In the Name of God

Journal of
Information Systems & Telecommunication

Vol. 1, No. 2, April-June 2013

Research Institute for Information and Communication Technology
Iranian Association of Information and Communication Technology

Affiliated to: Academic Center for Education, Culture and Research (ACECR)

Administrative Manager: Shirin Gilaki
Executive Assistant: Behnoosh Karimi
Art Designer: Parvin Jalilvand, Amir Azadi
Publisher: Iran University Press
ISSN: 2322-1437
eISSN: 2345-2773
Publication License: 91/13216

Editorial office Address: No.5, Saeedi Alley, Kalej Intersection., Enghelab Ave., Tehran, Iran,
P.O.Box: 13145-799 Tel: (+9821) 88930150 Fax: (+9821) 88930157
Email: info@jist.ir
URL: www.jist.ir

Indexed in:

- Research Institute for Information and Communication Technology	www.ictrc.ir
- Islamic World Science Citation Center (ISC)	www.isc.gov.ir
- Scientific Information Database (SID)	www.sid.ir
- Regional Information Center for Sciences and Technology (RICeST)	www.srlst.com
- Magiran	www.magiran.com

This Journal is published with scientific supported by the Advanced Information systems Research Group (AIS) and Information Technology Business Model Research Group (ITBM) in Research Institute for Information and Communication Technology.

Acknowledgement

JIST Editorial-Board would like to gratefully appreciate the following distinguished referees for spending their invaluable time and expertise in reviewing the manuscripts and their constructive suggestions, which had a great impact on the enhancement of this issue of the JIST Journal.

(A-Z)

- Abdolali Abdipour, Amirkabir University of Technology, Tehran, Iran
- Ali Abdollahi, Shahid Beheshti University, Tehran, Iran
- Mohammad Javad Akbari, Islamic Azad University of Arak, Arak, Iran
- Ahmad Akbari Azirani, Iran University Science and Technology, Tehran, Iran
- Hamid Reza Amindavar, Amirkabir University of Technology, Tehran, Iran
- Ayoub Bagheri, Isfahan University of Technology, Isfahan, Iran
- Ahmad Hatam, Islamic Azad University, Naein Branch, Naein, Iran
- Seyed Morteza Hatefi, University of Tehran, Tehran, Iran
- Ahmad Hossein Beig, Semnan University, Semnan, Iran
- Mohammad Darzi, Academic Center for Education Culture and Research (ACECR), Tehran, Iran
- Hamed Ghanbari,
- Amin Dehghani, Khaje Nasir-edin Toosi University of Technology, Tehran, Iran
- Zeinab Ghassabi, Islamic Azad university, science and research branch, Tehran, Iran
- Peiman Kabiri, Iran University Science and Technology, Tehran, Iran
- Shohreh Kasaei, Sharif University of Technology, Tehran, Iran
- Mohammad Ali Mansouri, University of Sistan and baluchestan, Zahedan, Iran
- Kamal Mohamed pour, Khaje Nasir-edin Toosi University of Technology, Tehran, Iran
- Gholamreza Moradi, Amirkabir University of Technology, Tehran, Iran
- Ali Nikfarjam, Khaje Nasir-edin Toosi University of Technology, Tehran, Iran
- Alireza Rezvanian, Amir Kabir University of Technology, Tehran, Iran
- Ramezan Ali Sadegh Zadeh, Khaje Nasir-edin Toosi, Tehran, Iran
- Ramin Shaghaghi, Academic Center for Education Culture and Research (ACECR), Tehran, Iran
- Mohammad Taghipour, Academic Center for Education Culture and Research (ACECR), Tehran, Iran
- Alireza Yari, Cyber Space Research Institue, Tehran, Iran
- Vahid Zarrabi, Academic Center for Education Culture and Research (ACECR), Tehran, Iran

Editorial Note

It is a great privilege for us as the members of the Journal of Information Systems and Telecommunication Editorial Board and Iranian academic community in the field of Telecommunication and Computer Engineering, to present you the second issue of JIST.

Overwhelming responses, congratulations, and best wishes that were received by the JIST Editorial Department after the publication of the first issue, not only strengthens our will to continue the efforts to make the JIST a refereed and highly respected international journal, but also reinforces our determination to work harder toward providing a professional forum for dialogues among Iranian scholars and global experts community. To achieve such momentous goals, the JIST Editorial Board has prepared a long-term plan with specific guidelines and milestones. To be successful, it requires demanding tasks and great dedication of the JIST peoples. An elementary stage of this plan, which has been followed from the early days of this journal, is to start a broad communication with the expert peoples who are active in the Telecommunication and Computer Engineering fields worldwide. We are pleased to mention that taking a look at the names, affiliations, and nationalities of the authors and reviewers of the JIST, first couple of issues confirm a good start from this point of view. Of course, so much more are needed to be done in this regard.

Becoming a pleasant sound to be heard as a pronounced refereed journal in a broader society, any journal needs to be covered by major scientific and technical indexing databases in the world. The work on this guideline of the JIST long-term plan was started even before the publication of its first issue. Just one month after its publication, JIST had a delightful success in this way. The dialogue with several institutions continues in this regard and we hope to expand our co-operations in foreseeing future.

The Second guideline of the JIST long-term plan emphasizes on its accessibility. To be accessible for most researchers and scientific institutions worldwide, a journal requires to be ordered in a simple way. Although people can order the JIST journal by direct subscription method, or just order the reprint of any particular article which they are interested in; unfortunately, the premature situation of the e-business in Iran has not permitted us to accept orders by e-payment method up to this stage yet, we hope to offer this subscription service in near future. Of course, the other way would be to present the subscriptions using the services of a major international publishing incorporation. This method is now being seriously considered as an alternative solution by the JIST Managing Director.

The good news for the academia is that JIST has decided to provide complementary copies of its articles for non-profit research in public organizations worldwide. This service is available on the Internet .Interested people may present their requests to the JIST Operational Center by sending an e-mail to info@jist.ir. This would be a helpful service, especially for the researchers in the developing countries. Another major guideline in our long-term plan points out the dedication of a special section in each issue of JIST to a particular field of its broad scope, at least to the extent that is possible for a semiannually published journal. This has also been followed by us, starting with the current issue.

Also, the announcement of the call for papers for a *Special issue* planned for the third of 2013 is another step toward dedicating of special sections to particular fields of interests in the future, which we anticipate to be warmly welcomed and responded by our distinguished readers.

Pleasant Reading,
Masuod Shafiee (Professor)
Editor-in-Chief and Chairman of ICT Society

Table of Content

Papers:

Performance Analysis of SVM-Type Per Tone Equalizer Using Blind and Radius Directed Algorithms for OFDM Systems

Babak Haji Bagher Naeeni*
Communication, Ph.D, Electrical Engineering, IRIB University
naeeni@iribu.ac.ir
Hamidreza Amindavar
Communication, Ph.D, Electrical Engineering, Amirkabir University of Technology
hamidami@aut.ac.ir

Received: 09/Sep/2012 Accepted: 01/Jul/2013

Abstract

In this paper, we present Support Vector Machine (SVM)-based blind per tone equalization for OFDM systems. Blind per tone equalization using Constant Modulus Algorithm (CMA) and Multi-Modulus Algorithm (MMA) are used as the comparison benchmark. The SVM-based cost function utilizes a CMA-like error function and the solution is obtained by means of an Iterative Re-Weighted Least Squares Algorithm (IRWLS). Moreover, like CMA, the error function allows to extend the method to multilevel modulations. In this case, a dual mode algorithm is proposed. Dual mode equalization techniques are commonly used in communication systems working with multilevel signals. Practical blind algorithms for multilevel modulation are able to open the eye of the constellation, but they usually exhibit a high residual error. In a dual mode scheme, once the eye is opened by the blind algorithm, the system switches to another algorithm, which is able to obtain a lower residual error under a suitable initial ISI level. Simulation experiments show that the performance of blind per tone equalization using support vector machine has better than blind per tone equalization using CMA and MMA, from viewpoint of average Bit-Error Rate (BER).

Keywords: Constant Modulus Algorithm (CMA); Multi-Modulus Algorithm (MMA); Support Vector Machine (SVM); Orthogonal Frequency Division Multiplexing (OFDM).

1. Introduction

Orthogonal Frequency Division Multiplexing (OFDM) is a robust multi-carrier modulation technology that has been selected for a number of radio standards including Wireless LAN (IEEE 802.11a.g [1], HiperLAN/2[2]), DVB-T[3] and Wireless MAN (IEEE 802.16a [4]).

The first two standards are related to wireless home networking, while DVB-T and wireless MAN are concerned with digital video distribution and broadband wireless access, respectively. Among these, IEEE 802.11a, ERP-OFDM of IEEE 802.11g and HiperLAN/2 are standards for Wireless Local Area Net-works (WLAN) and they have similar physical layers based on the technology of OFDM. OFDM is a multicarrier modulation scheme that partitions a broadband channel into a number of parallel and independent narrowband sub channels. For the sub channels to be independent, the convolution of the signal and the channel must be a circular convolution. It is actually a linear convolution, so it is made to appear circular by adding a cyclic prefix (CP) to the start of each data block, which is obtained by prepending the last samples of each block to the beginning of the block. The conventional OFDM system employs a Guard Interval (GI) and a 1-tap Frequency-domain Equalizer (FEQ) to prevent delay spread distortions.

Provided that the GI is larger than the Channel Impulse Response (CIR), InterSymbol Interference (ISI) can be eliminated. Thus, the effect of delay spread is constrained to the frequency selective fading of the individual subband. This fading can easily be cancelled by the 1-tap FEQ. This scheme used by the conventional OFDM system is simple to implement, but provides low spectral efficiency due to the use of the GI. Moreover its performance is poor, due to the lack of multipath diversity and the energy loss contained within the GI. Also in the case where the CIR is larger than the GI, the system performance is limited by ISI and InterCarrier Interference (ICI). We adopt SVM approach for adaptive blind per tone equalization of OFDM channel. SVM is state-of-

* Corresponding Author

the-art tool for linear and nonlinear input-output knowledge discovery [5]. SVM methodology has been successfully utilized in many signal processing applications, especially, in channel equalization.

Recently, this framework has been used to formulate the blind equalization of constant modulus signals [6-8]. The remainder of this paper is organized as following. In section II, the system model is described. In section III, the blind per tone equalization problem is formulated. Section IV describes the channel model used and the simulation results. Some conclusions are provided in section V.

2. SYSTEM MODEL

In an OFDM system, the incoming serial bit-stream is divided into parallel streams, which are used to QAM-modulate the different tones. After modulation with an inverse fast Fourier transform (IFFT), a cyclic prefix is added to each symbol. If the prefix is longer than the channel impulse response, demodulation can be implemented by means of an FFT, followed by a (complex) 1-tap frequency- domain equalizer (FEQ) per tone to compensate for the channel amplitude and phase effects. If the CP is not as long as the channel delay spread, then inter-channel interference (ICI) and inter-symbol interference (ISI) will be presented, and a channel-shorting (time-domain) equalizer, or TEQ, is needed. The TEQ is chosen such that the convolution of the channel and TEQ has almost all of its energy in a time window no longer than the CP length. TEQ design (for a static environment) has been well explored, notably in [9]-[12]. Mathematically, the received signal vector y is obtained from the transmitted data X via

$$\overbrace{\begin{bmatrix} \mathrm{y}_{\mathrm{ks}+\nu-\mathrm{T}+2} \\ \vdots \\ \mathrm{y}_{(\mathrm{k}+1)\mathrm{s}} \end{bmatrix}}^{\mathrm{y}} = \begin{bmatrix} 0_{(1)} & \begin{vmatrix} \mathrm{h} & \dots & 0 \\ \ddots & \ddots & \ddots \\ 0 & \dots & \mathrm{h} \end{vmatrix} & 0_{(2)} \end{bmatrix}$$

$$\begin{bmatrix} \mathrm{P\,Q_N} & 0 & 0 \\ 0 & \mathrm{P\,Q_N} & 0 \\ 0 & 0 & \mathrm{P\,Q_N} \end{bmatrix} \overbrace{\begin{bmatrix} \mathrm{X}_{1:\mathrm{N}}^{(\mathrm{k}-1)} \\ \mathrm{X}_{1:\mathrm{N}}^{(\mathrm{k})} \\ \mathrm{X}_{1:\mathrm{N}}^{(\mathrm{k}+1)} \end{bmatrix}}^{\mathrm{X}} + \overbrace{\begin{bmatrix} \mathrm{n}_{\mathrm{ks}+\nu-\mathrm{T}+2} \\ \vdots \\ \vdots \\ \mathrm{n}_{(\mathrm{k}+1)\mathrm{s}} \end{bmatrix}}^{\mathrm{n}}$$

$$= \mathrm{HX} + n \tag{1}$$

Where N is the symbol size expressed in samples, k the time index of a symbol, $\mathrm{x_i(k)}$ is a complex sub-symbol for tone i, $i = 1, \dots., N$ to be transmitted at symbol period K, $Y_i(k)$ the demodulated output for tone i (after the FFT) and $z_i(k)$ the final output (after frequency - domain equalization). Further, ν denotes the length of the cycle prefix, $s = N + \nu$ the length of a symbol including prefix. $\{h_l, \dots, h_0, \dots, h_{-k}\}$ the channel impulse response in reverse order and n is additive noise or interference. The $\odot$ represents a component wise multiplication. The effective channel H includes the physical channel h, the addition of the cyclic prefix (inserted by p), and the Q_N matrices are $N{\times}N$ IFFT matrices and modulate the input symbols and X contains the symbol of interest as well as the preceding and succeeding symbols. To describe the data model, we consider three successive symbols $X_{1:N}^{(c)}$ to be transmitted at $c = k-1, k, k+1$ respectively. The k th symbol is the symbol of interest; the previous and the next symbol are used to include interferences with neighboring symbols in our model. $0_{(1)}$ and $0_{(2)}$ are zero matrices of size $(N{+}T{-}1){\times}(N{+}\nu - T + 1 - L + \nu)$ and $(N{+}T{-}1){\times}(N{+}\nu - T + 1 - L + \nu)$ respectively. Perfect synchronization at the receiver is assumed in this paper. Van Acker et al. [13] have proposed an alternate equalization structure, called per tone equalization, which accomplishes the same task as the TEQ/FEQ, but with improved performance and comparable complexity. The full details of the per tone structure can be found in [13] briefly, demodulation is accomplished by an FFT of size N which is done by premultiplying y by F_N Per tone equalization of bin i is accomplished by forming a linear combination of the iFFT output and $T-1$ difference terms of the pre-FFT signal, y:

$$z_i = \bar{v}_i^T \underbrace{\left[\begin{array}{c|c|c} I_{T-1} & 0 & -\,I_{T-1} \\ \hline 0 & \multicolumn{2}{c}{F_N(i,:)} \end{array}\right]}_{F_i} y \tag{2}$$

where $\bar{v}_i^T$, F_N an $N \times N$ FFT-matrix and $F_N(i,:)$ the i th row of F_N The linear combiner (not a tapped delay line) $\bar{v}_i$ is the time-reversal of v_i defined for convenience; and z_i is the equalized data for tone i . The notation on (1) and (2) was introduced in [13], but is repeated here for reference. Determination of the per tone equalizer coefficients has been explored in [13] and [14]. In [13], the optimal coefficients are calculated in a least-squares manner, based on knowledge of the transmission channel, and the signal and noise statistics. In [14], the coefficients are determined in a less computationally-intensive fashion through the use of recursive least-squares (RLS), which requires training through out the adaptation. Imad Barhumi and Marc Moonen have been considered turbo equalization of doubly selective channels in [15].

These approaches are well-suited to a system that has plentiful training and computational power. In this paper, we propose a new method (support vector machine) for determination of the per tone equalizer coefficients and compare its performance with constant modulus algorithm (CMA) from view point of average BER.

In next section, we describe and formulate the multilevel SVM-based blind per tone equalization and CMA-based and MMA-based blind per tone equalization.

3. PROBLEM FORMULATION

3.1 Multilevel SVM-Based Blind Per Tone Equalization

In this section, we describe and formulate the multilevel SVM-based blind per tone equalization and CMA-based and MMA-based blind per tone equalization.

- Blind algorithm

The proposed algorithm [6,7,8] minimizes the following SVM-based cost function for tone i :

$$L_p(\overline{v}_i) = \frac{1}{2}\|\overline{v}_i\|^2 + c\sum_{k=1}^{M} L_\varepsilon(u_i(k)) \tag{3}$$

Where

$$L_\varepsilon(u_i) = \begin{cases} 0, & u_i < \varepsilon \\ u_i^2 - 2u_i\varepsilon + \varepsilon^2, & u_i \geq \varepsilon \end{cases} \tag{4}$$

is a $\boldsymbol{\varepsilon}$-insensitive quadratic loss function modified to guarantee a continuous derivative. Continuity of the derivative is necessary for the numerical stability of the algorithm. We select a suitable penalization term called $u_i(k)$ in order to apply aforementioned cost function for blind equalization. Here, we propose to use $u_i(k) = |e_i(k)|$ with the error term $e_i(k)$ being

$$z_i(k) = \overline{v}_i{}^T F_i y(k) \tag{5}$$

and

$$e_i(k) = |z_i(k)|^2 - R_{2,i} = z_i(k)z_i^*(k) - R_{2,i} \tag{6}$$

$R_{2,i}$ is the Godard constant, for tone i and superindex * denotes the complex conjugate. The Godard algorithms [16] adapt the equalizer to minimize the following cost function

$$j_G(\overline{v}_i) = E\left[(|z_i(k)|^p - R_{p,i})^2\right] \tag{7}$$

the ratio $\mathrm{R_{P,i}}$ contains the a priori knowledge about the current modulation

$$R_{p,i} = \frac{E[|X_i|^{2p}]}{E[|X_i|^p]} \tag{8}$$

CMA is the Godard algorithm for $p = 2$. The proposed method introduces a penalty term inspired by the CMA cost function. For optimality reasons, IRWLS is used. This procedure has been successfully applied to solve SVM's [17] and it has recently proven to converge to the SVM solution [18]. A first order Taylor series expansion of $L_\varepsilon(u_i)$ is used to obtain the cost function that produces the IRWLS algorithm

$$L'_p(\overline{v}_i) = \frac{1}{2}\|\overline{v}_i\|^2 + \tag{9}$$
$$C\left[\sum_{k=1}^{M} L_\varepsilon\big(u_i(j,k)\big) + \frac{dL_\varepsilon(u_i)}{du_i}\bigg|_{u_i(j,k)} [u_i(k) - u_i(j,k)]\right]$$

where $u_i(j,k) = |e_i(j,k)|$ and $e_i(j,k) = \left|\bar{v}_j^T(j,k)F_i y(k)\right|$ - $R_{2,i}$ error term after the $j - th$ iteration. Then, a quadratic approximation is constructed as following.

$$L''_p(\overline{v}_i) = \frac{1}{2}\|\overline{v}_i\|^2 + C\left[\sum_{k=1}^{M} L_\varepsilon\big(u_i(j,k)\big) + \right.$$
$$\left.\frac{dL_\varepsilon(u_i)}{du_i}\bigg|_{u_i(j,k)} \frac{(u_i(k))^2 - (u_i(j,k))^2}{2u_i(j,k)}\right]$$
$$= \frac{1}{2}\|\overline{v}_i\|^2 + \frac{1}{2}\left[\sum_{k=1}^{M} \alpha_i(k)|e_i(k)|^2 + CTE\right] \tag{10}$$

CTE represents constant terms that do not depend on

$\bar{v}_i$, and the weights $a_i(k)$ are

$$\alpha_i(k) = \frac{C}{u_i(j,k)}\frac{dL_\varepsilon(u_i)}{du_i}\bigg|_{u_i(j,k)} \tag{11}$$
$$= \begin{cases} 0, \; u_i(j,k) < \varepsilon \\ \frac{2C(u_i(j,k)-\varepsilon)}{u_i(j,k)}, \; u_i(j,k) \geq \varepsilon \end{cases} \tag{12}$$

$L''_P(\bar{v}_i)$ is a quadratic functional for $L_P(\bar{v}_i)$ in (3) that presents the same value $L''_P\big(\bar{v}_i(j)\big) = L_P(\bar{v}_i(j))$ and gradient for $\nabla_{\bar{v}_i} L''_P\big(\bar{v}_i(j)\big) = \nabla_{\bar{v}_i} L_P(\bar{v}_i(j))$ for $\bar{v}_i = \bar{v}_i(j)$. Therefore, we can define $\bar{p}_i(j) = \bar{v}_i(s) - \bar{v}_i(j)$ as a descending direction for $L_P(\bar{v}_i)$, where $\bar{v}_i(s)$ is the least square solution to (10), and we can use it to construct a line search method [19], $i.e.$ $\bar{v}_i(j+1) = \bar{v}_i(j) + \eta_i(j)\; p_i(j)$. The value to $\eta_i(j)$ can be computed using a backtracking line search [18], in which $\eta_i(j)$ is initially set to 1 and if $L_P(\bar{v}_i(j+1)) \geq L_P\big(\bar{v}_i(j)\big)$, it is iteratively reduced until a strict decrease in the functional in (3) is observed. To obtain the solution to $L''_P(\bar{v}_i)$, its gradient is set to zero

$$\nabla_{\overline{v}_i} L''_p(\overline{v}_i) = \overline{v}_i + 2\textstyle\sum_{k=1}^{M} \alpha_i(k)\big(|\lambda_i|^2 - R_{2,i}\big)\xi_i = 0 \tag{13}$$

where $\lambda_i = \bar{v}_i^T F_i y(k)$ and $\xi_{i=}\bar{v}_i^T F_i y(k) F_i^* y^*(k)$. Equation (13) is a nonlinear function of $\bar{v}_i$. In order to circumvent this nonlinearity, the per tone equalizer output $z_i(k)$ is considered fixed, which leads to

$$\nabla_{\overline{v}_i} L_p''(\overline{v}_i) = \overline{v}_i + 2\sum_{k=1}^{M} \alpha_i(k)\left(\beta_i - R_{2,i}\right)\xi_i = 0 \quad (14)$$

where $\beta_{i=}\bar{v}_i^T F_i y(k) z_i^*(k)$ and $\zeta_{i=}z_i(k) F_i^* y^*(k)$, (14) can be expressed in matrix form as

$$\left[2X_i^H D_{\alpha,i} D_{|z|^2,i} X_i + I\right]\overline{v}_i = 2R_{2,i} X_i^H D_{\alpha,i} Z_i \qquad (15)$$

where $X_i^T = [F_i y(1), F_i y(2), \dots, F_i y(M)], D_{a,i}$ is a diagonal matrix with diagonal elements $a_i(k)$ and $D_{|z|^2,i}$ is another diagonal matrix with diagonal elements $|z_i(k)|^2$ and $z_i^T = [z_i(1), z_i(2), \dots, z_i(M)]$ for k=*1,2,...,M, I* is the identity matrix, and H denotes the Hermitian operator.

Implementation Details: With respect to parameters C and $\boldsymbol{\varepsilon}$, although further research is necessary to determine their optimal values, but the algorithm is not very sensitive to its choice. Typically, values of $C = 10$ and $\boldsymbol{\varepsilon}$ =0.01 produce suitable results under a wide range of channels and signal to noise ratios.

Consideration: $e_i(j,k)$ denotes the error for tone i after *j-th* iteration for $k = 1,2,\dots,M$. In $e_i(j,k)$ =$|\bar{v}_i^T(j) F_i y(k|^2$-$R_{2,i}$ for tone i, $(i = 1,2,\dots,N)$, amounts of $y(k)$, $(k = 1,2,\dots,M)$ are constant for each of iterations, $(j = 1,2,\dots,J)$ and for one realization of channel and amounts of $y(k)$ change with changing the tap coefficients of the channel (another realization of channel). For example: for tone i, after computing $\bar{v}_i^T(1)$ in 1-th iteration, we have $e_i(1,1) = \left|\bar{v}_j^T(1) F_i y(1)\right| - R_{2,i}$, $e_i(1,2) = \left|\bar{v}_j^T(1) F_i y(2)\right|$- $R_{2,i}$,....,$e_i(1,M) = \left|\bar{v}_j^T(1) F_i y(M)\right|$-$R_{2,i}$. amounts of $y(k)$ for $k = 1,2,\dots,M$are constant for other iterations until complete convergence and change with changing the tap coefficients of the channel and this method repeats for one thousand realization of channel.

Finally, the IRWLS procedure is summarized in the following steps:

1. Initialization: initialize $\bar{v}_i(1)$, obtain $z_i(k)$ by (5), $e_i(k)$ by (6), calculate $u_i(k) = e_i(k)$ and compute $a_i(k)$ from (11). Set $j = 1$.
2. Compute $\bar{v}_i(s)$ by solving (15) and set $\eta_i(j) = 1$.
3. Set $\bar{v}_i(j+1)$=$\bar{v}_i(j) + \eta_i(j)[\,\bar{v}_i(s) - \bar{v}_i(j)]$. If $L_P(\bar{v}_i(j+1)) < L_P(\bar{v}_i(j))$ go to step 5.
4. Set $\eta_i(j)$=$\boldsymbol{\rho}\eta_i(j)$ with *0<ρ<1* and go to step 3.
5. Recompute $e_i(k), u_i(k)$ and $a_i(k)$, set $j = j + 1$ and go to step 2 until convergence.

Radius directed algorithm: The radius directed algorithm is formulated by replacing $R_{2,i}$ in the blind algorithm by the radius $R_{m,i}(k)$, which is defined as

$R_{m,i}(k) = min_{R_{m,i}}\left(\left||z_i(k)|^2 - R_{m,i}\right|\right)$

here, $R_{m,i}(k)$, are the different values of $|X_i|^2$ in the underlying signal constellation. For instance, for a 16-QAM with levels ±3, ±1 in both the phase and quadrature components, $R_{m,i} = 2{,}10{,}18$. With this simple modification, the error term to be penalized is

$$e_i(k) = |z_i(k)|^2 - R_{m,i}(k) \qquad (16)$$

and the matrix system to obtain the solution $\bar{v}_i(s)$ becomes

$$\left[2X_i^H D_{\alpha,i} D_{|z|^2,i} X_i + I\right]\overline{v}_i = 2X_i^H D_{\alpha,i} D_{R,i} Z_i \qquad (17)$$

$D_{R,i}(i)$, is a diagonal matrix with diagonal elements $R_{m,i}(k)$. The corresponding IRWLS algorithm is the same one summarized in blind algorithm with the following differences:

- Step 1: Since this algorithm is used as the second step of a dual mode algorithm, $\bar{v}_i(1)$ is the value of $\bar{v}_i$ provided by the blind algorithm.

- Steps 1 and 5: $e_i(k)$ is evaluated by (17), instead of (6).

- Step 2: $\bar{v}_i(s)$ is obtained by solving (18), instead of (15).

3.2 CMA-based blind adaptive per tone equalization

The constant modulus algorithm is a popular alternative in decision-directed algorithms. A detailed review of its convergence behaviour in single-carrier systems can be found in [20]. CMA attempts to minimize the dispersion of the equalized symbols by performing a stochastic gradient descent of

$$J_{CM,i} = E[(|z_i(k)|^2 - \gamma_i)^2] \qquad (18)$$

for each bin i, where $z_i(k)$ is the per tone equalizer output and $\gamma_{i=E[|X_i|^4]/E[|X_i|^2]}$. The resulting algorithm; i.e., CMA-based blind adaptive per tone equalization, for $i = 1,\dots,N$ and $k = 1, 2, 3, \dots$, is

$$z_i(k) = \overline{v}_i^T(k) F_i y(k)$$
$$\overline{v}_i(k+1) = \overline{v}_i(k) - \mu z_i(k)(|z_i(k)|^2 - \gamma_i) F_i^* y^*(k) \quad (19)$$

C. MMA-based blind adaptive per tone equalization

Oh and chin [21], and Yang et al. [22] proposed a modified CMA called the multimodulus algorithm (MMA), whose cost function is

$$\mathcal{J}_{MMA,i} = \mathcal{J}_{R,i} + \mathcal{J}_{I,i} + E\left[\left(z_{R,i}^2(k) - \gamma_{R,i}\right)^2\right] + E\left[(z_{I,i}^2(k) - \gamma_{I,i})^2\right] \qquad (20)$$

for each bin i, where $z_{R,i}(k)$ and $z_{I,i}(k)$ are the real and imaginary parts of the per tone equalizer output, respectively; $\gamma_{R,i}$ and $\gamma_{I,i}$ are given by

$$\gamma_{R,i} = \frac{E[X_{R,i}^4]}{E[X_{R,i}^2]} \quad and \quad \gamma_{I,i} = \frac{E[X_{I,i}^4]}{E[X_{I,i}^2]} \qquad (21)$$

in which $X_{R,i}(k)$ and $X_{I,i}(k)$ denote the real and imaginary parts of X_i respectively. Decomposing the cost function of MMA into the real and imaginary parts, thus allows both the modulus and the phase of the per tone equalizer output to be considered; therefore, joint blind per tone equalization and carrier-phase recovery may be simultaneously accomplished, eliminating the need for a rotator to perform separate constellation-phase recovery in steady-state operation. The resulting algorithm; i.e., MMA-based blind adaptive per tone equalization, for $i = 1, \dots, N$ and $k = 1, 2, 3, \dots$, is

$$z_i(k) = \overline{v}_i^T(k) F_i y(k)$$
$$\overline{v}_i(k+1) = \overline{v}_i(k) - \mu e_i(k) F_i^* y^*(k) \qquad (22)$$

where $e_i(k) = e_{R,i}(k) + j e_{I,i}(k)$, in which $e_{R,i}(k) = z_{R,i}(k)(z^2{}_{R,i}(k)$ - $\gamma_{R,i}$) and $e_{I,i}(k) = z_{I,i}(k)(z^2{}_{I,i}(k)$ -$\gamma_{I,i}$).

4. Channel model and simulation results

A multipath fading channel in [23] with $L = J - 1)L_1 + L_2$ taps is used based on the following impulse response model

$$h(l) = \sum_{j=0}^{J-1} e^{-\beta_1 j} \sum_{m=jL_1}^{j\,L_1+L_2-1} \alpha_m e^{-\beta_2(m-jL_1)} \delta(l-m) \quad (23)$$

where a_m is a zero mean complex, circularly symmetric, Gaussian random process such that $E\left[a_m a_j^*\right] = \delta(m - j,$ β_1 and β_2 are exponential decay factors. In simulations, $J = 3, L_1 = L_2 = 7$ for L=21 and $J = 4, L_1 = L_2 = 6$ for $L = 24, = 0,$ and $\beta_1 = 0$ $\beta_{2=}0.25$ are chosen. The CIR intervals are $L = 21$ and $L = 24$ which are longer than the CP interval and the additive Gaussian noise, $n(k)$, is a white process. One thousand independent realizations of $h\,(l)$ based on (23) have been used in simulations for a 16-QAM and 64-QAM OFDM systems with $N = 64$ subcarriers and a CP interval $\upsilon = 16$ Number of taps for per tone equalization is $T = \nu + 1.$ A burst of 2500 OFDM symbols is assumed to be transmitted ($M = 2500$). Hence the CIR is assumed constant for each burst. Each data point in the simulation results (Figures1, 2 and 3) is obtained by averaging over 1000 such bursts. Without loss of generality, 16-QAM and 64-QAM mapping for all sub channels has been employed and all sub channels are used.

Where a_m is a zero mean complex, circularly symmetric, Gaussian random process such that $E\left[a_m a_j^*\right] = \delta(m - j,$ β_1 and β_2 are exponential decay factors. In simulations, $J = 3,$ $L_1 = L_2 = 7$ for $L = 21$ and $J = 4, L_1 = L_2 = 6$ for $L = 24, = 0,$ and $\beta_1 = 0$ $\beta_{2=}0.25$ are chosen. The CIR intervals are L = 21 and $L = 24$ which are longer than the CP interval and the additive Gaussian noise, $n(k)$, is a white process. One thousand independent realizations of $h\,(l)$ based on (23) have been used in simulations for a 16-QAM and 64-QAM OFDM systems with $N = 64$ subcarriers and a CP interval $\upsilon = 16$ Number of taps for per tone equalization is $T = \nu + 1.$ A burst of 2500 OFDM symbols is assumed to be transmitted ($M = 2500$). Hence the CIR is assumed constant for each burst. Each data point in the simulation results (Figures 1, 2 and 3) is obtained by averaging over 1000 such bursts. Without loss of generality, 16-QAM and 64-QAM mapping for all sub channels has been employed and all sub channels are used. The simulation results for per tone equalization using CMA and MMA and blind SVM have been shown in Figures 1 and 2. They show the average bit-error rate (BER) as a function of SNR for 16-QAM and $L = 21$ and $L = 24$, respectively. Fig 3. shows the average bit-error rate (BER) as a function of SNR for 64-QAM and $L = 21$. These figures show that the performance of SVM-based blind adaptive per tone equalization using radius directed algorithm and without using it are better than CMA-based and MMA-based blind adaptive per tone equalization from the viewpoint of average BER for 16-QAM and 64-QAM.

5. Conclusion

In this paper, we proposed a new blind OFDM channel equalization method based on SVM for multilevel signals. In order to determine the equalizer coefficients, we used the difference of the per tone equalizer output and the $R_{2,i}$ parameter of the CMA algorithm. Our simulations showed that the average BER for per tone equalization using blind-SVM was better than per tone equalization using CMA and MMA for 16-QAM.

