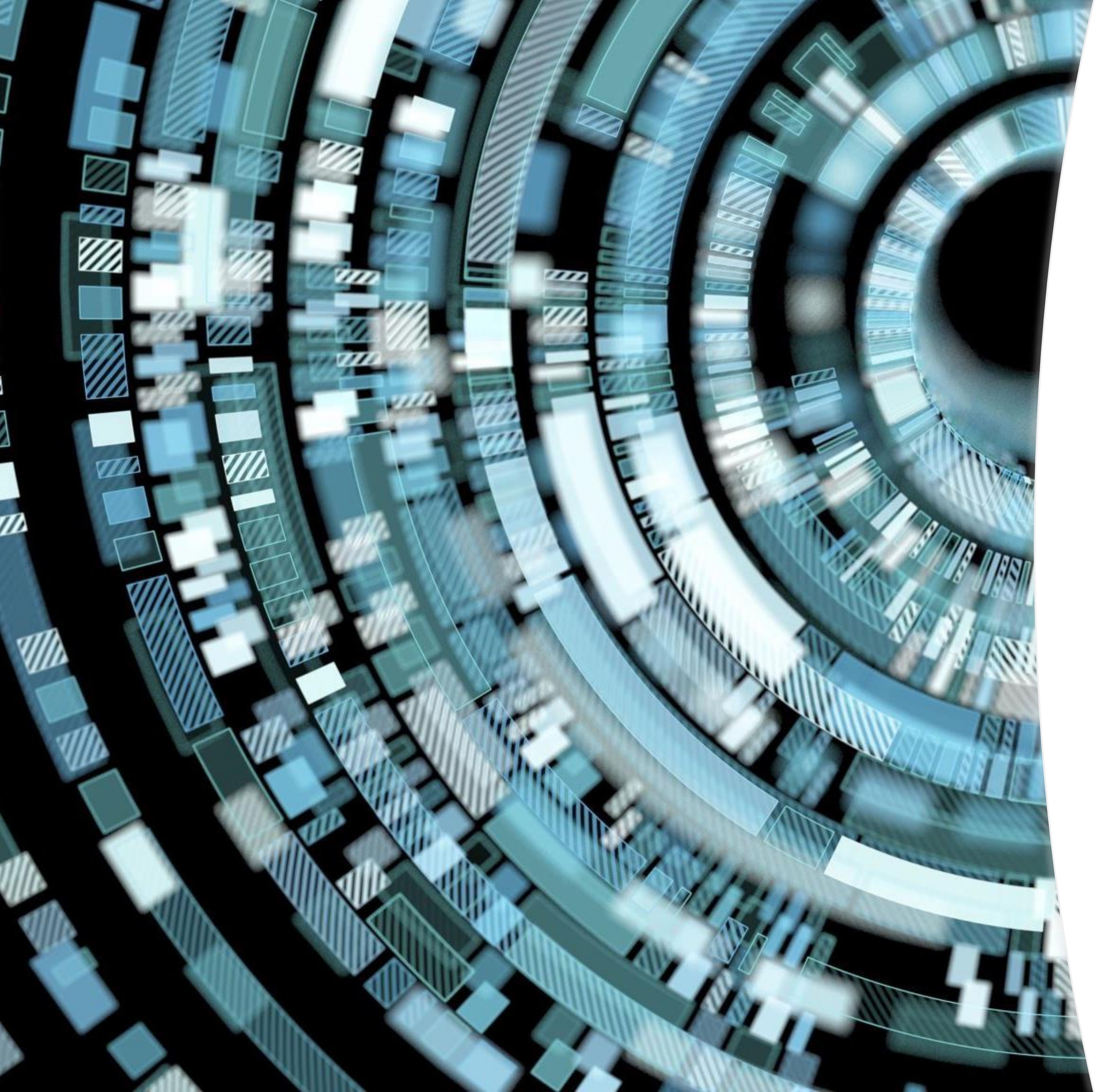
- A steganography technique involves hiding sensitive information within an ordinary, non-secret file or message, so that it will not be detected. The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection. Steganography is an additional step that can be used in conjunction with encryption in order to conceal or protect data.
- Steganography is a means of concealing secret information within (or even on top of) an otherwise mundane, non-secret document or other media to avoid detection. It comes from the Greek words steganos, which means “covered” or “hidden,” and graph, which means “to write.” Hence, “hidden writing".

