International Journal on Advanced Science Engineering Information Technology

Vol.6 (2016) No. 5
ISSN: 2088-5334

SNR Improvement and Bandwidth Optimization Technique Using PCM-DSSS Encryption Scheme

N. Sakib[#], A. Hira[#], M. N. Mollah[#], S. M. Sharun[*], S. B. Mohamed[*], M. A. Rashid[*]

[#] *Khulna University of Engineering & Technology, Khulna 9203, Bangladesh*
E-mail: sakib483@yahoo.com, avi_ece910@yahoo.com, mnnabi@eee.kuet.ac.bd

** FSTK, Universiti Sultan Zainal Abidin, 21300 Kuala Terengganu, Malaysia*
E-mail: marashid@unisza.edu.my; sitimaryam@unisza.edu.my, saifulbahri@unisza.edu.my

***Abstract*— Cryptography, the scheme of information stashing and verification, entirely deals with protocols, algorithms and strategies to ensure the precise security facility of the signal consistently by hindering unauthorized access to the confidential information. Albeit in most of the encryption schemes, certain impediments are faced by the service providers such as the expansion of required bandwidth, the fragile encryption technique, the consumption of maximum bandwidth in security purpose, less priority to improvement of SNR of the system, the complexity in decryption and so forth. This paper illustrates the SNR enhancement & bandwidth optimization technique in security purpose using PCM- DSSS sample by sample encryption scheme. For this purpose, after sampling of a signal, simple mathematical operation is performed in each sample with a time varying arbitrary weights. This arbitrary weight can be obtained from D/A conversion of pseudo noise sequence. Since the bandwidth consumption in security purpose can be minimized in this scheme, a significant portion of unused bandwidth can be used to improve the SNR of the system by reducing quantization noise of encrypted samples. By the same token, the possibility of SNR improvement is demonstrated by reckoning the quantization noise while introducing additional quantization step.**

***Keywords*— Encryption; Bandwidth; SNR; SQR.**

I. INTRODUCTION

Encryption, the process of encoding messages (or information), is the way to keep data unreadable to the eavesdroppers or hackers, but still readable to the authorized parties. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable format. This process is usually accomplished with the use of an encryption algorithm which specifies how the message is to be encoded. On the contrary, an authorized party, however, is able to decode the message or information using a decryption algorithm. Some modern techniques to accelerate communication speed and improve the bandwidth facilities are studied and referred to enhance the overall quality of the communication security [1-8]. In this course, Spread Spectrum (SS), the strategy primitively developed for the non-civil-military purposes, is an art to provide consistently the secure communication by spreading out the signal over a large frequency band. In a nutshell, SS Occupies a bandwidth that is much larger than the minimum bandwidth (1/2T) required transmitting a data sequence. In fewer words, the spectrum is spread by means of a pseudo-noise code in this purpose. The idea behind the SS is to use more bandwidth than the original message while keeping the signal power the same. An SS signal does not have a precisely distinguishable peak in the spectrum. This makes the signal much more enigmatic to figure out from noise and, therefore, more difficult to jam or interrupt. There are two predominant techniques to spread the spectrum: i) Frequency hopping (FH), ii) Direct sequence (DS).

A. DSSS bit generation

The DSSS modulation is very convenient and lucrative technique to attain the secure communication, principally, because of its intransigence to interference and minimal probability of detection [9]. In DSSS Scheme, the rapid phase transition of data engaged it within larger bandwidth. Since the time span of a signal gets shorter (or data rate increases), the bandwidth of the signal augments in a similar fashion [10]. DSSS modulation multiplies the data bit rate when transmitting the original signal as a "noise" signal. Literally, this noise signal is a pseudorandom sequence of 1 and −1 values at a frequency much greater than that of the original signal. The DSSS encoded bit pattern and expansion

of signal in required transmission bandwidth are depicted in Fig. 1.