References

[1] IEEE 802.11g "Further higher data rate extension in the 2.4 GHz band," IEEE Std 802.11g-2003.

[2] ETSI TR 101 683 (V 1.1.2): Broadband Radio Access Networks;
HIPERLAN/2 System Overview.

[3] ETSI ETS 300 744: Digital Video Broadcasting (\DVB-T).

[4] IEEE P802.16a/D7-2002.

[5] B. Scholkopft, A. Smola, Learning With Kernels, MIT Press, Cambridge, MA, 2002.

[6] I. Santamaria, J. Ibanez, L. Vielva, and C. Pantaleon, "Blind equalization of constant modulus signals via support vector regression," {\em ICASSP}, April 2003, Vol.II, pp.737-740.

[7] I. Santamaria, C. Pantaleon, L. Vielva, J. Ibanez, "Blind equalization of constant modulus signals using support vector machines," IEEE Trans. on Signal Processing}, in Press, 2004.

[8] M. Lazaro, I. Santamaria, J. Via, D. Erdogmus, "Blind equalization of multilevel signals using support vetor machines," Proc. of the European Signal Processing Conf., Sept. 2004.

[9] N. Lashkarian and S. Kiaei, "Optimum equalization of multicarrier systems: A unified geometric approach," IEEE Trans. on Commun., Vol.49, pp.1762-1769. Oct. 2001.

[10] P.J. W. Melsa, R.C. Younce, and C.E. Rohrs, "Impulse response shortening for Discrete Multitone Transceivers," IEEE Trans. on Commun., Vol.44, pp.1662-1672, Dec. 1996.

[11] G. Arslan, B.L. Evans, and S. Kiaei, "Equalization for discrete multitone receivers to maximize bitrate," IEEE Trans. on signal processing, Vol.49, No.12, pp.3123-3135, Dec. 2001.

[12] B. Farhang-Boroujeny and M. Ding, "Design methods for time-domain equalizer in DMT transceivers," IEEE Trans. on Commun.}, Vol.49, No.3, pp.554-562, Mar. 2001.

[13] K. Van Acker, G. Leus, M. Moonen, O. van de Weil, and T. Pollet, "Per tone equalization for DMT-based systems," IEEE Trans.

[14] K. Van Akcer, G. Leus, M. Moonen, and T. Pollet, "RLS based initialization for per tone equalizers in DMT-receivers," Proc. of the European Signal Processing Conf., Sept. 2000.

[15] I. Barhumi and M. Moonen, "Turbo equalization of doubly selective channels," Wiley, Wireless communications and mobile computing, 2012.

[16] D. N. Godard, "Self-recovering equalization and carrier tracking in two dimensional data communication systems," IEEE Trans. on Commun., Vol.28, pp.1867-1875, Nov. 1980.

[17] F. Perez-Cruz, A. Navia-Vazquez, P. Alarcon-Diana, and A. Artes-Rodriguez, "An \IRWLS\ procedure for SVR," Proc. of the EUSIPCO, Sept. 2000.

[18] F. Perez-Cruz, C. Bousono-Calzon, C.-H. Lin, and A. Artes-Rodriguez, "Convergence of the \IRWLS\ procedure to the support vector machine solution," IEEE Trans. on Neural Networks}, Vol.14, No.2, pp.296-303, 2003.

[19] J. Nocedal and S.J. Wright, Numerical Optimization, Springer, 1999.

[20] C.R. Johnson, Jr. P. Schniter, T. J. Endres, I.D, D.R. Brown, R.A. Casas, "Blind equalization using the constant modulus criterion: A Review," {\em Proc. of the IEEE}, Vol.86, pp.1927-1950, Oct. 1998.

[21] K. N. Oh and Y. O. Chin, "Modified constant modulus algorithm: blind equalization and carrier phase recovery algorithm," Proc. IEEE Int. Conf. Commun., Vol.1, pp.498-502, 1995.

[22] J. Yang, J.-J. Werner, and G. A. Dumont, "The multimodulus blind equalization and its generalized algorithms," {\em IEEE J. Sel. Areas Commun.} Vol.20, No.6, pp.997-1015, Jun. 2002.

[23] H. Zamiri-Jafarian, H. Khoshbin, Subbarayan Pasupathy, "Time-Damain equalizer for \OFDM\ systems based on SINR maximization," IEEE Trans. on Commun., Vol.53, No.6, Jun. 2005

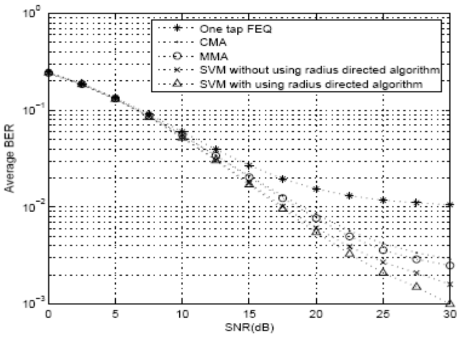


Fig.1 The average bit-error rate as a function of SNR, CIR interval is L=21, 16-QAM

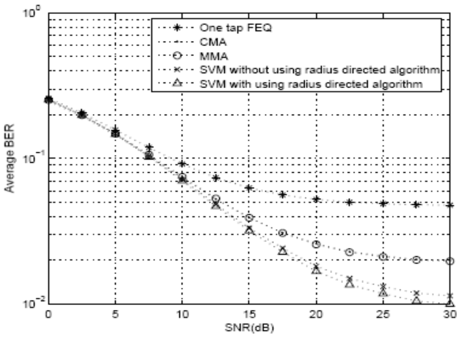


Fig.2 The average bit-error rate as a function of SNR, CIR interval is L=24, 16-QAM

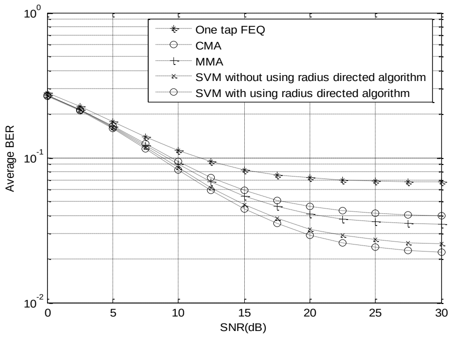


Fig.3 The average bit-error rate as a function of SNR, CIR interval is L=21,64-QAM

Multimodal Biometric Recognition Using Particle Swarm Optimization-Based Selected Features

Sara Motamed*
Artificial Intelligence, Ph.D. Student, Computer and Science, Islamic Azad University, Fuman Branch
Samotamed@yahoo.com
Ali Broumandnia
Artificial Intelligence, Assistant Professor, Computer Department, Islamic Azad University, South Tehran Branch
Broumandnia@azad.ac.ir
Azamossadat Nourbakhsh
Artificial Intelligence, Ph.D. Student, Computer Department, Islamic Azad University, Lahijan Branch
Nourbakhsh@liau.ac.ir

Received: 20/Dec/2012 Accepted: 12/Jun/2013

Abstract

Feature selection is one of the best optimization problems in human recognition, which reduces the number of features, removes noise and redundant data in images, and results in high rate of recognition. This step affects on the performance of a human recognition system. This paper presents a multimodal biometric verification system based on two features of palm and ear which has emerged as one of the most extensively studied research topics that spans multiple disciplines such as pattern recognition, signal processing and computer vision. Also, we present a novel Feature selection algorithm based on Particle Swarm Optimization (PSO). PSO is a computational paradigm based on the idea of collaborative behavior inspired by the social behavior of bird flocking or fish schooling. In this method, we used from two Feature selection techniques: the Discrete Cosine Transforms (DCT) and the Discrete Wavelet Transform (DWT). The identification process can be divided into the following phases: capturing the image; pre-processing; extracting and normalizing the palm and ear images; feature extraction; matching and fusion; and finally, a decision based on PSO and GA classifiers. The system was tested on a database of 60 people (240 palm and 180 ear images). Experimental results show that the PSO-based feature selection algorithm was found to generate excellent recognition results with the minimal set of selected features.

Keywords: Biometric, Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT).

1. Introduction

It is known that a good feature extractor for a human recognition system is claimed to select as much as possible the best discriminate of features which are not sensitive to arbitrary environmental variations such as variations in pose, scale and illumination. Feature selection algorithms mainly fall into two categories: geometrical features extraction and statistical (algebraic) features extraction [2-8]. Single modal biometric system depends on only one biometric feature of a person. Single modal biometric systems are less accurate and not universally accepted [1]. They are more susceptible to the factors that generate false results like environmental noise, change of biometric features with time and condition, illness or accidents and spoofing [21]. Multi-modal biometric systems [23] are expected to be more reliable due to the presence of multiple pieces of evidence. These systems are also able to meet the stringent performance requirements imposed by various applications [24]. Multimodal systems address the problem of non-universality: It is possible for a subset of users which do not possess particular biometrics. In such instances, it is useful to acquire multiple biometric traits to verify identity. Multimodal systems also provide anti-spoofing measures by it making difficult for an intruder spoofing multiple biometric traits simultaneously. By asking the user to present a random subset of biometric traits, the system ensures that a _live_ user is indeed present at the point of acquisition. However, an integration scheme is required to fuse the information presented by the individual modalities. Moreover, multimodal biometric system takes more than one single feature into account [31]. This helps in identifying and verifying the person with more accuracy even if one of the features gives less matching score [32,34,35]. Our multimodal biometric identification system is based on

* Corresponding Author

features extracted from palm and ear images by alternative algebraic methods, which are based on transforms called discrete cosine transform (DCT) and the discrete wavelet transform (DWT). Transformation based feature extraction methods such as the DCT and DWT were found to generate good rate of accuracies with very low computational cost [8]. DCT is one of approaches used in image compressing which is also used to extract features [9], [10]. Wavelet analysis has both a good qualities in time domain and frequency domain which is an ideal tool in unsteady signals analyzing. The DCT and the DWT Feature extraction methods are explained in detail in Section 2.

Feature extraction in pattern recognition involves the derivation of feature subset from the raw input data to reduce the amount of data used for classification, and simultaneously provide enhanced discriminatory power. The extraction of an appropriate set of features often exploits the design criteria such as redundancy minimization, and minimizing the reconstruction error. For many pattern classification problems, usage of a higher number of features does not necessarily translate into higher recognition rate [11]. In some cases the performance of algorithms is devoted to speed and predictive accuracy of the data characterization can even decrease. Therefore, feature extraction can serve as a pre-processing tool of great importance before solving the classification problems. The purpose of feature extraction is reducing the maximum number of irrelevant features while maintaining acceptable classification accuracy. Feature extraction is considerably important in pattern classification, data analysis, multimedia information retrieval, biometrics, remote sensing, computer vision, medical data processing, machine learning, and data mining applications. Feature extraction seeks for the optimal set of d features out of m [11-13] one possible approach is an exhaustive search among all possible feature subsets $\binom{m}{d}$ and choosing the best one according to the optimization criterion at hand. However, such an approach is computationally very expensive. Several methods have been previously used to perform feature extraction on training and testing data, branch and bound algorithms [14], sequential search algorithms [15], mutual information [16], tabu search [17] and greedy algorithms [12].

To avoid the prohibitive complexity feature selection algorithms, we usually involve heuristic or random search strategies. Among the various methods proposed for feature extraction, population-based optimization algorithms such as Genetic Algorithm (GA)-based method [7], [18], [19] and Ant Colony Optimization (ACO)-based method have been attracted a lot of attention [20]. These methods attempt to achieve better solutions by using knowledge from previous iterations with no prior knowledge of features. In this paper, palm and ear recognition algorithms using a PSO-based feature selection approach is presented. The algorithm utilizes a novel approach that employs the binary PSO algorithm to effectively explore the solution space for the optimal feature subset. The selection algorithm is applied to feature vectors extracted using the DCT and the DWT. The search heuristics in PSO is iteratively adjusted and guided by a fitness function definition in terms of maximizing class separation. The proposed algorithm was found to generate excellent recognition results with less selected features. Our paper is divided into 6 sections that are introduced with following sequences: To use feature selection algorithms by palm and ear recognition based on the binary PSO algorithm in Section 1. The DCT and the DWT Feature selection techniques are described in Section 2. An overview of Particle Swarm Optimization (PSO) is presented in Section 3. In Section 4, we explain the proposed PSO- based feature selection algorithm. Finally, Sections 5 and 6 attain the experimental results and conclusion.

2. Feature Extraction

In this section, two methods of feature extraction for building ear and palm features vector are introduced. DCT and DWT were used for feature extraction as explained in the following Sections.

2.1 Discrete Cosine Transform (DCT)

DCT, as a popular transformation technique, has been widely used in signal and image processing. This is due to its strong “energy compaction” property: most of the signal information tends to be concentrated in a few low-frequency components of the DCT. DCT is found to be an effective method that yields high recognition rates with low computational complexity. DCT exploits inter-pixel redundancies to render excellent decorrelation for most natural images. After decorrelation, each transform coefficient can be encoded independently without losing compression efficiency. The DCT helps separating image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). DCT transforms the input into a linear combination of weighted basis functions. These basis functions are frequency components of the input data. DCT is similar to the discrete Fourier transform (DFT) in the sense that they transform a signal or image from the spatial domain to the frequency domain, use sinusoidal base functions and exhibit good decorrelation and energy compaction characteristics. The major difference is that the DCT transform uses simple cosine-based basis functions whereas DFT is a complex transform and therefore, stipulates that both image magnitude and phase information be encoded. In addition, studies have shown that DCT provides better energy compaction than DFT for most natural images [33]. The general equation for the DCT of an $N \times M$ image *f(x,y)* is defined by the following equation:

$$f(U,V) = \propto (U) \propto (V) \sum_{X=0}^{N-1} \quad \sum_{Y=0}^{M-1} \quad COS[\frac{\pi .U}{2 .N} (2 \times +1)] COS[\frac{\pi .U}{2 .N} (2 \times +1)] f(X,Y) \qquad (1)$$

Where *f(x,y)* is the intensity of the pixel in row *x* and column *y; u = 0,1, ..., N-1* and *v=0,1, ..., M-1* and the functions *α(u)*, *α(v)* are defined as:

$$\propto (U). \propto (V) = \begin{cases} \sqrt{\frac{1}{N}} & For \quad u, v{=}0 \\ \\ \sqrt{\frac{2}{N}} & For \quad u, v{=}0 \end{cases} \qquad (2)$$

For most images, much of the signal energy lies at low frequencies (corresponding to large DCT coefficient magnitudes); these are relocated to the upper-left corner of the DCT array. Conversely, the lower-right values of the DCT array represent higher frequencies, and turn out to be small enough to be truncated or removed with little visible distortion, especially as *u* and *v* approach the sub-image width and height, respectively. This means that the DCT is an effective tool that can pack the most effective features of the input image into the fewest coefficients [33].

The palm and ear images can be roughly reconstructed only by few DCT coefficients. This increases selecting DCT coefficient initially used in the palm and ear recognition system very critical. The effect of the number of DCT coefficients used as features for palm and ear recognition is examined in Section 5. This part includes the effect of the number of coefficients on the reconstructed image's quality and the recognition rate. The study is extended by examining the performance of the dynamically generated feature subset generated by the PSO feature selection algorithm.

2.2 Discrete Wavelet Transform (DWT)

Wavelets have many advantages over other mathematical transforms such as the DFT or DCT. Functions with discontinuities and functions with sharp spikes usually take substantially fewer wavelet basis functions than sine-cosine functions to achieve a comparable approximation. Wavelets have been successfully used in image processing since 1985 [8], [22], [25], and [26]. Its ability for providing spatial and frequency representations of image simultaneously, motivate its use for feature extraction. The decomposition of input data into several layers of division in space and frequency allows us to isolate the frequency components introduced by intrinsic deformations due to expression or extrinsic factors (like illumination) into certain sub-bands. Wavelet-based methods prune away these variable sub-bands, and focus on the space/frequency sub-bands that contain the most relevant information to better represent the data and aid in the classification between different images.

It represents a signal by localizing it in both time and frequency domains. Wavelets can be used to improve image registration accuracy by considering both spatial and spectral information and by providing multi-resolution representation to avoid losing any global or local information. Additional advantages of using wavelet-decomposed images include bringing data with different spatial resolution to a common resolution using low frequency sub-bands while providing access to edge features using the high frequency sub-bands. As shown in Figure 1, at each level of the wavelet decomposition, four new images are created from the original $N \times N$ -pixel image. The size of these new images is reduced to ¼ of the original size, i.e., the new size is $N/2 \times N/2$. The new images are named according to the filter (low-pass or high-pass), which is applied to the original image in horizontal and vertical directions. For example, the LH image is a result of applying the low-pass filter in horizontal direction and high-pass filter in vertical direction. Thus, the four images produced from each decomposition level are LL, LH, HL, and HH. The LL image is considered a reduced version of the original as it retains most details. The LH image contains horizontal edge features, while the HL contains vertical edge features. The HH only contains high frequency information, is typically noisy, and therefore, is not useful for the registration. In wavelet decomposition, only the LL image is used to produce the next level of decomposition [33].

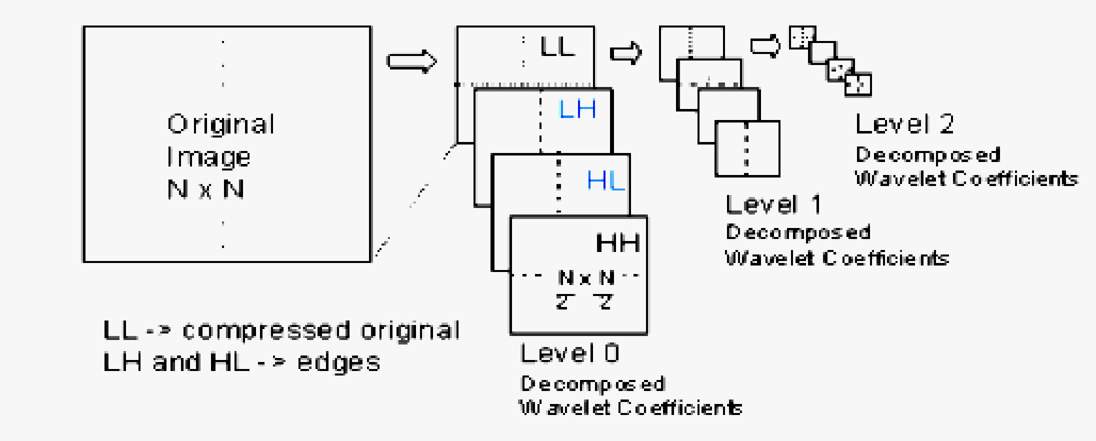


Figure 1. A 3-level wavelet decomposition of an N × N- pixel image

3. Particle Swarm Optimization (PSO)

PSO, which proposed by Dr. Eberhart and Dr. Kennedy in 1995, is a computational paradigm based on the idea of collaborative behavior and swarming in biological populations inspired by social behavior of bird flocking or fish schooling [27], [28], [29], and [30]. Recently PSO has been applied as an effective optimizer in many domains such as training artificial neural networks, linear constrained function optimization, wireless network optimization, data clustering, and many other areas where GA can be applied [29]. Computation in PSO is based on a population (swarm) of processing elements called particles in which each particle represent a candidate solution. PSO shares many similarities with evolutionary computation techniques such as GA's. The system is initialized with a population of random solutions and searches for optima by updating generations. The search process utilizes a combination of deterministic and probabilistic rules that depend on information sharing among their population members to enhance their search processes. However, unlike GA's, PSO has no evolution operators such as crossover and mutation. Each particle in the search space evolves its candidate solution over time, making use of its individual memory and knowledge gained by the swarm as a whole. Compared with GA's, the information sharing mechanism in PSO is considerably different. In GAs, chromosomes share information with each other, so the whole population moves like one group towards an optimal area. In PSO, the global best particle found among the swarm is the only information shared among particles. It is a one-way information sharing mechanism. Computation time in PSO is significantly less than in GA's, because all the particles in PSO tend to converge to the best solution quickly [29].

3.1 PSO Algorithm

When PSO is used to solve an optimization problem, a swarm of computational elements, called particles, is used to explore the solution space for an optimum solution. Each particle represents a candidate solution and is identified with specific coordinates in the dimensional search space. The position of the *i*-th particle is represented as *Xi = (xi1, xi2, ..., xiD)*. The velocity of a particle (rate of the position change between the current position and the next) is denoted as *Vi = (vi1, vi2, ..., viD)*. The fitness function is evaluated for each particle in the swarm and is compared to the fitness of the best previous result for that particle and to the fitness of the best particle among all particles in the swarm. After finding the two best values, the particles evolve by updating their velocities and positions according to the following equations:

$$V_i^{t+1} = w * v_i^{t} + c_1 * rand_1{}^{*}(p_{i-best} - x_i{}^{t}) + c_2 * rand_2 * (g_{best} - x_i{}^{t}) \qquad (3)$$

$$x_i{}^{t+1} = x_i{}^{t} + v_i{}^{t-1} \qquad (4)$$

Where *i =(1, 2, …, N)* and *N* is the size of the swarm; *pi_best* is the particle best reached solution and *gbest* is the global best solution in the swarm. *c1* and *c2* are cognitive and social parameters that are bounded between 0 and 2. *rand1* and *rand2* are two random numbers, with uniform distribution *U(0,1)* [33]. In equation (3), the first component represents the inertia of pervious velocity. The inertia weight *ω*, is a factor used to control the balance of the search algorithm between exploration and exploitation; the second component is "cognitive" component representing the private experience of the particle itself; the third component is "social" component, representing the cooperation among the particles. The recursive steps will go on until reaching to the termination condition (maximum number of iterations *K*).

3.2 Binary PSO and Feature Selection

A binary PSO algorithm has been developed in [30]. In the binary version, the particle position is coded as a binary string that imitates the chromosome in a genetic algorithm. The particle velocity function is used as a probability distribution for the position equation. That is, the particle position in a dimension is randomly generated using that distribution. The equation that updates the particle position becomes the following: [33]

$$\text{IF} rand_3 < \frac{1}{1+e^{-vi+1}}\ then\ x_i{}^{t+1} = 1 : else\ x_i{}^{t+1} = 0 \qquad (5)$$

4. PSO-Based Feature Selection

The task for the binary PSO algorithm is to search for the most representative feature subset through the extracted DCT or DWT feature space. Each particle in the algorithm represents a possible candidate solution (feature subset). Evolution is driven by a fitness function defined in terms of class separation (scatter index) which gives an indication of the expected fitness on future trials [33].

4.1 Chromosome Representation

The initial coding for each particle is randomly produced where each particle is coded for imitating a chromosome in a genetic algorithm; each particle was coded to a binary alphabetic string *P = F1F2… Fn, n = 1, 2, …, m;* where m is the length of the feature vector extracted by the DCT or the DWT. Each gene in the *m*-length chromosome represents the feature selection. *"1"* denotes that the corresponding feature is selected, otherwise denotes rejection. The binary PSO algorithm is used to search the *2m* gene space for the optimal feature subset where optimality is defined with respect to class separation. For example, when a 10- dimensional data set *(n=10) P = F1 F2 F3 F4 F5 F6 F7 F8 F9 F10* is analyzed using binary PSO to select features, we can select any subset of features smaller than n, i.e. PSO can choose a random 6 features, *F1 F2 F4 F6 F8 F9* by setting bits *1, 2, 4, 6, 8,* and *9* in the particle chromosome. For each particle, the effectiveness of the selected feature subset in retaining the maximum accuracy in representing the original feature set is evaluated based on its fitness value [33].

4.2 Fitness Function

The m-genes in the particle represent the parameters to be iteratively evolved by PSO. In each generation, each particle (or individual) is evaluated, and a value of *goodness or fitness* is returned by a fitness function. This evolution is driven by the fitness function *F* that evaluates the quality of evolved particles in terms of their ability to maximize the class separation term indicated by the scatter index among the different classes [3]. We have two classes and number of images within each class and we find the means of corresponding classes and the grand mean in the feature space, Mi can be calculated as:

$$M_i = \frac{1}{N_i}\sum_{j=1}^{N_i} W_j^{(i)} \qquad (6)$$

where *Wj(j) , j=1,2,…,Ni,* represents the sample images from class *wi* and the grand mean M_0 is:

$$M_0 = \frac{1}{N}\sum_{i=1}^{L} N_i M_i \qquad (7)$$

Where *n* is the total number of images for all the classes. Thus, between class scatter fitness function *F* is computed as follows:

$$F = \sqrt{\sum_{i=1}^{l}\ (M_i - M_0)^t (M_i - M_0)} \qquad (8)$$

In the next step of our algorithm, we use the Euclidean distance by means of measuring the similarity between the test vector and the train vectors in each class. Equation of Euclidean distance is defined by (9):

$$D = \sqrt{\sum_{i=1}^{N}(p_i - q_i)^2} \qquad (9)$$

Where *pi* (or *qi*) is the coordinate of *p* (or *q*) in dimension *i.* query image to every image in the database are calculated. The index of the image which has the smallest distance with the image under test is considered to be the required index.

5. Results and Discussion

The block diagram of the proposed is shown in Figure 2. The block diagram shows various processing steps of an input image in the training and recognition stages.

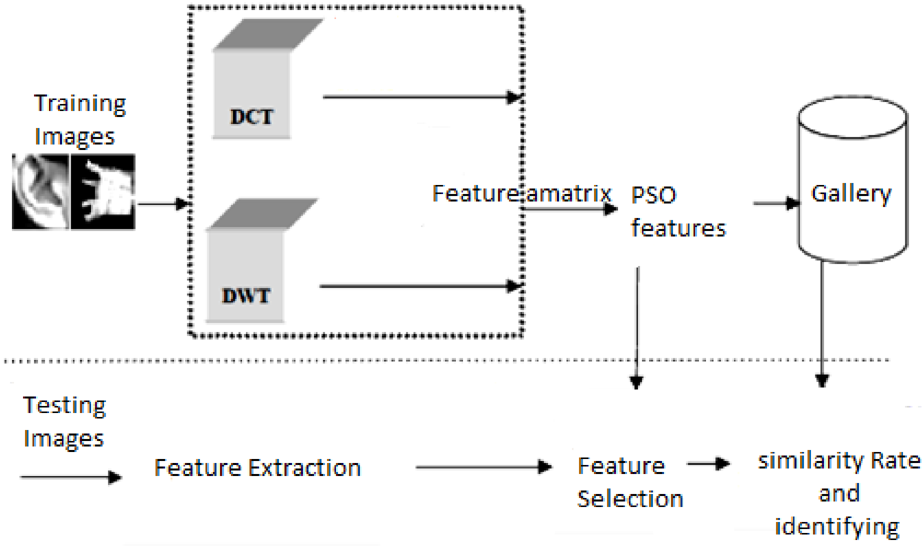


Figure 2. Block diagram of the proposed multimodal recognition system

We have constructed our database as follows: The palm and ear data consisting of 60 users [36,37]. Each user has been asked to provide three ear images and four palm impressions (of the same palm). In the preprocessing step the palm images are cropped to a size of 384 × 284 pixels and also ear images are cropped to a size of 150 × 150 pixels. The normalization step includes geometric normalization, masking and photometric normalization. In this phase, all images are scaled in a standard 80 × 80 size. In the next step, we remove unessential palm and ear areas with masking. Also, we rotate some palm and ear images in each class and run our model. Different levels of masking are experimented for finding the best one to get as good performance as possible for the algorithm. Finally, the images are normalized for illumination. Then, these images are given for feature selection level. In the last section, we compare the performance of the proposed PSO-based features selection algorithm with the performance of a GA-based features selection algorithm. The parameters used for the binary PSO and the GA algorithms are given in Table 1.

Swarm size N	60
Cognitive parameters c1	2
Social parameter c2	2
Inertia weight ^{ɯ}	0.6
Number of iterations	100

Table 1. (a) PSO parameter setting

The population	60
Crossover probability (pc)	0.8
Mutation probability (pm)	0.5
Number of iterations	100

(b) GA parameter setting

5.1 Experiment 1

In this test, our algorithm based on PSO had feature vectors with different subset sizes of DCT coefficients. Subset sizes 40 × 40 , 30 × 30 , 20 × 20 and 10 × 10 of the original 80 × 80 DCT array are used in this experiment as input to the subsequent feature extraction phase. Table 2 showed the best average recognition rate of 96.5% which achieved by using the DCT (40 × 40) feature vector and the PSO-based feature selection algorithm. In general, PSO and GA selection algorithms have comparable performance in terms of recognition rates, but in all test cases, the number of selected features is smaller by using the PSO selection algorithm. We have found that PSO-based selection algorithm takes more time than GA-based selection algorithm but the rate of recognition by using PSO is higher in comparison with GA. Moreover, we can claim that our method is rotate invariant.

DCT	PSO	GA
40 x 40	100	70
30 x 30	80	50
20 x 20	50	30
10 x 10	20	10

Table 2. (a) Training Time (sec)

DCT	PSO	GA
40 x 40	96.5	92.1
30 x 30	96.3	92.0
20 x 20	96.1	91.7
10 x 10	95.8	91.3

(b) Recognition Rate

In continue, DWT coefficient features have been extracted from each palm and ear image. Table 3 shows the best average recognition rate of 97.3% by using PSO algorithm.

DWT	PSO	GA
40x40	80	60
20x20	70	60
10x10	40	30
5x5	10	10

Table 3. (a) Training Time (sec)

DWT	PSO	GA
40x40	97.3	95.2
20x20	97.1	94.6
10x10	96.8	93.3
5x5	96.3	93.1

(b) Recognition Rate

In table 4, performance of the proposed algorithm in terms of its recognition rate is compared to various feature recognition algorithms found in the literature using the POLYU and USTB databases [34,35].

Table 4 indicates the superiority of the proposed algorithm utilizing the DWT feature extraction and PSO feature selection. As far as feature selection is concerned with the algorithm, it selects the optimal number of elements in the feature vector which has a great influence on the training and recognition times of the algorithm.

Method	Recognition rate	Test condition
DCT+PSO feature selection	96.55%	Four images (two ear and two palm) per person were used in the training set and remaining images were used for testing. The average recognition time for recognizing an input image is 1.05 sec.
DWT+PSO feature selection	97.3%	
Eigen ear	80%	
Eigen palm	90%	
Eigen palm+Eigen ear	92%	

Table 4. Comparison of recognition for various feature recognition algorithm

6. Conclusion

In this paper, we used a famous algorithm called PSO in multimodal recognition systems based on the POLYU and USTB databases for palm and ear images have been used. In the step of feature extraction by using the DCT and the DWT, two feature vectors were selected. By using these techniques subset feature space was built. After feature extraction level, PSO and GA feature selection methods were used for selecting the best features and those features were the entrance of classification level. Experimental results showed PSO-based feature selection algorithm in generating excellent recognition rather than GA-based feature selection algorithm.

References

[1] Jain, A. and Ross, A. “Information Fusion in Biometrics.” In Proceedings AVBPA, Halmstad, Sweden, June 2001, pp.354-359.

[2] R. Brunelli and T. Poggio, “Face Recognition: Features versus Templates,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol.15, No.10, pp.1042-1052, 1993.

[3] C. Liu and H. Wechsler, “Evolutionary Pursuit and Its Application to Face Recognition,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol.22, No.6, pp.570-582, 2000.

[4] M. A. Turk and A. P. Pentland, “Face Recognition using Eigenfaces,” *Proc. of IEEE Conference on Computer Vision and Pattern Recognition*, pp.586-591, June 1991.

[5] L. Du, Z. Jia, and L. Xue, “Human Face Recognition Based on Principal Component Analysis and Particle Swarm Optimization -BP Neural Network,” *Proc. 3rd Conference on Natural Computation (ICNC 2007)*, Vol.3, pp.287-291, August 2007.

[6] X. Yi-qiong, L. Bi-cheng and W. Bo, “Face Recognition by Fast Independent Component Analysis and Genetic Algorithm,” *Proc. of the 4th International Conference on Computer and Information Technology (CIT’04)*, pp.194-198, Sept. 2004.

[7] X. Fan and B. Verma, “Face recognition: a new feature selection and classification technique,” *Proc. 7th Asia-Pacific Conference on Complex Systems*, December 2004.

[8] A. S. Samra, S. E. Gad Allah, R. M. Ibrahim, “Face Recognition Using Wavelet Transform, Fast Fourier Transform and Discrete Cosine Transform,” *Proc. 46th IEEE International Midwest Symp. Circuits and Systems (MWSCAS'03)*, Vol.1, pp.272-275, 2003.

[9] C. Podilchuk and X. Zhang, “Face Recognition Using DCT-Based Feature Vectors,” *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP’96)*, Vol.4, pp.2144-2147, May 1996.

[10] Z. Yankun and L. Chongqing, “Efficient Face Recognition Method based on DCT and LDA,” *Journal of Systems Engineering and Electronics*, Vol.15, No.2, pp.211-216, 2004.

[11] C.-J. Tu, L.-Y. Chuang, J.-Y. Chang, and C.-H. Yang, “Feature Selection using PSO-SVM,” *International Journal of Computer Science (IAENG)*, Vol.33, No.1, IJCS_33_1_18.

[12] E. Kokiopoulou and P. Frossard, “Classification-Specific Feature Sampling for Face Recognition,” *Proc. IEEE 8th Workshop on Multimedia Signal Processing*, pp.20-23, 2006A.

[13] Y. Yang, J. Wright,Y. Ma, and S. S. Sastry, “Feature Selection in Face Recognition: A Sparse Representation Perspective,” submitted for publication, 2007.

