Chapter 7

Conclusion and Comments
7.1 Discussion and Conclusion

The work presented in this thesis has been aimed at implementation of some low-cost, efficient and secure message communication techniques. Some novel circuits implementing Frequency Hopping Spread Spectrum (FHSS) systems, Pseudo-noise (PN) sequence generators and Pulse Time Modulation (PTM) techniques have been developed. The proposed schemes have been implemented, using hardware modules, for experimental investigation.

Frequency Hopping Spread Spectrum (FHSS) modulation techniques are found to be simple and inexpensive as compared to Direct Sequence Spread Spectrum (DSSS) in terms of code synchronization. Besides hardware implementation, FHSS has been popularly used as an anti-jamming technique since World War II. The anti-jamming capability is determined by the type of the hopping used in the system. In a slow-FHSS technique, several bits (or symbols) are transmitted over single carrier frequency. This results into poor anti-jamming capability, however, utilizing lesser bandwidth and easy code synchronization. On the other hand, a good anti-jamming is achieved in fast-FHSS modulation technique, wherein each message bit (or symbol) is transmitted over several carrier frequencies. However, it takes a great deal of spectrum and involves complex circuitry to attain code synchronization in case of fast-FHSS. In Intermediate FHSS (IFHSS) technique, the hopping rate of the carrier is approximately equal to message bit rate. IFHSS offers moderate anti-jamming capability and utilizes a moderate bandwidth compared to slow and fast FHSS systems. A novel technique for Intermediate Digital Frequency Hopping Spread Spectrum (IDFHSS) has been
proposed in this thesis. The codes used to achieve frequency hopping are obtained as a function of previously transmitted message bits stored in a shift register. The output obtained from the proposed system is purely digital. The proposed digital FHSS system can be operated only in coherent environment. However, the technique can be implemented as a non-coherent analog FHSS system. The proposed technique has been tested in the laboratory with satisfactory results. Receiver circuit for the proposed IDFHSS system has been also implemented and the original message has been recovered faithfully.

Code Division Multiple Access (CDMA) is one of the main applications/advantages of SS techniques used for enhancing user capacity in a given geographical region. A new method for Frequency Hopping Code Division Multiple Access (FH-CDMA) has been presented with enhanced user capacity and an added advantage of reduced hardware complexity in terms of code synchronization. The proposed system has been implemented for two users. Demodulated FM signal received from a local broadcast station has been used as the required code to achieve spectrum expansion at the transmitter and the intended receiver. The FM demodulators, at the transmitter and the receiver, are tuned properly to maintain same frequency and amplitude level at any instant of time. The demodulated analog signals are next converted into digital form by using A/D converters. In case of a multi-user system, code converters are used to ensure a unique code for each user in the system. Since the same reference signal is received and digitized by all the users in the given multi-user communication system, a different code and hence a different frequency can be generated by all the users. Therefore the frequency used by a particular user at a particular instant of time can be used by another user at another instant of time with no interference.
Code selection has a large impact on the performance of a Spread Spectrum system. Longer the code, higher the process gain and hence better the interference rejection capability of a secure message communication system. Maximal sequences (m-sequences), a class of periodic sequences used as the spread code or key, have been discussed in detail. These sequences are generally generated by Linear Feedback Shift Registers (LFSRs) where the complexity of code depends upon the number of stages in the shift register. Gold codes, generated by combining the output of two m-sequences, provide better anti-jamming capability and message security. Besides these parameters, Gold codes perform better than m-sequences while attaining code synchronization between the transmitter and the receiver. However, in both m-sequence as well as Gold code generators, the feedback tapings of the shift registers are fixed, and hence can, sometimes, prove easy for a cryptanalyst or jammer to discover. Two novel techniques for the generation of m-sequences and Gold code sequences have been presented in this thesis, wherein the feedback tapings of the LFSRs change pseudorandomly. This enhances the anti-jamming capability and level of encryption at a relatively low-cost and reduced circuit complexity.

A new technique for the generation of unpredictable key has been presented in this thesis, which has been used for data encryption and decryption in a multi-user environment. The proposed technique simplifies synchronization problems involved in the generation of synchronous keys used at the transmitter and the receiver. In this technique, a signal from a local FM radio broadcast station has been used to obtain the secret code for implementing encryption/decryption at the transmitter/receiver. The proposed technique can be preferably used for short distance communication. The experimental results carried out over the hardware modules of the proposed system are found to be satisfactory.
Pulse Time Modulation (PTM) techniques, including Digital Pulse Position Modulation (DPPM) and Digital Pulse Width Modulation (Digital Pulse Width Modulation), are found to be attractive, in terms of power efficiency and reduced system complexity, for optical fibre and infrared communication systems as compared to Pulse Code Modulation (PCM). Further, since data generated by many digital devices is generally in PCM form, a PCM-to-DPPM or DPWM conversion is required if DPPM/DPWM is to be used for data transmission. In this thesis two novel circuits for PCM-to-DPPM and PCM-to-DPWM have been presented. The proposed circuits are inexpensive and very simple for laboratory demonstration and industrial use. Corresponding circuits for DPPM/DPWM-to-PCM conversion have also been implemented. The proposed circuit for PCM-to-DPPM conversion has been modified by incorporating encryption using a 3-stage PN code generator. The circuits have been tested experimentally in the laboratory and the results thus obtained have been fairly good.

Various secure and efficient communication techniques developed throughout the course of this study have been implemented using hardware electronic circuitry and tested for their performance. The results of experimental investigation presented in the thesis, in the form of photographs and sketches of various waveforms, prove the efficacy of the proposed techniques for their respective applications. Though the message security provided by most of the secure message communication techniques presented in this thesis may not be comparable to that provided by high end secure communication techniques, however, in many commercial applications, where the cost of information is not high, the proposed low-cost secure communication schemes have a high market potential.
7.2 Scope for Future Work

In this thesis some novel techniques for low-cost, efficient and secure message communication have been presented. The subject is, however, wide open for further research work towards the development of new techniques as well as the modification of the proposed circuits.

The proposed circuits have been implemented using medium scale integrated (MSI) and large scale integrated (LSI) circuits. The same techniques could be implemented by using single-chip Custom ICs and microcontrollers to enable more circuit reliability, cost efficiency and compactness for commercial use.

The proposed Intermediate Frequency Hopping Spread Spectrum (IFHSS) technique could be modified by combining it with the Time Hopping Spread Spectrum (THSS) technique to form a hybrid system. The thus developed technique would result into efficient utilization of power.

Instead of using demodulated FM signal, as a reference code for achieving spectrum expansion in the proposed FH-CDMA system, a secure digital signal can be transmitted among all the users for the generation of reference code. This will enhance the message hiding capability of the system. Further the proposed system has been tested for only two users for laboratory demonstration. The system could be checked for more number of users.