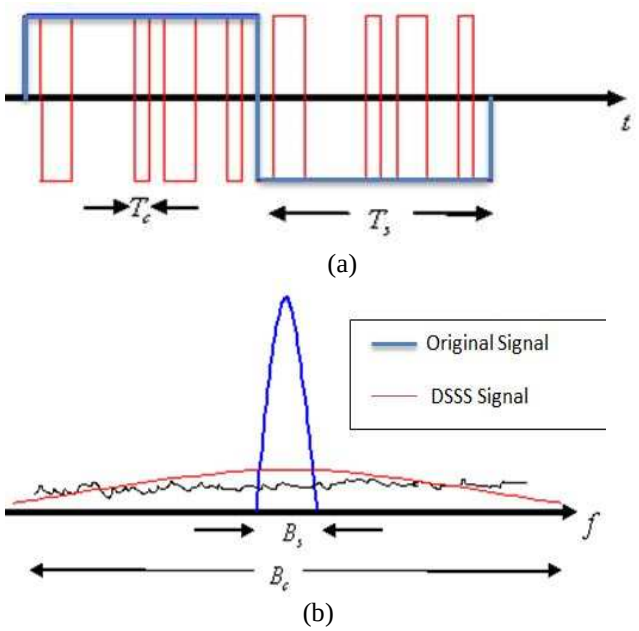


Fig.1: a) DSSS encoded bit, b) spreading in transmission bandwidth.

B. DSSS in voice transmission

Audio signal is analog valued, like all other naturally demonstrated signal, irregular in pattern, and can't be characterized by particular mathematical model or expression. It is transmitted in the form of digital sequence by performing three precise steps- sampling, quantizing and encoding. These three specific operations on an analog signal in a single scheme are generally cognized as Pulse Code Modulation (PCM). In order to assure user immune communication, DSSS encoding is relied upon PCM bit pattern. The entire procedure is illustrated in Fig. 2.

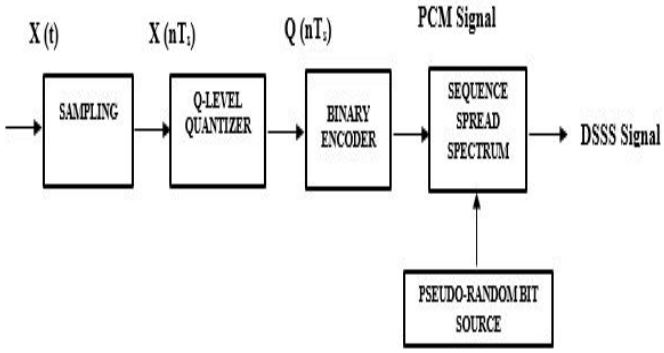


Fig.2: DSSS encoding scheme for voice signal.

1) Sampling

The conversion of an analog voice signal into a digitized pulse train is initiated with regular sampling of the audio signal at uniform intervals. These periodic spells are determined by the conventional Nyquist Sampling Theorem. It delineates the probability to reconstruct the sampled signal such that any signal may be successfully re-constructed from its representative samples if it is sampled at minimum twice of the maximum frequency regarding the interest. Satisfying the Nyquist theorem, the typical telecommunication system is designed at worldwide standard of 8 kHz sampling, since all voice signals are band-limited to 4 kHz.

2) Quantizing & Encoding

The samples still illustrate the voice signal in discrete time valued analog pattern. For precise digital representation, two additional steps are required. The first following step is quantization, where each sample is assigned by some specific quantizing interval. Therefore, the output of the quantizer is titled as the discrete time – discrete valued signal or simply as digital signal [11]. The second phase of the conversion process to obtain binary PCM data for transmission involves the encoding of the 256 quantizing intervals assigned to individual PAM samples in 8-bit binary words (7 data bits and 1 sign bit).

BIT NUMBER	1	2	3	4	5	6	7	8	
BIT WEIGHT -MSB	±	2^6	2^5	2^4	2^3	2^2	2^1	2^0	LSB

3) Quantization Noise & SQR

The error introduced in the signal due to the inefficiency of quantization process is called Quantization error. It can be denoted mathematically by

$$\epsilon = X_q(nT_s) - X(nT_s) \quad (1)$$

Let, an input signal has amplitude in the range of $-X_{max}$ to X_{max}. The total amplitude range is $2\ X_{max}$. If 'v' bit is used to represent every sample, then total quantization level q is related by, $q=2^v$. And quantization step is denoted as, $\Delta = 2X_{max} / 2^v$. The quantization noise power $N_q = \Delta^2/12$ [12].