WHO ARE THE END END USERS OF THIS PROJECT

- **Security and Intelligence Agencies**: Government agencies involved in national security, intelligence gathering, and law enforcement often utilize steganography to covertly transmit and receive sensitive information. This ensures that critical data remains protected from interception and detection by unauthorized parties.
- **Corporate Entities**: Businesses and organizations may employ steganography to secure proprietary information, trade secrets, financial data, and confidential communications. This helps in maintaining competitive advantage and protecting sensitive corporate assets from industrial espionage or unauthorized access.
- **Military Organizations**: Military units and defense contractors use steganography for secure communication in tactical operations, ensuring operational security and confidentiality of mission-critical information.
- **Journalists and Activists**: Individuals working in journalism, activism, or human rights advocacy may use steganography to securely communicate and protect the anonymity of sources or sensitive information, especially in regions with restricted freedom of speech or surveillance concerns.

YOUR SOLUTION AND ITS VALUE PROPOSITION

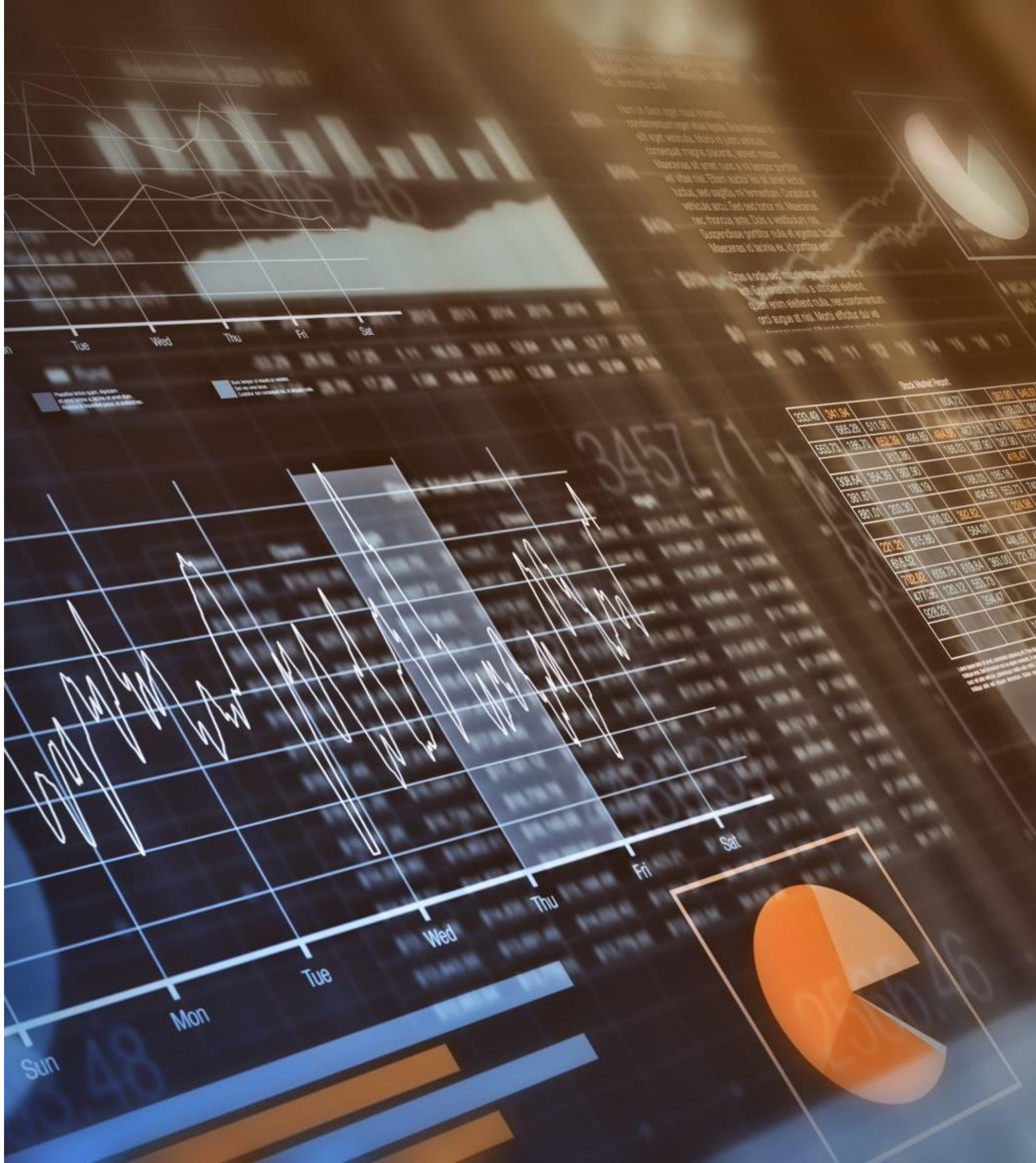
- **Security and Stealth**: My solution ensures high levels of security by hiding information within the least significant bits of the cover media, making it extremely difficult for unauthorized users to detect the hidden data without the proper decryption key or algorithm.
- **Versatility**: It supports embedding various types of data formats (text, binary files, etc.) into different types of media files, ensuring flexibility and applicability across different use cases.
- **Efficiency**: The embedding process is efficient and does not significantly alter the original media file's quality or characteristics, preserving its integrity and minimizing the chances of detection.



