Abstract

The importance of secure message communication along with a brief literature survey has been presented in this thesis. Various encryption and spread spectrum modulation techniques have been discussed. Pseudo-noise (PN) sequences with their properties and implementation have also been described. Design and implementation of some novel circuits for secure and reliable message communication have been worked out and proposed in this thesis. Hardware modules of the proposed techniques have been tested in the laboratory for their viability.

Frequency Hopping Spread Spectrum (FHSS) modulation technique has been used in military applications since long due to various advantages including interference cancellation, Inter Symbol Interference (ISI) rejection and anti-jamming capability. Scrambling an FHSS signal increases its message hiding capacity. A new technique for frequency hopping spread spectrum called as Intermediate Digital Frequency Hopping Spread Spectrum (IDFHSS) has been presented, wherein the code bits for frequency hopping are obtained as a function of message bits. A modified IDFHSS system has been proposed incorporating scrambling of the FHSS signal.

Code Division Multiple Access (CDMA) is a modulation technique, wherein various users share a given frequency-band enabling efficient use of frequency spectrum at the cost of increased circuit complexity in terms of synchronization. A novel technique for Frequency Hopping Code Division Multiple Access (FH-CDMA) system with enhanced user capacity along with reduced synchronization complexity has been presented.
Complexity of PN-code sequences used for encryption as well as SS systems is of vital importance in military as well as commercial applications. In this thesis two novel techniques for the generation of code sequences with enhanced code complexity have been presented.

A novel method for the generation of an unpredictable key for low speed data encryption has been presented, wherein a signal received from a specific secret FM broadcast station is used to generate the necessary key used at the transmitter and at the authorized receiver. The proposed technique simplifies the problems for the generation of synchronous complex keys at the transmitter and at the intended receiver in a multi-user environment.

Pulse Time Modulation (PTM) techniques are found to be attractive for Optical Fibre (O.F) and Infrared (IR) wireless applications due to better power efficiency and less circuit complexity. However, data generated by many digital devices is generally in Pulse Code Modulation (PCM) form. Thus PCM-to-PTM converters are often needed for data transmission over O.F and IR wireless links. Two novel techniques for Pulse Code Modulation PCM-to-PTM conversion and vice-versa have been developed in this work. Transmission and reception of 3-bit PCM message has been experimented out using the proposed circuits. The proposed circuits have been modified to incorporate message security as well.

Prototype hardware modules of the proposed schemes presented in this thesis have been developed for experimental investigation. The thesis concludes with a discussion over the work done during the course of this research. A bibliography of concerned literature consulted has also been presented.