Now, the signal to quantization noise ratio is given as:

$$\frac{S}{N_q} = \frac{\textit{Normalized signal power}}{\textit{Normalized noise power}} = \frac{3P * 2^{2v}}{X_{max}^2} \quad (2)$$

From the above mathematical alliance, it is very obvious to point out that, if the number of bits to represent each sample (v) is increased, a significant diminution in quantization noise as well as improvement in signal to noise ratio (SNR) can be demonstrated.

C. DSSS data rate

In DSSS scheme, each of PCM bits is represented by several bits to assure explicit security that provides jamming. Hence, the data rate of DSSS depends entirely on the PCM data rate and the spreading factor. In conventional voice telephony, standard PCM consumes 8 KHz of sampling frequency and 8 bits of encoder that results a data rate of 64 kilo-bit per second. Consequently, the DSSS data rate is M times higher than 64 Kbps. Therefore, a 10 bit spreading code spreads the signal across a frequency band that is 10 times greater than PCM code. The more the bit is used to represent each binary data bit, the more the security of the SS scheme can be demonstrated. At the same time, on the

contrary, it increases the total number of bits to be transmitted over the communication channel.

D. Limitations of conventional DSSS scheme

It is a common concern that all practical communication channels are band limited. The required channel bandwidth and bit rate of any binary sequence are directly proportional to each other [13]. In order to ensure reliable data transmission, the minimum channel bandwidth required should be half of the bit rate. So, transmission bandwidth required in DSSS is "M" times higher than the original binary signal obtained from the PCM. The cardinal objective of DSSS scheme is to provide a high level confidentiality, integrity, and authenticity for the transmission of signal exchanged over networks. But, it consumes the major portion of channel bandwidth in security purpose. Consequently, it diminishes the scope of facilitating more users in a particular communication channel.

Again, PCM signal deteriorates from quantization noise due to the usage of q-level quantizer. Hence, signal to quantization noise ratio (SQR) is considered as a substantial factor in voice telephony. SQR can be enhanced by increasing the quantization level. On the other hand, expansion of encoding bit raises the PCM as well as DSSS data rate that results in a larger bandwidth requirement. According to Shannon's second theorem, commonly known as noisy channel coding theorem, it is evident that for reliable data communication over a noisy channel data rate must be less than the channel capacity [17]. Where, capacity (C) of any channel depends on signal to noise ratio of the signal to be transmitted over the channel. The mathematical relationship between channel capacity and SNR can be related as C = log (1+ SNR). Therefore, by improving SNR, capacity as well as transmission rate over the noisy channel can be augmented.

II. MATERIALS AND METHODS

In the era of modern digital world, the question of data security, like the other salient issues in communication engineering, gets notable priority to the service provider by reason of the expeditious advancement of digital communications and networking technologies. To illustrate, the data protection methodology is inherently involved with the cryptographic primitives for secure data transmission and reception by assuming that both sides must trust each other. DSSS is a well-known and widely practiced cryptographic standard since 1980. But, at the movement of advances, this method experiences certain disadvantages of promoting limited scope to facilitate user over any communication channel having fixed bandwidth. Besides, it produces significant quantization error due to the limited quantizing step of PCM.

A. Bandwidth optimization

The conventional DSSS scheme operates bit by bit encryption, which augments the total transmission bandwidth. The complication for undesired enhancement of bandwidth in DSSS scheme can be solved exclusively by introducing novel sample by sample encryption technique [14-15]. In this scheme, the voice signal undergoes through sample by sample encryption instead of bit by bit encryption. The samples can easily be modified into a different pattern from which it is possible to return back to the origin for the authorized receiver. The encrypted sample pattern can be obtained using an appropriate algorithmic approach. After quantizing and encoding these encrypted samples, a bit pattern will be obtained which is quite different from the original bit pattern. The signal samples can be modified by simple mathematical operations such as addition, subtraction, multiplication, division sequentially over a finite period with arbitrary weights. The weights may be either constant [16] or continuously varying over the entire range of encryption. In the meantime, varying arbitrary weight can also be generated by the pseudo noise generator and D/A converter of fixed length bit stream [18].

If the full scale and the quantization steps or the number of bits to represent each level is permitted as equivalent as binary PCM, then the total number of encrypted bits will be as invariable as the original binary PCM signal. So, it is evident that the signal will be encrypted, but the total number of bits will remain unchanged. In brief, the sample by sample encryption scheme spends zero bandwidth in security purpose. The generalized steps of the sample by sample encryption scheme are depicted in Fig. 3.

