For use by the project lecturer	Approved		Revision required	
Feedback				

To be completed by the student							
PROJECT PROPOSAL 2019				Project no	TDR7	Revision no	1
Title Mr.	Surname Gouws	Initials JR	Student no 16033915	Study leader (title, initials, surname) Mr. D. Ramotsoela			
Project title A secure communication system using steganography							

Language editor name	Language editor signature
Student declaration I understand what plagiarism is and that I have to complete my project on my own.	**Study leader declaration** This is a clear and unambiguous description of what is required in this project
Student signature	Study leader signature

1. Project description

What is your project about? What does your system have to do? What is the problem to be solved?

The increase in modern computing power that is becoming more freely available raises a concern to traditional encryption methods, as ordinary citizens have access to powerful computers that are able to break such methods. There is thus a requirement for an alternative technique to provide a secure data communication platform. The project will implement an alternative secure data communication platform, known as steganography. Steganography is a method of hiding data, which is to be communicated securely, within any public media such as images, video, audio files, etc. For the purpose of this project, audio steganography will be considered, where secret data will be communicated securely by making use of an audio file as host media. The system will provide a secure communication platform, implemented from first principles. The system should be implemented on a standalone device using a hardware platform that can be plugged into any commercial computer and provide a user with the secure communication platform. All of the processing and signal processing required for the communication platform will be required to be done on the standalone device. The system will provide strong user authentication and confidentiality in order to protect the data that is required to be communicated.

2. Technical challenges in this project

Describe the technical challenges that are beyond those encountered up to the end of third year and in other final year modules.

2.1 Primary design challenges

The efficiency of steganographic algorithms depend on requirements known as transparency, capacity, robustness and complexity, where a trade-off between these requirements need to be considered. The Human Auditory System is more sensitive than the Human Visual System, with an audible range of 20Hz-20kHz. Mathematical equations simulating transparency, inaccurately represents the Human Auditory System and need to be considered. Audio signal processing, such as theoretical sampling theorems, lossy compression, re-sampling and re-quantization, are required to represent the audio signal, but are not independent of the steganographic performance requirements, as it may degrade signal quality through errors such as quantization errors, introducing an unintentional attack.

2.2 Primary implementation challenges

The encoding and decoding algorithms need to execute with reasonable time and space complexity in order to be processed on an external hardware platform and it is required to get familiar with the hardware platform. Audio steganography performance varies as audio file characteristics (Jazz, Rock, etc.) differ. Thus, the steganographic file performance will need to be evaluated for various audio file types. The effect of noise during sampling will need to be considered, as it will influence the performance of the encoding and decoding algorithm. The hardware platform should support strong user authentication, such as cryptographic methods, which will in turn introduce further processing required on the hardware platform, increasing the encoding time for steganography.

3. Functional analysis

3.1 Functional description

Describe the design in terms of system functions as shown on the functional block diagram in section 3.2. This description should be in narrative format.

FU1, the user authentication process, will interact with FU5 in order to prompt for information that is user specific, in order to validate if the user is authentic or not. If the user is not authentic, the user will be denied access to the system, including access to FU2, FU3 and FU4. If the user is authentic, then the information that was entered will be communicated to FU3 in the case of encryption or FU4 in the case of decryption.

