International Journal of Technology 10(5): 953-960
ISSN 2086-9614 © IJTech 2019

A NEW METHOD FOR BUILDING LOW-DENSITY-PARITY-CHECK CODES

Tehami Mohammed Amine[1*], Djebbari Ali[1]

[1]*Telecommunications and Digital Signal Processing Laboratory, Djillali liabes University of Sidi Bel Abbes, Algeria*

(Received: December 2017 / Revised: February 2019 / Accepted: October 2019)

ABSTRACT

This paper proposes a new method for building low-density-parity-check codes, exempt of cycle of length 4, based on a circulant permutation matrix, which needs very little memory for storage it in the encoder and a dual diagonal structure is applied to guarantee that parity check bits can be recursively computed with linear calculation complexity. The Bit Error Rate performance of the new low-density-parity-check codes was compared to the uncoded bi-phase-shift-keying over additive-white-gaussian-noise channel. This simulation shows that the proposed codes are very efficient over additive-white-gaussian-noise. The proposed codes ensure a very low encoding complexity and reduce the memory storage required for the parity-check matrix, which can be more easily built than others codes used in channel coding.

Keywords: Circulant permutation matrix; Dual-diagonal matrix; Girth; Low-density-parity-check codes; Parity-check matrix

1. INTRODUCTION

Because of their prodigious performance, low-density-parity-check (LDPC) codes are now considered optimal (Gallager, 1962). These codes are a part of linear block codes which have acquired considerable importance in error correcting performances (Yahya et al., 2009). LDPC codes can be presented by specific parity check matrix H that includes a high density of 0'-s and a low density of 1'-s (Mackay, 1999). The Tanner graph (Tanner, 1981) is a bipartite graph comprising two groups of nodes: the variable nodes and check nodes. Variable nodes depicting columns and rows are represented by check nodes and connections between these two sets are known as edges (Tanner, 1981; Juwono et al., 2013). In the Tanner graph, a cycle is defined as a path which starts and ends at the same node, if the graph contains a cycle; its minimum length is known as 'girth' (Tanner, 1981). Cycles especially those of length 4 decrease the bit-error-rate (BER) performance of LDPC codes, because of their impact on the independence of extrinsic information exchanged in the decoding process (Johnson & Weller, 2001). Gallager codes are classified: as regular if the weight of columns and rows (i.e. density of 1's) is constant and as irregular if column weight and row weight are variable (Yahya et al., 2009).

The construction of these codes is of two types; the first is random construction that is flexible in design and construction (Mackay, 1999). The parity-check matrix is a superposition and/or concatenation of sub-matrices and this construction has significant drawbacks in term of the stocking and accessing a large parity-check matrix. As random building does not guarantee small cycle lengths, a second form of construction was developed; this is known as deterministic construction (Moura el al., 2004; Shin et al., 2014).

*Corresponding author's email: chahoub_88@yahooo.com, Tel. +213-662-810521

Permalink/DOI: https://doi.org/10.14716/ijtech.v10i5.1144

In this paper, we depict a particular category of LDPC codes, excluding cycles of length 4, which can be linearly coded by matrix H. The parity check matrix is divided into two sections: the first, which matches to the parity bits, is a dual-diagonal structure (Guolei & Dong, 2010) and the second, which matches the information bits, is a quasi-cyclic structure. For that reason, this new LDPC code is classified as irregular code.

This paper is organized as follows. Section 2 discusses the construction of the new LDPC code based on a quasi-cyclic and a dual diagonal matrix. In section 3, we propose a deterministic rule for constructing parity-check matrix with various rates. Section 4 describes the LDPC reduced-complexity encoding method, and section 5 discusses decoding complexity. Section 6 specifies the advantages of the proposed method, followed by conclusions in Section 7.

2. PROPOSED CONSTRUCTION OF MATRIX *H*

Girth is one of the most important factors affecting the performance of LDPC code (Gallager, 1962; Liu et al., 2009). As several studies have shown that a small girth (generally of length 4) affects the decoding process. Therefore, many researches on building a LDPC code with girth large (greater than 4) are still used for various applications (Tanner, 1981).