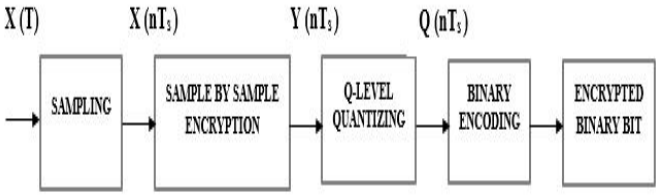


Fig.3: Block diagram of sample by sample encryption scheme.

B. SNR Improvement

From the above discussion, it is very evident that the encryption of samples doesn't consume a single portion of allocated bandwidth in security purpose. Hence, this conserves a large amount of bandwidth compared to the DSSS. In DSSS scheme of spreading factor 5, security purpose adopts a data rate of 256 Kbps to implement the encryption policy. But, using PCM-DSSS sample by sample encryption scheme, it spares 256 Kbps data rate as well as a bandwidth of 128 KHz. Now, this stored data rate can be utilized in SNR improvement, more accurately in SQR improvement function, by curtailing quantization noise where additional bit will be used to represent each encrypted sample. According to the conventional PCM theorem, each additional bit in encoder adopts 8 Kbps data rate while enhances 6 dB of SQR as well as SNR. From this indubitable argument, it is obvious that PCM-DSSS sample by sample spares 256 kbps of the data rate that may spend in security purpose. Now, this managed data rate can be utilized in SNR improvement. Hence, one or more bit can be added in encoding. The proposed modified method of PCM-DSSS scheme for SNR improvement and bandwidth optimization is figured out in Fig. 4.

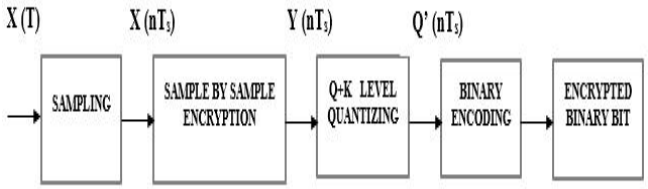


Fig.4: Modified PCM-DSSS scheme for SNR improvement.

Here, K represents the number of additional bits applied to SNR improvement purpose. The larger the value of K, the more the SNR will be enhanced. Therefore, Data rate can be compressed significantly by using these techniques.

III. Result and Discussion

This section demonstrates the numerical validation and observation. The conventional PCM has a data rate of 64 Kbps that demands a transmission bandwidth of 32 KHz. In this paper, a modified PCM-DSSS sample by sample encryption technique is proposed that suggests encoding of every sample with an encoding subsystem of more than 8 bits to revamp the signal to quantization noise ratio. Since the pictorial representation of 8 bit or more than 8 bit encoder is rarely possible, the mathematical validation of PCM-DSSS scheme for SNR improvement by rigorous calculation of data rate, transmission bandwidth and allocation of voice channel for any communication channel of fixed bandwidth can be a reasonable alternative to verify our assertion.

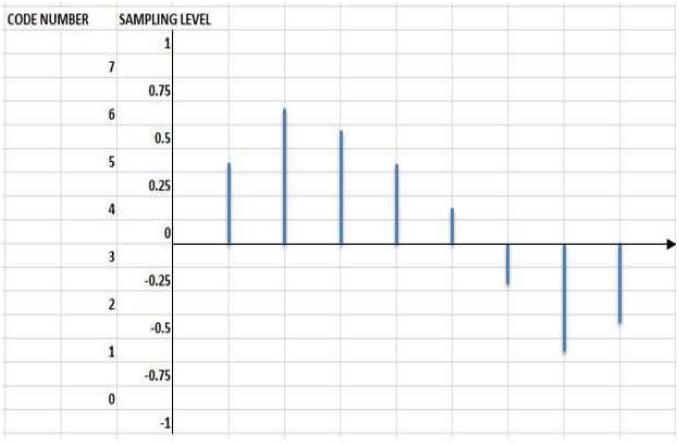
A. Bandwidth optimization

Assume, DSSS scheme having a spreading factor of 5 is applied to conventional PCM scheme and it generates a data rate of 320 Kbps that requires a bandwidth of 160 KHz. Though protection of information over the communication channel is very much challenging, the imprudent consumption of valuable bandwidth is surely undesirable. In brief, the sample by sample encryption scheme conserves the bandwidth of 128 KHz. Now, the extent of conserved bandwidth can be introduced as the scope of SNR improvement. If we apply 10 bit encoder, then required transmission bandwidth will be 40 KHz. It is 8 KHz higher than standard PCM scheme, but 120 KHz lower than DSSS. In the meanwhile 12 dB of SNR will be enhanced.