- **Robustness**: The hidden data remains intact even after typical modifications to the media file, such as compression, resizing, or format conversion, ensuring robustness against unintentional alterations.
- **Accessibility**: The solution includes easy-to-use tools or APIs that allow users to encode and decode hidden messages with minimal effort, making it accessible to both technical and non-technical users.
- **Scalability**: It can handle large volumes of data efficiently, suitable for applications ranging from secure communication and data storage to digital watermarking and intellectual property protection.

HOW DID YOU COSTIMIZE THE PROJECT AND MAKE IT YOUR OWN

- **Algorithm Selection and Enhancement**: I would carefully select and possibly enhance steganographic algorithms to ensure they meet modern security standards while optimizing them for efficiency and robustness. This might involve implementing newer algorithms or improving existing ones to handle larger data payloads or to be more resistant to statistical analysis.
- **User Interface and Experience**: Designing an intuitive and user-friendly interface is crucial. I would customize the user interface to make the embedding and extraction processes straightforward, possibly integrating drag-and-drop functionality, progress indicators, and clear instructions to enhance usability.



- **Integration of Security Measures**: Apart from embedding data, ensuring the security of the embedded information is paramount. I would integrate strong encryption techniques (like AES) for encrypting the data before embedding it, ensuring that even if the carrier file is compromised, the embedded information remains secure.

- **Performance Optimization**: Optimizing the performance of the steganography operations is essential for real-world usability. This could involve minimizing computational overhead during embedding and extraction, optimizing memory usage, and ensuring that the process runs efficiently on various hardware configurations.