Let *H*, the parity-check matrix, have a size *M* by *N*. where *M* is the number of rows and *N* is the number of columns. This matrix can be represented in the following form:

$$H = [H^d \; H^p] \tag{1}$$

where *c* is a codeword written as *c* = [*d p*], the parity relationship (Ping et al., 1999) is written as:

$$Hc^T = 0 \tag{2}$$

where *d* and *p* refer to the data and parity bits respectively (Lin et al., 2008).

H^p is a dual-diagonal matrix of size *M* by *M* that can be represented as follow

$$H^p = \begin{bmatrix} 1 & & & 0 \\ 1 & 1 & & \\ & \ddots & \ddots & \\ 0 & & 1 & 1 \end{bmatrix} \tag{3}$$

H^d is a matrix of size M by $(N - M)$. The proposed method can be constructed in two steps:

2.1. Step 1: Construction of Initial Matrices

First, an identity sub-matrix *I* of size *m*×*m* is generated, where m must be greater than 2. Next, another sub-matrix called *S* of size *m*×*m* is generated which is symmetrically constructed in relation to rows of *I* with the elements $S_{i,j}$, $1 \le i \le m$ and $1 \le j \le m$, defined as:

$$S_{i,j} = I_{(m+1-i),j} \tag{4}$$

where $I_{i,j}$ are elements of identity sub-matrix *I*.

The following is an example for *m* = 3

$$I_{3x3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The obtained sub-matrix *S* is:

$$S_{3x3} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

2.2. Step 2: Construction of Matrix H^d based on a Quasicyclic Matrix

Making a permutation of *S* (from right to left) by *n* locations, where *n*, represents the number of sub-matrices and must be inferior to *m*, the matrix H^d can be written as

$$H^d = \begin{bmatrix} I & I & \cdots & I \\ S_{p(1)} & S_{p(2)} & \cdots & S_{p(n)} \end{bmatrix} \tag{5}$$

where *Sp(n)* is the n^{th} permuted version of *S*.

It follows that H^d *is* a matrix of size $2m \times (n \times m)$.

In the above example, there are two permuted versions:

$$S_{p(1)} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$S_{p(2)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

H^d of size 6×6 can then be represented as follows:

$$H^d = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

and the matrix *H* can be represented as:

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Figure 1 shows the bipartite graph of matrix *H* :

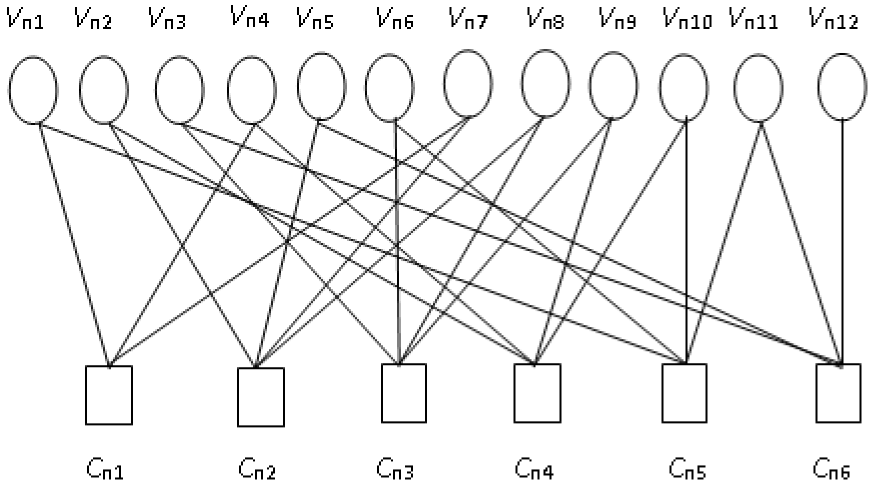

Figure 1 Tanner graph of matrix H

3. LDPC CODES CONSTRUCTION FOR VARIOUS RATES

Based on the proposed method, the size of matrix H is $(N-k)\times N$, where K represents data length and N represents codeword length and $N = K + M$.