This recommended scheme can bolster more number of voice channel utilization. Suppose, for any communication channel having a bandwidth of 5 MHz, DSSS scheme (spreading factor 5) accommodates 31 voice channels while the modified 10 bit PCM-DSSS will accommodate 125. This comparison bolsters the endeavour of cost effective approach of this proposed scheme. In this discussion, to keep the theory and its justification simple, a DSSS scheme is assumed to have spreading factor of 5. But, in practical application more spreading ranges are widely used. The proposed scheme could be absolutely effective while spreading factor is equal or more than 2.

B. SNR improvement

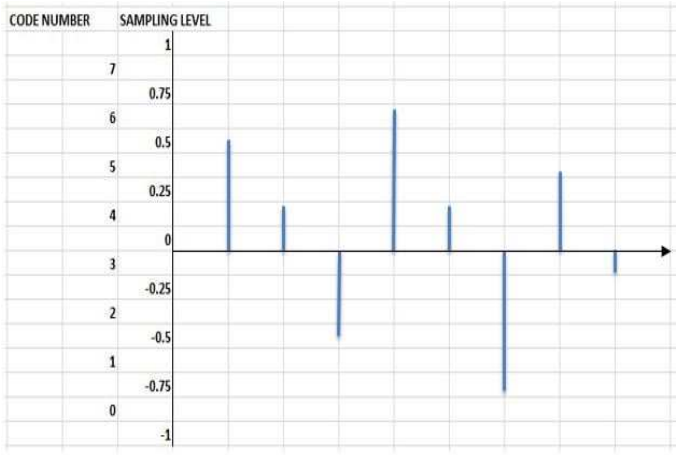
Possibility of SNR improvement using PCM-DSSS sample by sample encryption technique is illustrated by speculating 3 bit encoder as standard and 4 bit encoding scheme for our proposed SNR improvement technique. A typical 8 discrete samples and their PCM bits are depicted in Fig. 5. The PCM bit in serial transfer will be 001001010100101101110101. Hence, quantization noise power ($\Delta^2/12$) is -22.83 dB.



SAMPLE VALUE:	0.42	0.71	0.59	0.41	0.17	-0.22	-0.56	-0.41
QUANTIZED VALUE:	0.50	0.75	0.50	0.50	0.25	-0.25	-0.50	-0.50
CODE NUMBER:	5	6	5	5	4	2	1	1
BINARY CODE:	101	110	101	101	100	010	001	001

Fig. 5: 3 bit PCM coding.

Now, let the signal be encrypted using a repetition of 4 samples while operators are chosen in the sequence of division (/), subtraction (-), multiplication (*) and addition (+) with a fixed arbitrary weights of 0.73, 0.49, -0.72 and 0.31 according to the methodology described in [8].



SAMPLE VALUE:	0.57	0.22	-0.42	0.72	0.23	-0.71	0.40	-0.10
QUANTIZED VALUE:	0.50	0.25	-0.50	0.75	0.25	-0.75	0.50	0
CODE NUMBER:	5	4	2	6	4	1	5	3
BINARY CODE:	101	100	010	110	100	001	101	011

Fig. 6: Encrypted samples of 3 bit encoding scheme.

The encrypted samples are demonstrated in Fig.6 [10]. Consequently, after applying encryption technique, the bit streams are readily found as 011101001100110010100101, which is completely different from the original one which validates efficacy of the encryption of samples. It produces the same noise contribution (-22.83 dB) as the original one. In this standpoint, more than 3 bit encoding scheme is to be introduced to scale down the quantization noise. Four bit encoding scheme for SNR improvement of encrypted signal are illustrated in Fig. 7.