[14] P. M. Narendra and K. Fukunage, “A Branch and Bound Algorithm for Feature Subset Selection,” *IEEE Trans. Computers*, Vol.6, No.9, pp.917-922, Sept. 1977.

[15] P. Pudil, J. Novovicova, and J. Kittler, “Floating Search Methods in Feature Selection,” *Pattern Recognition Letters*, Vol.15, pp.1119-1125, 1994.

[16] B. Roberto, “Using Mutual Information for Selecting Features in Supervised Neural Net Learning,” *IEEE Trans. Neural Networks*, Vol.5, No.4, pp.537-550, 1994.

[17] H. Zhang and G. Sun, “Feature Selection Using Tabu Search Method,” *Pattern Recognition Letters*, Vol.35, pp.701-711, 2002.

[18] D.-S. Kim, I.-J. Jeon, S.-Y. Lee, P.-K. Rhee, and D.-J. Chung, “Embedded Face Recognition based on Fast Genetic Algorithm for Intelligent Digital Photography,” *IEEE Trans. Consumer Electronics*, Vol.52, No.3, pp.726-734, August 2006.

[19] M. L. Raymer, W. F. Punch, E. D. Goodman, L.A. Kuhn, and A. K Jain, “Dimensionality Reduction Using Genetic Algorithms,” *IEEE Trans. Evolutionary Computation*, vol. 4, no. 2, pp. 164-171, July 2000.

[20] H. R. Kanan, K. Faez, and M. Hosseinzadeh, “Face Recognition System Using Ant Colony Optimization- Based Selected Features,” *Proc. IEEE Symp. Computational Intelligence in Security and Defense Applications (CISDA 2007)*, pp.57-62, April 2007.

[21] S. Cruz-Llanas, J. Fierrez-Aguilar, J. Ortega Garcia and J. Gonzalez-Rodriguez, “A Comparative Evaluation of Global Representation-Based Schemes for Face Verification”, Proc. Intl. Conf. on Image Processing, ICIP 2003.

[22] M. Yu, G. Yan, and Q.-W. Zhu, “New Face recognition Method Based on DWT/DCT Combined Feature Selection,” *Proc. 5th International Conference on Machine Learning and Cybernetics*, pp.3233-3236, August 2006.

[23] Hong, L., Jain, A.k, "Integrating faces and fingerprints for personal identification," IEEE Trans. PAMI 20 (12), 1295-1307. 1998.

[24] Zuev, Y., Ivanon, S., 1996. "The voting as a way to increase the decision reliability. In: Foundations of Information/Decision Fusion with Applications to Engineering Problems," Washington, DC, USA. pp.206–210.

[25] D.-Q. Dai and H. Yan, “Wavelets and Face Recognition,” in Face Recognition, K. Delac and M. Grgic, Eds. I-Tech, Vienna, Austria, 2007, pp.558.

[26] J. Sergent, “Microgenesis of face perception,”. In: H.D. Ellis, M.A. Jeeves, F. Newcombe and A. Young, Editors, *Aspects of Face Processing*, Nijhoff, Dordrecht (1986).

[27] J. Kennedy and R. Eberhart, “Particle swarm optimization,” *Proc. IEEE International Conference on Neural Networks*, pp.1942-1948, 1995.

[28] R. C. Eberhart and J. Kennedy, “A New Optimizer Using Particles Swarm Theory,” *Proc. Roc. 6th International Symp. Micro Machine and Human Science*, pp.39-43, Oct. 1995.

[29] R. C. Eberhart and Y. Shi, “Comparison between Genetic Algorithms and Particle Swarm Optimization,” *Proc. 7th international Conference on Evolutionary Programming*, pp.611-616, 1998.

[30] J. Kennedy and R. C. Eberhart, “A Discrete Binary Version of the Particle Swarm Algorithm,” *Proc. IEEE International Conference on Systems, Man, and Cybernetics*, Vol.5, pp.4104-4108, Oct. 1997.

[31] Jain, A.K., Hong, L., Pankanti, S,“Can multibiometrics improve performance?” In Proc. AutoID_99, Summit, NJ, USA. pp.59-64. 1999. [32] A. S. Tolba, A.H. El-Baz, and A.A. El-Harby “Face Recognition: A Literature Review,” *International Journal of Signal Processing*, Vol.2, No.2, pp.88-103. 2006.

[32] L. Xu, A. Kryzak and C.Y. Suen, "Methods of Combining Multiple Classifiers and Their Application to Handwriting Recognition," IEEE Trans. on Systems, Man and Cybernetics, Vol.22, No.3, pp.418-435, May-June 1992.

[33] R. M. Ramadan, R.Raheb, and F.Abdel-Kader “Face Recognition Using Particle Swarm Optimization-Based Selected features,” *International Journal of Signal Processing*, Vol.2, No.2, June 2009.

[34] Jain, A. K. and Ross, A., “Multibiometric Systems”, In Communications of the ACM, Special Issue on Multimodal Interfaces, Vol.47, No.1, pp.34-40, January 2004.

[35] Kittler, J., Hatef, M., Duin, R. P. and Matas, J.G. “On Combining Classifiers”, IEEE Transactions on PAMI 20 (3) (1998) 226-239.

[36] http://www.ustb.edu.cn/resb

[37] http://www.comp.polyu.edu.hk/_biometrics

A Wideband Low-Noise Downconversion Mixerwith Positive-Negative Feedbacks

Hadi Naderian*
RF Circuit, M.Sc, Electrical Engineering Department, Shahid Bahonar University of Kerman
h.naderian@eng.uk.ac.ir
Ahmad Hakimi
RF Circuit and Microwave Components, Ph.D, Electrical Engineering Department, Shahid Bahonar University of Kerman
Hakimi@uk.ac.ir

Received: 07/Apr/2013 Accepted: 15/Jun/2013

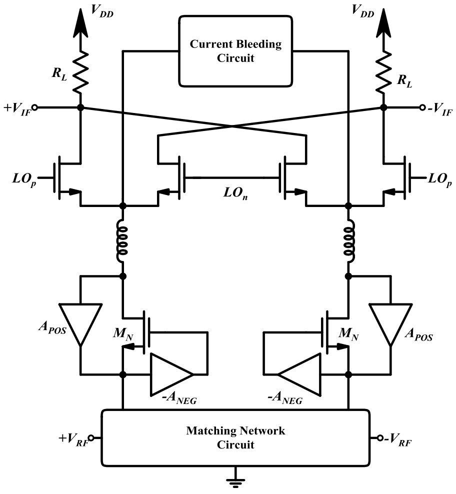
Abstract

This paper presents a wideband low-noise mixer in CMOS 0.13-um technology that operates between 2–10.5 GHz. The mixer has a Gilbert cell configuration that employs broadband low-noise trans conductors designed using the negative-positive feedback technique used in low-noise amplifier designs. This method allows broadband input matching. The current-bleeding technique is also used so that a high conversion gain can be achieved. Simulation results show excellent noise and gain performance across the frequency span with an average double-sideband noise figure of 2.9 dB and a conversion gain of 15.5 dB. It has a third-order intermodulation intercept point of -8.7 dBm at 5 GHz.

Keywords: Current-Bleeding, Feedback, Low-Noise, Noise Cancellation, Wideband.

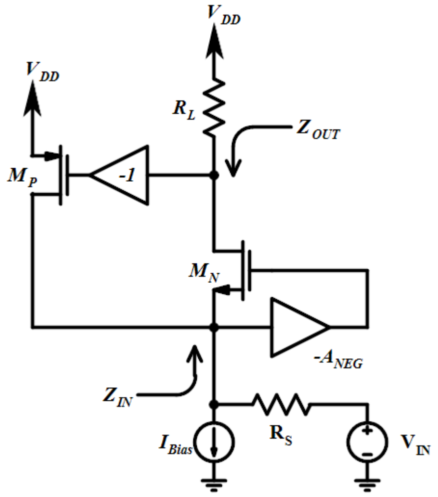
1. Introduction

Active mixers based on the Gilbert cell configuration often exhibit a large amount of noise. This leads to strict requirements for the noise figure (NF) of the low-noise amplifier (LNA) preceding the mixer such that a particular signal-to-noise ratio can be achieved. This usually requires at least one very low-noise LNA that has enough gain and noise performance to mitigate the noise added by the mixer. Power consumption is also a problem as the LNA NF decreases when larger transistors are used. However, these requirements can be much relaxed or the LNA can be removed if the mixer NF is low enough. The Gilbert cell mixer has been widely used in integrated circuit (IC) design even though it exhibits moderate noise. However, its NF can be drastically reduced by combining the LNA and mixer into a single component. Narrowband low-noise mixers have been proposed in other works [1]–[4], where the transconductors were replaced by inductive-degenerated LNAs.



Block diagram of proposed mixer circuit.

* Corresponding Author



Simplified block diagram of transconductor.

To convert a Gilbert cell into a wideband low-noise mixer, the trans conductors must be wideband in terms of NF, gain, and input matching. Many broadband and UWB LNAs have been proposed [5]–[7]. In [5], an active feedback approach was used to achieve broadband input matching and gain. The circuits in [6] and [7] use filters to achieve broadband input matching and low noise performance. Another broadband LNA design method is the noise-cancelling technique [8], which has been used for mixer in [9].

A common-gate (CG) LNA has been widely investigated because it features superior bandwidth, linearity, stability, and robustness to PVT variations compared to a common-source (CS) topology [10]. In spite of these advantages, the dependence of gain and NF on the restricted transconductance (gm) makes this topology unsuitable for various wireless applications. The input impedance of a CG LNA is simplified as 1/gm, and the noise factor is inversely proportional to gm [11]. In order to achieve high gain and low NF, gm should be increased, which deteriorates the 50Ω input impedance matching for a conventional CG LNA.

In this paper to achieve high gain and low NF without sacrificing bandwidth, linearity, and power consumption, a differential gm-boosted CG transconductors with a positive-negative feedback technique is proposed. The proposed mixer with output buffers delivers a maximum conversion gain of 15.5 dB, a minimum NF of 2.6 dB, an IIP3 of -8.7 dBm, and 22.44mW power consumption.

2. Circuit Description

The proposed wideband low-noise mixer block diagram is shown in Figure 1. The mixer based on the Gilbert cell topology with some modifications. The mixer is comprised of four building blocks: positive-negative feedback transconductors, peaking inductors, current bleeding and switching pairs. A detailed design analysis of the positive-negative feedback transconductors block is provided first, followed by a description of each block.

2.1 Positive- Negative Feedback Trans conductors

The proposed topology, shown in Figure 2, consists of cross-coupled capacitors in negative and PMOS transistors in positive feedback branches in a differential CG configuration.RL is the mixer load resistor, assuming there is no loss through the switch, and the tail capacitance of the off switch is negligible compared to the load resistor. The differential signals flow to the sources of the NMOS transistors, and are also cross-coupled to the gates of the opposite NMOS transistors through capacitors, which results in a shunt-series negative feedback path [12]-[15]. The outputs of the NMOS transistors are coupled to the sources of the opposite NMOS transistors creating a shunt-shunt positive feedback loop.

The input impedance is obtained as

$$Z_{\text{IN}} = \frac{1}{g_{mMn}(1+A_{NEG})(1-A_{POS})}. \qquad (1)$$

using input shunt-negative and shunt-positive feedback theory [16]. ANEG, which is approximately given by $C_C/(C_C+C_{gs})$, is almost unity. Positive feedback is equivalent to $g_{mMp}R_L$, can be varied from 0 to 1 for an arbitrary choice of g_{mMp} required to achieve an input matching condition. The output impedance is given by

$$Z_{OUT} = \frac{R_L\left[r_{ds}+R_S\left\{1+(1+A_{NEG})g_m r_{ds}\right\}\right]}{R_L+r_{ds}+R_S\left\{1+(1+A_{NEG})g_m r_{ds}\right\}(1-A_{POS})} \qquad (2)$$

r_{ds} is the output impedance of transconductance transistor. While A_{POS} is increased, the output impedance, as well as g_{mMn} for the input matching, can be increased. In this architecture, the voltage gain is given by

$$A_V = \frac{g_m(1+A_{NEG})}{2}\times\frac{2}{\pi} \times\frac{R_L\left[r_{ds}+R_S\left\{1+(1+A_{NEG})g_m r_{ds}\right\}\right]}{R_L+r_{ds}+R_S\left\{1+(1+A_{NEG})g_m r_{ds}\right\}(1-A_{POS})} \qquad (3)$$

where 2/π is an approximation of switching gain. With the help of gm boosting through the capacitor cross-coupling (CCC) negative feedback, effective transconductance (G_M) is the same as the NMOS transconductance itself. As a result, the voltage gain (=G_M.Z_{OUT}) can be high with relatively low power consumption through the large Z_{OUT} and large G_M.

The NF of the circuit can be computed considering thermal channel noise of transconductance transistors and load noise. For high IF thermal noise is dominant, so flicker noise of switching stage was neglected [17]. In this case [18],

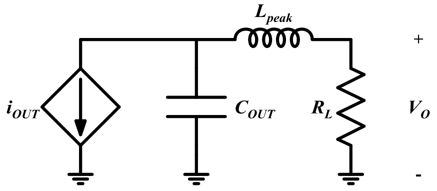
$$F = 1 + \frac{\gamma(1 - A_{POS})}{\alpha(1 + A_{NEG})} + g_{mMp} R_S \frac{\gamma}{\alpha} + \frac{R_S}{R_L}(2 - A_{POS})^2 \qquad (4)$$

Where γ is the MOS transistor thermal noise coefficient, α is defined as the ratio of g_{mMn} to the zero-bias drain conductance g_{d0}. The second term represents the channel noise contribution of g_{mMn}, which can be greatly reduced through A_{NEG} as well as A_{POS}. The channel noise of M_N flows to the gate and source of an opposite M_N with the same phase through C_C and the positive path, respectively. Thus, the combination of positive feedback and the negative feedback loop contributes to channel-noise cancellation. The third and fourth terms show the noise induced by M_P in the positive feedback path, and the load, respectively. The noise due to M_P can be decreased by using small g_{mMp}, and the load noise is reduced by A_{POS}.

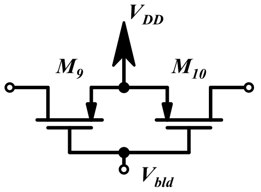
2.2 Inductive Peaking

The mixer bandwidth can be significantly affected by the large output capacitance from transconductors, as well as from the bleeding circuit and switching pairs. Inductive peaking can be used for bandwidth extension. Series peaking is used in this design and the peaking inductors are placed between the switching pairs and the transconductors, as shown in Figure 1.

To understand the operation of these inductors, a simplified circuit is shown in Figure 3 when only one of the switches is on. Preceding the mixer core is the transconductors, which can be approximated by a voltage-controlled current source; C_{out} is the collective output capacitance from the transconductor and the bleeding circuit; R_L is the mixer load resistor, assuming there is no loss through the switch, and the tail capacitance of the off switch is negligible compared to the load resistor.The basic theory of inductive peaking can be explained with Figure 3 and the step response. Imagine the circuit without the inductor, the rise time at the output is about 2.2RC, if the rise time is defined to be the elapsed time between 10%–90% of the final output voltage value. To decrease the charge time, i.e., increase the bandwidth, the inductor is used. At t=0, there is a sudden step change in the current source.



Two-pole series peaking network [9].



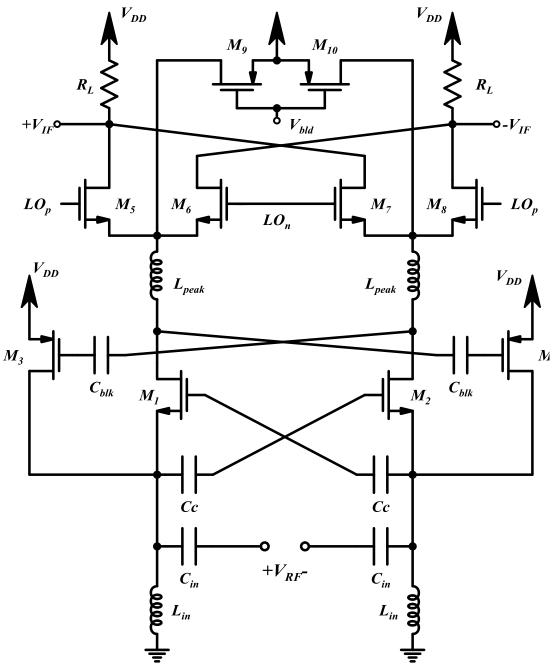
PMOS bleeding circuit.

The high impedance of the inductor decouples the resistor from the capacitor, which means all the current goes into charging the capacitor. Therefore, the rise time decreases, and hence the bandwidth is enhanced.

2.3 Switching Pairs and Current Bleeding

In general, increasing the bias current of the RF transconductance stage makes higher gain and better linearity possible, but a larger LO switching current causes voltage headroom issue. Therefore, as shown in Figure 4, the static current bleeding technique is implemented by using two PMOSFETs to reduce the bias current of the LO switches [19].

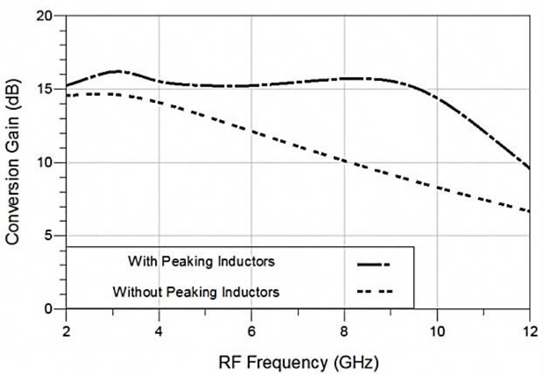
The gain of the mixer is maximized by fast switching similar to a square wave. The turn-on voltage for the switching pairs is proportional to their overdrive voltage, and it needs to be low to ensure fast switching. By having a lower overdrive voltage, the size of the load resistors can be increased to achieve an even higher gain.



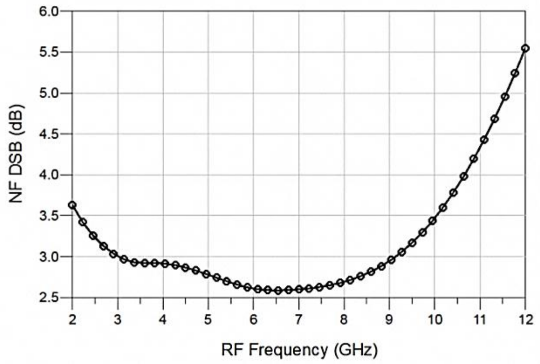
Complete circuit schematic of the proposed mixer.

3. Simulation Results

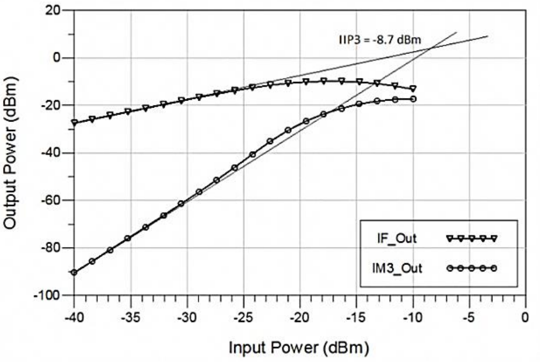
The mixer was designed using TSMC's CMOS 0.13-µm technology. Simulation was run using Advanced Design System (ADS) software. The mixer is designed to operate between 2–10.5 GHz with a local oscillator (LO) power of 0 dBm. Quality factor of peaking inductors and input inductors has been set to 4 and 10, respectively.



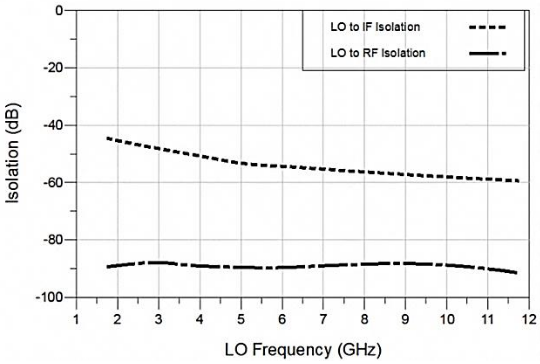
Conversion gain of the proposed mixer.



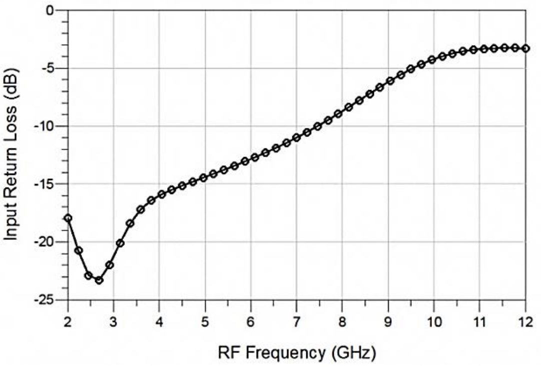
DSB Noise Figure simulation result.



Output powers of the IF and the IM3 product with the input at 5 GHz.



Port-to-Port isolations versus LO frequency.



Input matching of the mixer.

For all simulation results, the IF is always kept at a constant 250 MHz, while the RF and LO frequencies are being changed together with the LO being 250 MHz lower than the RF. Two source-follower buffers were used to combine the differential IF signal into a single-ended output.

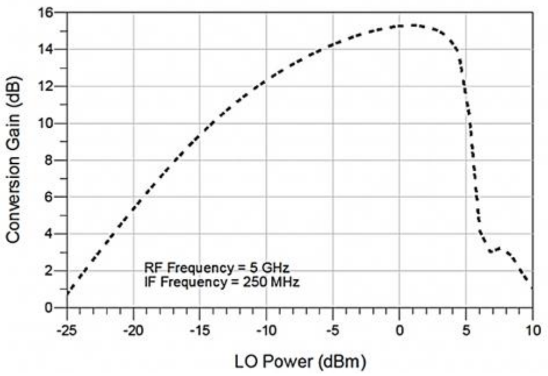
The conversion gain of the mixer is measured across the input frequency ranging from 2 to 10.5 GHz. The input RF power was kept at -40 dBm. Figure 6 shows the conversion gain simulated results. This plot also includes the simulated result without the peaking inductors. The importance of the peaking inductors can be clearly seen in this plot, where there is a much sharper gain roll off compared to the simulated result with peaking.

When characterizing the noise performance of a mixer, either the double- or single-sideband NF can be used [15]. Figure 7 shows the simulated double-sideband NF of the mixer versus input frequency. The circuit has a low and relatively flat NF across bandwidth. The minimum value of NF is 2.6 dB at 6.5 GHz and the maximum is 3.9 dB at 10.5 GHz.

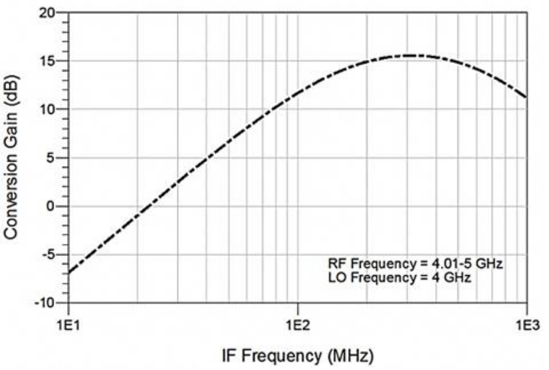
The third-order intermodulation intercept point (IIP3) of the mixers was simulated. To simulate the IIP3, a two-tone signal separated by 1 MHz was used. Shown in Figure 8 is the simulated IF and third-order intermodulation (IM3) output powers with the input RF frequency at 5 GHz. The extrapolated IIP3 was -8.7 dBm.

Table I Comparison of Wideband Down-Converters with This Work

Parameters	This Work	[20]	[9]	[21]	[22]	[23]z
CMOS Technology	0.13 um	0.13 um	0.13 um	65 nm	90 nm	0.18 um
RF Bandwidth (GHz)	2 - 10.5	3.1 - 10.6	1 - 5.5	2 - 8	0.1 – 3.85	0.2 - 13
Conversion Gain (dB)	15.5	9.8 - 14	17.5	23 (Voltage)	12.1	9.9
NF DSB (dB)	2.9	14.5 - 19.6	3.9	4.5	8.4-11.5 (SSB)	11.7
IIP3 (dBm)	-8.7	-11	+0.84	-7	N/A	-10
LO Power (dBm)	0	3	0	N/A	1	5
Voltage Supply (V)	1.2	1.2	1.5	1.2	1.2	0.8
Power Consumption (mW)	22.44	1.85	34.5	39	9.8	0.88



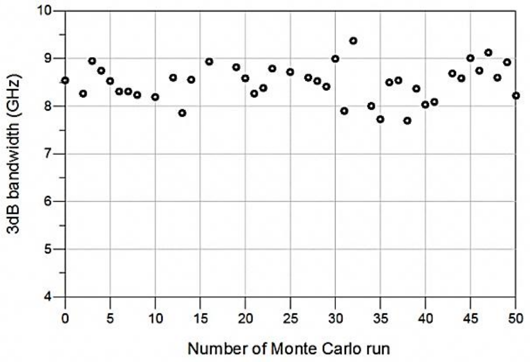
Conversion gain versus LO power.



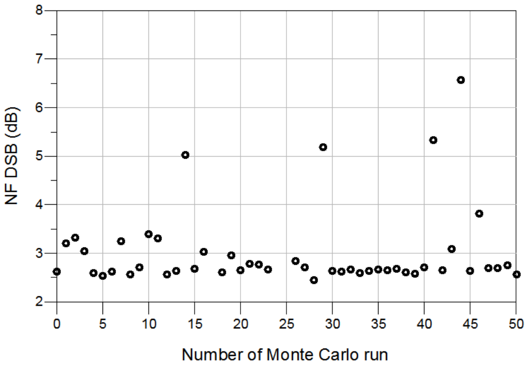
Simulation results of IF bandwidth.

The LO-to-RF port-to-port isolation and LO-to-IF port-to-port isolation were simulated. Since the LO is 250 MHz lower than the RF, the isolation was simulated from 1.75 GHz to 11.75 GHz. Figure 9 shows the simulated mixer ports isolation.

Figure 10 shows the input return loss. The simulation results of conversion gain versus LO input



Result of Monte Carlo analysis of the mixer bandwidth.



Result of Monte Carlo analysis of the mixer bandwidth

power is shown in Figure 11 which shown that 0 dBm LO power is optimum value for this circuit. The simulation of IF bandwidth is shown in Figure 12 that shows 3-dB bandwidth of conversion gain at the IF port is about 700 MHz. The mixer core draws a total current of 3.54 mA and buffers draws 15.6 mA from a 1.2-V supply, respectively.

The impact of the process and mismatch variations on the mixer frequency response and noise figure has been evaluated by utilizing the well-known Monte-Carlo statistical analysis. Device variations are fluctuations in MOS parameters and include, Effective gate length (L_{eff}), Threshold voltage (V_t), Thickness of the gate oxide (T_{ox}), and the drain/source region parasitic resistance (R_{dsw}) [24]. The Monte-Carlo simulation of the mixer bandwidth and noise figure is depicted in Figure 13 and Figure 14, respectively. In the noise figure Monte-Carlo analysis has been performed in 6 GHz RF frequency.

Table 1 shows a comparison between this work and recently published broadband down-converters in CMOS. The mixer outperforms others in terms of noise performance while still having a comparable gain. Their circuit structures are also different. This work and [9] have a current reuse structure, whereas [21] is a LNA Mixer TIA in cascade and [22] is a folded mixer with a folded low-noise transconductors. [23] uses bulk-injection and switched biasing techniques together.

4. Conclusion

A double-balanced Gilbert-type mixer based on the positive-negative feedback technique was designed using a 0.13-um CMOS process covering the frequency band between 2 and 10.5 GHz. The noise-cancelling technique allows broadband input matching and noise cancellation at the same time. Together with the current-bleeding technique, a high conversion gain was also achieved. Moreover, parasitic capacitances cancellation was done by adding an extra inductor between switching and transconductance stages to obtain better NF and gain performance. The circuit exhibits 2.9 dB average noise figure while the mixer core draws only 3.54 mA form a 1.2-V supply.

Acknowledgments

This work has been supported under grant UK91-05-07 by the Education & Research Institute for ICT (ERICT) of Iran (Contract number 6987/500). The authors would like to thank Dr. Masoud Movahhedi for his constructive suggestions to improve the manuscript.

References

[1] H. Sjoland, A. Karimi-Sanjaani, and A. Abidi, "A merged CMOS LNA and mixer for a WCDMA receiver," IEEE J. Solid-State Circuits, Vol.38, No.6, pp.1045-1050, Jun. 2003.

[2] E. Sacchi, I. Bietti, S. Erba, L. Tee, P. Vilmercati, and R. Castello, "A 15mW, 70 kHz 1/f corner direct conversion CMOS receiver," in Proc. IEEE Custom Integr. Circuits Conf., Sep. 2003, pp.459-462.

[3] T.-A. Phan, C.-W. Kim, M.-S. Kang, S.-G. Lee, and C.-D. Su, "A high performance CMOS direct down conversion mixer for UWB system," IEICE Trans. Electron., Vol. E88-C, No.12, pp.2316–2321, Dec. 2005.

[4] A. Liscidini, A. Mazzanti, R. Tonietto, L. Vandi, P. Andreani, and R.Castello, "Single-stage low-power quadrature RF receiver front-end: The LMV cell," IEEE J. Solid-State Circuits, Vol.41, No.12, pp.2832–2841, Dec. 2006.

[5] S. Andersson, C. Svenson, and O. Drugge, "Wideband LNA for a multistandard wireless receiver in 0.18 _m CMOS," in Proc. 29th Eur.Solid-State Circuits Conf., Sep. 2003, pp.655–658.

[6] A. Bevilacqua and A. Niknejad, "An ultrawideband CMOS low-noise amplifier for 3.1–10.6-GHz wireless receivers," IEEE J. Solid-State Circuits, Vol.39, No.12, pp.2259-2268, Dec. 2004.

[7] A. Bevilacqua, C. Sandner, A. Gerosa, and A. Neviani, "A fully integrated differential CMOS LNA for 3-5-GHz ultrawideband wireless receivers," IEEE Microw. Wireless Compon. Lett., Vol.16, No.3, pp.134-136, Mar. 2006.

[8] F. Bruccoleri, E. Klumperink, and B. Nauta, "Wide-band CMOS lownoise amplifier exploiting thermal noise canceling," IEEE J. Solid-State Circuits, Vol.39, No.2, pp.275-282, Feb. 2004.

[9] Stanley S. K. Ho, and Carlos E. Saavedra, "A CMOS Broadband Low-Noise Mixer With Noise Cancellation," IEEE Transactions On Microwave Theory And Techniques, Vol.58, No.5, May 2010.

[10] H. Darabi and A. A. Abidi, "A 4.5mW 900MHz CMOS Receiver for Wireless Paging,"IEEE J. Solid-State Circuits, Vol.35, No.8, pp.1085-1096, Aug. 2000.

[11] X. Guan, A. Hajimiri, "A 24GHz CMOS Front-End," IEEE J. Solid-State Circuits, Vol.39, issue 2, pp.368-373, Feb. 2004.

[12] S. Woo , W. Kim , C. Lee , K. Lim and J. Laskar "A 3.6 mW differential common-gate CMOS LNA with positive–negative feedback", IEEE Int. Solid-State Circuits Conf. Tech. Dig., pp.218-219, 2009.

[13] Naderian, H.; Hakimi, A.; Movahhedi, M.; "A wideband low-noise down conversion mixer with positive-negative feedbacks," Electrical Engineering (ICEE), 2012 20th Iranian Conference on , Vol., No., pp.206-210, 15-17 May 2012.

[14] Sanghyun Woo; Woonyun Kim; Chang-Ho Lee; Hyoungsoo Kim; Laskar, J.; "A Wideband Low-Power CMOS LNA With Positive–Negative Feedback for Noise, Gain, and Linearity Optimization," Microwave Theory and Techniques, IEEE Transactions on, Vol.60, No.10, pp.3169-3178, Oct. 2012.

[15] W. Zhuo, X. Li, Shekhar, S. H. K. Embabi, J. P. de Gyvez, D. J.Allstot, and E. Sanchez-Sinencio, "A Capacitor Cross-Coupled Common-Gate Low-Noise Amplifier", IEEE Journal of Transactions on Circuits and Systems, Dec. 2005, No.12, pp.875-879.

[16] Paul R. Gray, Paul J. Hurst, Stephen H. Lewis, Robert G. Meyer, "Analysis and Design of Analog Integrated Circuits", 5th Edition, John Wiley & Sons,May 2009.

[17] Wei Cheng; Annema, A.J.; Croon, J.A.; Nauta, B.; "Noise and Nonlinearity Modeling of Active Mixers for Fast and Accurate Estimation," Circuits and Systems I: Regular Papers, IEEE Transactions on, Vol.58, No.2, pp.276-289, Feb. 2011.

[18] A. Liscidini, et al., "Analysis and Design of Configurable LNAs in Feedback Common-Gate Topologies," IEEE Trans. Circuits and Systems-II, Vol.55, No.8, pp.733-737, Aug.2008.

[19] H. Darabi and J. Chiu, "A noise cancellation technique in active-RF CMOS mixers," in Int. Solid-State Circuits Conf., 2005, pp.544-545, Session 29.

[20] S. Jeong-Bae, K. Jong-Ha, S. Hyuk, and Y. Tae-Yeoul, "A Low-Power and High-Gain Mixer for UWB Systems," Microwave and Wireless Components Letters, IEEE, Vol.18, pp.803-805, 2008.