$R=\frac{K}{N}$, where R represents code rates. To obtain various rates, H^d must be constructed using the following rule:

Let n be an integer inferior to m where N must divide $(n+2)$.

Table 1 presents the detail of these codes.

Table 1 Various-rate LDPC codes constructed using the proposed method (without cycle 4)

n	R	m	$N=m(n+2)$	$M=(2m)$	$K=(n\times m)$
2	1/2	10…80…576	40…320…2304…	20…160…1152…	20…160…1152…
4	2/3	10…80…576	60…480…3456…	20…160…1152…	40…320…2304…
6	3/4	10…80…576	80…640…4608…	20…160…1152…	60…480…3456…
8	4/5	10…80…576	100…800…5760…	20…160…1152…	80…640…4608…

4. ENCODING CONCEPT

Comparing column-weights of 2 and at least 3, Gallager found that the minimum distance increases logarithmically with code length. However, the minimum distance increases linearly with code length when column weight is at least 3 (Gallager, 1962). These codes have proved efficient in several domains, such as partial response channels (Song et al., 2002; Song et al., 2004). Additionally, these codes require less computation by virtue of their column weight.

Despite their excellent performance, hardware implementation of these codes is challenging because of the random of row-column connections and large size of LDPC codes (Malema & Liebelt, 2007), despite their performance has been proved to be great (Malema & Liebelt, 2007). The complexity of hardware implementation has been reduced by using structured codes (Malema & Liebelt, 2007), and girth (smallest cycle) has been decreased by introducing the constraint of row-column connections (Fossorier, 2004). It has been shown that when girth increases, decoding performance increases also improves (O'Sullivan, 2006; Mao & Banihasherni, 2001). Girth determines also determines which path starts and ends at the same node. In general, increased girth improves the performance of structured codes.

Based on Equations 1 and 2, results:

$$[(H^{d})_{(2m).(N-2m)}(H^{p})_{(2m).(2m)}][d\,p]^{T}=0 \tag{6}$$

$$H^{d}d^{T}=H^{p}p^{T} \tag{7}$$

$$p^{T}=(H^{p-1}H^{d})d^{T} \tag{8}$$

As H^p is always a dual-diagonal matrix, it is always invertible.

Based on the structure of H^p and Equation 6, for a given data $d=\{d_i\}$ as in (Ping et al., 1999), the parity-check bits $p=\{p_j\}$ are easily computed:

$$p_1=\sum_j h_{1j}^{d}\,d_j \tag{9}$$

and

$$p_i=(p_{i-1}+\sum_j h_{ij}^{d}\,d_j\,)\;mod\;(2) \tag{10}$$

where h^{d}_{ij} are the elements of H^{d}.

A comparative study of LDPC code has shown that there are several advantages if parity-check matrix H is broken into $H = [H^{d} \;\; H^{p}]$, where H^{p} has a dual-diagonal structure (Ping et al., 1999).

- H^{p} is always invertible (non-singular); the method yields in any given rate directly and precisely.
- Gaussian elimination is not necessary for encoding.
- When H^{d} is sparse, the parity-check matrix H requires very little memory to stock the data in the encoder.
- Additionally, this method has the following advantages.
- The use of permutations matrices in the proposed H^{d} considerably reduces required-storage memory.
- H^{d} is proposed because of the very low encoding complexity when H^{d} is effectively sparse.

5. DECODING COMPLEXITY

The decoding complexity of LDPC codes is dependent on the number of branches '*Br*' in the Tanner graph or on the number of '1's in the parity-check matrix (Berrou, 2010). The iterative decoding algorithm 'Belief propagation' includes several steps. At each step, the extrinsic and total information associated with the corresponding node must be calculated (Divsalar et al., 2009). In the case of a regular code (N, W_c, W_r), where W_c and W_r represent the number of rows and the number of columns respectively, the number of branches '*Br*' is:

$$B_r = W_c \times N = W_r \times M \tag{11}$$

Table 2 compares the number of branches of the proposed LDPC codes with: the Gallager (1962) and Mackay (1999) codes.