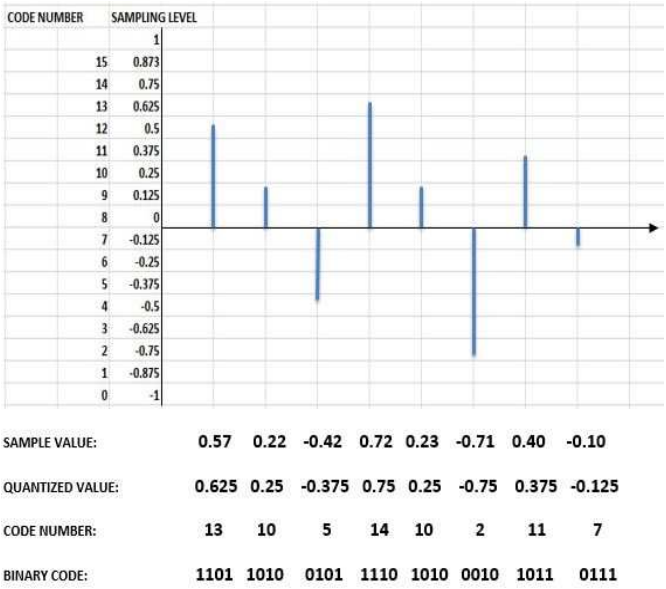


Fig. 7: Encrypted samples of 4 bit encoding scheme.

Now, the adjusted bit sequences are 011110110010101011100101101101101 and the demonstrated noise power is 28.85 dB. A significant attribute is investigated that any change in encoding scheme i.e. change in number of bits to represent every sample will result in a notable change in bit pattern. Though sample by sample encryption scheme spares a considerable amount data rate, it is fairly possible to choose a random number of additional bits (K) in SNR improvement purpose. Since different values of K will result in different bit sequences, so it is very appreciable to inspect it as an additional security parameter in sample by sample encryption scheme to keep the confidential information more enigmatic to pick upon it for the eavesdroppers.

C. Reduction in bit error probability

Channel noise has great influence on the time duration of the signal passing over it [12]. The higher rated data possess shorter duration which is roughly corrupted by channel noise. Noise component, finite in time, affects more number of bits of any representative signal having a larger data rate than lower one that tends to increase the probability of bit error as well as bit error rate. The sample by sample encryption scheme has a data rate lower than conventional DSSS. Therefore, the bit error probability of the proposed encryption scheme will be lower than DSSS. In Fig. 8 a noise element of 47 µS is illustrated which will corrupt 3, 15 and 4 bits of standard PCM, 5 bit DSSS and 10 bit PCM-DSSS respectively.

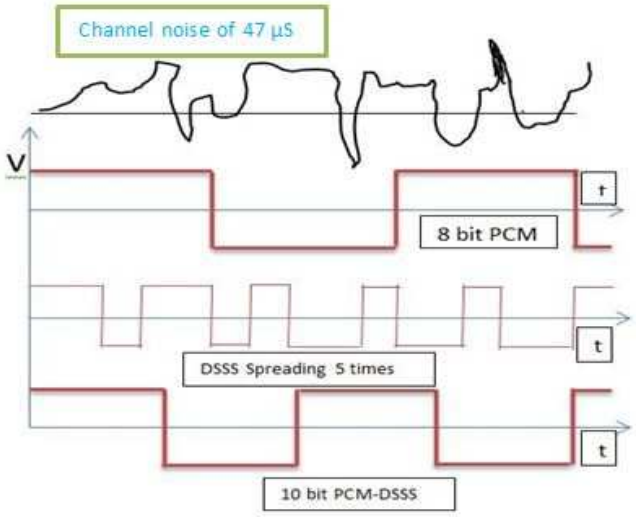


Fig.8: Comparison of bits corrupted by channel noise.

IV. CONCLUSIONS

In this paper, a mere adjustment in PCM-DSSS sample by sample encryption technique is illustrated to introduce the possibility of SNR improvement, reduction of probability of bit error by utilizing more the data rate/bandwidth in encoding subsystem available due to the selection of sample by sample encryption rather than conventional DSSS. The proposed scheme is much cost effective in the aspect of the voice channel allocation. The sample by sample encryption scheme assures strong security by providing a wide range opportunity of varying security parameters. Beside those, this recommended proposal adds another security parameter; K number of additional bits participates in SNR improvement purpose. The larger the value of K is, the more the SNR will be enhanced in the acceptable range. Though several uncomplicated theory based numeric enumerations and pictorial representations are illustrated, it is very evident that modified PCM-DSSS scheme can improve the SNR and optimize the bandwidth by allowing additional bits in encoding subsystem. Besides that, some modern techniques to accelerate communication speed and improve the bandwidth facilities are studied and referred to enhance the overall quality of this proposal.