[21] S. Lee, J. Bergervoet, K. Harish, D. Leenaerts, R. Roovers, R. van de Beek, and G. van der Weide, "A broadband receive chain in 65 nm CMOS," in IEEE Int. Solid-State Circuits Conf. Tech. Dig., Feb. 2007, pp.418–612.

[22] A. Amer, E. Hegazi, and H. F. Ragaie, "A 90-nm wideband merged CMOS LNA and mixer exploiting noise cancellation," IEEE J. Solid-State Circuits, Vol.42, No.2, pp.323-328, Feb. 2007.

[23] Myoung-Gyun Kim; Hee-Woo An; Yun-Mo Kang; Ji-Young Lee; Tae-Yeoul Yun, "A Low-Voltage, Low-Power, and Low-Noise UWB Mixer Using Bulk-Injection and Switched Biasing Techniques," Microwave Theory and Techniques, IEEE Transactions on , Vol.60, No.8, pp.2486,2493, Aug. 2012.

[24] Venkatraman, V.; Burleson, W., "Impact of process variations on multi-level signaling for on-chip interconnects," VLSI Design, 2005. 18th International Conference on, Vol., No., pp.362,367, 3-7 Jan. 2005.

A Robust Data Envelopment Analysis Method for Business and IT Alignment of Enterprise Architecture Scenarios

Mehdi Fasanghari*
Industrial Engineering, University of Tehran
fasanghari@gmail.com
Mohsen Sadegh Amalnick
Industrial Engineering, University of Tehran
amalnick@ut.ac.ir
Reza Taghipour Anvari
Malek Ashtar University of Technology
taghipour@cra.ir
Jafar Razmi
Industrial Engineering, University of Tehran
jrazmi@ut.ac.ir

Received: 01/May/2013 Accepted: 19/Jun/2013

Abstract
Information Technology is recognized as a competitive enabler in today's dynamic business environment. Therefore, alliance of business and Information Technology process is critical, which is mostly emphasized in Information Technology governance frameworks. On the other hand, Enterprise Architectures are deployed to steer organizations for achieving their objectives while being responsive to changes. Thus, it is proposed to align the business and Information Technology through investigating the suitability of Enterprise Architecture scenarios. In view of this fact, investigating a flexible decision making method for business and information technology alignment analysis is necessary, but it is not sufficient since the subjective analysis is always perturbed by some degree of uncertainty. Therefore, we have developed a new robust Data Envelopment Analysis technique designed for Enterprise Architecture scenario analysis. Several numerical experiments and a sensitivity analysis are designed to show the performance, significance, and flexibility of the proposed method in a real case.

Keywords: Group Data Envelopment Analysis, Enterprise Architecture, IT Governance, COBIT, Robust Optimization.

1. Introduction

Due to the ever increasing struggle to persist in changing environment of today's market, Information Technology (IT) is recognized as one of the best enablers and strategic partner of business capturing the most capital investments in many enterprises [1]. IT governance frameworks define the mechanism of IT-related responsibilities and decision-making structure and are mostly recognized as a series of processes by which business and IT are aligned. However, effective implementation of an IT governance framework is a rather difficult and costly task, since it requires the acquirement of current status of organizations and an understanding of the desired to-be structure of the organization to find the gaps therein and set for improvements. Increasingly, mangers figure out the great contribution of such governance architectures for depicting the right overview of the organization mission, business objective, information systems, and their relationship. For this, managers in charges with their consultants may propose different IT architecture or scenarios to set the roadmap for the requested business strategies which ensures long-term success and cost-efficiency according to the available budget and resource. Enterprise Architecture (EA) is one of the most effective approaches offering these benefits in an integrated and efficient information system by presenting distinctive architectures for the four key areas of business, data, application, and infrastructure [2-4]. Therefore, planning the EA scenarios or IT master plans can show the systematic approach for transforming the enterprise IT infrastructure for achieving the business strategies and goals. Evaluating the EA scenarios is vital as an EA scenario is really expensive and time-consuming for implementation [5, 6]. IT and business alignment is the most important aspect of EA scenario analysis, which was out of consideration for many years. To this

* Corresponding Author

aim, we have used the COBIT framework for EA scenarios analysis. Data Envelopment Analysis (DEA) is a well-known decision making tool to evaluate a set of decision making units (DMUs) based on the multi input-output performance measures [7]. In some real applications of DEA, the respected performance criteria are collected based on the expert opinions. However, when several experts with different knowledge and experiences are to submit their points of view, finding the most proper DMU is not an easy task. In addition, experts' opinions data are mostly perturbed by uncertainty due to several reasons. In this paper, we intend to analyze the EA scenarios by introducing a new expert-based decision-making technique that embraces distinct preferences' weights of experts contaminated by a bounded degree of hesitancy. More specifically, we introduce a novel DEA technique by incorporating the robust optimization concept. In summary, developing a new robust DEA method for EA scenario analysis in view of the IT and business alignment is the primitive contribution in this paper. Analyzing a real case study in Iran Telecommunication Research Center (ITRC) is done to show the reliability and applicability of our proposed idea.

For this, the paper structure is as follows. First, we take a look at the works deemed to our study. Then, we lay the background of our works with introduction of the models and specific related works, namely DEA and robust optimization technique. Our models, both deterministic and its robust counterpart, is also explained in this section. After that, introducing the case study for the numerical experiments will be presented. The performance evaluation follows next, which include empirical results of the deterministic and robust version of the proposed DEA model. Finally, we conclude in the last Section.

2. Related Works

In this Section, we review some of the literature around EA analysis domain, and then take a look at IT governance frameworks, especially COBIT framework.

2.1 EA analysis review

According to [8], some of the researches focus on the complexity of EA systems. This category can be divided into three dimensions of structure, behavior statistics, and dynamic behavior. It means that some analysis such as Niemann [4] model notices on the complexity and dependency of EA components and their influence on the organization. Yu model [9] extends this structural analysis and describes the transition phase to achieve to the desired status of the organization. Now, if the experts' opinions are considered in the analysis, the behavior sub-category works such as [10] emerges. Considering the pathological effects and the behavior of the organization in the time, gives rise to the dynamic analysis of EA scenarios [11]. Time reference is another dimension of the comparison. Some analyses deal with existing established EA and some evaluate the to-be structure of the future EA in the organization. Jacob et el. [10] provides a dynamic model which is able to analyze the current and desired status of EA and detects the conditions leading to the target status. Another category considers whether the EAs under study are already implemented [9-12] or the scenarios based on that EA are being investigated [4,13]. The analysis technique used for evaluation is another important dimension in three sub categories of expert-based [4,9,13], rule-based [11] and indicator-based [4,5,10,14,15] methods. Analysis using experts' opinions are the most flexible approach [8], but time-consuming. A more formal method is the rule based approach, but it can just recognize presence or absence of a pattern in structure. Indicator based approaches can capture better properties such as convergence, and interoperability, though it is very dependent on the assumption and interpretation of the architecture under analysis.

More generally, Multi Criteria Decision Making (MCDM) techniques are tailored for finding an optimum solution among a set of alternatives which are judged on multiple attributes. Such techniques can be used in investigating various quality attributes of software architecture or project selections [13,16-20]. Among the methods of MCDM, Analytical Hierarchical Process (AHP) [21] has been used to judge and select the best architecture candidate or project [13,16,18,22]. Specifically, Razavi et el. [13] have proposed an AHP-based approach for analysis and selection of EA scenarios. Further, Data Envelopment Analysis (DEA) is recognized as a very efficient approach in the decision making domain with easy implementation. A large body of researches and applications has been proposed for DEA [7] pivoted on efficacy measurement in various domains. DEA techniques are used for assessing IT impact on firm performance [23] and using IT as a tool for selection of projects among various proposals [24]. Such analysis of DEA helps to find the source of efficacy and inefficacy and establishes the roadmap for improvement in the organization.

Group-decision making based on AHP approach has gained popularity in the decision-making domain [25,26]. However, AHP has some limitations in confronting the uncertainty. Specifically, it can just handle uncertainty of fuzzy type. Overall, EA scenarios selection problems are usually treated without considering uncertainty of experts [27].

2.2 IT Governance background

There are several IT governance standards available as governmental draft or industry standards (e.g., CMMI, COBIT, ITIL, MOF, ISPL1, ASL2, ISO, Six Sigma, DSDM3) which support the governance of IT in a way that is aligned with the business. One of the most effective frameworks proposed is the Control Objectives for IT and related Technology (COBIT) created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992 [28]. This framework provides managers and auditors with a set of measures and processes which help them to maximize their benefit through the responsible use of resources, appropriate management of risk and alignment of business and IT.

Acting as an integrator of different aspects of both IT and business, COBIT presents its structure and metrics in a manageable and logical structure of four domains namely: 1) plan and organize, 2) acquire and implement, 3) deliver and support and 4) monitor and evaluate. Each of these domains is described through a set of control objectives or measures. A short description of the main domains is summarized as follows [29-33]:

- Plan and organize: This domain presents the strategy and tactics of the way IT can assist to business goals. These visions should be contributed to different people throughout the organization.
- Acquire and implement: For achieving the IT strategies and tactics, IT solutions should be acquired and implemented and finally be integrated into the business process. Further, if there are preexisting systems available, ensuring the continuity of their functionality is handled in this domain.
- Deliver and support: The required service should be delivered and all other processes regarding the management of data and security concerns in addition to supportive activities are dealt with in this domain.
- Monitor and evaluate: all IT processes should be regularly evaluated to meet their quality requirement. So internal controls and regulatory compliance are addressed in this domain.

Robust optimization models can be used as a good approach for encountering the uncertainty in decision making, especially it is useful in the following situations [34]:

- Some parameters are estimates and carry estimation risk.
- There are constraints with uncertain parameters to be satisfied regardless of their values of these parameters.
- The objective functions/optimal solutions are particularly sensitive to perturbations.
- The decision-maker cannot afford low-probability high-magnitude risks.

It is necessary for a decision-making process to reduce the sensitiveness of its results regarding to the input parameters and data. Thus, in this paper, we propose a group DEA model with uncertain data. Experts present their judgment with interval data (lower bound, nominal bound, and upper bound for expressing their opinion).

3. The proposed robust group decision making method based on DEA

In this section, we elaborate the proposed robust decision making method, which is developed based on a robust DEA model. The proposed robust DEA model has the capability to incorporate the opinions of a group of decision makers to evaluate a set of homogeneous decision making units or alternatives (here EA scenarios). The robust DEA model is inspired from the classical CCR DEA model. Therefore, we first briefly review the classical CCR DEA model. After that, the robust DEA model is introduced. To cope with uncertainty of experts' judgment, we use a technique based on the robust optimization. Hence, in the subsequent sub-section, we explain this model and then introduce our robust counterpart of the DEA model provided to handle the uncertainty existed in the input data gathered from experts' opinions.

3.1 The classical CCR DEA model

Data Envelopment Analysis is a non-parametric mathematical programming for measuring the relative efficiency and ranking of various productive units, termed decision making units (DMUs) [35]. It does not require any production or the cost function and measures the performance DMUs based on their multiple inputs and outputs. The relative efficiency measures of DMUs is obtained through determining a piecewise linear efficiency frontier along the most efficient DMU, and the least efficient DMU is recognized by comparison with its frontier curve. The original input oriented DEA model is written as follows:

$$P(I): E^{*}_{so}: \max \sum_{r=1}^{k} u_r y^{s}_{ro}$$

subject to:

$$\begin{aligned} &\sum_{r=1}^{k} u_r y^{s}_{rj} - \sum_{i=1}^{m} v_i x^{s}_{ij} \le 0 \\ &\sum_{i=1}^{m} v_i x^{s}_{io} = 1 \\ &u_r, v_i \ge 0. \end{aligned} \qquad (1)$$

In this model, a set of n homogenous decision making unit ($j = 1,...,n$) with m inputs ($i = 1,...,m$) and k outputs ($r = 1,...,k$) is assessed where x^{s}_{ij} denotes the ith input data of the jth DMU obtained from the sth expert's opinion. Similarly, y^{s}_{rj} denotes the rth output data of the jth DMU obtained from the sth expert's opinion. Furthermore, E^{*}_{so} denotes the efficiency of oth DMU when the input and output data are obtained from the sth expert's opinion. We also call E^{*}_{so} the ideal efficiency score of oth DMU from sth expert view. Model (1) is repeatedly solved for each DMU to obtain its efficiency score.

In the aforementioned model, it is assumed that inputs and outputs are explicitly defined. However, there are many real cases that data are used without inputs (such as index data or pure output data). In this case, the original DEA model converts to a DEA model with k outputs and one dummy input of 1 for all DMUs [36]. In this situation, the original DEA model (1) cannot evaluate DMUs. Hence, to fill the gap of this area, we propose a new Group Decision Making Method which is inspired by classical DEA model (1) to evaluate DMUs based on several matrix input-output data that each of which is collected according to one expert' opinions.

3.2 Robust Optimization

The classical DEA model has no mechanism to deal with uncertainty in input or output data. Several methods such as Chance Constraint Programming (CCP) [37] and Stochastic Programming (SP) are introduced to handle such uncertainty. For some of the representative works related to these models, Sengupta [38-40] and Cooper [41-43] can be considered. In these models, uncertain data are estimated with probabilities, and an error distribution should be determined. These issues limit the real world applications of these models.

As an alternative approach for dealing with uncertainty, robust optimization versions of DEA have recently been raised which covers the decision making process when data are of the form of interval data. Robust optimization can handle the uncertainty in the form of box, ellipsoidal, and polyhedral uncertainty sets [44]. The concept was first introduced by [45] who discussed uncertainty in column vector of the constraint matrix. Subsequently, Ben-tal and Nemirovski [44,46,47] and more recently Bertsimas et el. [48,49] have proposed methods to deal with ellipsoidal and polyhedral uncertainty types. These methods are usually named as BT and BN approach and have some distinguishing differences in terms of preserving the class of the problem after applying the robust approach or the number of variables and constraints [34]. Various works have been suggested according to these techniques. For example, Sadjadi and Omrani [34] applied robust optimization approach to DEA and utilized their model to evaluate the performance of Iranian electricity distribution companies. They suppose uncertainty of ellipsoidal uncertainty to demonstrate the efficiency of robust approaches for ranking strategies of their application. Furthermore, Wang and Wei [50] proposed a non-linear programming for robust data envelopment analysis. In another work, Sadjadi [51] combined the idea of robust optimization with traditional bootstrapped DEA [52,53] to propose a general model for performance assessment and ranking of DMUs with case study of telecommunication companies. The input and output data in [51] can be changed in an interval, and the results overcomes the incurrent bias. Shokouhi [54] used the combination of super-efficiency DEA and robust BA approach for handling uncertainty in both inputs and output which is considered to be of ellipsoidal type for efficiency assessment of gas companies.

Next, we explain the robust optimization of Ben-Tal et el. [55] with the box uncertainty sets to set the background for elaborating the robust counterpart of our proposed robust DEA model. The main advantage of Ben-Tal et el. approach [55] using the box uncertainty set is that the resulted robust counterpart model becomes a linear programming model whereas applying this approach with ellipsoidal uncertainty leads to obtain a nonlinear robust counterpart model, which increases the time complexity. Therefore, we utilize box uncertainty sets to develop the robust counterpart of our proposed model. For this, consider the following linear optimization model:

$$\min cx,$$

$$\text{subject to: } Ax \geq b \tag{2}$$

where x is the vector of decision variables and A is the matrix of constraints with elements a_{ij} . In this model, c, A, b are constant. Now, if these parameters are uncertain in a specific range of U, which is called the uncertainty set, and we wish our solution yet stays in an immune range while addressing the uncertainty of those parameters, we use the robust optimization approach.

$$\min \ cx,$$

subject to:

$$\begin{aligned} & Ax \geq b, \\ & c, A, b \in U \end{aligned} \tag{3}$$

The robust approach for addressing the box uncertainty of entry $\tilde{a} = \{\tilde{a}_{ij}\}_{i=1,\dots,m,\, j=1,\dots,n}$ is as follows:

$$U = \{\tilde{a}_{ij} \in R^n : |\tilde{a}_{ij} - \bar{a}_{ij}| \leq G_{ij}, i = 1,\dots,m, j = 1,\dots,n\} \tag{4}$$

Here, we take uncertainty in row i of constraint matrix. Similarly, uncertainty can be focused in the objective coefficients. In this set, $\bar{a}_{ij}$ is the mean value of $\tilde{a}_{ij}$ and G_{ij} is the uncertainty scale of a given entry. Hence, the robust counterpart model can be written as:

$$\left\{\min_{\tilde{a} \in U} \ \{\sum_{j=1}^{n} \tilde{a}_{ij} x_j\}\right\} \geq b_i \quad or$$

$$\left\{\min_{\tilde{a}_{ij} \in R^n : |\tilde{a}_{ij} - \bar{a}_{ij}| \leq G_{ij}} \ \{\sum_{j=1}^{n} \tilde{a}_{ij} x_j\}\right\} \geq b_i \tag{5}$$

According to uncertainty set U presented in (6), and since the scale uncertainty G_{ij} is a positive number, the minimum value of $\sum_{j=1}^{n} \tilde{a}_{ij} x_j$ on the box uncertainty set U is occurred for the lower bound of $\tilde{a}_{ij}$, which become $\bar{a}_{ij} - G_{ij}$.

$$U = \{\tilde{a}_{ij} \in R : \bar{a}_{ij} - G_{ij} \leq \tilde{a}_{ij} \leq \bar{a}_{ij} + G_{ij}, \quad i = 1,\dots,m, j = 1,\dots,n\} \tag{6}$$

Therefore, inequality (5) is reformulated as follows:

$$\sum_{j=1}^{n} \bar{a}_{ij} x_j - \sum_{j=1}^{n} G_{ij} x_j \geq b_i \tag{7}$$

which is the robust counterpart of constraint $Ax \geq b$ of model (2) and thus the robust LP model is solvable.

3.3 Robust counterpart of the proposed DEA model

In our application, due to the expert based nature of data, experts cannot express an exact value for input and output data and therefore, uncertainties are inherent in experts' opinions. We, therefore, represent the robust version of our model to handle this kind of uncertainty. If we suppose that output data obtained from experts' opinions (y_{rj}^{s}) are defined as the box uncertainty sets, the robust counterpart of the robust DEA can be expressed as:

$P(II)$: max z

subject to:

$$\begin{aligned} & \left\{\min_{\tilde{y}_{ro}^{s} \in u^B} \{\sum_{s=1}^{S} w_s \sum_{r=1}^{k} u_r \tilde{y}_{ro}^{s}\}\right\} \geq z, \\ & \sum_{i=1}^{m} v_i x_{io}^{s} = 1, \quad \forall s \\ & \left\{\max_{\tilde{y}_{rj}^{s} \in u^B} \{\sum_{r=1}^{k} u_r \tilde{y}_{rj}^{s}\}\right\} - \sum_{i=1}^{m} v_i x_{ij}^{s} \leq 0, \quad \forall j,s \\ & \left\{\min_{\tilde{y}_{ro}^{s} \in u^B} \{\sum_{r=1}^{k} u_r \tilde{y}_{ro}^{s}\}\right\} \geq E_{so}^{*}, \quad \forall s \\ & u_r, v_i \geq 0. \end{aligned} \tag{8}$$

It is worthy to mention that we first move the objective function into constraints by introducing new decision variable z, and then provide the robust equivalence of all constraints of the robust DEA model. As a result, the first constraint of the above model is equivalent to the objective function of the robust DEA model. Similarly, the two last constraints of model P(II) are the robust counterpart of the DEA model.

The uncertainty set of model P(II) is defined as follows:

$$U^B = [\bar{y}_{rj}^{s} - G_{rj}^{s}, \bar{y}_{rj}^{s} + G_{rj}^{s}] \tag{9}$$

where $\bar{y}_{rj}^{s}$ is the nominal data assigned to rth output (here benefit-type criteria) in jth DMU whose value determined according to the sth expert opinion.

It is noted that the minimum and maximum value of $\tilde{y}_{rj}^{s}$ on the box uncertainty set U^B , are occurred for the lower and upper bounds of $\tilde{y}_{rj}^{s}$, which are $\bar{y}_{rj}^{s} - G_{rj}^{s}$ and $\bar{y}_{rj}^{s} + G_{rj}^{s}$ respectively. Therefore, when minimizing the left-hand of the first constraint on the box uncertainty of U^B , it became equal to $\sum_{s=1}^{S} w_s \sum_{r=1}^{R} u_r [\bar{y}_{ro}^{s} - G_{ro}^{s}]$, since $\tilde{y}_{ro}^{s} \geq 0$. A similar method can be used for maximizing the two last constraints of model P(II). Finally, the robust counterpart model can be written as:

$P(III)$: max z

subject to:

$$\begin{aligned}
&\sum_{s=1}^{S} w_s \sum_{r=1}^{k} u_r[\bar{y}_{ro}^s - G_{ro}^s] \ge z\\
&\sum_{i=1}^{m} v_i x_{io}^s = 1, \quad \forall \text{s}\\
&\sum_{r=1}^{k} u_r[\bar{y}_{rj}^s + G_{rj}^s] - \sum_{i=1}^{m} v_i x_{ij}^s \le 0, \quad \forall \text{j,s}\\
&\sum_{r=1}^{k} u_r[\bar{y}_{ro}^s - G_{ro}^s] \ge E_{so}^*, \quad \forall \text{s}\\
&u_r, v_i \ge 0.
\end{aligned} \tag{10}$$

In this model, $\bar{y}_{rj}^s$ and G_{rj}^s are the nominal data and scale uncertainty of data obtained from sth expert on rth output of jth DMU.

The existing robust DEA models which take benefit of BT approach are non-linear programming model due to usage of ellipsoidal uncertainty form [34,50]. However, our technique uses box uncertainty which leads to a linear programming model. Linear models have the benefit of simplicity and also the higher accuracy of the computational result in comparison to nonlinear programming models.

4. The application of proposed robust DEA for EA scenario evaluations

Our case study is studied for the ITRC in Iran as the greatest organizations handling ICT projects with a variant degree of importance and complexity. Having four faculties of IT, CT, security, and strategic planning, the center considers transformations of its process for approaching e-organizations objectives. To fulfill his vision, ITRC considers developing some practical scenarios for successful accomplishment of its task. EA has been accepted as a tool for planning and managing the process. Therefore, a group of IT experts designed 12 EA scenarios stated in Table 1 which correspond to 12 DMUs for our model. In fact, there are four distinct scenarios including planning for ERP implementation, web service implementation, portal implementation, and the process integration of ITRC and each can be implemented via in-sourcing (using the ITRC's own resources and employees), out-sourcing (a recovery-oriented proposal for downsizing and cost reduction), and co-sourcing (combining the in-source and out-source capability through contracting an out-sourced firm to provide part of IT solutions) [56].

Table 1. The 12 EA scenarios (ICT master plan) for ITRC migration to e-organization

DMU No.	EA scenario	Explanation
DMU1	In-source ERP	Implementing an ERP by in-sourcing
DMU2	Out-source ERP	Out-sourcing an ERP for implementation
DMU3	co-sourcing ERP	Implementing an ERP through co-sourcing
DMU4	In-source web services	Delivering the web services by in-sourcing
DMU5	Out-source web services	Delivering the web services through out-sourcing
DMU6	co-sourcing web services	Delivering the web services through co-sourcing
DMU7	In-source portal	Integration of ITRC departments through in-source portal implementation
DMU8	Out-source portal	Integration of ITRC departments through out-source portal implementation
DMU9	co-sourcing portal	Integration of ITRC departments through co-sourcing portal implementation
DMU10	In-source process integration	Integration the process of ITRC by in-sourcing
DMU11	Out-source process integration	Integration the process of ITRC by out-sourcing
DMU12	co-sourcing process integration	Integration the process of ITRC through co-sourcing

Executing each of these plans, demands high investments with high risks and hidden costs and it is safer to scrutinize the selection of EA against a robust analytical tool. To satisfy business objectives, information needs correspondence to certain several control objectives such as: efficiency, effectiveness, confidentiality, integrity, accessibility, availability, compliance, and reliability. These metrics correspond to the criteria covered in COBIT's framework which are utilized for evaluating the proposed EA scenarios before implementation by experts and our method. In fact, four experts are asked to submit their view on the suitability of each scenario in regard to every process of COBIT framework and then the proposed robust PRS-DEA method is deployed for obtaining the overall efficacy score of these EA according to all experts' preferences. The objective of this evaluation is to signify the maturity level of COBIT in the EA proposals and then selecting the best balanced improvement plan considering the IT processes of COBIT framework which meets almost all of the ICT ministries' objectives. So, the scenario which covers all or most of COBIT processes with high maturity is more likely to gain higher overall ranking and is expected to provide business and IT alignments efficiently.

Tables A-1 to A-4 present each expert's opinions regarding the estimated maturity of each process for the scenario under judgment. The range of maturity levels is from 0 to 10 which indicate the degree of realization of a specific process under a given scenario. Therefore, lower value of maturity level is an indication of weak realization and the higher value is an indication of high realization of that process when a specific scenario is implemented. Further, as data are inexact, experts present their estimated maturity in an interval of lower and higher bound. Further, the nominal value denoted by $\bar{y}_{rj}^{s}$ reflects the average estimated maturity of rth process under implementation of jth scenario from sth expert's viewpoint which is obtained by averaging the lower and upper bound values. For example, the reported data in Appendix

Table A-1 presents the lower, nominal and upper bound for the estimated maturity levels of COBIT processes through the implementation of different proposed EA scenarios from the first expert's viewpoint.

The information in these tables can be used to identify IT processes which are estimated to be affected at most or at least when implementing a given EA scenario. This information can be used to reflect the strengths and weaknesses of implementing that specific EA scenario which is then can be a source of value for recognizing the activities for reaching the desired status for processes.

The output parameters of the model are equal to 34 processes of COBIT and for the input parameter, a dummy input of 1 is considered [36]. The evaluation results are presented in the next section.

5. Performance Evaluation

We utilize several numerical experiments to validate the applicability and significance of the robust counterpart of our proposed method. As mentioned before, four experts' opinions are used in this experiment and scoring to the 34 processes of COBIT are regarded as the closed box uncertainty due to inherent imprecise nature of experts' opinion. In fact, the data for COBIT processes are considered as the interval of $[\bar{y}_{rj}^{s} - G_{rj}^{s}, \bar{y}_{rj}^{s} + G_{rj}^{s}]$ with G_{rj}^{s} as the scale uncertainty associated with sth expert' opinion about rth COBIT process in jth EA scenario.

To compute the ideal efficiency score (E_{so}^{*}) from each expert's point of view, we solve model P(I) with nominal data $(\bar{y}_{rj}^{s})$. It is worthy to mention that the best efficiency scores from each expert's point of view can be provided when uncertainty is not considered in model P(I). If we solve model P(I) with uncertain data to obtain ideal efficiency scores, the objective function (E_{so}^{*}) does not function as expected. For this reason, the resulted efficiency scores cannot be considered as ideal efficiency scores. Therefore, it is logical to provide ideal efficiency scores by solving model P(II) with nominal data $(\bar{y}_{rj}^{s})$. The respected results are reported in Table 2. For example, the second column of Table 2 reports the ideal efficiency scores according to data gathered from the first expert. According to the results, DMU1, 4, 5, 6 and 8 attain the efficiency score of one.

Further, we set $w_1 = w_2 = w_3 = w_4 = 0.25$. Please note that the proposed robust model turns into a deterministic model when the uncertainties are not considered in the model parameters.

Table 2. Ideal efficiency scores according to the experts' opinion

DMU No.	Expert 1	Expert 2	Expert 3	Expert 4
DMU1	1	1	1	1
DMU2	0.818	0.733	0.818	0.747
DMU3	0.750	0.724	0.857	0.714
DMU4	1	1	1	1
DMU5	1	1	1	1
DMU6	1	1	1	1
DMU7	0.955	1	0.875	1
DMU8	1	1	1	1
DMU9	0.875	1	1	1
DMU10	0.857	0.750	0.857	0.808
DMU11	0.750	0.750	0.714	0.750
DMU12	0.750	0.724	0.828	0.857

For the analysis, first, we solve the deterministic model $P(II)$ using the nominal data and calculate the performance of each DMU. The second column of Table 3 reports the corresponding results. As indicated, DMU4 and DMU5 acquire the maximum efficiency score of 1 and DMU3 holds the least efficiency score (0.546). Then, the robust counterpart model is solved. As it was expected, the deterministic model generates the higher efficiency score when it compares to the robust counterpart model. On the other hand, the efficiency scores generated by the deterministic model are greater than those produced by the robust counterpart model, since it protects decision making model against uncertainty. Furthermore, the efficiency score of each DMU is decreased by increasing the uncertainty level. This is the expected trend, since the efficiency of DMUs is predicted with a higher degree of uncertainty. The resulted efficiency scores are also graphically depicted in Figure 1. Moreover, the proposed robust DEA model, provide more discriminative results, which are more suitable for DMU ranking purpose.

Table 3. Efficiency scores obtained by the deterministic and robust Model

DMU number	Deterministic model	Robust model
DMU1	0.908	0.650
DMU2	0.615	0.394
DMU3	0.546	0.345
DMU4	1	0.713
DMU5	1	0.847
DMU6	0.833	0.639
DMU7	0.694	0.5
DMU8	0.859	0.708
DMU9	0.735	0.564
DMU10	0.553	0.403
DMU11	0.611	0.451
DMU12	0.601	0.461

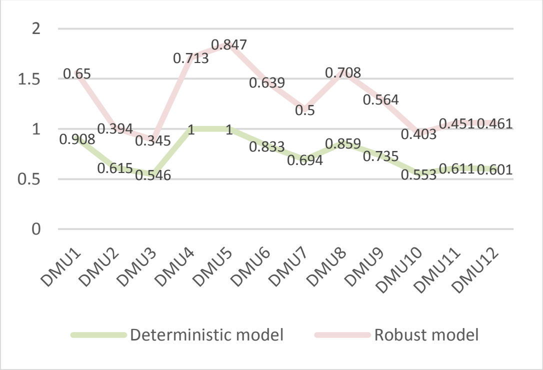


Figure 1. Efficiency scores under the proposed deterministic and robust optimization models

Based on achieved results, one can easily derive ranking of EA scenario according to the uncertainty level in mind. For example, if a manager wants to have its decision-making process with the highest protection and reliability level, then he should select the fifth EA scenario (i.e., “Out-source web services” scenario), which gains the highest efficiency score and is selected as the most preferred scenario for making ITRC objectives for alignments of IT and business realized.

6. Conclusion

In this paper, we have developed a robust DEA approach which embraces the effects of bounded uncertainties in experts’ opinions using the robust optimization technique. This method is tested for a case study of EA scenario analysis, which determines the best scenario for implementation in a governmental institute of Iran (ITRC). The flexibility of the proposed robust DEA model with the integration of bounded uncertainty of experts’ data in the proposed decision-making technique makes it a very reliable and efficient approach. Extensive experiments are carried out to prove the feasibility of the model with various degrees of uncertainty. The results show a promising research perspective in the field of both IT (IT Governance and EA evaluation problem) and MCDM domains. Through the presented method for business and IT alignment assessment, the variation of experts’ opinion has no effect on final results. In fact, our analysis model is protected against the input data variation, and the output results are robust against the uncertainty. Specifically, the proposed analytical tool is intrinsically able to deal with different uncertainty in input data of decision making processes without any constraints. Therefore, as a future work, one may endeavor to try other types of uncertainty in EA evaluation scenarios.