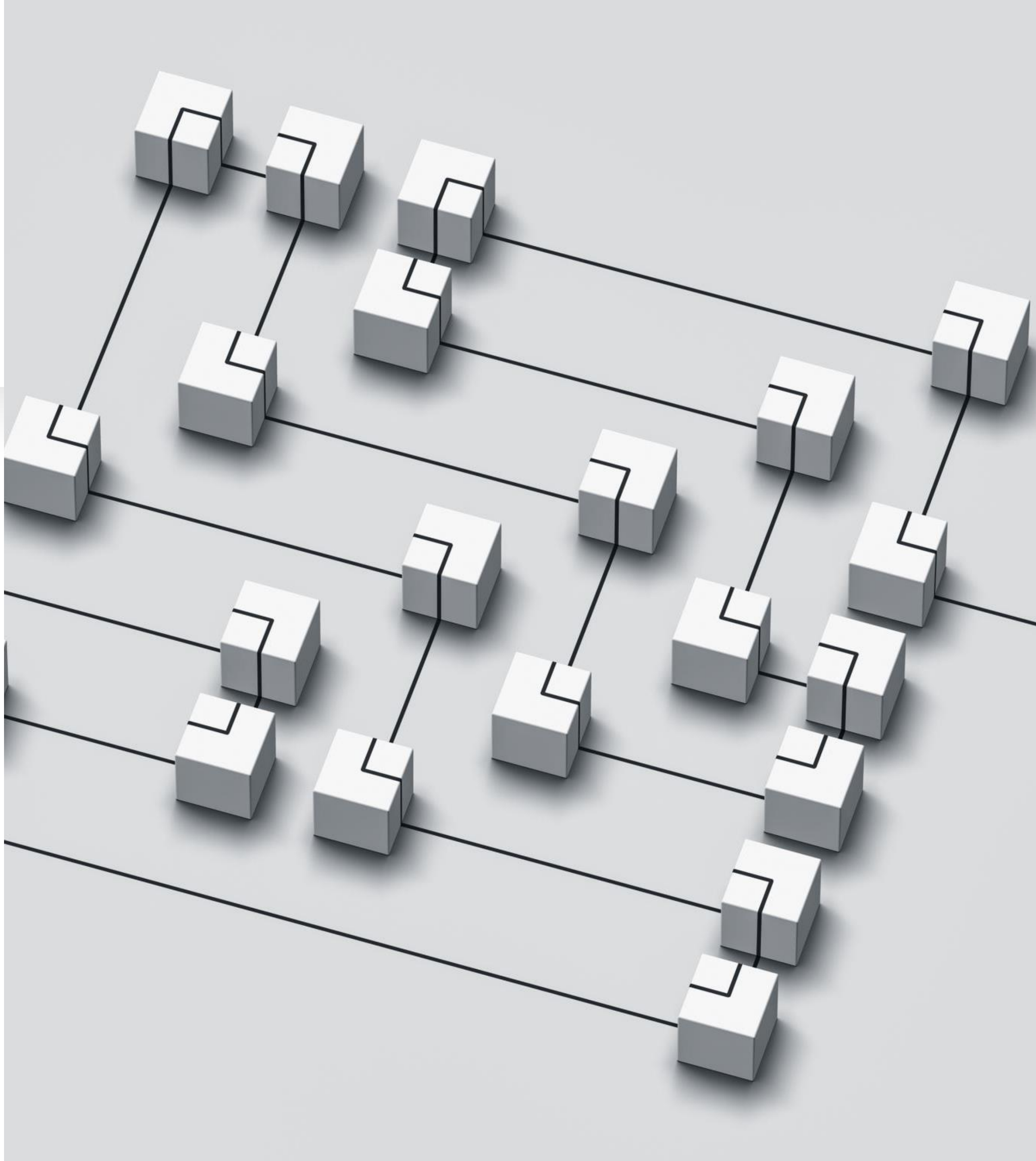
- **Customization and Extensibility**: Providing options for customization allows users to tailor the steganography process to their specific needs. This might include adjustable parameters for embedding density (how much data to embed relative to the cover media), support for different file formats, and the ability to choose different embedding algorithms depending on the desired level of security versus invisibility.

- **Documentation and Support**: Clear documentation and responsive support channels are crucial for users to understand and effectively use the steganography tool. Customizing the documentation to include detailed examples, FAQs, and troubleshooting tips would enhance user confidence and satisfaction.

- **Testing and Validation**: Rigorous testing and validation are essential to ensure the reliability and security of the steganography solution. Customizing the testing process to include comprehensive test cases, security audits, and performance benchmarks would validate the effectiveness of the solution.