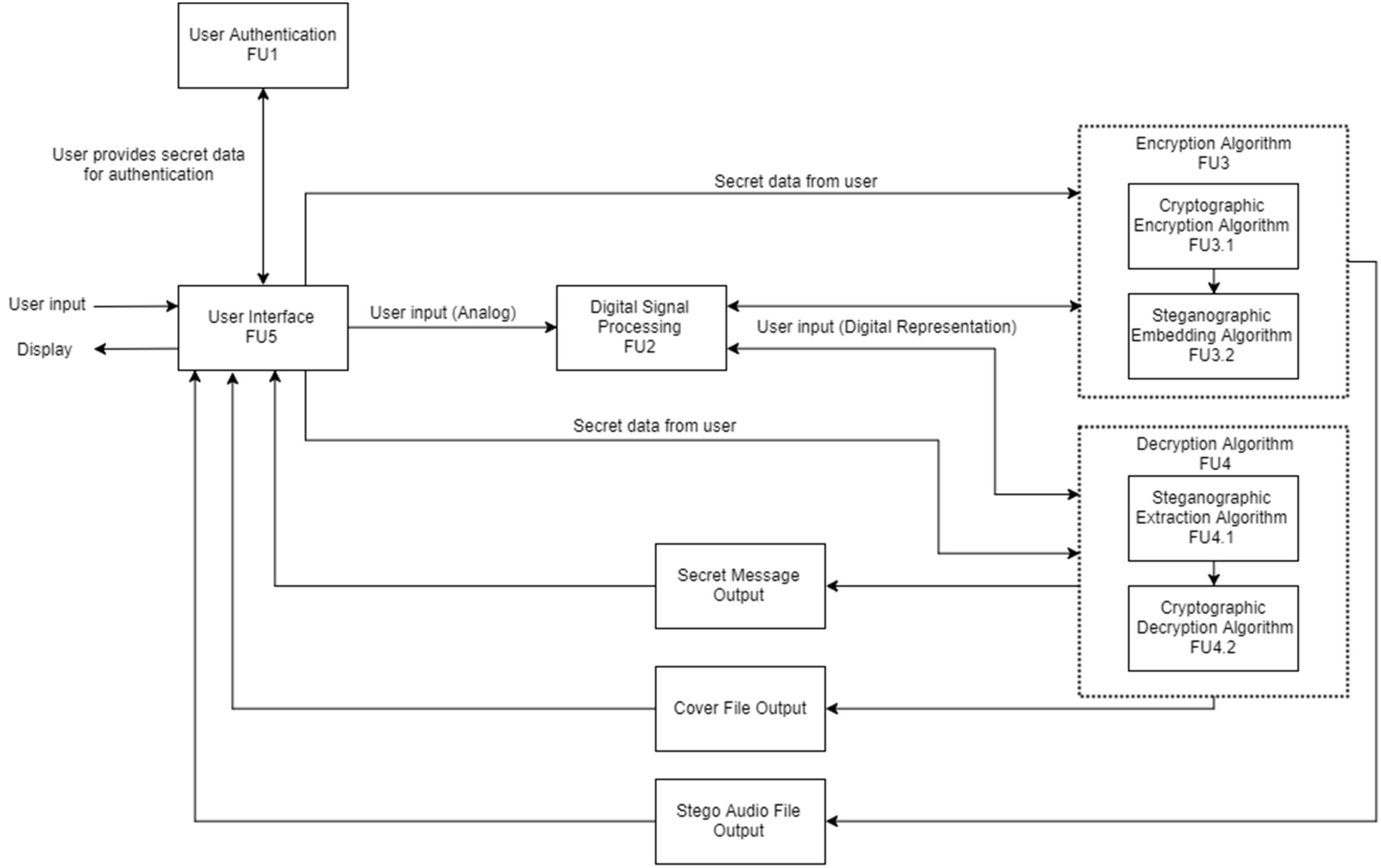
FU2, the digital signal processing of the audio file, will represent the data provided by the user (cover file, secret message or steganographic file) in a digital format that can be used to embed or extract the secret message. FU2 will also reconstruct the signals after FU3 produced the embedded signal or when FU4 produced the secret message and cover files.

FU3, the encryption algorithm, consists of FU3.1 and FU3.2, working together to provide the secure message. FU3.1 takes the secret message and encrypts it with the secret data provided by the user in FU1, through making use of cryptographic algorithms. FU3.2 takes the result of FU3.1 and embeds it into the cover file, using steganographic methods, which satisfies the core requirements of steganography. The secret message and the cover file are taken as inputs from FU2, while the secret user information is provided by FU5.