Table 2 Comparison of proposed LDPC codes with Gallager codes and Mackay codes (by number of branches)

Block length	Proposed LDPC	Gallager codes	Mackay codes
N = 500 and M = 250	B_r = 999	B_r = 1500	B_r = 1500
N = 1000 and M = 500	B_r = 1999	B_r = 3000	B_r = 3000

Table 2 shows that the new LDPC codes have a fewer branches than the Gallager and Mackay codes, indicating that the proposed parity-check matrices H are of reduced density (i.e. fewer 1s than 0s), in turn reducing decoding complexity.

6. SIMULATION RESULTS

Monte Carlo simulations were used to evaluate the BER performance of LDPC codes. Iterative belief propagation and AWGN (additive white Gaussian noise) were employed as the decoding algorithm and channel, respectively. For simulation purposes, we used the rate ($R = {}^{1}/_{2}$) and block length (N = 504). The simulation was run for at least 10^{3} code-words, with a maximal iteration of 80.

The performance of the new LDPC code is presented for comparison with other LDPC codes. Signal-to-noise-ratio (*SNR)* for the coded and the uncoded bi-phase-shift-keying (BPSK) were defined as in (Moura et al., 2004); for the former, $SNR_1 = 10\log_{10}(E_b/2\sigma^2 R)$ and for the latter, $SNR_2 = 10\log_{10}(E_b/2\sigma^2)$, where E_b and σ^2 represent energy per bit and noise variance, respectively.

Figure 2 shows BER performance of the proposed LDPC codes and the uncoded BPSK with $N = 504$, W_c=2 (where W_c, is column weights) and $R = {}^1/_2$. For the BPSK modulated system in a Gaussian channel $BER = Q(\sqrt{SNR})$.