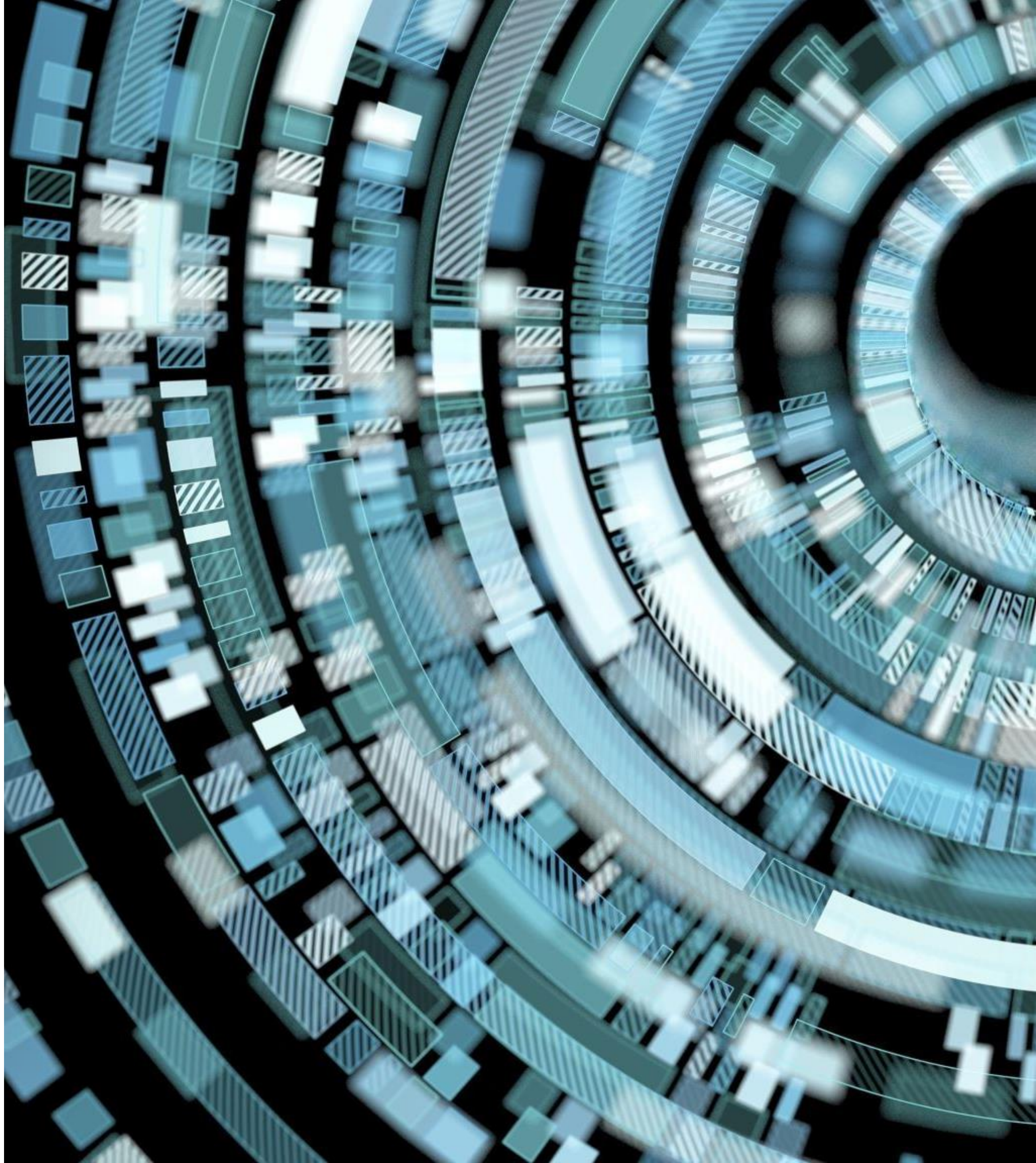
MODELING

- **Data Model**: This involves defining how data will be represented and manipulated within the steganography system. It includes decisions on data formats (text, binary, etc.), encoding schemes, and how data will be structured for embedding and extraction.
- **Embedding Model**: This specifies the technique or algorithm used to embed hidden data into a cover media (such as an image or audio file). Modeling here involves determining how to modify the carrier file to embed the hidden information while minimizing perceptible changes and maintaining cover media integrity.
- **Extraction Model**: This defines the method for extracting hidden data from the carrier media. Modeling the extraction process ensures that the embedded information can be accurately retrieved, even after potential alterations to the carrier file.