ACKNOWLEDGMENT

The Authors would like to acknowledge the financial and technical supports from Khulna University of Engineering and Technology (KUET), Bangladesh and the Universiti Sultan Zainal Abidin (UniSZA), Malaysia for the completion of the research work successfully.

REFERENCES

[1] J. Liu, X. Xu, Q. Wu, J. T. Sheridan, and G.Situ, "Information encryption in phase space," Opt. Lett. vol.40, pp. 859-862, 2015.

[2] X. Kang, R. Tao and F. Zhang, "Multiple-parameter discrete fractional transform and its applications," IEEE Transactions on Signal Processing, vol. 64, no. 13, pp. 3402-3417, July1, 1 2016. doi: 10.1109/TSP.2016.2544740

[3] S. Sharma, L. Kumar, H. Sharma, “Encryption of an Audio File on Lower Frequency Band for Secure Communication”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 7, 2013.
[4] J. Choi, "Secure Transmissions via Compressive Sensing in Multicarrier Systems," IEEE Signal Processing Letters, vol. 23, no. 10, pp. 1315-1319, Oct. 2016. doi: 10.1109/LSP.2016.2595524
[5] G. Ye and X. Huang, "An Image Encryption Algorithm Based on Autoblocking and Electrocardiography," IEEE MultiMedia, vol. 23, no. 2, pp. 64-71, Apr.-June 2016. doi: 10.1109/MMUL.2015.72
[6] S. M. T. Nezhad, M. Nazari and E. A. Gharavol, "A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks," IEEE Communications Lett., vol. 20, no.4, pp.700-703, April 2016. doi: 10.1109/LCOMM.2016.2517622
[7] G. Li and S. Lyu, "Extracting Chaotic Signal from Noisy Environment: A Random Searching Method," Chinese Journal of Electronics, vol. 24, no. 3, pp. 584-589, 07 2015. doi: 10.1049/cje.2015.07.025
[8] G. Ye and X. Huang, "An Image Encryption Algorithm Based on Autoblocking and Electrocardiography," IEEE MultiMedia, vol. 23, no. 2, pp. 64-71, Apr.-June 2016. doi: 10.1109/MMUL.2015.72
[9] S. Rajanarayanan, A. Pushparaghavan, “Recent developments in signal encryption–A critical survey”, International Journal of Scientific and Research Publications, vol. 2, no. 6, 2012.
[10] B. Scheers and V. L. Nir, “A Modified Direct Sequence Spread Spectrum Modulation Scheme for Burst Transmission”, CISS Department, Royal Military Academy, Belgium.
[11] S. Ma, L. Nguyen, W. M. Jang, Y. Yang, “Multiple-Input Multiple - Output Self-Encoded Spread Spectrum System with Iterative Detection”, in Proc. IEEE ICC 2010, 2010.
[12] W. Stallings, 8th Ed., Data and Computer Comm unications, Prentice Hall Of India Private Limited, 2010.
[13] R. Bose, 2nd Ed., Information Theory, Coding and Cryptography, The McRraw-Hill Companies, 2013.
[14] A. Hira, N. Sakib, N. Sarker, “PCM Based Audio Signal Security System”, In Proc. ICAEE 2013, Dhaka; Bangladesh.
[15] A. Hira, N. Sakib, N. Sarker, M. N. Mollah, S. B. Mohamed, M. A. Rashid, “A Novel Approach to Signal Encryption: Improved Version of Conventional DSSS Scheme”, Adv. Sci. Lett., vol. 20 (10-11), pp. 1824-1828, Oct 2014.
[16] T. Song, K. Zhou and T. Li, "CDMA System Design and Capacity Analysis Under Disguised Jamming," IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2487-2498, 2016, doi: 10.1109/TIFS.2016.2585089
[17] S. Parvez, N. Sakib, M. N. Mollah, “Advanced investigation on EBG structures: A critical analysis to optimize the performance of asymmetric couple-line bandpass filter”, in Proc. ICEEICT 2015, 2015.
[18] S. Haykin, 6th Ed., Digital Communications, John Wiley & Sons.