FU4, the decryption algorithm, consists of FU4.1 and FU4.2, working together to retrieve the hidden message. FU4.1 takes the embedded signal and extracts the encrypted secret message, using a steganographic decryption algorithm. The message is then decrypted by FU4.2, through a cryptographic decryption algorithm and results provided to FU5.

FU5, the user interface, will interact with the user for information needed from the user (secret message, audio cover, steganographic file, user authentication information) and display the results of processing and authentication on the user interface afterwards.

3.2 Functional block diagram



4. System requirements and specifications

These are the core requirements of the system or product (the mission-critical requirements) summarised in table format .

	Requirement 1: fundamental functional and performance requirement	Requirement 2	Requirement 3
1. Core mission requirements of the system or product. Solution of the problem will be the most important requirement. Capture this in the set of requirements.	Embed the secret information using the encoding algorithm in a way that satisfies the mathematical requirements of transparency for the steganographic file and the recovered cover file.	Embed secret information in a host audio file in such a way that there is not an audible difference in the host file when played to an audience. The resultant steganographic audio file should thus satisfy the requirement of transparency.	The algorithm should be able to provide sufficient storing capacity. The storing capacity should be satisfied with the trade-off being the robustness, as robustness is more related to watermarking than steganography.
2. What is the target specification (in measurable terms) to be met in order to achieve this requirement?	In an objective test, a signal to noise ratio of at least 20dB is required, with the signal to noise ratio defined as the cover file, relative to the magnitude difference between the cover file samples and the steganographic file samples.	Carry out a subjective test with a target score of at least 4 on a scale from 1-5. The cover file and the steganographic file will be presented to multiple humans to rate the difference heard, with 5 being no difference and 1 being a big difference.	A capacity that is achieved in typical standard least significant bit encoding schemes will be required, where 1 bit is embedded within a host sample of 16 bits.
3. Motivation: how will meeting this specification solve the problem?	The International Federation of the Phonographic Industry provides the minimum requirements for the SNR to allow for transparency of the steganographic file. These requirements will prevent steganalysis tools from succeeding.	The International Federation of the Phonographic Industry provides the minimum requirements of the SDG test. This will also provide further validation due to the inaccurate mathematical simulation of the Human Auditory System.	This will satisfy the requirement of capacity and is comparable to existing LSB encoding for obtaining high capacity. This will allow more data to be inserted into a host audio file, as the LSB method is known for high capacity capabilities.
4. How will you *demonstrate* at the examination that this requirement has been met?	The encoding and decoding of the audio will be demonstrated. Results will be presented on the SNR that were obtained for different types of audio files, such as Jazz, Rock, Classical, etc.	A subjective test will be carried out by examiners to evaluate whether a difference can be detected in steganographic file. Results will be presented on the SDG test that were obtained for different types of audio files, such as Jazz, Rock, etc.	Results will be presented on the capacity obtained, without compromising transparency,using multiple audio host files with different audio characteristics.
5. What is the deliverable? What are the aspects that you will design and implement yourself to meet this requirement? If none, indicate clearly.	The deliverable is to provide a steganographic algorithm that satisfies the requirement of transparency to steganalysis tools. The encoding and decoding algorithm, requiring signal processing, will be implemented from first principles.	The deliverable is to provide a steganographic algorithm that satisfies the requirement of transparency to the human ear. The encoding and decoding algorithm, requiring signal processing, will be implemented from first principles.	The deliverable is to provide a steganographic algorithm that satisfies the requirement of capacity of conventional LSB encoding. The encoding and decoding algorithm, requiring signal processing, will be implemented from first principles.
6. What are the aspects to be taken off the shelf to meet this requirement? If none, indicate clearly.	The hardware platform and the computer interfacing with the hardware platform will be taken off the shelf.	The hardware platform and the computer interfacing with the hardware platform will be taken off the shelf.	The hardware platform and the computer interfacing with the hardware platform will be taken off the shelf.

