Lab-2 Audio Steganography

Himanshu Goyal 17CS02011

Aim:

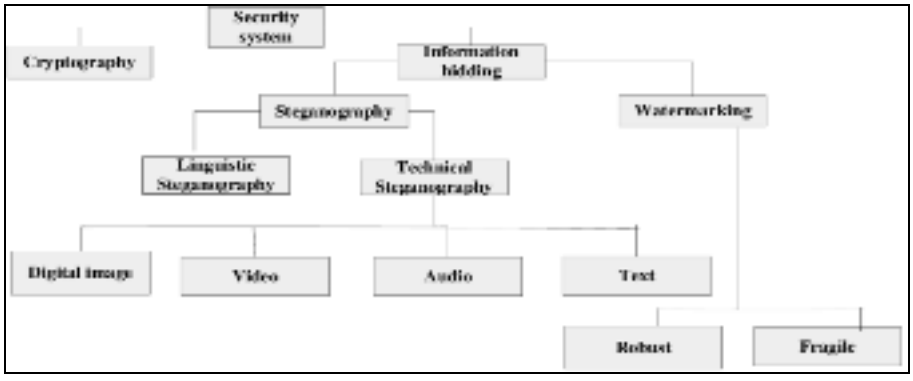
- Design and implementation of an algorithm to hide secret messages into the cover audio file using all possible bit manipulation.

Theory:

Cryptography: is a method to hide information, (or: authenticate information, authenticate users, exchange keys, etc.). It is based on keys and applying keyed transformation to data and the data changes to encrypted data so that with the key one can reverse the transformation (or check authenticity, etc). There are many primitives in cryptography: symmetric encryption where key for encryption and decryption is the same, public-key cryptography where the keys above are different. There are digital signatures, MAC-ing information, and so on many other methods. RSA is a primary example of public key, Diffie-Hellman is a primary example of key exchange, AES is a primary example of symmetric key ciphers etc.

Steganography: is a method to modify text or other form of information transforming the source to a target file (say text) which encodes a message but without knowing the key the text simply looks like a normal text (while secretly embedding a message). Say the key tells you to take every 5th word and look at its third letter and this is the hidden message.

Watermarking: is a method to embed an identifier in some hidden way in a file (typically in non text files) so that if you have the key you can authenticate the existence of the watermark. The method is typically hidden to the naked eye, but may be detectable. It's goal is authentication of the source of the data.