7. Appendix

Table A-1. The input and output data for IT research projects of ITRC including summary statistics expressed by expert 1 (E1)

	DMU1			DMU2			DMU3			DMU4			DMU5			DMU6			DMU7			DMU8			DMU9			DMU10			DMU11			DMU12			Min	Max	Mean
	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U			
PO1	7	8	9	4	5	6	0	1	2	7	8	9	7	8	9	5	6	7	2	3	4	8	9	10	5.5	6	6.5	4.5	5	5.5	4.5	5	5.5	2.5	3	3.5	1	9	5.58
PO2	5	6	7	2	3	4	0	1	2	6	7	8	6	7	8	5	6	7	1	2	3	6	7	8	4.5	5	5.5	5.5	4.5	6.5	2.5	3	3.5	4.5	2	5.5	1	7	4.46
PO3	6	7	8	3	4	5	5	6	7	5	6	7	7	8	9	5	6	7	5	6	7	3	4	5	5.5	6	6.5	0.5	2.5	1.5	3.5	4	4.5	3.5	6	4.5	2.5	8	5.46
PO4	5	6	7	4	5	6	4	5	6	5	6	7	8	9	10	6	7	8	5	6	7	8	9	10	4.5	5	5.5	5.5	6	6.5	5.5	6	6.5	3.5	6	4.5	5	9	6.33
PO5	7	8	9	2	3	4	0	1	2	5	6	7	7	8	9	5	6	7	5	6	7	6	7	8	5.5	6	6.5	3.5	3.5	4.5	2.5	3	3.5	1.5	6	2.5	1	8	5.29
PO6	7	8	9	2	3	4	3	4	5	5	6	7	8	9	10	3	4	5	2	3	4	5	6	7	4.5	5	5.5	1.5	3	2.5	3.5	4	4.5	5.5	3	6.5	3	9	4.83
PO7	5	6	7	2	3	4	1	2	3	6	7	8	7	8	9	7	8	9	3	4	5	5	6	7	2.5	3	3.5	3.5	4	4.5	3.5	4	4.5	5.5	4	6.5	2	8	4.92
PO8	6	7	8	3	4	5	3	4	5	8	9	10	7	8	9	7	8	9	4	5	6	2	3	4	4.5	5	5.5	3.5	4	4.5	3.5	4	4.5	2.5	5	3.5	3	9	5.50
PO9	5	6	7	4	5	6	2	3	4	4	5	6	7	8	9	6	7	8	1	2	3	6	7	8	4.5	5	5.5	4.5	4.5	5.5	3.5	4	4.5	4.5	2	5.5	2	8	4.88
PO10	7	8	9	5	6	7	2	3	4	7	8	9	8	9	10	6	7	8	4	5	6	2	3	4	3.5	4	4.5	2.5	4	3.5	4.5	5	5.5	5.5	5	6.5	3	9	5.58
AI1	6	7	8	4	5	6	3	4	5	7	8	9	9	9.5	10	4	5	6	6	7	8	5	6	7	2.5	3	3.5	0.5	3.5	1.5	5.5	6	6.5	2.5	7	3.5	3	9.5	5.92
AI2	6	7	8	2	3	4	4	5	6	9	9.5	10	9	9.5	10	5	6	7	3	4	5	7	8	9	4.5	5	5.5	4.5	5	5.5	4.5	5	5.5	3.5	4	4.5	3	9.5	5.92
AI3	6	7	8	4	5	6	5	6	7	5	6	7	7	8	9	6	7	8	4	5	6	2	3	4	5.5	6	6.5	4.5	5	5.5	4.5	5	5.5	2.5	5	3.5	3	8	5.67
AI4	7	8	9	2	3	4	1	2	3	5	6	7	9	9.5	10	6	7	8	1	2	3	3	4	5	3.5	4	4.5	4.5	4.5	5.5	3.5	4	4.5	2.5	2	3.5	2	9.5	4.67
AI5	6	7	8	4	5	6	1	2	3	6	7	8	9	9.5	10	5	6	7	2	3	4	7	8	9	4.5	5	5.5	2.5	3.5	3.5	3.5	4	4.5	2.5	3	3.5	2	9.5	5.25
AI6	7	8	9	5	6	7	5	6	7	5	6	7	7	8	9	5	6	7	2	3	4	8	9	10	5.5	6	6.5	3.5	3.5	4.5	2.5	3	3.5	5.5	3	6.5	3	9	5.63
AI7	7	8	9	4	5	6	2	3	4	6	7	8	9	9.5	10	5	6	7	1	2	3	6	7	8	5.5	6	6.5	4.5	5.5	5.5	5.5	6	6.5	2.5	2	3.5	2	9.5	5.58
DS1	6	7	8	4	5	6	1	2	3	8	9	10	8	9	10	3	4	5	4	5	6	4	5	6	5.5	6	6.5	3.5	4.5	4.5	4.5	5	5.5	3.5	5	4.5	2	9	5.54
DS2	5	6	7	1	2	3	2	3	4	9	9.5	10	9	9.5	10	5	6	7	5	6	7	5	6	7	5.5	6	6.5	5.5	5.5	6.5	4.5	5	5.5	1.5	6	2.5	2	9.5	5.88
DS3	7	8	9	5	6	7	4	5	6	6	7	8	6	7	8	4	5	6	2	3	4	4	5	6	4.5	5	5.5	4.5	5	5.5	4.5	5	5.5	2.5	3	3.5	3	8	5.33
DS4	5	6	7	4	5	6	1	2	3	6	7	8	7	8	9	4	5	6	5	6	7	4	5	6	4.5	5	5.5	5.5	5	6.5	3.5	4	4.5	3.5	6	4.5	2	8	5.33
DS5	7	8	9	2	3	4	3	4	5	5	6	7	6	7	8	6	7	8	6	7	8	3	4	5	3.5	4	4.5	1.5	3	2.5	3.5	4	4.5	4.5	7	5.5	3	8	5.33
DS6	6	7	8	5	6	7	4	5	6	5	6	7	7	8	9	4	5	6	0	1	2	3	4	5	5.5	6	6.5	4.5	5	5.5	4.5	5	5.5	2.5	1	3.5	1	8	4.92
DS7	6	7	8	3	4	5	3	4	5	4	5	6	9	9.5	10	5	6	7	4	5	6	6	7	8	5.5	6	6.5	4.5	5	5.5	4.5	5	5.5	4.5	5	5.5	4	9.5	5.71
DS8	5	6	7	4	5	6	3	4	5	8	9	10	9	9.5	10	6	7	8	4	5	6	7	8	9	2.5	3	3.5	3.5	4.5	4.5	4.5	5	5.5	4.5	5	5.5	3	9.5	5.92
DS9	5	6	7	3	4	5	1	2	3	8	9	10	7	8	9	3	4	5	6	7	8	4	5	6	4.5	5	5.5	1.5	3.5	2.5	4.5	5	5.5	1.5	7	2.5	2	9	5.46
DS10	7	8	9	4	5	6	5	6	7	5	6	7	7	8	9	7	8	9	6	7	8	7	8	9	2.5	3	3.5	2.5	4.5	3.5	5.5	6	6.5	4.5	7	5.5	3	8	6.38
DS11	5	6	7	5	6	7	1	2	3	5	6	7	7	8	9	6	7	8	5	6	7	3	4	5	6.5	7	7.5	3.5	3.5	4.5	2.5	3	3.5	5.5	6	6.5	2	8	5.38
DS12	5	6	7	5	6	7	2	3	4	7	8	9	7	8	9	5	6	7	2	3	4	4	5	6	5.5	6	6.5	1.5	3.5	2.5	4.5	5	5.5	1.5	3	2.5	3	8	5.21
DS13	6	7	8	4	5	6	5	6	7	8	9	10	7	8	9	4	5	6	2	3	4	3	4	5	3.5	4	4.5	4.5	4	5.5	2.5	3	3.5	4.5	3	5.5	3	9	5.08
ME1	5	6	7	4	5	6	1	2	3	8	9	10	7	8	9	3	4	5	6	7	8	3	4	5	5.5	6	6.5	3.5	4	4.5	3.5	4	4.5	1.5	7	2.5	2	9	5.50
ME2	6	7	8	3	4	5	1	2	3	6	7	8	8	9	10	7	8	9	4	5	6	7	8	9	5.5	6	6.5	3.5	4	4.5	3.5	4	4.5	4.5	5	5.5	2	9	5.75
ME3	5	6	7	5	6	7	1	2	3	6	7	8	9	9.5	10	6	7	8	4	5	6	7	8	9	3.5	4	4.5	4.5	4	5.5	2.5	3	3.5	5.5	5	6.5	2	9.5	5.54
ME4	7	8	9	5	6	7	4	5	6	9	9.5	10	9	9.5	10	3	4	5	1	2	3	4	5	6	4.5	5	5.5	1.5	3.5	2.5	4.5	5	5.5	4.5	2	5.5	2	9.5	5.38

L=Lower bound value $(\bar{y}_{rj}^{1} - G_{rj}^{1})$

N=Nominal value $(\bar{y}_{rj}^{1})$

U=Upper bound vale $(\bar{y}_{rj}^{1} + G_{rj}^{1})$

Table A-2. The input and output data for IT research projects of ITRC including summary statistics expressed by expert 2 (E2)

	DMU1			DMU2			DMU3			DMU4			DMU5			DMU6			DMU7			DMU8			DMU9			DMU10			DMU11			DMU12			Min	Max	Mean
	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U			
PO1	4	6	8	3	5	7	4	6	8	4	6	8	9.5	9.75	10	7.5	8	8.5	3.5	4	4.5	7.5	8	8.5	4	5	6	3	5	5	5	6	7	5	4	7	4	9.75	6.06
PO2	4	6	8	2	4	6	0	2	4	5	7	9	9.5	9.75	10	3.5	4	4.5	5.5	6	6.5	4.5	5	5.5	5	6	7	2	4	4	4	5	6	3	6	5	2	9.75	5.40
PO3	4	6	8	3	5	7	2	4	6	5	7	9	6.5	7	7.5	5.5	6	6.5	6.5	7	7.5	3.5	4	4.5	5	6	7	4	4	6	2	3	4	1	7	3	3	7	5.50
PO4	6	8	10	3	5	7	0	1	3	6	8	10	9.5	9.75	10	4.5	5	5.5	2.5	3	3.5	3.5	4	4.5	5	6	7	4	5.5	6	5	6	7	3	3	5	1	9.75	5.35
PO5	6	8	10	2	4	6	2	4	6	8	9	10	9.5	9.75	10	5.5	6	6.5	1.5	2	2.5	4.5	5	5.5	5	6	7	4	5	6	4	5	6	2	2	4	2	9.75	5.48
PO6	5	7	9	3	5	7	0	2	4	4	6	8	8.5	9	9.5	5.5	6	6.5	3.5	4	4.5	3.5	4	4.5	3	4	5	4	4	6	2	3	4	1	4	3	2	9	4.83
PO7	4	6	8	3	5	7	3	5	7	5	7	9	8.5	9	9.5	4.5	5	5.5	3.5	4	4.5	4.5	5	5.5	3	4	5	3	4.5	5	4	5	6	3	4	5	4	9	5.29
PO8	5	7	9	2	4	6	0	2	4	7	8.5	10	8.5	9	9.5	7.5	8	8.5	6.5	7	7.5	6.5	7	7.5	4	5	6	1	4	3	5	6	7	5	7	7	2	9	6.21
PO9	6	8	10	3	5	7	0	2	4	6	8	10	7.5	8	8.5	3.5	4	4.5	4.5	5	5.5	4.5	5	5.5	6	7	8	1	3.5	3	4	5	6	4	5	6	2	8	5.46
PO10	6	8	10	4	6	8	1	3	5	7	8.5	10	7.5	8	8.5	4.5	5	5.5	6.5	7	7.5	6.5	7	7.5	2	3	4	3	5	5	5	6	7	4	7	6	3	8.5	6.13
AI1	4	6	8	2	4	6	4	6	8	8	9	10	6.5	7	7.5	4.5	5	5.5	1.5	2	2.5	3.5	4	4.5	2	3	4	1	2.5	3	2	3	4	5	2	7	2	9	4.46
AI2	5	7	9	2	4	6	3	5	7	6	8	10	8.5	9	9.5	6.5	7	7.5	4.5	5	5.5	7.5	8	8.5	4	5	6	3	4	5	3	4	5	2	5	4	4	9	5.92
AI3	5	7	9	0	2	4	0	2	4	8	9	10	8.5	9	9.5	6.5	7	7.5	5.5	6	6.5	5.5	6	6.5	4	5	6	2	4	4	4	5	6	4	6	6	2	9	5.67
AI4	6	8	10	1	3	5	0	2	4	8	9	10	8.5	9	9.5	4.5	5	5.5	3.5	4	4.5	7.5	8	8.5	4	5	6	2	3.5	4	3	4	5	3	4	5	2	9	5.38
AI5	5	7	9	3	5	7	1	3	5	5	7	9	7.5	8	8.5	7.5	8	8.5	0.5	1	1.5	6.5	7	7.5	5	6	7	3	4.5	5	4	5	6	4	1	6	1	8	5.21
AI6	5	7	9	1	3	5	0	2	4	5	7	9	8.5	9	9.5	5.5	6	6.5	6.5	7	7.5	4.5	5	5.5	3	4	5	1	4	3	5	6	7	3	7	5	2	9	5.58
AI7	4	6	8	0	2	4	0	2	4	6	8	10	8.5	9	9.5	4.5	5	5.5	1.5	2	2.5	7.5	8	8.5	2	3	4	1	3	3	3	4	5	4	2	6	2	9	4.50
DS1	4	6	8	1	3	5	0	2	4	4	6	8	7.5	8	8.5	6.5	7	7.5	5.5	6	6.5	7.5	8	8.5	3	4	5	4	4.5	6	3	4	5	4	6	6	2	8	5.38
DS2	5	7	9	2	4	6	3	5	7	6	8	10	9.5	9.75	10	3.5	4	4.5	3.5	4	4.5	5.5	6	6.5	6	7	8	3	4.5	5	4	5	6	2	4	4	4	9.75	5.69
DS3	4	6	8	4	6	8	2	4	6	7	8.5	10	8.5	9	9.5	7.5	8	8.5	5.5	6	6.5	4.5	5	5.5	4	5	6	3	4	5	3	4	5	4	6	6	4	9	5.96
DS4	4	6	8	1	3	5	3	5	7	3	5	7	8.5	9	9.5	6.5	7	7.5	5.5	6	6.5	4.5	5	5.5	3	4	5	0	2	2	2	3	4	2	6	4	2	9	5.08
DS5	4	6	8	0	2	4	1	3	5	7	8.5	10	6.5	7	7.5	5.5	6	6.5	5.5	6	6.5	4.5	5	5.5	3	4	5	4	4.5	6	3	4	5	1	6	3	2	8.5	5.17
DS6	5	7	9	3	5	7	2	4	6	6	8	10	6.5	7	7.5	6.5	7	7.5	1.5	2	2.5	8.5	9	9.5	5	6	7	1	2.5	3	2	3	4	4	2	6	2	9	5.21
DS7	5	7	9	3	5	7	0	1	3	4	6	8	7.5	8	8.5	7.5	8	8.5	0.5	1	1.5	4.5	5	5.5	6	7	8	4	5.5	6	5	6	7	4	1	6	1	8	5.04
DS8	4	6	8	2	4	6	3	5	7	6	8	10	7.5	8	8.5	5.5	6	6.5	3.5	4	4.5	6.5	7	7.5	5	6	7	5	5.5	7	4	5	6	3	4	5	4	8	5.71
DS9	5	7	9	3	5	7	0	2	4	4	6	8	6.5	7	7.5	3.5	4	4.5	4.5	5	5.5	4.5	5	5.5	6	7	8	3	4	5	3	4	5	1	5	3	2	7	5.08
DS10	6	8	10	0	2	4	2	4	6	8	9	10	6.5	7	7.5	3.5	4	4.5	2.5	3	3.5	8.5	9	9.5	6	7	8	1	3.5	3	4	5	6	4	3	6	2	9	5.38
DS11	5	7	9	2	4	6	3	5	7	7	8.5	10	8.5	9	9.5	3.5	4	4.5	5.5	6	6.5	5.5	6	6.5	4	5	6	0	2.5	2	3	4	5	3	6	5	2.5	9	5.58
DS12	5	7	9	1	3	5	0	2	4	6	8	10	9.5	9.75	10	5.5	6	6.5	1.5	2	2.5	3.5	4	4.5	5	6	7	2	3.5	4	3	4	5	3	2	5	2	9.75	4.77
DS13	6	8	10	3	5	7	0	2	4	6	8	10	6.5	7	7.5	7.5	8	8.5	6.5	7	7.5	2.5	3	3.5	4	5	6	4	4.5	6	3	4	5	3	7	5	2	8	5.71
ME1	5	7	9	3	5	7	0	1	3	5	7	9	7.5	8	8.5	5.5	6	6.5	6.5	7	7.5	7.5	8	8.5	5	6	7	2	4.5	4	5	6	7	4	7	6	1	8	6.04
ME2	4	6	8	2	4	6	2	4	6	5	7	9	9.5	9.75	10	4.5	5	5.5	4.5	5	5.5	5.5	6	6.5	6	7	8	0	3	2	4	5	6	3	5	5	3	9.75	5.56
ME3	5	7	9	0	2	4	0	2	4	8	9	10	7.5	8	8.5	5.5	6	6.5	5.5	6	6.5	7.5	8	8.5	2	3	4	2	4	4	4	5	6	5	6	7	2	9	5.50
ME4	5	7	9	2	4	6	0	2	4	7	8.5	10	8.5	9	9.5	4.5	5	5.5	3.5	4	4.5	5.5	6	6.5	3	4	5	5	4.5	7	2	3	4	5	4	7	2	9	5.08

L=Lower bound value $(\bar{y}_{rj}^{2} - G_{rj}^{2})$

N=Nominal value $(\bar{y}_{rj}^{2})$

U=Upper bound vale $(\bar{y}_{rj}^{2} + G_{rj}^{2})$

Table A-3. The input and output data for IT research projects of ITRC including summary statistics expressed by expert 3 (E3)

	DMU1			DMU2			DMU3			DMU4			DMU5			DMU6			DMU7			DMU8			DMU9			DMU10			DMU11			DMU12			Min	Max	Mean
	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U			
PO1	4	6	8	1	3	5	0	2	4	6	8	10	6.5	7	7.5	4.5	5	5.5	5.5	6	6.5	5.5	6	6.5	3	4	5	0	2.5	2	3	4	5	5	6	7	2	8	4.96
PO2	4	6	8	2	4	6	0	1	3	4	6	8	8.5	9	9.5	5.5	6	6.5	1.5	2	2.5	6.5	7	7.5	3	4	5	1	3	3	3	4	5	5	2	7	1	9	4.50
PO3	4	6	8	3	5	7	3	5	7	8	9	10	6.5	7	7.5	6.5	7	7.5	4.5	5	5.5	2.5	3	3.5	4	5	6	0	2.5	2	3	4	5	4	5	6	2.5	9	5.29
PO4	6	8	10	3	5	7	0	2	4	6	8	10	7.5	8	8.5	6.5	7	7.5	5.5	6	6.5	5.5	6	6.5	5	6	7	4	4.5	6	3	4	5	1	6	3	2	8	5.88
PO5	6	8	10	4	6	8	0	2	4	4	6	8	7.5	8	8.5	6.5	7	7.5	1.5	2	2.5	7.5	8	8.5	3	4	5	3	4.5	5	4	5	6	5	2	7	2	8	5.21
PO6	5	7	9	1	3	5	0	2	4	4	6	8	7.5	8	8.5	6.5	7	7.5	3.5	4	4.5	6.5	7	7.5	3	4	5	0	3	2	4	5	6	5	4	7	2	8	5.00
PO7	5	7	9	3	5	7	1	3	5	7	8.5	10	8.5	9	9.5	6.5	7	7.5	4.5	5	5.5	5.5	6	6.5	5	6	7	4	4.5	6	3	4	5	5	5	7	3	9	5.83
PO8	6	8	10	0	2	4	1	3	5	7	8.5	10	8.5	9	9.5	5.5	6	6.5	1.5	2	2.5	4.5	5	5.5	5	6	7	3	3.5	5	2	3	4	3	2	5	2	9	4.83
PO9	6	8	10	3	5	7	0	2	4	3	5	7	8.5	9	9.5	6.5	7	7.5	0.5	1	1.5	5.5	6	6.5	5	6	7	0	2	2	2	3	4	2	1	4	1	9	4.58
PO10	4	6	8	3	5	7	3	5	7	4	6	8	8.5	9	9.5	6.5	7	7.5	0.5	1	1.5	6.5	7	7.5	3	4	5	3	5	5	5	6	7	3	1	5	1	9	5.17
AI1	5	7	9	2	4	6	0	2	4	7	8.5	10	8.5	9	9.5	6.5	7	7.5	2.5	3	3.5	8.5	9	9.5	5	6	7	0	3	2	4	5	6	3	3	5	2	9	5.54
AI2	5	7	9	3	5	7	3	5	7	6	8	10	8.5	9	9.5	7.5	8	8.5	5.5	6	6.5	5.5	6	6.5	4	5	6	4	4.5	6	3	4	5	4	6	6	4	9	6.13
AI3	5	7	9	2	4	6	0	2	4	3	5	7	7.5	8	8.5	4.5	5	5.5	3.5	4	4.5	7.5	8	8.5	3	4	5	2	4	4	4	5	6	5	4	7	2	8	5.00
AI4	4	6	8	1	3	5	1	3	5	3	5	7	8.5	9	9.5	6.5	7	7.5	5.5	6	6.5	3.5	4	4.5	4	5	6	3	4.5	5	4	5	6	1	6	3	3	9	5.29
AI5	5	7	9	1	3	5	0	1	3	4	6	8	9.5	9.75	10	4.5	5	5.5	1.5	2	2.5	8.5	9	9.5	3	4	5	1	3	3	3	4	5	2	2	4	1	9.75	4.65
AI6	6	8	10	3	5	7	3	5	7	8	9	10	8.5	9	9.5	7.5	8	8.5	2.5	3	3.5	2.5	3	3.5	5	6	7	2	3	4	2	3	4	4	3	6	3	9	5.42
AI7	4	6	8	1	3	5	2	4	6	5	7	9	7.5	8	8.5	3.5	4	4.5	2.5	3	3.5	2.5	3	3.5	2	3	4	2	3	4	2	3	4	2	3	4	3	8	4.17
DS1	4	6	8	3	5	7	3	5	7	5	7	9	7.5	8	8.5	6.5	7	7.5	4.5	5	5.5	4.5	5	5.5	2	3	4	5	5	7	3	4	5	2	5	4	3	8	5.42
DS2	4	6	8	4	6	8	3	5	7	7	8.5	10	7.5	8	8.5	4.5	5	5.5	6.5	7	7.5	7.5	8	8.5	5	6	7	0	2	2	2	3	4	1	7	3	2	8.5	5.96
DS3	5	7	9	1	3	5	0	2	4	3	5	7	7.5	8	8.5	4.5	5	5.5	6.5	7	7.5	6.5	7	7.5	3	4	5	4	4	6	2	3	4	3	7	5	2	8	5.17
DS4	5	7	9	4	6	8	0	1	3	6	8	10	8.5	9	9.5	4.5	5	5.5	4.5	5	5.5	6.5	7	7.5	3	4	5	1	3	3	3	4	5	4	5	6	1	9	5.33
DS5	6	8	10	1	3	5	0	2	4	6	8	10	7.5	8	8.5	6.5	7	7.5	6.5	7	7.5	8.5	9	9.5	4	5	6	1	3	3	3	4	5	5	7	7	2	9	5.92
DS6	4	6	8	3	5	7	4	6	8	4	6	8	9.5	9.75	10	6.5	7	7.5	4.5	5	5.5	6.5	7	7.5	3	4	5	4	4	6	2	3	4	3	5	5	3	9.75	5.65

	DMU1			DMU2			DMU3			DMU4			DMU5			DMU6			DMU7			DMU8			DMU9			DMU10			DMU11			DMU12			Min	Max	Mean
	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U			
DS7	5	7	9	4	6	8	1	3	5	6	8	10	6.5	7	7.5	5.5	6	6.5	2.5	3	3.5	5.5	6	6.5	4	5	6	2	4	4	4	5	6	4	3	6	3	8	5.25
DS8	5	7	9	0	2	4	4	6	8	4	6	8	9.5	9.75	10	4.5	5	5.5	3.5	4	4.5	8.5	9	9.5	6	7	8	2	3.5	4	3	4	5	4	4	6	2	9.75	5.60
DS9	6	8	10	0	2	4	1	3	5	6	8	10	7.5	8	8.5	6.5	7	7.5	3.5	4	4.5	3.5	4	4.5	2	3	4	1	3	3	3	4	5	3	4	5	2	8	4.83
DS10	5	7	9	3	5	7	1	3	5	4	6	8	7.5	8	8.5	4.5	5	5.5	0.5	1	1.5	2.5	3	3.5	4	5	6	2	3	4	2	3	4	2	1	4	1	8	4.17
DS11	5	7	9	3	5	7	3	5	7	6	8	10	8.5	9	9.5	7.5	8	8.5	6.5	7	7.5	7.5	8	8.5	3	4	5	2	3.5	4	3	4	5	2	7	4	3.5	9	6.29
DS12	5	7	9	4	6	8	2	4	6	4	6	8	8.5	9	9.5	4.5	5	5.5	5.5	6	6.5	4.5	5	5.5	5	6	7	2	3	4	2	3	4	3	6	5	3	9	5.50
DS13	4	6	8	2	4	6	1	3	5	5	7	9	6.5	7	7.5	7.5	8	8.5	3.5	4	4.5	3.5	4	4.5	3	4	5	0	3	2	4	5	6	1	4	3	3	8	4.92
ME1	6	8	10	3	5	7	3	5	7	6	8	10	8.5	9	9.5	5.5	6	6.5	4.5	5	5.5	5.5	6	6.5	5	6	7	5	4.5	7	2	3	4	2	5	4	3	9	5.88
ME2	4	6	8	3	5	7	4	6	8	5	7	9	6.5	7	7.5	3.5	4	4.5	2.5	3	3.5	3.5	4	4.5	6	7	8	5	5.5	7	4	5	6	3	3	5	3	7	5.21
ME3	5	7	9	3	5	7	0	1	3	5	7	9	7.5	8	8.5	7.5	8	8.5	2.5	3	3.5	7.5	8	8.5	3	4	5	3	4	5	3	4	5	4	3	6	1	8	5.17
ME4	5	7	9	3	5	7	2	4	6	4	6	8	8.5	9	9.5	3.5	4	4.5	5.5	6	6.5	7.5	8	8.5	2	3	4	1	4	3	5	6	7	5	6	7	3	9	5.67

L=Lower bound value $(\bar{y}_{rj}^{3} - G_{rj}^{3})$

N=Nominal value $(\bar{y}_{rj}^{3})$

U=Upper bound vale $(\bar{y}_{rj}^{3} + G_{rj}^{3})$

Table A-4. The input and output data for IT research projects of ITRC including summary statistics expressed by expert 4 (E4)

	DMU1			DMU2			DMU3			DMU4			DMU5			DMU6			DMU7			DMU8			DMU9			DMU10			DMU11			DMU12			Min	Max	Mean
	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U	L	*N*	U			
PO1	6.5	7	7.5	3.5	4	4.5	1.5	2	2.5	9.5	9.75	10	7	8	9	7	8	9	4	5	6	7	8	9	3	4	5	5	4.5	7	2	3	4	2	5	4	2	9.75	5.69
PO2	5.5	6	6.5	3.5	4	4.5	0.5	1	1.5	5.5	6	6.5	7	8	9	7	8	9	5	6	7	5	6	7	2	3	4	1	3	3	3	4	5	5	6	7	1	8	5.08
PO3	6.5	7	7.5	4.5	5	5.5	2.5	3	3.5	8.5	9	9.5	7	8	9	7	8	9	3	4	5	8	9	10	6	7	8	2	3.5	4	3	4	5	3	4	5	3	9	5.96
PO4	5.5	6	6.5	4.5	5	5.5	5.5	6	6.5	8.5	9	9.5	7	8	9	7	8	9	0	1	2	3	4	5	5	6	7	3	4.5	5	4	5	6	3	1	5	1	9	5.29
PO5	5.5	6	6.5	3.5	4	4.5	4.5	5	5.5	7.5	8	8.5	7	8	9	4	5	6	2	3	4	7	8	9	4	5	6	0	2	2	2	3	4	1	3	3	2	8	5.00
PO6	7.5	8	8.5	2.5	3	3.5	5.5	6	6.5	8.5	9	9.5	8	9	10	6	7	8	5	6	7	4	5	6	4	5	6	1	3.5	3	4	5	6	4	6	6	3	9	6.04
PO7	7.5	8	8.5	4.5	5	5.5	1.5	2	2.5	8.5	9	9.5	8	9	10	4	5	6	3	4	5	3	4	5	3	4	5	3	3.5	5	2	3	4	2	4	4	2	9	5.04
PO8	6.5	7	7.5	3.5	4	4.5	4.5	5	5.5	6.5	7	7.5	6	7	8	5	6	7	0	1	2	6	7	8	3	4	5	4	4.5	6	3	4	5	3	1	5	1	7	4.79
PO9	6.5	7	7.5	2.5	3	3.5	1.5	2	2.5	7.5	8	8.5	7	8	9	5	6	7	2	3	4	4	5	6	4	5	6	0	3.5	2	5	6	7	3	3	5	2	8	4.96
PO10	6.5	7	7.5	2.5	3	3.5	2.5	3	3.5	8.5	9	9.5	7	8	9	4	5	6	4	5	6	7	8	9	3	4	5	4	5	6	4	5	6	4	5	6	3	9	5.58
AI1	5.5	6	6.5	4.5	5	5.5	2.5	3	3.5	8.5	9	9.5	7	8	9	5	6	7	0	1	2	3	4	5	4	5	6	1	3	3	3	4	5	3	1	5	1	9	4.58
AI2	7.5	8	8.5	5.5	6	6.5	5.5	6	6.5	5.5	6	6.5	9	9.5	10	6	7	8	5	6	7	5	6	7	6	7	8	3	4	5	3	4	5	2	6	4	4	9.5	6.29
AI3	5.5	6	6.5	5.5	6	6.5	1.5	2	2.5	9.5	9.75	10	6	7	8	7	8	9	1	2	3	5	6	7	4	5	6	3	4.5	5	4	5	6	5	2	7	2	9.75	5.27
AI4	5.5	6	6.5	5.5	6	6.5	3.5	4	4.5	9.5	9.75	10	6	7	8	4	5	6	4	5	6	5	6	7	4	5	6	3	5	5	5	6	7	3	5	5	4	9.75	5.81
AI5	6.5	7	7.5	3.5	4	4.5	0.5	1	1.5	5.5	6	6.5	6	7	8	4	5	6	1	2	3	2	3	4	6	7	8	0	2.5	2	3	4	5	5	2	7	1	7	4.21
AI6	7.5	8	8.5	2.5	3	3.5	3.5	4	4.5	8.5	9	9.5	9	9.5	10	3	4	5	5	6	7	3	4	5	5	6	7	5	4.5	7	2	3	4	1	6	3	3	9.5	5.58
AI7	6.5	7	7.5	4.5	5	5.5	0.5	1	1.5	4.5	5	5.5	7	8	9	5	6	7	5	6	7	3	4	5	5	6	7	1	3.5	3	4	5	6	2	6	4	1	8	5.21
DS1	7.5	8	8.5	2.5	3	3.5	2.5	3	3.5	9.5	9.75	10	8	9	10	5	6	7	3	4	5	4	5	6	4	5	6	2	4	4	4	5	6	1	4	3	3	9.75	5.48
DS2	7.5	8	8.5	2.5	3	3.5	3.5	4	4.5	5.5	6	6.5	8	9	10	5	6	7	2	3	4	5	6	7	5	6	7	1	3.5	3	4	5	6	3	3	5	3	9	5.21
DS3	7.5	8	8.5	1.5	2	2.5	3.5	4	4.5	7.5	8	8.5	6	7	8	3	4	5	0	1	2	5	6	7	4	5	6	2	3.5	4	3	4	5	2	1	4	1	8	4.46
DS4	6.5	7	7.5	2.5	3	3.5	1.5	2	2.5	7.5	8	8.5	8	9	10	6	7	8	4	5	6	2	3	4	5	6	7	3	4	5	3	4	5	1	5	3	2	9	5.25
DS5	5.5	6	6.5	2.5	3	3.5	2.5	3	3.5	8.5	9	9.5	9	9.5	10	5	6	7	1	2	3	8	9	10	2	3	4	2	4	4	4	5	6	2	2	4	2	9.5	5.13
DS6	5.5	6	6.5	3.5	4	4.5	0.5	1	1.5	6.5	7	7.5	8	9	10	3	4	5	4	5	6	4	5	6	6	7	8	3	4.5	5	4	5	6	4	5	6	1	9	5.21
DS7	6.5	7	7.5	3.5	4	4.5	4.5	5	5.5	5.5	6	6.5	8	9	10	6	7	8	1	2	3	7	8	9	2	3	4	4	5.5	6	5	6	7	5	2	7	2	9	5.38
DS8	5.5	6	6.5	3.5	4	4.5	2.5	3	3.5	9.5	9.75	10	7	8	9	7	8	9	5	6	7	6	7	8	6	7	8	1	3	3	3	4	5	3	6	5	3	9.75	5.98
DS9	5.5	6	6.5	2.5	3	3.5	4.5	5	5.5	5.5	6	6.5	7	8	9	4	5	6	6	7	8	6	7	8	5	6	7	5	5	7	3	4	5	3	7	5	3	8	5.75
DS10	5.5	6	6.5	4.5	5	5.5	2.5	3	3.5	6.5	7	7.5	6	7	8	3	4	5	6	7	8	5	6	7	2	3	4	2	4	4	4	5	6	4	7	6	3	7	5.33
DS11	6.5	7	7.5	1.5	2	2.5	4.5	5	5.5	4.5	5	5.5	8	9	10	5	6	7	2	3	4	6	7	8	4	5	6	2	3	4	2	3	4	2	3	4	2	9	4.83
DS12	7.5	8	8.5	5.5	6	6.5	3.5	4	4.5	8.5	9	9.5	9	9.5	10	4	5	6	3	4	5	8	9	10	5	6	7	1	3.5	3	4	5	6	1	4	3	3.5	9.5	6.08
DS13	5.5	6	6.5	4.5	5	5.5	3.5	4	4.5	5.5	6	6.5	6	7	8	3	4	5	4	5	6	7	8	9	5	6	7	5	5.5	7	4	5	6	3	5	5	4	8	5.54
ME1	6.5	7	7.5	5.5	6	6.5	3.5	4	4.5	7.5	8	8.5	8	9	10	6	7	8	2	3	4	7	8	9	2	3	4	4	5	6	4	5	6	2	3	4	3	9	5.67
ME2	6.5	7	7.5	4.5	5	5.5	4.5	5	5.5	7.5	8	8.5	7	8	9	6	7	8	6	7	8	4	5	6	5	6	7	2	3.5	4	3	4	5	2	7	4	3.5	8	6.04
ME3	5.5	6	6.5	5.5	6	6.5	1.5	2	2.5	8.5	9	9.5	8	9	10	4	5	6	1	2	3	6	7	8	5	6	7	4	4.5	6	3	4	5	3	2	5	2	9	5.21
ME4	6.5	7	7.5	3.5	4	4.5	2.5	3	3.5	6.5	7	7.5	7	8	9	6	7	8	3	4	5	7	8	9	5	6	7	1	3	3	3	4	5	4	4	6	3	8	5.42

L=Lower bound value $(\bar{y}_{rj}^{4} - G_{rj}^{4})$

N=Nominal value $(\bar{y}_{rj}^{4})$

U=Upper bound vale $(\bar{y}_{rj}^{4} + G_{rj}^{4})$

References

[1] Weill, P. and J.W. Ross, *IT governance: How top performers manage IT decision rights for superior results.* 2004: Harvard Business Press.