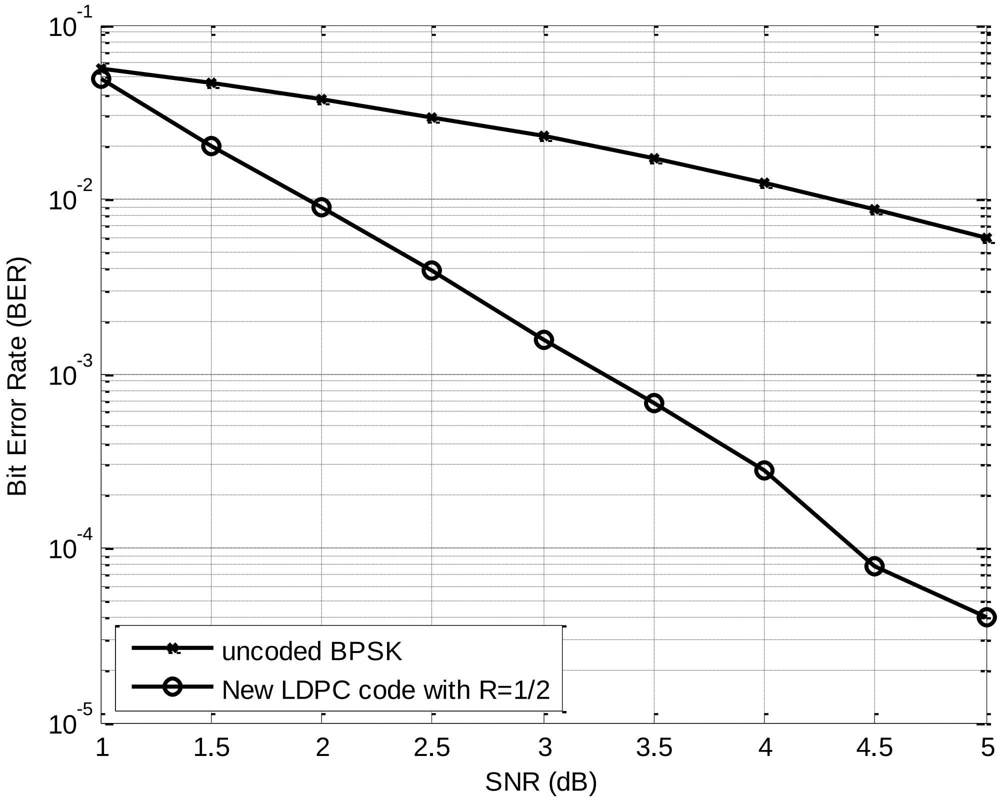

Figure 2 Bit-error-rates of the proposed LDPC codes and the uncoded BPSK (N = 504, W_c = 2, R = ½)

Table 3 compares the BER performance of the proposed LDPC (N = 504, W_c) with two other LDPC codes: Progressive Edge Growth (PEG) and Quasi-Cyclic (QC).

Table 3 Comparison of BER performance of proposed LDPC codes with PEG-LDPC and QC-LDPC

BER	Proposed LDPC codes	PEG-LDPC (E_b/N_0)	QC-LDPC
10^{-2}	2	3.15	3.15
10^{-3}	3.25	3.7	3.7
10^{-4}	4.4	4.2	4.1

N_0 is the one-sided power density spectrum of the additive white Gaussian noise

Table 3 shows the proposed codes exhibit performance gains of about 1.65 dB and 1.3 dB when compared to the PEG codes and QC codes, respectively, at a BER of 10^{-2}. The proposed LDPC codes perform better than the PEG codes by 0.3 dB at a BER of 10^{-3} over the AWGN channel; this significant BER performance gain owes to simple encoding and the exclusion of girth 4.

At a BER of 10^{-4} the proposed LDPC show only 0.1 dB loss in BER performance when compared to the random PEG codes, which are considered excellent for transmitting short blocks on the AWGN channel. This, confirms that the proposed LDPC codes' uniform construction and low complexity hardware implementation (based on fewer logic gates and simple shift registers), return an error rate performance similar to or slightly better than complex unstructured LDPC codes. Importantly, forward error correction coding for cellular technologies in the Third Generation Partnership Project (3GPP) (Asvial et al., 2015) will be recorded by new radio access (NR) (Richardson & Kudekar, 2018). The LDPC codes have replaced turbo codes in the third and fourth generation (3G, 4G) (Suryanegara & Miyazaki, 2012) and fifth generation (5G) coding schemes (Richardson & Kudekar, 2018).

7. CONCLUSION

To address quality of reception and implementation constraints, LDPC code must be constructed with a low error floor, linear encoding and less complex decoding. This paper proposes a new method for constructing parity-check matrix that include girths of length 4, for different rates. Memory requirements are significantly reduced by the use of the quasi-cyclic matrices and dual- diagonal, which reduce encoding complexity

8. REFERENCES

3GPP2, 2008. C.S0084-001-0 v3.0, Physical Layer for Ultra Mobile Broadband (UMB) Air Interface Specification. Version 3.0.

Asvial , M., Dewandaru, G., Rachman, A.N., 2015. Modification of Round Robin and Best CQI Scheduling Method for 3GPP LTE Downlink. *International Journal of Technology*, Volume 6(2), pp. 130–138

Berrou, C., 2010. *Code and Turbo-code*. Bretagne: ENST Bretagne Edition

Divsalar, D., Dolinar, S., Jones, C.R., Andrews, K., 2009. Capacity-approaching Protograph Codes. *IEEE Journal on Selected Areas in Communications*, Volume 27(6), pp. 876–888

Fossorier, M.P.C., 2004. Quasi-cyclic Low-density Parity-check Codes from Circulant Permutation Matrices. *IEEE Transaction on Information Theory*, Volume 50(8), pp. 1788−1793

Gallager, R.G., 1962. Low-density Parity-check Codes. *IRE Transaction on Information Theory*, Volume 4, pp. 21–28