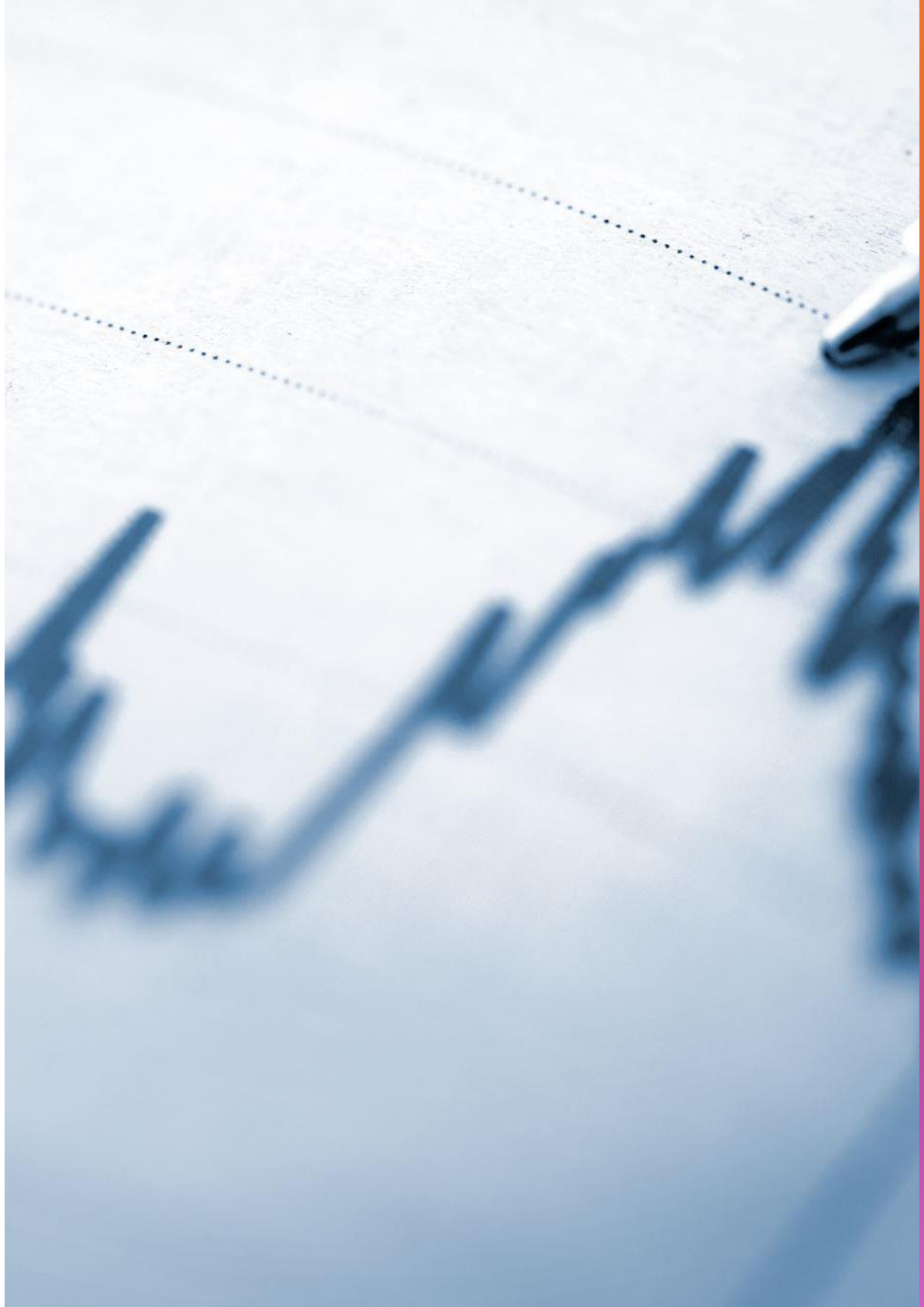
TYPES OF STEGANOGRAPHY

- Image Steganography
- Audio Steganography
- Video Steganography
- Text Steganography
- File Steganography
- Network Steganography
- Printed Steganography



RESULT

- **Efficient and Secure Data Embedding**: By meticulously designing the embedding model, the project ensures that hidden data can be seamlessly integrated into cover media while maintaining the media's integrity and quality. This efficiency reduces the likelihood of detection and preserves the secrecy of the embedded information.
- **Accurate Data Extraction**: Through a well-defined extraction model, the project enables the precise retrieval of hidden data from the carrier media. This accuracy ensures that authorized users can access the concealed information without errors or loss of data integrity.
- **Robust Security Measures**: A comprehensive security model strengthens the project's defenses against unauthorized access and detection. Techniques such as encryption of hidden data before embedding, selection of advanced steganographic algorithms, and validation mechanisms contribute to safeguarding the confidentiality and integrity of sensitive information.
- **Optimized Performance**: The performance model focuses on optimizing computational resources and operational efficiency. This optimization minimizes processing.



LINKS

THANK YOU