[2] Davoudi, M.R. and F. Shams Aliee. *Characterization of Enterprise Architecture Quality Attributes. In Enterprise Distributed Object Computing Conference Workshops, 2009. EDOCW 2009. 13th 2009.*

[3] Davoudi, M.R. and F. Shams Aliee. *A New AHP-based Approach towards Enterprise Architecture Quality Attribute Analysis. In Research Challenges in Information Science, 2009. RCIS 2009. Third International Conference on. 2009.*

[4] Niemann, K.D., *From Enterprise Architecture to IT Governance- Elements of Effective IT Management.* 2006, Germany: Friedr. Vieweg & Sohn Verlag.

[5] Johnson, P., et al. *A Tool for Enterprise Architecture Analysis. In the 11th IEEE Enterprise Distributed Object Computing Conference.* 2007. USA: IEEE Computer Society.

[6] Lankes, J.K., *Metrics for Application Landscapes: Status Quo, Development, and a Case Study*. 2008.

[7] Cook, W.D. and L.M. Seiford, *Data envelopment analysis (DEA)–Thirty years on.* European Journal of Operational Research, 2009. 192 (1): pp.1-17.

[8] Buckl, S., F. Matthes, and C.M. Schweda. *Classifying Enterprise Architecture Analysis Approaches. In the 2nd IFIP WG5.8 Workshop on Enterprise Interoperability (IWEI'2009)*. 2009. Valencia, Spain.

[9] Yu, E., M. Strohmaier, and X. Deng. *Exploring intentional modeling and analysis for enterprise architecture. In the EDOC 2006 Conference Workshop on Trends in Enterprise Architecture Research (TEAR 2006)*. 2006. Hong Kong: IEEE Computer Society Press.

[10] Jacob, M.-E. and H. Jonkers, *Quantitative analysis of enterprise architectures.* Interoperability of Enterprise Software and Applications, ed. D. Konstantas, et al. 2006, Geneva, Switzerland: Springer.

[11] Boer, F.S., et al. *Enterprise architecture analysis with XML. In the 38th Annual Hawaii International Conference on System Sciences (HICSS 2005).* 2005. USA: IEEE Computer Society Press.

[12] Frank, U., et al. *Designing and utilizing business indicator systems within enterprise models-outline of a method. In Modeling Business Information Systems Conference (MobIS 2008).* 2008. Saarbrucken, Germany.

[13] Razavi, M., F. Shams Aliee, and K. Badie, *An AHP-based approach toward enterprise architecture analysis based on enterprise architecture quality attributes.* Knowledge and information systems, 2011. 28 (2): pp.449-472.

[14]Lagerström, R. *Analyzing System Maintainability Using Enterprise Architecture Models. In the 2nd Workshop on Trends in Enterprise Architecture Research (TEAR'07).* 2007. St Gallen, Switzerland.

[15] Lagerström, R. and P. Johnson. *Using Architectural Models to Predict the Maintainability of Enterprise Systems. in 12th European Conference on Software Maintenance and Reengineering.* 2008.

[16] Büyüközkan, G. and D. Ruan, *Evaluation of software development projects using a fuzzy multi-criteria decision approach.* Mathematics and Computers in Simulation, 2008. 77 (5): pp.464-475.

[17] Lee, K., et al., *Quantitative measurement of quality attribute preferences using conjoint analysis.* Interactive Systems. Design, Specification, and Verification, 2006: pp.213-224.

[18] Reddy, A., M. Naidu, and P. Govindarajulu, *An integrated approach of analytical hierarchy process model and goal model (AHP-GP Model) for selection of software architecture.* International Journal of Computer Science and Network Security, 2007. 7 (10): pp.108-117.

[19] Svahnberg, M., et al., *A quality-driven decision-support method for identifying software architecture candidates.* International Journal of Software Engineering and Knowledge Engineering, 2003. 13 (05): pp.547-573.

[20] Zhu, L., et al., *Tradeoff and sensitivity analysis in software architecture evaluation using analytic hierarchy process.* Software Quality Journal, 2005. 13 (4): pp.357-375.

[21]Saaty, T.L., *The analytical hierarchical process.* J Wiley, New York, 1980.

[22]Davidsson, P., S. Johansson, and M. Svahnberg, *Using the analytic hierarchy process for evaluating multi-agent system architecture candidates.* Agent-Oriented Software Engineering VI, 2006: pp.205-217.

[23]Wang, C.H., R.D. Gopal, and S. Zionts, *Use of data envelopment analysis in assessing information technology impact on firm performance.* Annals of Operations Research, 1997. 73: pp.191-213.

[24]Asosheh, A., S. Nalchigar, and M. Jamporazmey, *Information technology project evaluation: An integrated data envelopment analysis and balanced scorecard approach.* Expert Systems with Applications, 2010. 37(8): p. 5931-5938.

[25]Huang, Y.S., J.T. Liao, and Z.L. Lin, *A study on aggregation of group decisions.* Systems Research and Behavioral Science, 2009. 26 (4): pp.445-454.

[26]Chou, S.Y., Y.H. Chang, and C.Y. Shen, *A fuzzy simple additive weighting system under group decision-making for facility location selection with objective/subjective attributes.* European Journal of Operational Research, 2008. 189 (1): pp.132-145.

[27]Sengupta, J., *Dynamics of data envelopment analysis: Theory of systems efficiency.* 1995: Springer.

[28]ISACA, C., *Control Objectives for Information and realted Technologies.* 2010.

[29]Bernroider, E.W.N. and M. Ivanov, *IT project management control and the Control Objectives*

for IT and related Technology (CobiT) framework. International Journal of Project Management, 2011. 29 (3): pp.325-336.

[30]Hardy, G., *Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges.* Information Security Technical Report, 2006. 11 (1): pp.55-61.

[31]Huang, S.-M., et al., *Building the evaluation model of the IT general control for CPAs under enterprise risk management.* Decision Support Systems, 2011. 50 (4): pp.692-701.

[32]Tuttle, B. and S.D. Vandervelde, *An empirical examination of CobiT as an internal control framework for information technology.* International Journal of Accounting Information Systems, 2007. 8 (4): pp.240-263.

[33]Žvanut, B. and M. Bajec, *A tool for IT process construction.* Information and Software Technology, 2010. 52 (4): pp.397-410.

[34]Sadjadi, S. and H. Omrani, *Data envelopment analysis with uncertain data: An application for Iranian electricity distribution companies.* Energy Policy, 2008. 36 (11): pp.4247-4254.

[35]Charnes, A., W.W. Cooper, and E. Rhodes, *Measuring the efficiency of decision making units.* European Journal of Operational Research, 1978. 2 (6): pp.429-444.

[36]Liu, W., et al., *A study of DEA models without explicit inputs.* Omega, 2011. 39 (5): pp.472-480.

[37]Charnes, A. and W.W. Cooper, *Deterministic equivalents for optimizing and satisficing under chance constraints.* Operations research, 1963. 11 (1): pp.18-39.

[38]SENGUPTA, J.K., *Efficiency measurement in stochastic input-output systems†.* International Journal of Systems Science, 1982. 13 (3): pp.273-287.

[39]Sengupta, J.K., *Data envelopment analysis for efficiency measurement in the stochastic case.* Computers & operations research, 1987. 14 (2): pp.117-129.

[40]SENGUPTA, J.K., *Robust efficiency measures in a stochastic efficiency model.* International Journal of Systems Science, 1988. 19 (5): pp.779-791.

[41]Cooper, W.W., et al., *Chance constrained programming formulations for stochastic characterizations of efficiency and dominance in DEA.* Journal of Productivity Analysis, 1998. 9 (1): pp.53-79.

[42] Cooper, W., Z. Huang, and S.X. Li, *Chapter 13 Satisficing DEA models under chance constraints.* Annals of Operations Research, 1996. 66 (4): pp.279-295.

[43]Cooper, W.W., et al., *Chance constrained programming approaches to congestion in stochastic data envelopment analysis.* European Journal of Operational Research, 2004. 155 (2): pp.487-501.

[44]Ben-Tal, A. and A. Nemirovski, *Robust solutions of linear programming problems contaminated with uncertain data.* Mathematical Programming, 2000. 88 (3): pp.411-424.

[45]Soyster, A.L., T*echnical Note—Convex Programming with Set-Inclusive Constraints and Applications to Inexact Linear Programming.* Operations research, 1973. 21 (5): pp.1154-1157.

[46]Ben-Tal, A. and A. Nemirovski, *Robust convex optimization.* Mathematics of Operations Research, 1998. 23 (4): pp.769-805.

[47]Ben-Tal, A. and A. Nemirovski, *Robust solutions of uncertain linear programs.* Operations research letters, 1999. 25 (1): pp.1-13.

[48]Bertsimas, D., D. Pachamanova, and M. Sim, *Robust linear optimization under general norms.* Operations Research Letters, 2004. 32 (6): pp.510-516.

[49]Bertsimas, D. and M. Sim, *The price of robustness.* Operations research, 2004. 52 (1): pp.35-53.

[50]Wang, K. and F. Wei, *Robust data envelopment analysis based MCDM with the consideration of uncertain data.* Systems Engineering and Electronics, Journal of, 2010. 21 (6): pp.981-989.

[51]Sadjadi, S. and H. Omrani, *A bootstrapped robust data envelopment analysis model for efficiency estimating of telecommunication companies in Iran.* Telecommunications Policy, 2010. 34 (4): pp.221-232.

[52]Simar, L. and P.W. Wilson, *Sensitivity analysis of efficiency scores: How to bootstrap in nonparametric frontier models.* Management science, 1998: pp.49-61.

[53]Simar, L. and P.W. Wilson, *A general methodology for bootstrapping in non-parametric frontier models.* Journal of applied statistics, 2000. 27 (6): pp.779-802.

[54]Shokouhi, A.H., et al., *A robust optimization approach for imprecise data envelopment analysis.* Computers & Industrial Engineering, 2010. 59 (3): pp.387-397.

[55]Ben-Tal, A., L. El Ghaoui, and A. Nemirovski, *Robust optimization.* 2009: Princeton University Press.

[56]Tsai, W.-H., et al., *A MCDM approach for sourcing strategy mix decision in IT projects.* Expert Systems with Applications, 2010. 37 (5): pp.3870-3886.

Wideband Log Periodic-Microstrip Antenna with Elliptic Patches

Hamed Ghanbari Foshtami*
Department of Electrical Engineering, Majlesi Branch, Islamic Azad University, Isfahan, Iran
h.ghanbari@acecr.ac.ir
Ali Hashemi Talkhouncheh
Department of Electrical Engineering, Mohajer Institute of Technology, Technical & Vocational University (TVU), Esfahan, Iran
a.hashemi@iaumajlesi.ac.ir
Hossein Emami
Department of Electrical Engineering, Majlesi Branch, Islamic Azad University,Isfahan, Iran
h.emami@ieee.org

Received: 07/Apr/2013 Accepted: 15/Jun/2013

Abstract

A broadband microstrip antenna based on log periodic technique was conceived and demonstrated practically. The antenna exhibits a wideband characteristic comparing with other microstrip antennas. Over the operation frequency range, i.e. 2.5-6 GHz, a 50 Ω input impedance has been considered.

Keywords: Microstrip Antenna, Log-Periodic, VSWR, Gain, Pattern

1. Introduction

Currently, there are increasing demands for novel ultrawideband (UWB) antennas with low-profile structures and constant directional radiation patterns for both commercial and military applications [1], Microstrip antenna has gain popularity because of their small size and light weight. However a limitation of microstrip antenna is the narrow bandwidth of the basic element. The bandwidth of the antenna can be increased by reducing the substrate permittivity (εr) or increasing its thickness (h) [2]. Different techniques to enhance the bandwidth of microstrip antenna have been investigated. Most of the effort to enhance the bandwidth has been directed towards improving the impedance bandwidth of the antenna element. The bandwidth can be increased using multilayer structure antenna [3], parasitic element [4], non contact feeding technique [5], different shape slots [6] or log periodic technique [7]. A log-periodic antenna has been successfully operated as a broadband linearly polarized antenna element in free space since 1957 [8,9]. The log-periodic dipole array (LPDA) is an antenna with frequency independency advantage. The input impedance and gain of this antenna remains almost constant over its operating bandwidth, which can be very large. Practical designs of an LPDA could have one octave or more bandwidth [10,11].

In this article, we introduce a new hybrid log periodic-microstrip antenna (LPMA). This antenna is terminated by a novel compensating stub with length of T, instead of a matched load or open-circuit [12]. We show that the proposed LPMA gives better characteristics in comparison with others, especially by increasing the bandwidth. To do this, at first, radiator elements are considered rectangular patches. Next, they are replaced with elliptical patches. Finally, the simulation and measurement results of antenna are analyzed and compared together.

2. Antenna Design

The design principle for log periodic requires scaling of dimensions from period to period so that performance is periodic with the logarithm of frequency. This principle can be applied to an array of patch antennas. The patch length (L), the width (W) and Inset (D) are related to the scale factor τ by:

$$\tau = \frac{\mathrm{Lm}+1}{\mathrm{Lm}} = \frac{\mathrm{Wm}+1}{\mathrm{Wm}} = \frac{\mathrm{Dm,m}+1}{\mathrm{Dm}-1,\mathrm{m}} \qquad (1)$$

If we multiply all dimensions of the array by τ it scales into itself with element m becoming element m+l, element m+l becoming element m+2, etc. This self scaling properly implies that the array will have the same radiating properties at all frequencies that are related by a factor of τ. [2] In the equation, Dm,m+1 is distance between patch Pm+1 and Pm, also Wm and Lm are width and length of the patch Pm, respectively. In the elliptical patch design, the great length of the

* Corresponding Author

ellipse is considered Wm and the small length of the ellipse is Lm

An example of single-layer microstrip log periodic antenna is shown in Fig. 1. This antenna consists of square patches located on a FR4 substrate with dielectric constant equals to 4.4 and 1.6 mm thickness. It is feeding by coaxial cable with 50 ohms. Distance of patch from stripline is 0.2 mm, width of stripline is 3 mm and the distance of end line and the last patch of the strip is 4mm. Logarithmic factor, τ, is considered 1.1.

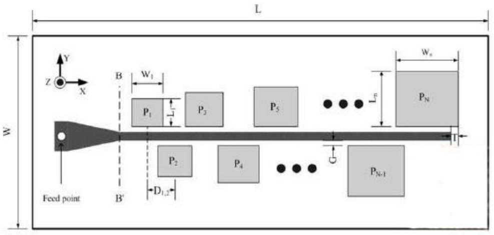


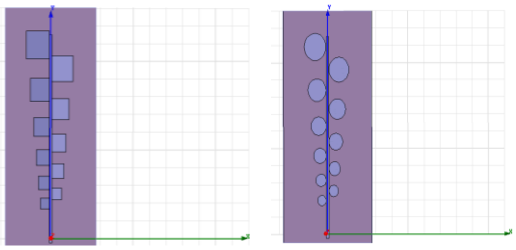
Fig 1- Structural configuration of Log-periodic microstrip antenna [10]

Dimensions, sizes and distances are tabulated in table 1. Antenna length (L) is 270 mm and it's width (W) is 110 mm.

TABLE I- Sizes and dimensions designed for log-periodic microstrip antenna with logarithmic factor of 1.1

m	f (GHz)	L_m (mm)	W_m (mm)	$D_{m,m+1}$ (mm)
1	2.3	10.62713	12.2212	10.62717
2	2.53	11.68985	13.44332	11.68989
3	2.783	12.85883	14.78765	12.85888
4	3.0613	14.14471	16.26642	14.14477
5	3.36743	15.55918	17.89306	15.55925
6	3.704173	17.1151	19.68237	17.11517
7	4.07459	18.82661	21.6506	18.82669
8	4.482049	20.70927	23.81566	20.70936
9	4.930254	22.7802	26.19723	22.78029
10	5.42328	25.05822	28.81695	25.05832
11	5.965608	27.56404	31.69865	27.56415

In the next stage, for comparison and verifying the results, elliptical patches are used instead of rectangular patches. We hypothesize that the elliptical patches can improve the results. Fig. 2 shows the geometrical structure of two kinds of antennas.

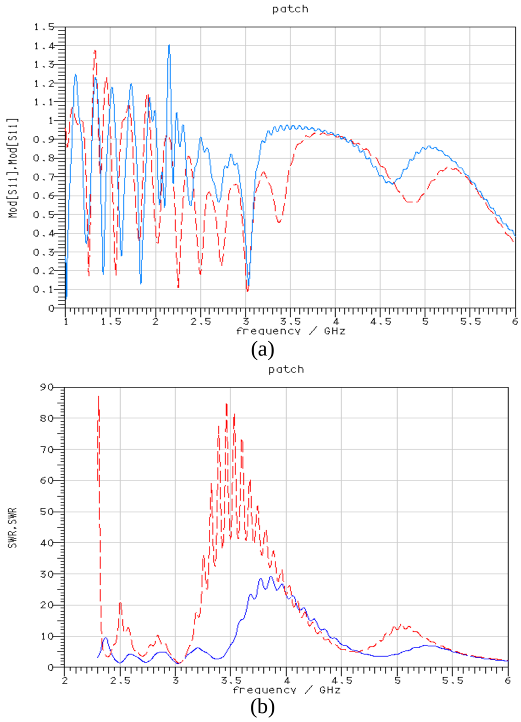


(a) (b)

Fig 2- (a) Simulated image of log-periodic microstrip antenna with rectangular patches (b) Simulated image of log-periodic microstrip antenna with elliptical patches

3. Simulation Results

In this section, to verify the design results, we simulated our design in software environment. We show simulated results of the proposed LPMA. All simulations have been done by CST. These results are shown in Fig. 3 to Fig. 9. Diagrams related to the antenna using rectangular patch is shown with discrete lines and antenna using elliptical patch with continuous line in all graphs.



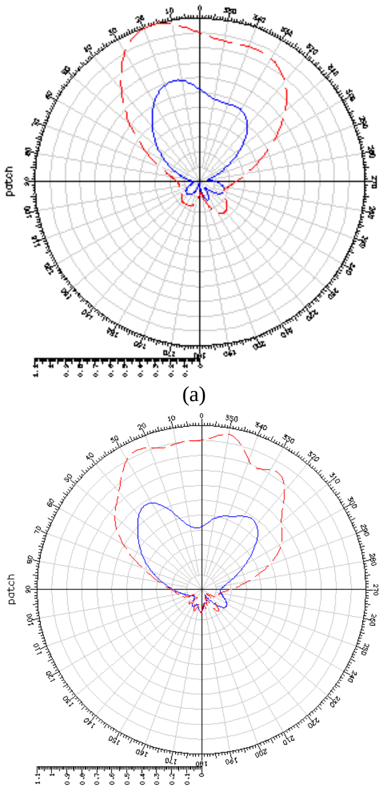
(a)

(b)

Fig 3- Comparison simulated S parameters between Using rectangular patches & elliptical patches (a) S11 (b) VSWR

As be seen in Fig.3, after replacing the elliptical patch, VSWR decreases to <2 from f=2.3 GHz to f=3.4 GHz

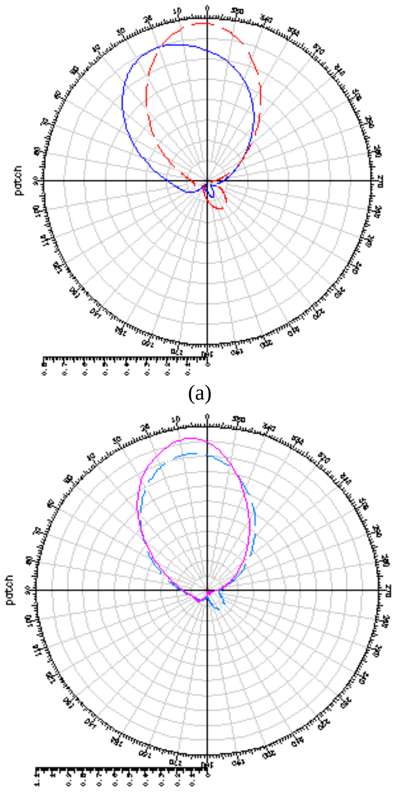
Figures 4 and 5, show the replacement of the elliptical patches with the rectangular patches causes in reducing the side lobes and increasing the directivity Rotation angles in some of directs which can be seen, is caused by differences in polarization in the elliptical shapes to the rectangular shapes. Photos the antenna structure using elliptical patches and rectangular patches also shows figure 6.



(a)

(b)

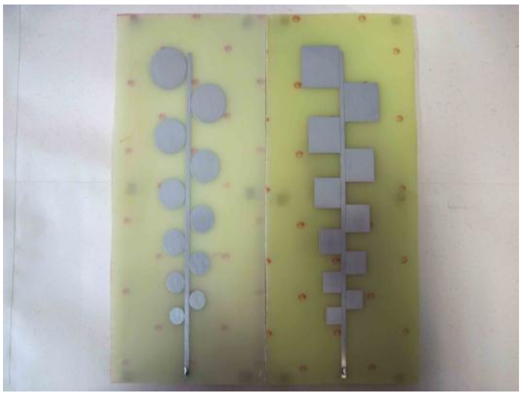
Fig 4- Comparison simulated pattern between Using rectangular patches & elliptical patches in f=2.3GHz (a) E plane (b) H plane.



(a)

(b)

Fig 5- Comparison simulated pattern between Using rectangular patches & elliptical patches in f=3.4GHz (a) E plane (b) H plane

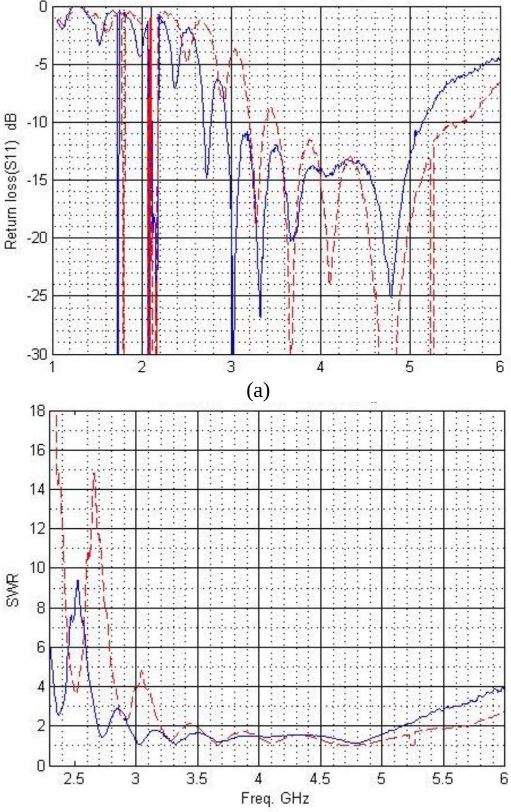


(a) (b)

Fig 6- photos the antenna structure (a) Using elliptical patches (b) Using rectangular patches

4. Experimental Results

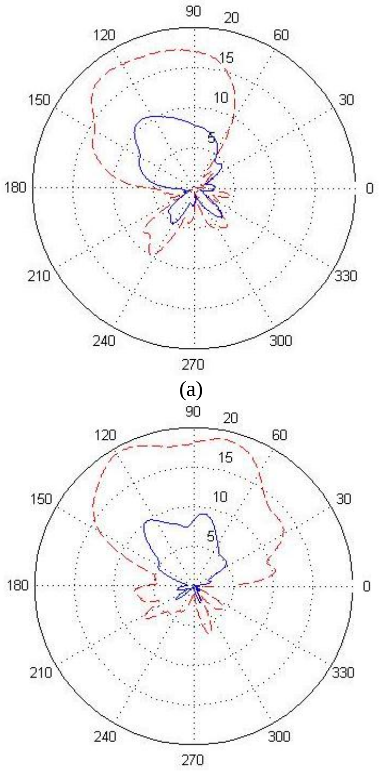
After the simulation phase and to obtain desired results, sample antenna with τ=1.1 was made (OR implemented) based on the dimensions and sizes in Table I. Substrate has chosen FR4 with dielectric constant 4.4. For comparison of results, conditions in implementation and simulation have been assumed similar. To improving the results, such as simulation, it is considered a 3 mm distance between substrate and the ground. Results from the implementation such as patterns and VSWR can be seen in Figures 7 to 9.



(a)

(b)

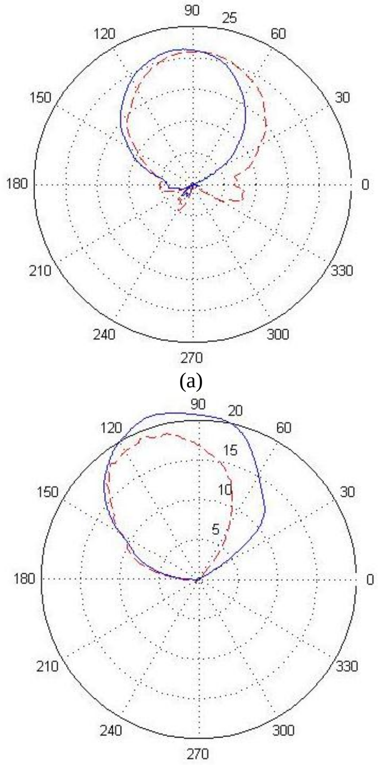
Fig 7- Comparison simulated S parameters between Using rectangular patches & elliptical patches (a) S11 (b) VSWR



(a)

(b)

Fig 8- Comparison Measurement pattern between Using rectangular patches and elliptical patches in f=2.3 GHz (a) E plane (b) H plane



(a)

(b)

Fig 9- Comparison Measurement pattern between Using rectangular patches and elliptical patches in f=3.4 GHz (a) E plane (b) H plane

Diagrams obtained from measurements are shown in Fig 7. As was predicted in simulations, Elliptical patches significantly to reduce the VSWR plots below the value 2. The patterns of electrical and magnetic field obtained from measurements sample made using of rectangular and elliptical patches are compared In Fig 8 and 9. Small differences can be seen in simulated and measured results to be due to the lack of ideal conditions as the building.

5. Conclusion

Simulation and manufacture results and compare them show that the use of elliptical patch in the design has increased bandwidth. Although it may not necessarily increase the bandwidth in the entire design, the results have shown that the replacing of elliptical patch with rectangular patch, have considerably improved VSWR due to the curvature of the corners. As we can see that the VSWR parameter is less than 2 from the initial frequency we designed (2.3 GHz) to the final frequency (6 GHz), which in this matter, can be considered ideal. Also In frequency with the proper directivity and high gain, the replacement of elliptical patch improves patterns and reduces annoying side lobes and patterns are becoming sharper. Finally we can say if the design using appropriate materials and frequency proportional to its, elliptical patch can be improve the expected results in most parameters in the designed frequency.

References

[1] Z. N. Chen, M. J. Ammann, X. Qing, X. H. Wu, T. S. P. See, and A. Cai, “Planar antenna,” IEEE Microwav. Mag., Vol.7, No.6, pp.63–73, Dec. 2006.

[2] Rahim, M.K.A.; Gardner, P. “The design of nine element quasi microstrip log periodic antenna” RF and Microwave Conference, 2004. RFM 2004. Proceedings 5-6 Oct. 2004, pp.132- 135.

[3] Croq, F., Kossiavas, G., Papiemik, A. 'Stacked resonators for bandwidth enhancement: A comparison of two feeding technique', IEE Proceedings on Microwave, Antenna and Propagation, Part H, Vol.1404, Aug.1993 pp.303-308

[4] Wood, C., 'Improved bandwidth of microstrip antenna using parasitic elements", IEE Proc H, Microwaves Opt. &Ant., 1980, 127, pp.231- 234

[5] Pozar, D.M., 'Microstrip Antena Aperture Coupled to Microstrip Line', Electronics Lenen, Vol.21, No.2, 1985, pp.49-50

[6] Chen H.M., Sze, J.Y., Lin, Y.F., 'A Broadband rectangular microstrip Antenna with a pair of U shaped slots', Microwave and Optical Tech. Leners, Vol.27, No.5, Dec. 2000,pp.369-370.

[7] Hall, P. S., 'Multioctave bandwidth Log periodic Microstrip Antenna Array', IEE proc. Vo1.133 R H. No.2 1986 pp.127-136.

[8] R.H. Duhamel and D.E. Isbell, “Broadband Logarithmically Periodic Antenna Structures,” IRE National Convention Recod, pp.119-128, 1957.

[9] R.H. Duhamel and F.R. Ore, “Logarithmically Periodic Antenna Designs,” IRE National Convention Record, pp.139-151, 1958.

[10] Kitchin, C.R. (2003): Astrophysical techniques, 4th edition, CRC Press.

[11] Thompson, A.R., Moran, J.M. and Swenson, G.W. Jr. (2001): Interferometer and Synthesis in radio Astronomy, John Wiley and Sons, Inc.

[12] Qi Wu, Ronghong Jin, and Junping Geng, A Single-Layer Ultrawideband Microstrip Antenna, IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION, Vol.58, No.1, JANUARY 2010.

A New Finite Field Multiplication Algorithm to Improve Elliptic Curve Cryptosystem Implementations

Abdalhossein Rezai*
Electrical Engineering, Ph.D. Student, Electrical and Computer Engineering Faculty, Semnan University
rezaie@acecr.ac.ir
Parviz Keshavarzi
Electrical Engineering, Associate Professor, Electrical and Computer Engineering Faculty, Semnan University
pkeshavarzi@semnan.ac.ir

Received: 21/Jan/2013 Accepted: 15/Jul/2013

Abstract

This paper presents a new and efficient implementation approach for the elliptic curve cryptosystem (ECC) based on a novel finite field multiplication in GF(2^m) and an efficient scalar multiplication algorithm. This new finite field multiplication algorithm performs zero chain multiplication and required additions in only one clock cycle instead of several clock cycles. Using modified (limited number of shifts) Barrel shifter; the partial result is also shifted in one clock cycle instead of several clock cycles. Both the canonical recoding technique and the sliding window method are applied to the multiplier to reduce the average number of required clock cycles. In the scalar multiplication algorithm of the proposed implementation approach, the point addition and point doubling operations are computed in parallel. The sliding window method and the signed-digit representation are also used to reduce the average number of point operations. Based on our analysis, the computation cost (the average number of required clock cycles) is effectively reduced in both the proposed finite field multiplication algorithm and the proposed implementation approach of ECC in comparison with other ECC finite field multiplication algorithms and implementation approaches.

Keywords: Computational Complexity, Network Security, Cryptography, Elliptic Curve Cryptosystem (ECC), Finite Field Multiplication, Scalar Multiplication.

1. Introduction

Elliptic curve cryptosystem (ECC) [1,2] has drawn more attentions in the network security issues due to its higher speed, lower power consumption and smaller key length in comparison with other existing public key cryptosystems [3,4]. These properties also make ECC more suitable for using in limited environments such as wireless sensor networks (WSNs) [3,5]. In ECC implementations, the total execution time and the power consumption are lowered by reducing the number of required clock cycles [3].

The most important operation in ECC is the scalar multiplication [6,7]. This operation is the most time-consuming operation and it takes 85% of the cryptosystem execution time [6,7].

Hardware implementation of ECC usually passes through three computational levels: Scalar multiplication, point operations and finite field operations that will be described in section 2.

There are many attempts to increase the efficiency of the elliptic curve scalar multiplication algorithm by increasing the computational efficiency of these three levels such as developing signed-digit scalar representation [8,9,10,11,12,13], sliding window method in scalar representation [7,9,12,13], parallel architecture in point operations [9], parallel architecture in finite field operations [6,14,15,16] and scalable modular multiplication [17,18]. A comprehensive review is also presented in [19].

High performance implementations of ECC depend heavily on the efficiency in the computation of finite field operations. Most popular finite fields which are commonly used in ECC are the prime fields GF(p) and the binary extension fields GF(2^m). Usually the binary extension fields GF(2^m) leads to a smaller and faster hardware [6,18].

In our previous work [20], the scalar multiplication is improved by using a novel finite field multiplication algorithm in GF(p). This paper presents a novel finite field multiplication algorithm in GF(2^m) based on the finite field multiplication in [20]. This new finite field multiplication uses a new signed-digit multiplier representation and multi bit scan-multi bit shift technique. Using this new signed-digit representation, the average Hamming weight of

* Corresponding Author

the multiplier is effectively reduced. Moreover, the zero chain multiplication is performed in only one clock cycle instead of several clock cycles. Therefore, the average number of required clock cycles (the computation cost) is considerably reduced in the proposed finite field multiplication algorithm. In addition, the proposed finite field multiplication algorithm is applied to the scalar multiplication algorithm in [9]. So, the computation cost of the elliptic curve scalar multiplication is also reduced considerably.