System requirements and specifications (continued)

	Requirement 4	Requirement 5	Requirement 6
1. <u>Core mission requirements of the system or product</u>. Solution of the problem will be the most important requirement. Capture this in the set of requirements.	Extract the secret information using the decoding algorithm in a way that satisfies the mathematical requirements of transparency for the retrieved signal.		
2. What is <u>the target specification</u> (in measurable terms) to be met in order to achieve this requirement?	A signal to noise ratio of at least 20dB is required, with the signal to noise ratio defined as the original secret message, relative to the magnitude difference between the original secret message and the retrieved secret message.		
3. Motivation: how will meeting this specification solve the problem?	The International Federation of the Phonographic Industry provides the minimum requirements for the SNR to allow for transparency of the steganographic file. These requirements will prevent an audible difference being picked up.		
4. How will you *demonstrate* <u>at the examination</u> that this requirement has been met?	Results will be presented on the SNR that were obtained for different types of audio files used as secret message, such as Jazz, Rock, Classical, recovered after encryption and decryption was performed.		
5. What is the deliverable? What are the aspects that <u>you will design and implement yourself</u> to meet this requirement? If none, indicate clearly.	The deliverable is to provide a steganographic algorithm that satisfies the requirement of transparency of a recovered audio file. The encoding and decoding algorithm, requiring signal processing, will be implemented from first principles.		
6. What are the aspects <u>to be taken off the shelf</u> to meet this requirement? If none, indicate clearly.	The hardware platform and the computer interfacing with the hardware platform will be taken off the shelf.		

5. Field conditions

These are the core requirements of the system or product (the mission-critical requirements) summarised in table format .

	Field condition 1	Field condition 2	Field condition 3
Field condition requirement. In which field conditions does the system have to operate? Indicate the one, two or three most important field conditions.	The system should be able to comply with the minimum requirements of transparency when exposed to additive white Gaussian noise to simulate an unintentional attack, simulating errors introduced during sampling and reconstruction.		
Field condition specification. What is the specification (in measurable terms) for this field condition?	The steganographic file will have to satisfy the SNR of at least 20dB after exposed to a 0 mean and up to 0.5 bits/sec/Hz additive white Gaussian noise.		

6. Student tasks

6.1 Design and implementation tasks

List your primary design and implementation tasks in bullet list format (5-10 bullets). These are *not* product requirements, but *your* tasks.

- A literature study on steganography design principles, user authentication and cryptography should be provided as well as documentation on the findings of the literature study.
- An encoding and decoding algorithm should be designed and implemented, capable of embedding and extracting a secret message in a cover file through implementing an audio steganography system from first principles.
- The encoding and decoding algorithms should be tested on a personal computer with known software and the findings should be documented.
- A graphical user interface should be implemented through which users will be authenticated and provided with the steganographic system.
- All the findings of simulations and results of designing and implementing the system should be documented.
- The encoding and decoding algorithms should be tested on the standalone hardware platform and the audio signal before and after encoding are to be plotted and compare to the results obtained on the personal computer findings need to be documented.

6.2 New knowledge to be acquired

Describe what the theoretical foundation to the project is, and which new knowledge you will acquire (beyond that covered in any other undergraduate modules).

- Steganography design principles with special attention to audio steganography design principles will be researched and knowledge will be acquired on how to implement these algorithms.
- New digital signal processing methods and manipulation of audio signals will be investigated and implemented.
- Knowledge will be acquired on what the impact of different audio file formats has on the performance of audio steganography and the quality of the decoded message.
- Steganography data security design principles will be investigated in detail and the investigation will provide a better understanding on the subject area.
- Knowledge will be gained on the implementation and testing of strong user authentication methods.
- Implementing the system will help to get familiar with the chosen hardware platform that will serve as the communication platform and interfacing the hardware platform with a personal computer.