STUDIES ON GENERATING OF ECG SIGNAL FOR MONITORING HEALTH CONDITION BY USING SECRUITY ALGORITHM

With the increasing number of aging population and a significant amount suffering from cardiac diseases, a need for monitoring ECG from remote place arises. Since the systems involve the transmission of person's confidential information, a proposal method is made to encrypt the person's name to ensure security of the data and embed the encrypted data onto the ECG signal and transmit. Since personal information is being sent on a public network, it is prone to misuse; hence it is important that person's data remains confidential throughout the process. Here DCT (Discrete cosine Transform) is used to decompose the ECG signal and a Hill Cipher encryption algorithm is proposed to encrypt the confidential data, the result of which is embedded onto the decomposed ECG. The method produces acceptable results with minimal distortion to the ECG and the signal remains diagnosable. There have been several protocols (or techniques) that have been researched and implemented to provide secure transmission of the information. These protocols can be classified into two broad categories, the first being encryption and cryptographic algorithms and the second being stenography. Encryption algorithm ensures who can access the data while the stenographic method to hide the person's encrypted confidential data into the person's biomedical signal. The ECG signal is used as a host signal and the size of an ECG signal is large compared to the information that needs to be embedded within. The watermarked ECG signal is now transmitted to the hospital. The size of the transmitted signal is the size of the ECG as the additional data that has been embedded will not act as an overhead. Any person can see the watermarked ECG signal but only the person with the shared key can access the confidential data that has been hidden inside the ECG signal.

Keywords: DCT, ECG, Confidential data, Hill Cipher Encryption