Guolei, Q., Dong, Z., 2010. Design of Structured LDPC Codes with Quasi-Cyclic and Rotation Architecture. *In:* IEEE Third International Conference on Advanced Computer Theory and Engineering, Chengdu, China, pp. 655–657

Johnson, S.J., Weller, S.R., 2001. Regular Low Density Parity Check Codes from Combinatorial Design. *In:* IEEE Information Theory Workshop, Cairns, Queensland, Australia, pp. 90–92

Juwono, F.H., Triprasetyo, Y., Gunawan, D., 2013. Exploiting LDPC Codes for Improving the Performance of Clipped-OFDM System. *International Journal of Technology*, Volume 4(1), pp. 93–99

Lin, C.Y., Wei, C.C., Ku, M.K., 2008. Efficient Encoding for Dual Diagonal Structured LDPC Codes based on Parity Bit Prediction and Correction. *In:* IEEE Asia Pacific Conference on Circuits and Systems, Macao, China, pp. 1648–1651

Liu, K., Fei, Z., Kuang, J., Li, X., 2009. A Novel Algorithm for Removing Cycles in Quasi-Cyclic LDPC Codes. *In:* IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, Tokyo, Japan, pp. 1054–1058

MacKay, D., 1999. Good Codes based on Very Sparse Matrices. *IEEE Transactions on Information Theory*, Volume 45(2), pp. 399–431

Malema, G., Liebelt, M., 2007. Quasi-Cyclic LDPC Codes of Column-weight Two using a Search Algorithm. *EURASIP Journal on Applied Signal Processing*, Volume 1(1), pp. 1–8

Mao, Y., Banihasherni, A.H., 2001. A Heuristic Search for Good Low-density Parity-check Codes at Short Block Lengths. *In:* IEEE International Conference on Communication, Helsinki, Finland, pp. 41–44

Moura, J.M.F., Lu, J., Zhang, H., 2004. Structured Low-density Parity-check Codes. *IEEE Signal Processing Magazine*, Volume 21(1), pp. 42–55

O'Sullivan, M.E., 2006. Algebraic Construction of Sparse Matrices with Large Girth. *IEEE Transaction on Information Theory*, Volume 52(2), pp. 718–727

Ping, L., Leung, W.K., Phamdo, N., 1999. Low Density Parity Check Codes with Semi-random Parity Check Matrix. *Electronic Letter*, Volume 35(1), pp. 38–39

Richardson, T., Kudekar, S., 2018. Design of Low-density Parity Check Codes for 5G New Radio. *IEEE Communications Magazine,* Volume 56(3), pp. 28–34

Shin, B., Park, H., Hong, S., No, J.S., Kim, S.H., 2014. Quasi-cyclic LDPC Codes using Overlapping Matrices and Their Layered Decoders. *AEU-International Journal of Electronics and Communications*, Volume 68(5), pp. 379–383

Song, H., Liu, J., Kumar, B.V.K.V., 2002. Low Complexity LDPC Codes for Partial Response Channels. *In:* IEEE Proceedings on Global Telecommunication Conference, Taipei, Taiwan, pp. 1294–1299

Song, H., Liu, J., Kumar, B.V.K.V., 2004. Large Girth Cycle Codes for Partial Response Channels. *IEEE Transaction on Magnetics*, Volume 40(4), pp. 3084–3086

Suryanegara, M., Miyazaki, K., 2012. Towards 4G Mobile Technology: Identifying Windows of Opportunity for a Developing Country. *International Journal of Technology*, Volume 3(1), pp. 85–92

Tanner, R., 1981. A Recursive Approach to Low Complexity Codes. *IEEE Transaction on Information Theory*, Volume 27(5), pp. 533–547

Yahya, A., Sidek, O., Salleh, M.F.M., Ghani, F., 2009. A New Quasi-Cyclic Low Density Parity Check Codes. *In:* IEEE Symposium on Industrial Electronics & Applications (ISIEA), Kuala Lumpur, Malaysia, Volume 1, pp. 239–242