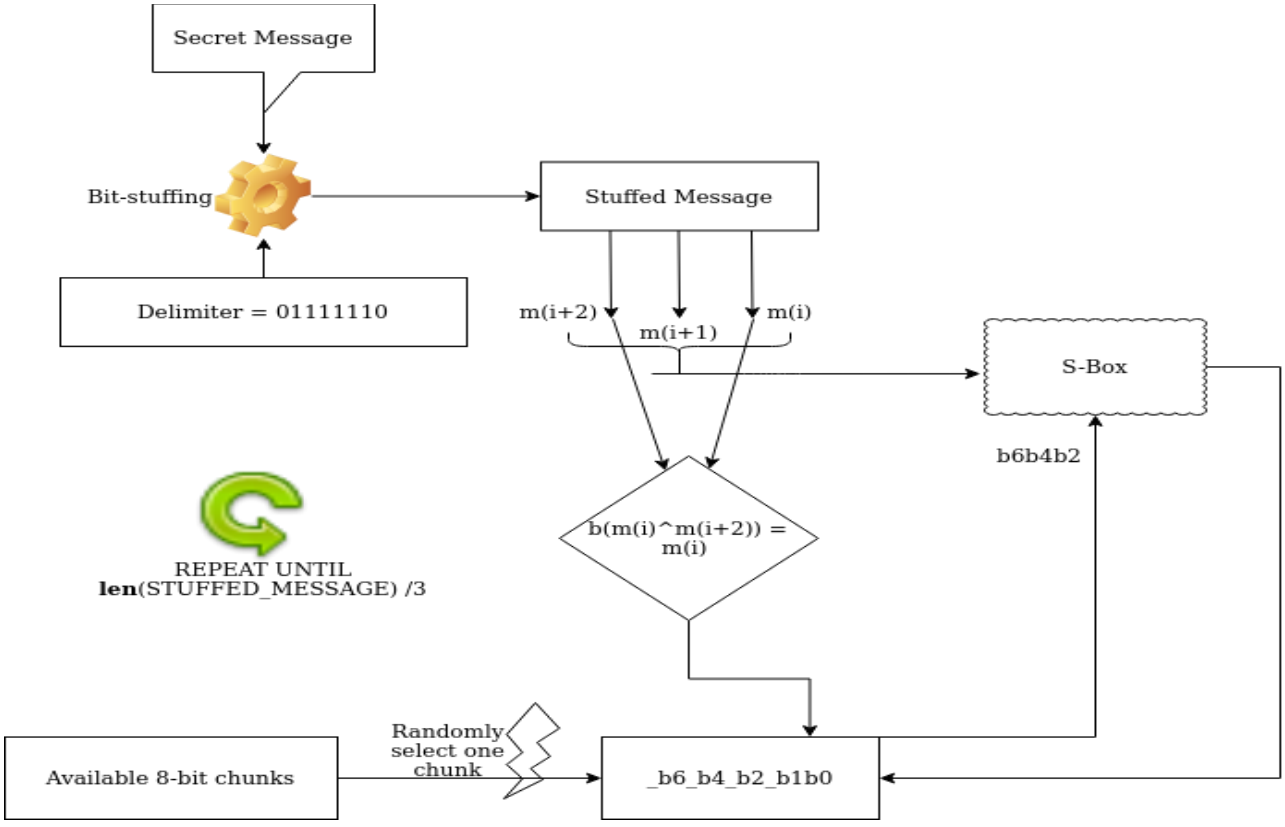


Self-Proposed Algorithm:-

Substitution(S) Box

Present bits ↓	**Incoming Bits →**							
	000	011	101	110	001	010	100	111
000	**x**	**_11**	**x**	**_11**	**__1**	**_1_**	**__1**	**_1_**
011	**10_**	**x**	**10_**	**x**	**_0_**	**__0**	**_0_**	**__0**
101	**x**	**_10**	**x**	**_10**	**__0**	**_1_**	**__0**	**_1_**
110	**_01**	**x**	**_01**	**x**	**_0_**	**__1**	**_0_**	**__1**
001	**__0**	**_1_**	**__0**	**_1_**	**x**	**_10**	**x**	**_10**
010	**_0_**	**__1**	**_0_**	**__1**	**_01**	**x**	**_01**	**x**
100	**__1**	**_1_**	**__1**	**_1_**	**x**	**_11**	**x**	**_11**
111	**_0_**	**__0**	**_0_**	**__0**	**_00**	**x**	**_00**	**x**

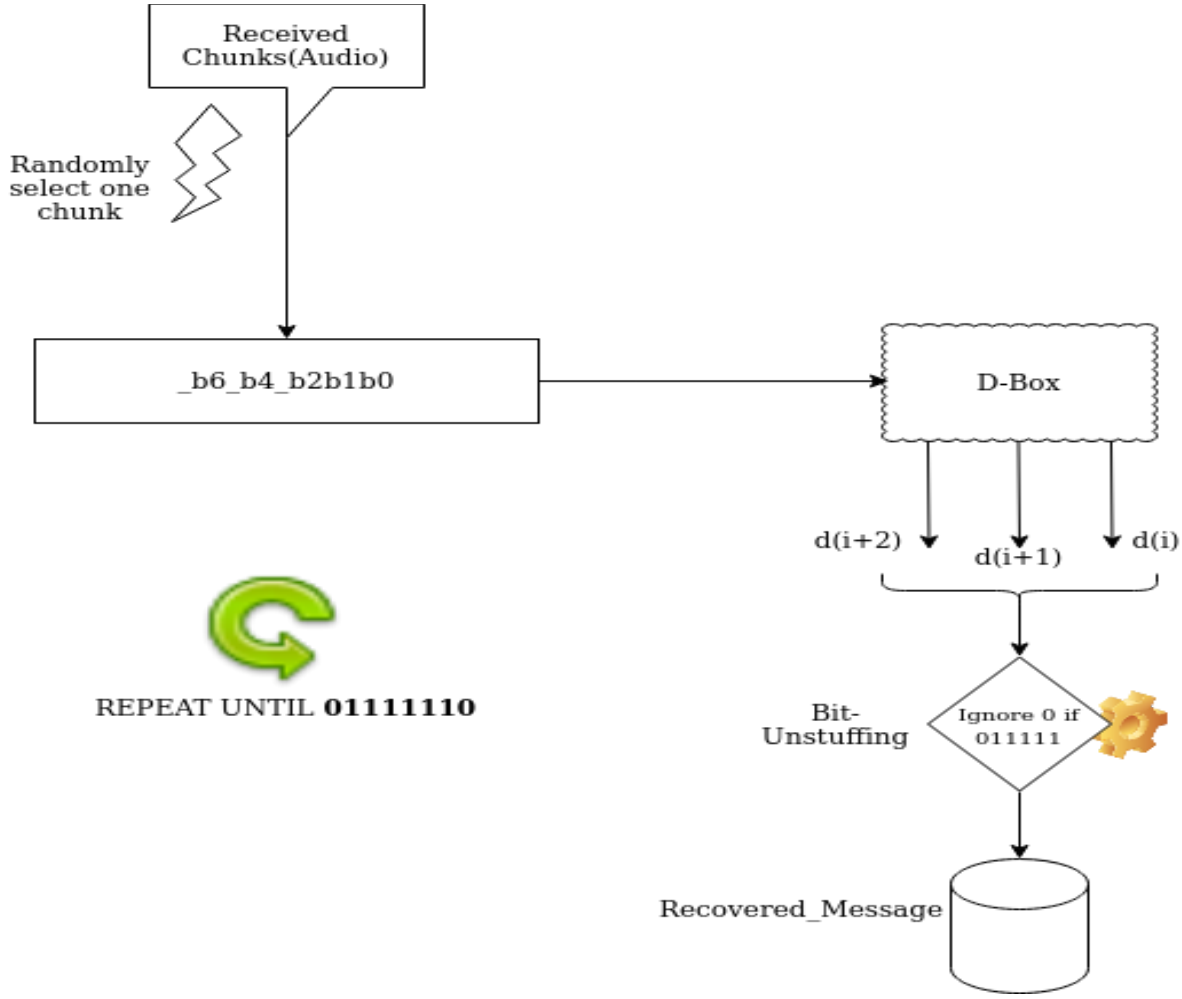
Encoding Algorithm



Decoding Algorithm:

D-box

b6^b4^b2	b6^b2=0	b6^b2=1
000	000	
011	101	
101 (0)		011
110		110
001		001
111		100
100 (1)	010	
010	111	



Conclusion:

The practical difference between steganography, cryptography and watermarking has become quite meaningful after performing this experiment. The use of PRNG, a well known tool in the security domain, has helped here to randomly select the 8-bit locations for hiding secret messages into the cover audio. The randomisation introduced in the self-proposed algorithm makes the job of adversary difficult to decipher in comparison to its counterpart available deterministic algorithms.

In Future, I would like to hide the secret message using concepts from frequency domain instead of continuous time domain.