The rest of this paper is organized as follows: section 2 describes the recoding technique, the ECC over GF(2^m), the methods of the scalar multiplication and the finite field multiplication algorithm. The proposed implementation approach of ECC is presented in section 3. Section 4 evaluates the proposed algorithms. Finally, conclusion is given in section 5.

2. Preliminaries

2.1 The Recoding Technique

A signed-digit representation of an integer k_{CR} is the sequence of digits $k_{CR}=(d_m,d_{m-1},\ldots,d_1,d_0)_{SD}$ such that $k_{CR}=\sum_{i=0}^{m} d_i 2^i$ where $d_i \in \{-1,0,1\}$. Booth recoding [21] and canonical recoding (CR) [22,23] are two well-known conversions which can reduce the average Hamming weight of the integer representation. Algorithm 1 shows the canonical recoding algorithm.

```
Algorithm 1: The canonical recoding (CR) algorithm
Input: k= $(k_{m-1}k_{m-2}\ldots k_1k_0)_2$
Output: $k_{CR}= (d_m d_{m-1}\ldots d_1 d_0)_{SD}$
$c_0 := 0$;
For i = 0 to m-1
    $c_{i+1} := \lfloor (k_i + k_{i+1} + c_i)/2 \rfloor$;
    $d_i := k_i + c_i - 2c_{i+1}$;
Return $k_{CR}$;
```

In this algorithm, the input is the scalar k and the output is k_{CR}. It should be noted that, the CR representation, which is also called non-adjacent form (NAF), guarantees the minimal Hamming weight of the integer representation. The average Hamming weight of an m-bit canonical recoded integer is about $\frac{m}{3}$ [11, 22, 23].

2.2 ECC Over GF(2^m)

As described in the previous section, the hardware implementation of ECC usually involves three computational levels: scalar multiplication, point operations and finite field operations [6,20]. These three computational levels are shown in figure 1.

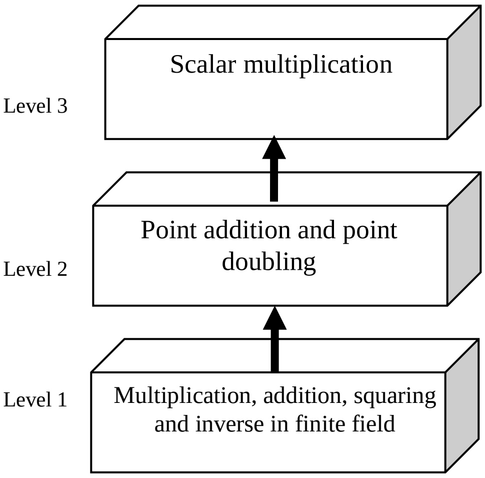

Level 3
Scalar multiplication
Level 2
Point addition and point doubling
Level 1
Multiplication, addition, squaring and inverse in finite field

Figure 1: The three-level model for elliptic curve scalar multiplication [6,20]

The scalar multiplication at the top of the hierarchy computes Q=kP with repeated point addition (Q=R+P) and point doubling (Q=2P) operations where k is a positive integer, and P and Q are elliptic curve points. The middle level of the hierarchy includes the point addition and point doubling operations, which are based on the coordinates used to represent the points. In the lowest level of the hierarchy, the finite field arithmetic includes four operations: finite field multiplication, finite field squaring, finite field addition and finite field inversion [6].

An elliptic curve E over GF(2^m) in affine coordinates is defined as the set of solutions of the reduced Weierstrass equation

$$\text{E}: \quad y^2 + xy = x^3 + ax^2 + b \qquad (1)$$

where $a, b \in GF(2^m), b \neq 0$, together with the point at infinity O [24,25]. Note that for b=1, equation (1) shows especial curves which are commonly called Koblitz curves [12].

The point addition operation $Q=(x_q,y_q)=R+P=(x_r,y_r)+(x_p,y_p)$ is defined by GF(2^m) operations as the following equations [24,25]:

$$\begin{cases} \lambda = (y_r + y_p)/(x_r + x_p) \\ x_q = \lambda^2 + \lambda + x_r + x_p + a \\ y_q = (x_p + x_q)\lambda + x_q + y_r \end{cases} \qquad (2)$$

Similarly, the point doubling operation $Q=(x_q,y_q)=2P=2(x_p,y_p)$ is defined by GF(2^m) operations as follows [24,25]:

$$\begin{cases} \lambda = x_p + \dfrac{y_p}{x_p} \\ x_q = \lambda^2 + \lambda + a \\ y_q = (x_p + x_q)\lambda + x_q + y_p \end{cases} \qquad (3)$$

These point operations involve finite field operations [24,25].

It should be noted that, the use of signed-digit representation for finite field operation in GF(2^m) is considered in [18]. The multiple-precision arithmetic for finite field operation in GF(2^m) is also investigated in [26].

2.3 The Methods of Scalar Multiplication

The most common method for performing an elliptic curve scalar multiplication (Q=kP) is the binary method which scans the bits of the scalar k either from left to right (the L2R binary method) or from right to left (the R2L binary method) [19,24]. The proposed implementation approach is based on the R2L binary method in GF(2^m) and its algorithm is shown in algorithm 2.

```
Algorithm 2: The R2L binary scalar multiplication algorithm
INPUT: $k=(k_{m-1}k_{m-2}\ldots k_0)_2$, P=(x,y);
OUTPUT: Q=(x',y')=kP;
1. Q ← 0;
2. For i= 0 to m-1 do
3.     If $k_i$=1 then Q ← Q+P;
4.     P←2P;
5. Return Q;
```

In algorithm 2, the inputs are the scalar k and the elliptic curve point P. The output is the elliptic curve point Q=kP. The computation cost in the binary multiplication method depends on the Hamming weight and the length of the binary representation of the scalar k (for m-bit scalar k, the binary multiplication method requires m point doubling operations and $\frac{m}{2}$ point addition operation on average).

The efficiency of the binary method may be enhanced by scanning w bits at a time as with the sliding window method [7,13] or reducing the Hamming weight as with the signed-digit recoding technique [10]. One of the efficient efforts to reduce the computation cost in ECC is the window scalar multiplication algorithm based on interleaving (IW algorithm) on Koblitz curves [9] which is shown in algorithm 3.

```
Algorithm 3:The window scalar multiplication algorithm based on interleaving (IW algorithm)[9]
INPUT: w; $k=(k_{m-1}k_{m-2}\ldots k_0)_2$; $P \in GF(2^m)$;
OUTPUT: Q=kP;
1. Use algorithm 3 in appendix [9] to compute ρ'=k partmod δ;
2. Use algorithm 4 in appendix [9] to compute $TNAF_w(\rho')= \sum_{i=0}^{l-1} u_i \tau^i$ ;
3. For $u \in U=\{1,3,5,\ldots,2^{w-1}-1\}$, let $Q_u \leftarrow 0$;
4. For i=l-1 to 0 do
   4.1. If $u_i \neq 0$ then
          Let u satisfy $a_u=u_i$ or $a_{-u}=-u_i$;
          If u>0 then $Q_u \leftarrow Q_u+P$;
          Else $Q_{-u} \leftarrow Q_{-u}-P$;
    4.2. $P \leftarrow \tau P$;
5. Compute $Q \leftarrow Q + \sum_{u \in U} u_i Q_u$ ;
6. Return Q;
```

The inputs of this algorithm are the scalar k, window width w, and elliptic curve point P. The output is the elliptic curve point Q=kP. Moreover, $\tau = \frac{\mu + \sqrt{-7}}{2}$, $\mu = (-1)^{1-a}$, $a = \{0,1\}$ and $\delta = \frac{\tau^m - 1}{\tau - 1}$ [9,12]. In the IW algorithm, the multiplication cost is reduced by using the sliding window method and the signed-digit representation (steps 1 and 2). In this algorithm, when $u_i \neq 0$, the point Q_u is computed in which u satisfies $a_u=u_i$ or, $a_{-u}=-u_i$ [9].

2.4 The Finite Field Multiplication Algorithm

The performance of ECC is primarily determined by the efficient realization of the arithmetic operations in the underlying finite field [6].

Modular addition in GF(2^m) is simple and relatively straight forward . As a result, it can be implemented by simply using XOR gates [14]. If projective coordinates are used for ECC, the inversion cost can be neglected because only one inversion operation is required to be performed at the end of the scalar multiplication. The modular squaring in GF(2^m) is simple and straight forward [6,14]. Therefore, the modular multiplication is the most important operation in ECC implementations.

The Montgomery modular multiplication algorithm [27] is widely used as an efficient algorithm [18,28]. Algorithm 4 shows the Montgomery modular multiplication algorithm for GF(2^m) [18]:

```
Algorithm 4: The Montgomery modular multiplication in GF($2^m$)
Input: A(x),B(x),P(x),n;
 Output: C(x) =A(x).B(x) $x^{-n}$ mod P(x);
1. C(x)=0;
2. For i=0 to n-1
3. $q(x) = (c_0(x) + a_i(x).b_0(x)).p_0^{'}(x)(\text{mod}\, x^r)$ ;
4. $C(x) = (C(x) + a_i(x).B(x) + q(x).P(x)) / x^r$ ;
5. Return C(x)
```

The inputs of this algorithm are A(x), B(x), P(x) and n, where A(x), B(x)$\in$GF(2^m), P(x) is the irreducible polynomial and n denotes the operand length. The output is C(x)=A(x).B(x)x^{-n} mod P(x). Moreover, r shows each digit length, $p_0^{'}(x) = p_0^{-1}(x)(\text{mod } x^r)$ and a_i(x) shows ith digit of A(x). The output of this algorithm is computed in n-clock cycle. Therefore, it is a time- consuming operation.

3. The Proposed Implementation Approach of ECC

This section presents a novel and efficient implementation approach for the elliptic curve cryptosystem based on the parallel structure and a new and efficient finite field multiplication algorithm in GF(2^m).

3.1 Scalar Multiplication

The basic operations in all scalar multiplication algorithms are point addition and point doubling operations over an elliptic curve [20]. Using parallel structure for these point operations, the speed of the cryptosystem is increased considerably. We also used the scalar multiplication algorithm [9] to compute point addition and point doubling operations in parallel. This algorithm is shown in algorithm 3 and was described in section 2.3.

3.2 The Finite Field Arithmetic

In the finite field multiplication, zero multiplication results in zero, but this zero multiplication is performed and implemented per clock cycle. In addition, partial result is shifted one bit per clock cycle [29]. This section presents a new finite field multiplication algorithm in GF(2^m) based on a new signed-digit multiplier representation and multi bit scan-multi bit shift technique. This new finite field multiplication performs zero chain multiplication in only one clock cycle instead of several clock cycles. The proposed finite field multiplication algorithm is based on Montgomery modular multiplication algorithm in GF(2^m). The proposed algorithm is shown in algorithm 5:

Algorithm 5: The proposed finite filed multiplication in GF(2^m)

```
Input: A(x), B(x), P(x) , n;
Output: C(x)= A(x).B(x) x^{-n} mod P(x);
1. C(x)=0;
{Canonical recoding phase}
2. Compute D(x) by applying algorithm 1 to A(x);
parallel begin
{partitioning phase}
 3.1. Building D*(x)=(u_{s-1}(x)u_{s-2}(x)…u_0(x)) by applying CLNZ sliding window method to D(x);
  3.2. s= #D*(x) ;
4. Compute and store table u_i(x).B(x)
parallel end
{multiplication phase}
5. For i = 0 to s-1
6.     C(x):= C(x) + u_i(x).B(x);
7.     q(x):= $P_0^{'}(x)$ .C(x) mod $x^{l_i}$ ;
8.     C(x):= (C(x)+q(x).P(x))/ $x^{l_i}$ ;
9. Return C(x)
```

In this algorithm, the inputs are A(x), B(x), P(x) and n, where A(x), B(x) $\in$ GF(2^m), P(x) is the irreducible polynomial and m denotes the operand length. The output of this algorithm is C(x)=A(x).B(x)x^{-m} mod P(x). Moreover, $p_0^{'}(x) = p_0^{-1}(x) \bmod x^{l_i}$, $u_i(x)$ is the ith partition of D*(x), l_i is the ith partition length (i.e. the number of digits in ith partition) and s= #D*(x) is the number of partitions in the multiplier representation.

In step 2 of the proposed finite field algorithm, the canonical recoding algorithm is performed on the multiplier. Then the constant length nonzero (CLNZ) partitioning is performed on the signed-digit multiplier. Therefore, the average Hamming weight of the multiplier and thereby the average number of multiplication steps (or required clock cycles) in the finite field multiplication algorithm are reduced considerably. In algorithm 5, the CLNZ partitioning method scans the multiplier from the least significant digit to the most significant digit according to a finite state machine, which is shown in figure 2.

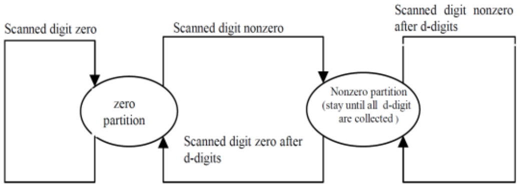

Scanned digit zero
Scanned digit nonzero
Scanned digit nonzero after d-digits
zero partition
Nonzero partition (stay until all d-digit are collected)
Scanned digit zero after d-digits

Figure 2: The finite state machine used in the CLNZ partitioning method

Using the CLNZ partitioning method, the zero partitions are allowed to have an arbitrary length, but the maximum length of the nonzero partitions should be the exact value (in figure 2, d digits). For example, for A(x) = $(01111111111100011111111101)_2$, the canonical recoding of A(x) is $D(x) = (010000000000\bar{1}00100000000\bar{1}01)_{CR}$ and for d=4, the partition formed will be as follows:
$D*(x) = ((0001),(000000000),(\bar{1}001),(000000),(0\bar{1}01))$.

As the least significant digit of the nonzero partition is either 1 or $\bar{1}$, the nonzero partition value is always an odd number. So, we only require pre-computation of $u_i(x)$.B(x) for the odd number of $u_i(x)$ in step 4 of the proposed finite field multiplication algorithm.

In the proposed finite field multiplication algorithm, step 4 is performed independently and parallel with steps 3.1 and 3.2. This parallel computation also increases the speed of the finite field multiplication algorithm.

The multiplication phase of the proposed finite field multiplication algorithm is performed s times. Recall that s denotes the number of partitions in the proposed multiplier representation. In each clock cycle of the multiplication phase of the proposed finite field multiplication algorithm, l_i bits of the multiplier and m-bit multiplicand are processed.

Figure 3 shows the block diagram of the hardware implementation of the proposed finite field multiplication.

In the proposed hardware implementation approach of the finite field multiplication, the new multiplier representation D*(x) makes multi bit scan possible, but the high-radix modular multiplication (k×m multiplier) is required in $u_i(x).B(x)$ and q(x).P(x) computation. In the proposed hardware implementation approach of the finite field multiplication, LUT1 and LUT2 are used for computing $u_i(x).B(x)$ and q(x).P(x) respectively. Thus, the high-radix partial multiplication problem in each clock cycle is also solved.

In addition, the modified (limited number of shifts) Barrel shifter is proposed to execute the required multi bit shift operation in a single clock cycle in step 8 of algorithm 5. The number of required shifts in ith clock cycle (l_i) is provided from the length of the ith digit of the new multiplier representation D*(x). These two properties imply the multi bit scan-multi bit shift technique. So, the zero chain multiplication and the required addition are performed in one clock cycle instead of several clock cycles.

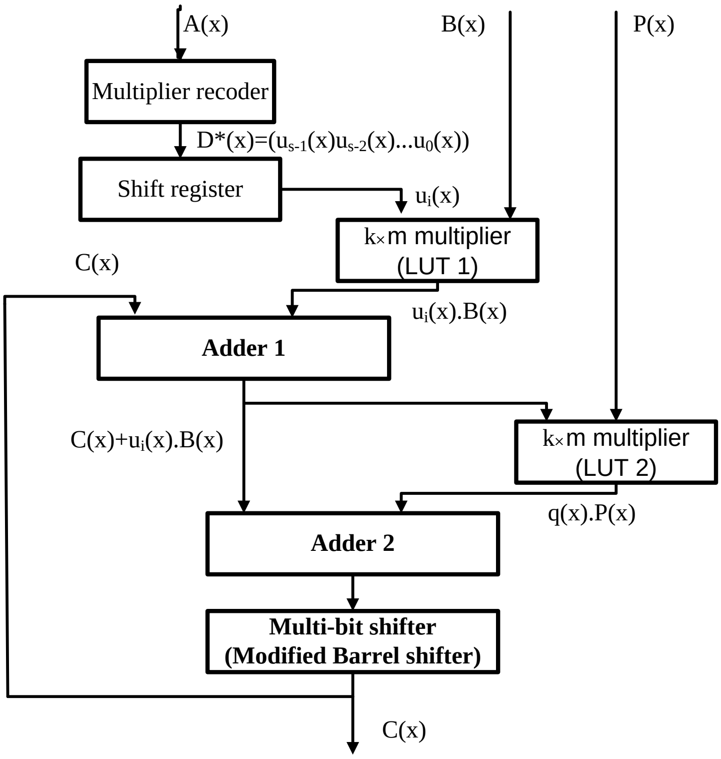


Figure 3: The block diagram of the proposed finite field multiplication

4. Evaluation

4.1 Evaluation of the Proposed Finite Field Multiplication Algorithm

In the proposed finite field multiplication algorithm, the CLNZ sliding window method is applied to the canonical recoded multiplier. So according to computation analysis of [30], the average Hamming weight of the multiplier is about $\frac{3m}{3d+4}$, where m denotes the multiplier length and d denotes the window width in the CLNZ partitioning method in the proposed finite field multiplication algorithm. Thus, the proposed finite field multiplication algorithm reduces the average number of multiplication steps by about:

$$1-\frac{\frac{6m}{3d+4}}{m}=1-\frac{6}{3d+4} \quad (4)$$

Table 1 shows the multiplication step (required clock cycle) improvement in the proposed finite field multiplication algorithm in comparison with Montgomery modular multiplication algorithm [27] for various d.

Table 1: Multiplication step improvement of the proposed finite field multiplication algorithm

d	Clock cycle improvement (%)	d	Clock cycle improvement (%)
2	40	7	76
3	53.8	8	78.6
4	62.5	9	80.6
5	68.4	10	82.4
6	72.7		

Based on our analysis which is shown in table 1, the proposed finite field multiplication algorithm reduces the average number of multiplication steps (required clock cycles) by about 40%-82.4% compared to Montgomery modular multiplication algorithm in GF(2^m) for d=2-10.

4.2 Evaluation of the Proposed Implementation Approach

According to the computational analysis of [9,20], the implementation approach of the traditional window NAF (TWN) scalar multiplication algorithm [12] will cost:

$$D+(2^{w-2}-1)A+\frac{\mathrm{m}}{w+1}A+\mathrm{m}D \qquad (5)$$

where D denotes the point doubling cost, A denotes the point addition cost, m denotes the operand length and w denotes the window width in the sliding window method in the scalar multiplication algorithm.

Moreover in the Karatsuba-Ofman method [6,14], the computation cost is computed from (5), but with different computation cost for the point addition and point doubling operations.

In addition, the implementation approach of the window scalar multiplication algorithm based on interleaving (IWN) [9] will cost:

$$\frac{\mathrm{m}}{w+1}A+\sum_{j=1}^{v}\frac{l_j}{w_j+1}A \qquad (6)$$

The proposed implementation approach of ECC is a combination of the proposed finite field multiplication algorithm and the IWN algorithm. So, the computation cost of the proposed implementation approach is computed from (6), but the cost of the point addition in the proposed implementation approach is reduced considerably based on table 1.

The point addition and point doubling operations have the same cost using affine coordinate, but the cost of the point addition operation is twice the cost of the point doubling operation using projective coordinate [9,24]. The computation cost of the implementation approaches in [6,9,12,14] and the proposed implementation approach are computed by analyzing (5) and (6) for various m, w and d. Figures 4-6 show the comparison of the computation cost of the proposed implementation approach with implementation approach in [6,9,12,14] for m=163 bit and various window width w using affine coordinate and projective coordinate for d=2,4,6,8 and 10.

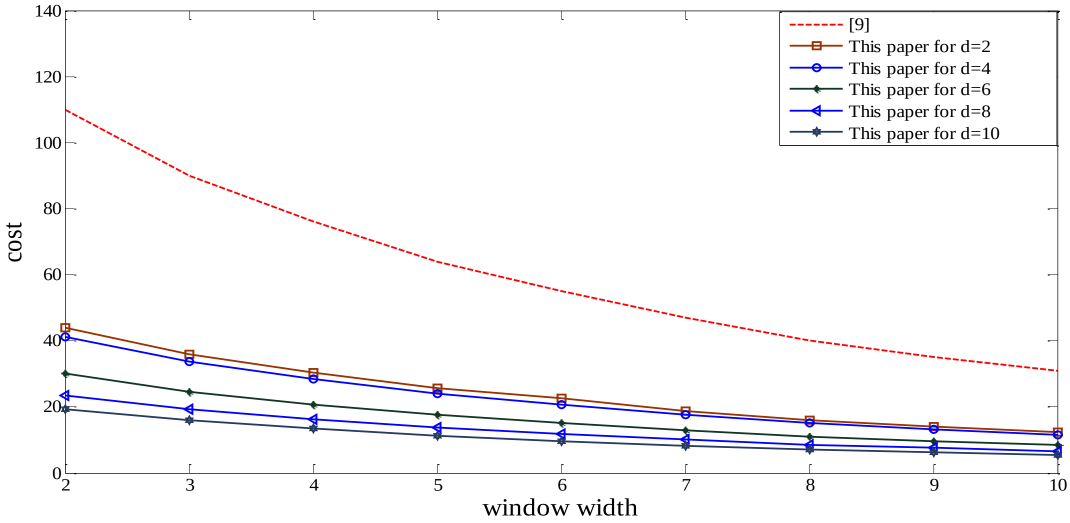


Figure 4: Comparison of the computation cost between the proposed implementation approach and the implementation approach in [9] using affine coordinate and projective coordinates

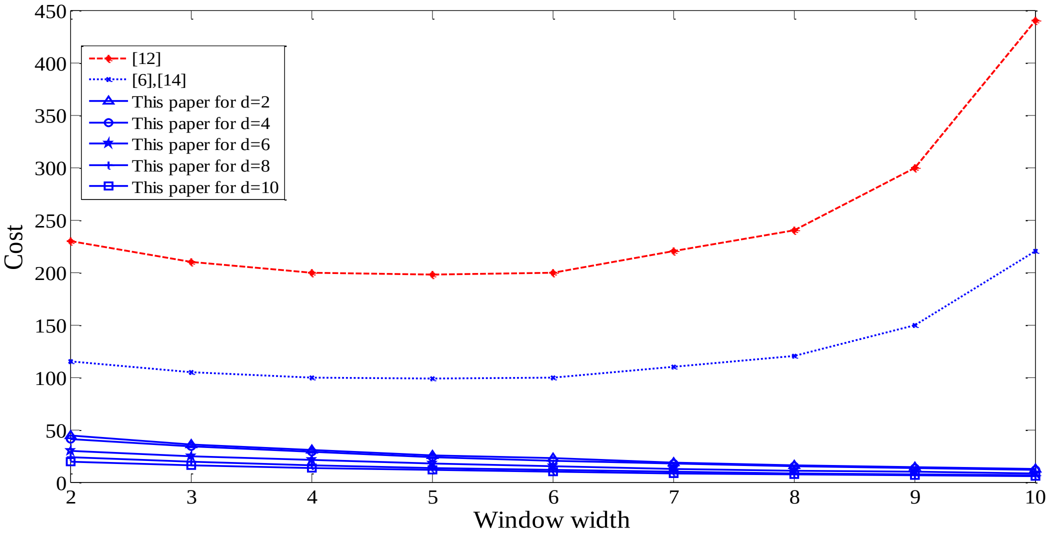


Figure 5: Comparison of the computation cost between the proposed implementation approach and the implementation approach in [6,12,14] using affine coordinate

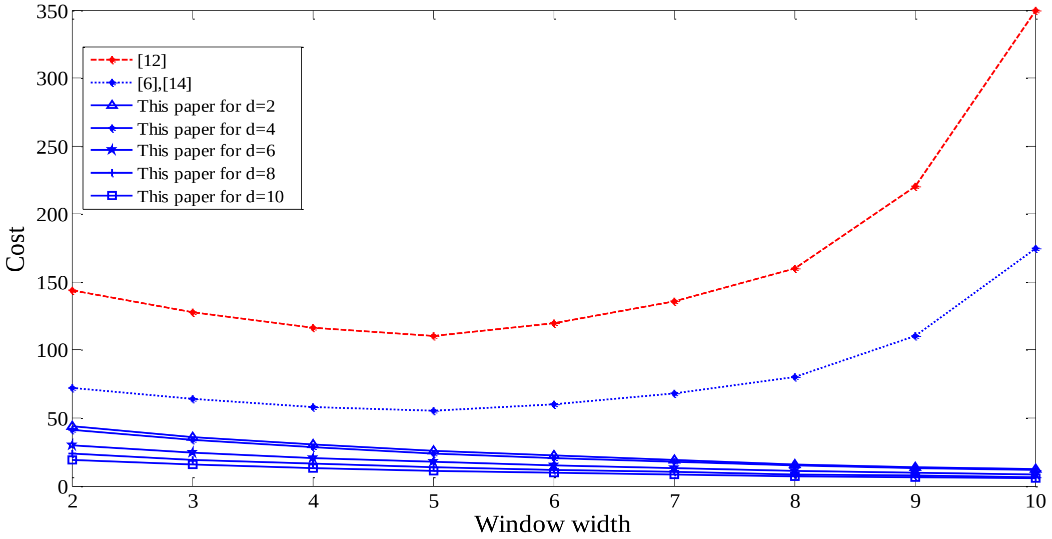


Figure 6: Comparison of the computation cost between the proposed implementation approach and the implementation approach in [6,12,14] using projective coordinate

As it is shown in figures 4-6, the computation cost of the proposed implementation approach is effectively reduced in comparison with the implementation approach in [6,9,12,14] where both window width in the scalar multiplication (w) and the window width in the proposed finite field multiplication (d) are varied from 2 to 10. Table 2 and figures 7-8 summarize the computation cost of the proposed implementation approach and the implementation approach in [6,9,12,14] for the operand length of 163, 193 and 233 in affine coordinate where w=4, d=8 and w=8, d=8.

Table 2: The comparative table for the computation cost using affine coordinate for d=8, w=4 and 8.

Operand length	Reference	Computation cost	
		w=4	w=8
163	[12]	199.6	245.1
	[6][14]	100	122.5
	[9]	65	36.1
	This paper	13.9	7.7
193	[12]	235.6	278.4
	[6][14]	117.8	139.1
	[9]	77.2	42.8
	This paper	16.5	9.2
233	[12]	283.6	322.9
	[6][14]	141.8	161.5
	[9]	93.1	51.4
	This paper	20	11

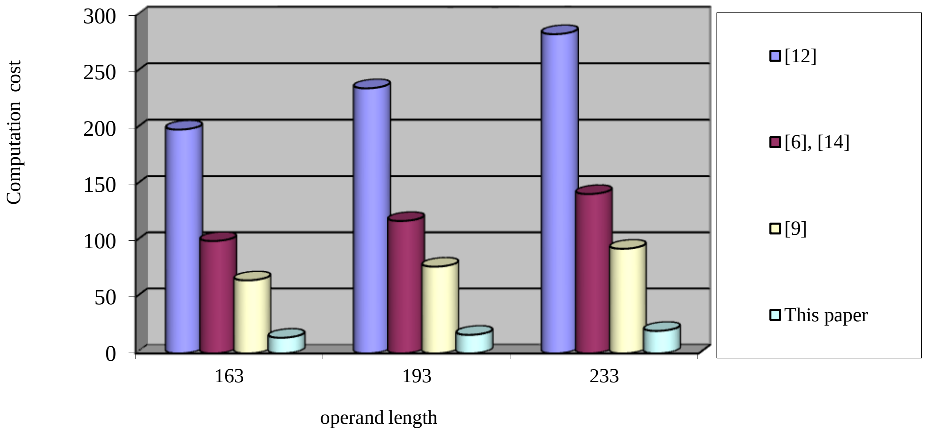


Figure 7: Comparison of the computation cost using affine coordinate for d=8, w=4

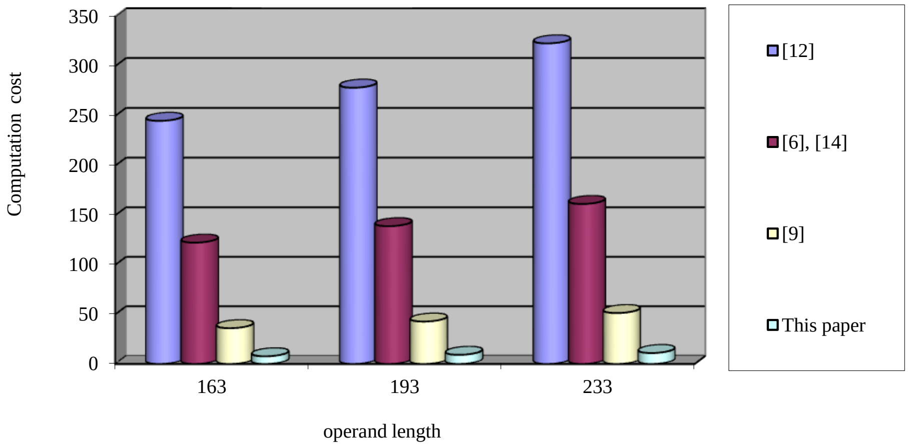


Figure 8: Comparison of the computation cost using affine coordinate for d=8, w= 8

Based on our analysis which is shown in table 2 and figures 7-8, the average computation cost of the proposed implementation approach is reduced by about 93%-96%, 86%-93% and 78.6% in comparison with the implementation approach in [12], [6] (and its extension in [14]) and [9] respectively for w=4, d=8 and w=8, d=8 using affine coordinate. Table 3 summarizes these improvements where the computation cost improvement is computed as follows:

$$\text{improvement}(\%) = (1 - \frac{\text{new cost}}{\text{old cost}}) \times 100 \qquad (7)$$

Table 3: The comparative table for the computation cost using projective coordinate for d=8

Reference	[12]		[6][14]		[9]	
Window width	w=4	w=8	w=4	w=8	w=4	w=8
Computation cost improvement (%)	93	96	86	93	78.6	78.6

As it is shown in (5), the computation cost in [12] has a multiplier as 2^w. So, by increasing the window width w, the computation cost in [12] is also increased.

In addition, table 4 and figures 9-10 summarize the computation cost of the proposed implementation approach and the implementation approach in [6,9,12,14] for the operand length of 163, 193 and 233 in projective coordinate where w=4, d=8 and w=8, d=8.

Table 4: The comparative table for the computation cost using projective coordinate for d=8, w=4 and 8.

Operand length	Reference	Computation cost	
		w=4	w =8
163	[12]	117.6	163.1
	[6][14]	58.8	81.6
	[9]	65.2	36
	This paper	13.9	7.7
193	[12]	138.6	181.4
	[6][14]	69.3	90.7
	[9]	77.2	42.8
	This paper	16.5	9.2
233	[12]	166.6	205.9
	[6][14]	83.3	103
	[9]	93.1	51.2
	This paper	20	11

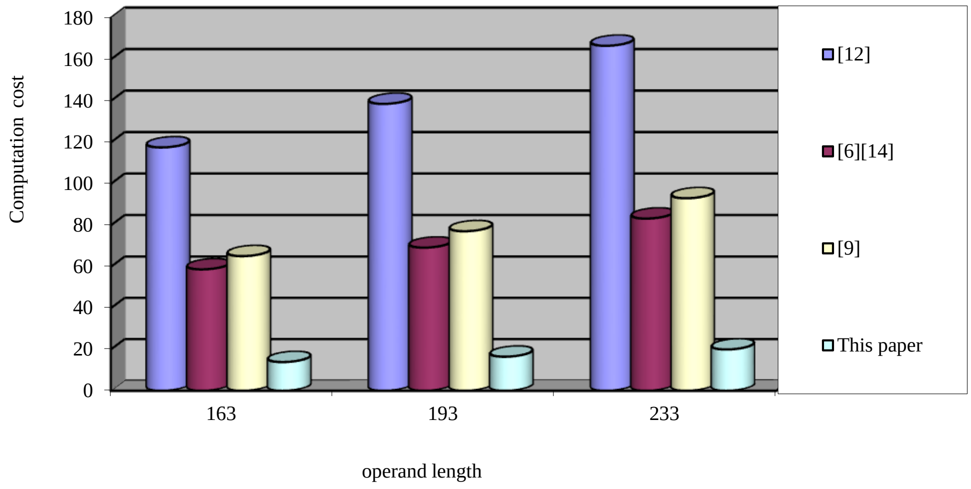


Figure 9: Comparison of the computation cost using projective coordinate for d=8, w=4.

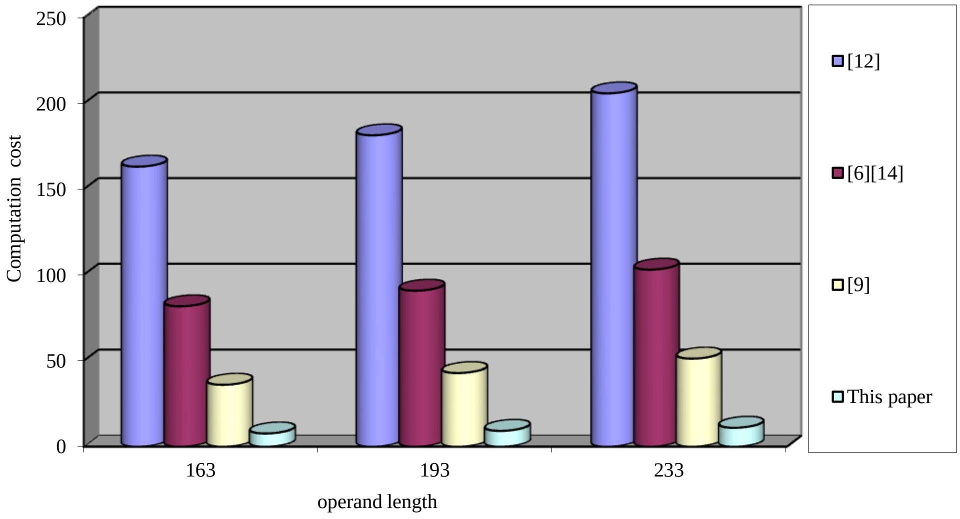


Figure 10: Comparison of the computation cost using projective coordinate for d=8 and w=8

As it is shown in table 4 and figures 9-10, the average computation cost of the proposed implementation approach is reduced by about 88%-95%, 76.1%-89.4% and 78.6% in comparison with the implementation approach in [12], [6] (and its extension in [14]) and [9] respectively using projective coordinate where w=4, d=8 and w=8, d=8. Table 5 summarizes these improvements.

Table 5: The comparative table for the cost using projective coordinate for d=8, w=4 and 8.

Reference	[12]		[6][14]		[9]	
Window width	w=4	w=8	w=4	w=8	w=4	w=8
Computation cost improvement (%)	88	95	76.1	89.4	78.6	78.6

As the computation cost of the point doubling operation using projective coordinate is half of the point addition operation, the computation cost improvement in comparison with [12] is reduced in projective coordinate compared to affine coordinate.

Therefore, using the proposed implementation approach for ECC, the efficiency of the computation cost of ECC is improved considerably.

5. Conclusion

In ECC implementation, the total execution time and the energy consumption is dependent on the required clock cycles for cryptosystem [3]. This paper presents a novel finite field multiplication algorithm in GF(2^m) based on a new signed-digit multiplier representation and multi bit scan-multi bit shift technique to reduce the required clock cycle in ECC. In this new finite field multiplication, the canonical recoding technique is used to increase probability of the zero bits in the multiplier. The CLNZ sliding window method is also applied to the signed-digit multiplier to reduce the average number of multiplication steps (required clock cycles) in the finite field multiplication algorithm. This new multiplier representation makes multi bit scan possible. The modified (limited number of shifts) Barrel shifter is also proposed to make multi-bit shift possible. Moreover, a new efficient implementation approach for the elliptic curve cryptosystem is presented by applying this new finite field multiplication to the scalar multiplication in [9]. In this new implementation approach, the point addition and point doubling operations are computed in parallel. In addition, both sliding window method and canonical recoding technique are used to reduce the computation cost considerably.

Our analysis shows that the computation cost of the proposed finite field multiplication algorithm is reduced by about 40%-82.4% in comparison with Montgomery modular multiplication algorithm for d=2-10. Moreover, the computation cost in the proposed implementation approach of the elliptic curve cryptosystem is reduced by about 88%-96%, 76%-93% and 78.6% in comparison with the implementation approach in [12], [6] (and its extension in [14]) and [9] respectively where w=4 and 8, and d=8.

References

[1] N. Koblitz, “Elliptic curve cryptosystem”, Mathematics of Computer, 1987, vol.48, pp.203-209.

[2] V. Miller, “Use of elliptic curves in cryptography”, in Proc. of advances in cryptology (CRYPTO), 1985, LNCS .218, 417–428.

[3] H. R. Ahmadi, and A. Afzali-kusha, “A low-power and low-energy flexible GF(p) elliptic-curve cryptography processor”, Journal of Zhejiang University-science C, 2010, Vol.11, No.9, pp.724-736.

[4] A. P. Fournaris, “Toward Flexible Security and Trust Hardware Structures for Mobile-Portable Systems”, IEEE Latin America Transactions, 2012, Vol.10, No.3, pp.1719-1722.

[5] H. Wang, and Q. Li, “Achieving distributed user access control in sensor networks”, Ad Hoc Networks, 2012, Vol.10, No.3, pp.272-283.

[6] N. Saqib, F. Rodriguez-Henriquez, and A. Diaz-perez, “A parallel architecture for fast computation of elliptic curve scalar multiplication over GF(2^m)”, in Proc. of the 18th IEEE. International parallel and distributed processing symposium, 4004, pp.144.

[7] P. Shah, X. Huang, and D. Sharma, “Sliding window method with flexible window size for scalar multiplication on wireless sensor network nodes”, in Proc. of the IEEE. International conference on wireless communication and sensor computing, 2010, pp.1-6.

[8] B. Qin, M. Li, F. Kong, and D. Li, “New left-to-right minimal weight signed-digit radix-r representation”, Computers and Electrical Engineering, 2009, Vol.35, No.1, pp.150-158.

[9] X. Yin, H. Zhu, and R. Zhao, “Window algorithm of scalar multiplication based on interleaving”, in Proc. of the IEEE. International conference on communications, circuits and systems, 2009, pp.318-321.

[10] P. Balasubramanian, and E. Karthikeyan, “Elliptic curve scalar multiplication algorithm using complementary recoding”, Applied mathematics and computation, 2007, Vol.190, No.1, pp.51-58.

[11] P. Balasubramaniam, and E. Karthikeyan, “Fast simultaneous scalar multiplication”, Applied mathematics and computation, 2007, Vol.192, No.2, pp.399-404.

[12] J. Solinas, “Efficient arithmetic on Koblitz curves”, Designs, codes and cryptography, 2000, Vol.19, No.2-3, pp.125-179.

[13] A. Rezai, and P. Keshavarzi, “CCS Representation: A new non-adjacent form and its application in ECC”, Journal of Basic and Applied Scientific Research, 2012, Vol.2, No.5, pp.4577-4586.

[14] S. Shohdy, A. Elsisi, and N. Ismail, “Hardware implementation of efficient modified Karatsuba multiplier used in elliptic curves”, International Journal of Network Security, 2010, Vol.11, No.3, pp.138-145.

[15] B. Ansari, and A. Hasan, “High-Performance architecture of elliptic curve scalar multiplication”, IEEE. Transactions on Computers, 2008, Vol.57, No.11, pp.1443-1453.

[16] Y. Dan, X. Zou, Z. Liu, Y. Han, and L. Yi, “High-performance hardware architecture of elliptic curve cryptography processor over GF(2^{163})”, Journal of Zhejiang University - Science A, 2009, Vol.10, No.2, pp.301-310.

[17] G. Orlando, and C. Paar, “A scalable GF(p) elliptic curve processor architecture for programmable hardware”, in Proc. of the third international workshop on cryptographic hardware and embedded systems (CHES2001), 2001, LNCS 2162, pp.348-363.

[18] E. Savas, and C. Koc, “Finite field arithmetic for cryptography”, IEEE. Circuits and Systems Magazine, 2010, Vol.10, No.2, pp.40-56.

[19] G. Dormale, and J. Quisquater, “High-speed hardware implementations of elliptic curve cryptography: a survey”, Journal of systems architecture, 2007, Vol.53, No.2-3,pp.72-84.

[20] A. Rezai, and P. Keshavarzi, “High-performance implementation approach of elliptic curve cryptosystem for wireless network applications”, in Proc. of the IEEE. International conference on consumer electronics, communications and networks, 2011, pp.1323-1327.

[21] A. Booth, “A signed binary multiplication technique”, Journal of mechanics and applied mathematics, 1951, Vol.4, pp.236-240.

[22] G. Reitwiesner, “Binary Arithmetic, Advances in computers”, 1960, Vol.1, pp.231-308.

[23] S. Arno, and F. Wheeler, “Signed digit representations of minimal Hamming weight”, IEEE Transactions on Computers, 1993, Vol.42, No.8, pp.1007-1010.

[24] D. Hankerson, A. Menezes, and S.Vanstone, Guide to Elliptic Curve Cryptography, New York: Springer-Verlag, 2004.

[25] G. Dormale, and J. Quisquater, “Area and time trade-offs for iterative modular division over GF(2^m): novel algorithm and implementations on FPGA”, International journal of electronics, 2007, Vol.94, No.5, pp.515-529.

[26] J. Großschädl, and G. A. Kamendje, “Instruction set extension for fast elliptic curve cryptography over binary finite fields GF(2^m)”, in Proc. of the 14th IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP 2003), 2003, pp.455-468.

[27] P. Montgomery, “Modular multiplication without trial division”, Mathematics of computation, 1985, Vol.44, No.170, pp.519-521.

[28] A. Rezai, and P. Keshavarzi, “High-performance modular exponentiation algorithm by using a new modified modular multiplication algorithm and common- multiplicand-multiplication method”, in Proc .of the IEEE. World congress on internet security, 2011, pp.192-197.

[29] A. Rezai, and P. Keshavarzi, “A new CMM-NAF modular exponentiation algorithm by using a new modular multiplication algorithm”, Trends in applied sciences research, 2012, Vol.7, No.3, pp.240-247.

[30] C. Koc, and C. Hung, “Adaptive m-ary segmentation and canonical recoding algorithms for multiplication of large binary numbers, Computers and Mathematics with Applications”, 1992, Vol.24, No.3, pp.3-12.

Cover Selection Steganography Via Run Length Matrix and Human Visual System

Sara Nazari*
Computer Engineering, M.Sc., Department of Computer Engineering, Arak Branch, Islamic Azad University
s-nazari@iau-arak.ac.ir
Mohammad-Shahram Moin
Electrical and Computer Engineering, Ph.D., IT Faculty, Cyberspace Research Institute
moin@csri.ac.ir

Received: 10/Jul/2012 Accepted: 18/May/2013

Abstract

A novel approach for steganography cover selection is proposed, based on image texture features and human visual system. Our proposed algorithm employs run length matrix to select a set of appropriate images from an image database and creates their stego version after embedding process. Then, it computes similarity between original images and their stego versions by using structural similarity as image quality metric to select, as the best cover, one image with maximum similarity with its stego. According to the results of comparing our new proposed cover selection algorithm with other steganography methods, it is confirmed that the proposed algorithm is able to increase the stego quality. We also evaluated the robustness of our algorithm over steganalysis methods such as Wavelet based and Block based steganalyses; the experimental results show that the proposed approach decreases the risk of message hiding detection.

Keywords: Steganography; Cover Selection; Run Length Matrix; Image Texture Features; SSIM.

1. Introduction

Steganography is a security technique to disguise messages in a media called cover, which is the object to be used as the carrier for embedding a hidden message. Many different types of objects have been employed as carriers, for example images, audio and video. The object which is carrying a hidden message, is called stego [1-3].

Steganography methods can be categorized into two groups: spatial-domain and transform-domain. In spatial domain methods, the secret messages are embedded in the image pixels directly. LSB [4] technique is a famous method in this group. In transform-domain methods, messages are embedded into coefficients obtained after applying a transform on the original image. Techniques such as the Discrete-Cosine Transform (DCT) [5,6,7], Discrete Fourier Transform (DFT) [8], Wavelet Transform (DWT) [9,10] and Contourlet transform [11,12,13] belongs to this category [14]. In steganography, one prefers to hide information as much as possible in a cover with a distortion as little as possible. Selection of a suitable cover plays an important role to achieve these goals, i.e. increasing payload and decreasing detectability. Different image cover selection methods have been suggested in the literature. Image cover selection technique proposed in [14] is concentrated in textured similarity. This technique replaces some blocks of a cover image with similar secret image blocks. The enhanced version of this method in [15], uses statistical features of image blocks and their neighborhood. In [16], some scenarios are discussed with a steganographer having complete or partial knowledge or no knowledge about steganalysis methods. In addition, some measures for cover selection are introduced. Another cover selection method is introduced in [17] based on computation of the steganography capacity as a property of images.

In this paper, we will exploit the textured characteristics of images to elicit suitable images from a large database as proper covers. Then, in order to generate the stego version of images, we embed a secret message into the selected images. Finally, we use Structural Similarity Measurement (SSIM), which is based on Human Visual System (HVS), instead of PSNR and MSE to measure the similarity between each selected image and its stego. Then, the image with maximum SSIM is selected as the best cover. Analysis of results showed that the proposed cover selection method extracts the best image with high payload and little distortion.

Rest of this paper is organized as follows. Section 2 explains Run Length Matrix and its

* Corresponding Author

features. In Section 3, we introduce several visual perceptual measures based on HVS. Our proposed approach is explained in Section 4. Experimentations and results are presented in Section 5. Finally, Section 6 concludes the paper.

2. Run Length Metrics and Texture Features

Texture is one of the most used characteristics in image analysis, and is applicable to a wide variety of image processing problems. In image processing, “texture” is related to repeated pixels in an image, producing a pattern. Texture is arranged in two categories: deterministic (regular), and statistical (irregular) textures. Deterministic texture is created by repetition of a fixed geometric shape such as a circle or square. Statistical textures are created by changing patterns with fixed statistical properties. Statistical textures are represented typically in term of spatial frequency properties. The human visual system is less sensitive to distortion in complex texture patterns compared to simple texture patterns. As a consequence, images with complex textures are preferred in information hiding [18], and selection of secure cover from an image database is an important phase in steganography methods. Some of the texture features used in this work are extracted from run length matrix [18,19]. In this section, we introduce these texture features.

Gray level Run length matrix: A gray-level run is a set of consecutive pixels having the same gray-level value. The number of pixels in the run is called Length of run. Run length features encode textural information related to the number of times each gray-level is repeated. Four run length matrix QRL are defined for four directions: 0◦, 45◦, 90◦ and 135◦. Element (i, j) in QRL illustrates the number of times a gray-level i appears in the image with run length j. Dimension of each QRL matrix is Ng * Nr array, where Nr and Ng are the largest possible run length and highest possible gray level value in the image, respectively. Many numerical texture features can be computed on the basis of run length matrix. The four features [19] of run length statistics used in this work are as follows:

Short Run Emphasis (SRE) measures the distribution of short runs. The SRE is highly dependent on the occurrence of short runs and is expected to be large for coarser images.

$$SRE = \frac{\sum_{i=1}^{Ng}\sum_{j=1}^{Nr}\left(\frac{Q_{RL}(i,j)}{j^2}\right)}{\sum_{i=1}^{Ng}\sum_{j=1}^{Nr} Q_{RL}\,(i,j)} \qquad (1)$$

Long-Run Emphasis (LRE) is a measure of distribution of long runs. It is small for coarser images.

$$LRE = \frac{\sum_{i=1}^{Ng}\sum_{j=1}^{Nr}(Q_{RL}(i,j)j^2\,)}{\sum_{i=1}^{Ng}\sum_{j=1}^{Nr} Q_{RL}(i,j)} \qquad (2)$$

Gray Level Non Uniformity (GLNU) shows the similarity of gray level values throughout an image. When runs are uniformly distributed among the gray levels, GLNU takes small values. Large run length values have a high contribution in this metric, because of existence of square. It is expected to be large for coarser images.

$$GLNU = \frac{\sum_{i=1}^{Ng}\left[\sum_{j=1}^{Nr} Q_{RL}(i,j)\right]^2}{\sum_{i=1}^{Ng}\sum_{j=1}^{Nr} Q_{RL}(i,j)} \qquad (3)$$

Run Length Non Uniformity (RLN) emphasizes on the similarity of the length of runs throughout the image. The RLN is expected to be small if the run lengths are alike throughout the image.

$$RLN = \frac{\sum_{j=1}^{Nr}\left[\sum_{i=1}^{Ng} Q_{RL}(i,j)\right]^2}{\sum_{i=1}^{Ng}\sum_{j=1}^{Nr} Q_{RL}(i,j)} \qquad (4)$$

3. Visual Specification Based on the Structural Similarity Measurement

Image quality assessment is an important field of signal processing. The MSE and PSNR are the most commonly used quality metrics. These are used widely because they are simple and easy to be calculated, but are not well correlated with human perception of quality [20,21]. Recently, various efforts have been made into the development of quality assessment methods that take advantage of known characteristics of the Human Visual System (HVS). Quality assessment (QA) algorithms based on HVS predict visual quality by comparing a distorted signal against a reference, typically by modeling the human visual system. These measurement methods consider HVS characteristics in an attempt to incorporate perceptual quality measures. SSIM, Structural Similarity Metric [22], is a quality measure which separates the task of similarity measurement between two images into three comparisons: luminance, contrast and structure [22,23,24]. Its value lies on the interval [0,1]. The steps of SSIM measurement are presented in Figure 1 [24]. Local structural similarity between two images x and y, is defined in Equation 5; $\mathrm{l}, \mathrm{c},$ and s represent luminance, contrast and structure, respectively.

$$S(x,y) = l(x,y).c(x,y).s(x,y) \qquad (5)$$

where

$$l(x,y) = \frac{2\,\mu_x\,\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1}\; c(x,y) = (\frac{2\,\sigma_x\,\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2})$$

$$S(x,y) = (\frac{\sigma_{xy} + C_3}{\sigma_x\,\sigma_y + C_3})$$

and x and y are original, and distorted signals, respectively. “Original” form of signal (x) is free of any distortions, and is therefore assumed to have perfect quality. μ_x and μ_y are the local sample means of x and y, respectively. σ_x and σ_y are the local sample standard deviations of x and y, and $\sigma_{xy}$is the sample cross correlation of x and y. The parameters C1, C2 and C3 are small positive constants which stabilize each term, so that near-zero sample means, variances, or correlations do not lead to numerical instability. The properties of SSIM are being symmetry, boundedness and unique maximum as follows:

Symmetry: *S(x,y) = S(y,x)*

Boundedness: *S(x,y) <= 1*

Unique maximum: *S(x,y) = 1* if and only if *x=y*

We have used the primitive similarity measure proposed in [22,23] as quality evaluation criterion between stego and cover image for selecting the secure cover. This measure helps us to select the best cover from an image database.

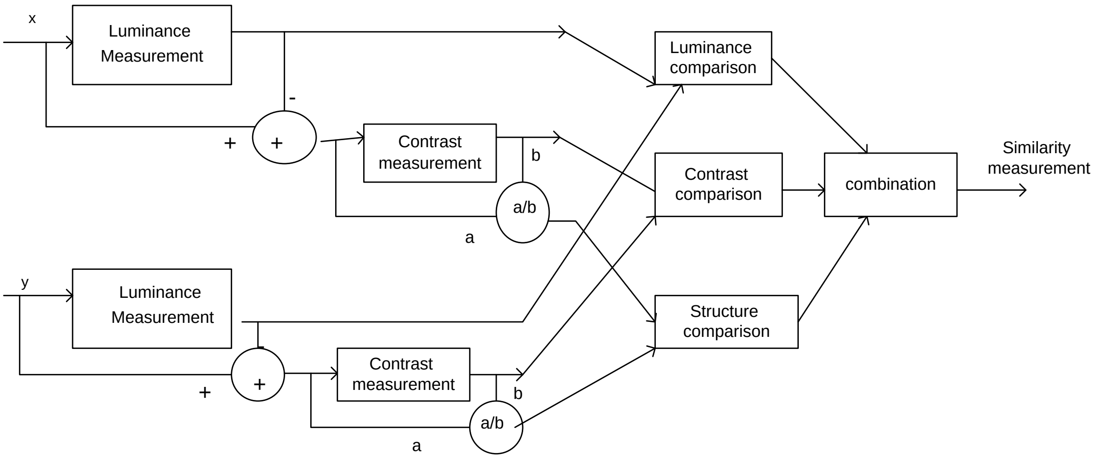


Figure1. Structural Similarity Measurement (SSIM) System [24]

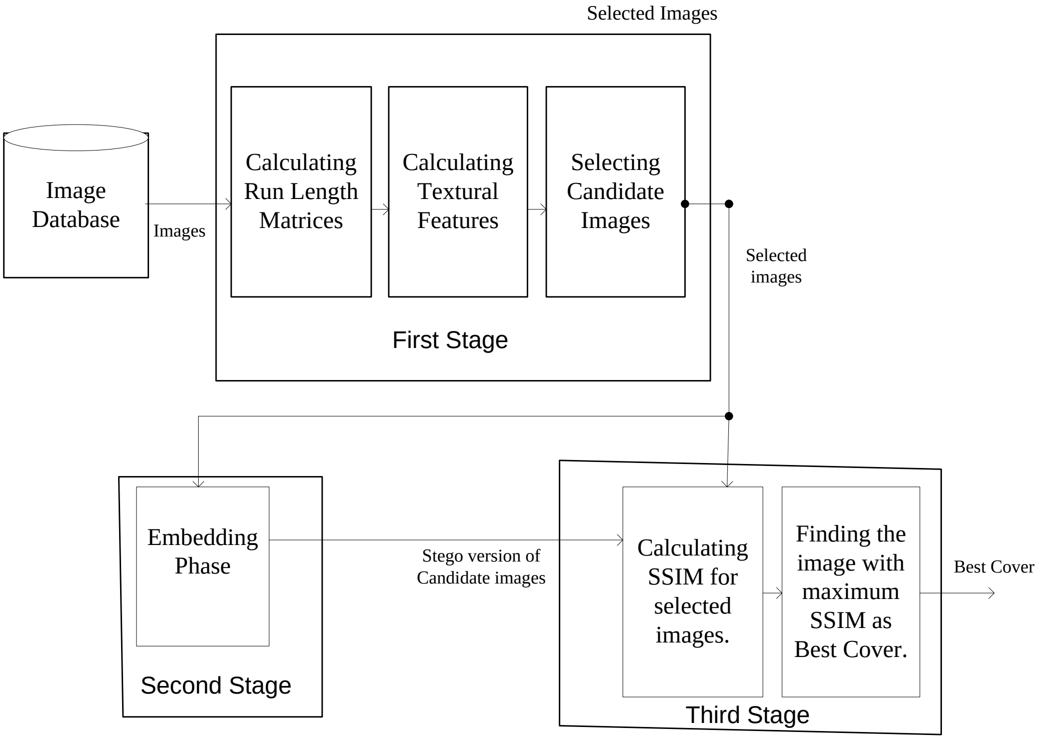

Selected Images
Image Database
Images
Calculating Run Length Matrices
Calculating Textural Features
Selecting Candidate Images
Selected images
First Stage
Embedding Phase
Second Stage
Stego version of Candidate images
Calculating SSIM for selected images.
Finding the image with maximum SSIM as Best Cover.
Best Cover
Third Stage

Figure 2. Block diagram of proposed algorithm

4. The Proposed Algorithm

The block diagram of proposed algorithm is shown in Figure 2. This algorithm contains three stages. In the first stage, the run-length matrix for each image in the database is calculated and then, texture features SRE, LRE, GLNU and RLN are calculated to select a set of image candidates which are suitable to be served as covers. In the second stage, data are embedded into the selected images using DWT steganography method. Consequently, the stego version of the selected images is formed. In the third stage, the best cover is extracted from the set of selected images by using SSIM measure. The proposed cover selection algorithm is described as follows:

Input: Image database

Output: Best cover

Step 1. Calculate Run length matrix in 4 directions 0°, 45°, 90° and 135° for each image of the database.

Step 2. Compute SRE, LRE, GLNU and RLN features for each image using run-length matrix.

Step 3. Select images with maximum SRE, GLNU, RLN and minimum LRE from database.

Step 4. Use DWT steganography embedding algorithm and then hide data in the images found in Step 3.

Step 5. Compute Structural Similarity (SSIM) between the original and stego versions of images obtained in Steps 3 and 4, respectively.

Step 6. Select the image having maximum similarity with its stego version (Step 5) as the best cover.

5. Experimental Results

All experiments were performed on a PC with core 2.35 GHZ processor and 4GB main memory. In order to evaluate our approach, we used the USC-SIPI Texture Database [27].

In this section, we illustrate the influence of our cover selection method on stego quality. Then, we evaluate the robustness of our method against steganalysis attacks.

A. Textural and SSIM Evaluations

We extracted the textural features for each image of database using run length matrix in 4 directions: 0°, 45°, 90° and 135° to obtain the selected images as candidate covers, and then, selected the best cover based on SSIM. The textured features are SRE, LRE, GLNU and RLN.

The selected images, were selected based on textured features that are shown in Figure 3. As it can be seen in Figure 3, results of using different textured measures might be identical images. The results of computing texture features for selected images (shown in Figure 3) are depicted in Tables 1 to 6.

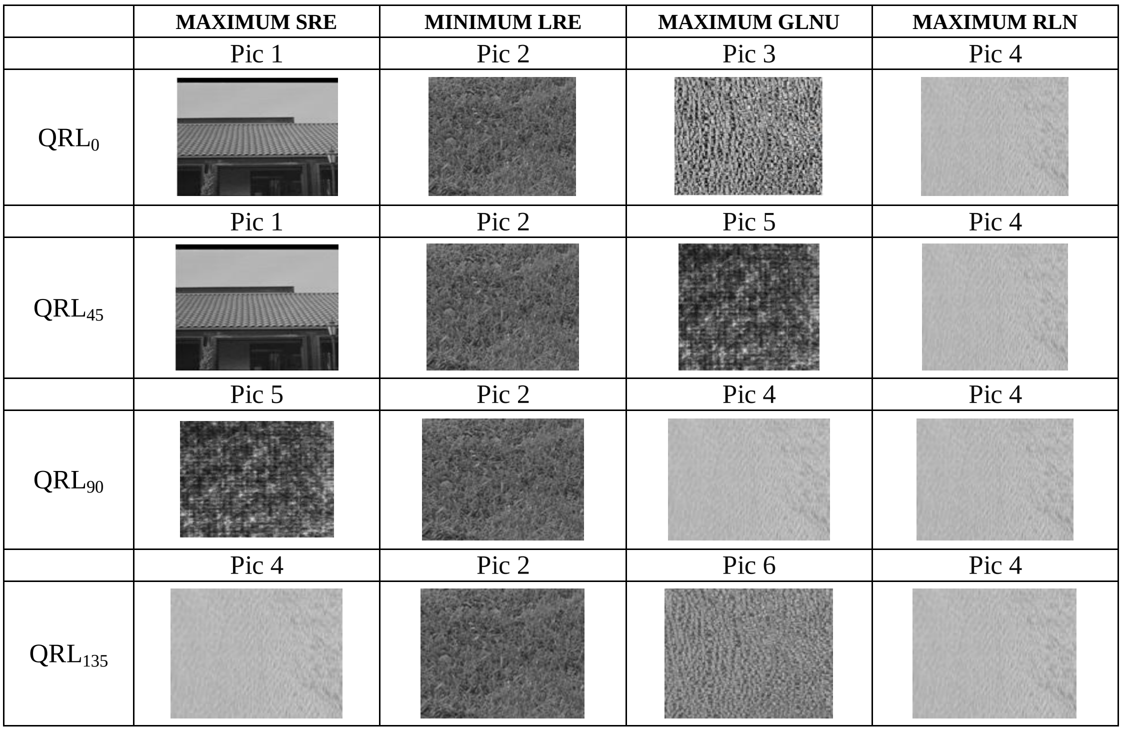


Figure 3. Candidate images based on textur features

After extracting candidate images based on texture features, random binary data are created and embedded into the selected pictures by using DWT steganography method [6]. As a result, several stego version of images with different payloads are obtained. It should be noted that the embedding process can be carried on by any steganography method including Contourlet, and Wavelet. Tables 1 to 6 contain original candidate images in Figure 3 with their stego versions, values of texture features, and SSIM between each selected image and its stego. The best cover, which maximizes SSIM, is depicted in Figure 4. The results of experiments confirm that the images with high SRE, GLNU and RLN and less LRE are good candidates for the best cover because they preserve the quality after embedding data.

There are a number of advantages in using proposed algorithm. The first advantage is that it restricts search space to several proper images based on texture features, which are suitable candidates for the best cover. Another advantage is quality assessment based on human visual system. Consequently, the extracted image with highest SSIM is the best cover among all images in database, since it preserves the structural specifications of image and influences the least distortion after embedding data into image. Additionally, as it can be seen in Table 7, the proposed method is able to preserve the quality of stego compared to traditional steganography methods such as DWT and Contourlet.

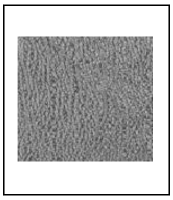


Figure 4. Best picture with maximum SSIM

Table 1. Textured feature for Cover candidate Pic 1

	SRE	LRE	GLNU	RLN	SSIM (Original Pic 1, stego Pic 1) = 0.6539
0	0.316	7.023	12524.215	23028.2831	Original Pic 1 Stego Pic 1
45	0.291	7.100	21475.359	36995.59	
90	0.284	7.254	21273.273	35067.147	
135	0.278	7.447	25918.064	39218.90	

Table 2. Textured feature for cover candidate Pic 2

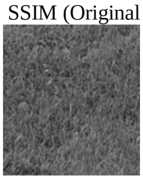
	SRE	LRE	GLNU	RLN	SSIM (Original Pic 2, Stego Pic 2) = 0.7069
0	0.2288	6.4966	14244.798	31772.291	 Original Pic 2 Stego Pic 2
45	0.233	6.4339	17285.013	34125.173	
90	0.2305	6.5691	9182.1280	24146.1759	
135	0.2275	6.5104	19904.8591	36749.9546	

Table 3. Textured feature for cover candidate Pic 3

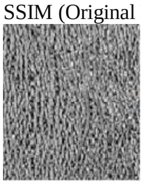
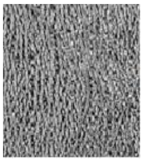
	SRE	LRE	GLNU	RLN	SSIM (Original Pic 3, Stego Pic 3) = 0.7658
0	0.20031	11.1264	70969.650	36409.807	 Original Pic 3  Stego Pic 3
45	0.2080	10.998	83860.266	38540.7957	
90	0.1959	10.9636	42386.300	30032.533	
135	0.2076	11.0405	76185.050	37038.2771	

Table 4.Textured feature for cover candidate Pic 4

Pic4	SRE	LRE	GLNU	RLN	SSIM (Original Pic 4, Stego Pic 4) = 0.5870
0	0.0995	11.7041	56333.207	120284.371	Original Pic 4 Stego Pic 4
45	0.09946	11.705	63884.576	126287.319	
90	0.09925	11.721	66351.635	114841.102	
135	0.0993	11.711	60150.5370	126585.202	

Table 5. Textured feature for cover candidate Pic 5

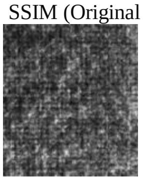
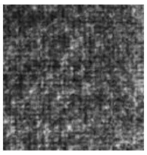
	SRE	LRE	GLNU	RLN	SSIM (Original Pic 5, Stego Pic 5) = 0.6967
0	0.2797	6.7079	61145.671	95578.7526	 Original Pic 5  Stego Pic 5
45	0.28156	6.6517	86087.757	112300.071	
90	0.28619	6.6502	48889.245	84681.3921	
135	0.2853	6.6180	77996.164	106393.578	

Table 6. Textured feature for cover candidate Pic 6

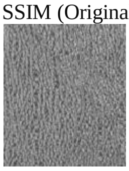
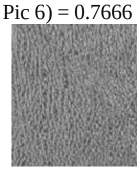
	SRE	LRE	GLNU	RLN	SSIM (Original Pic 6, Stego Pic 6) = 0.7666
0	0.2178	10.348	56395.577	33272.359	 Original Pic 6  Stego Pic 6
45	0.2261	9.9992	37138.731	27639.546	
90	0.2186	10.378	54113.767	32695.715	
135	0.2303	10.625	99762.5456	40307.402	

Table 7. Stego Visual Quality in proposed Algorithm

STEGANOGRAPHY METHODS	SSIM
PROPOSED COVER SELECTION + DWT STEGANOGRAPHY	0.7666
PROPOSED COVER SELECTION + CONTOURLET STEGANOGRAPHY	0.8612

B. Steganalysis Results

We evaluated the robustness of the proposed algorithm against steganalysis attacks such as Wavelet-based and Block-based steganalysis methods introduced in [25] [26]. They used nonlinear support vector machine classifier in training and testing phases. To make image cover database used in training and testing phases, we collected 800 JPEG images from Internet including Washington University image database [28]. All of the images were converted to grayscale with size of 512*512. Descriptions of these steganalysis methods are as follows:

1- Wavelet-based steganalysis (WBS) in [25] produces a model for clean images and then, it computes the distance between each image and its clean image model. It uses statistics such as mean, variance and skewness, extracting from each Wavelet sub-band of cover to detect a stego from clean image. Totally, 24 features are employed for classification.

2- Block-Based steganalysis (BBS) in [26] divides image blocks into multiple classes and defines a classifier for each class to determine whether a block is from a cover or stego image. Consequently, the steganalysis of the whole image can be conducted by fusing steganalysis results of all image blocks through a voting process.

Table 8. Detection Rate (%) of steganalses against our method composed with DWT embedding

Payload Rate (bits)	Embedding in DWT		Cover Selection and DWT Embedding	
	WBS	BBS	WBS	BBS
2000	60	59	55	55
5000	65	65	59	57
10000	67	66	60	62

Table 9. Detection Rate (%) of steganalses against our method composed with Contourlet embedding

Payload Rate (bits)	Embedding in Contourlet		Cover Selection and Contourlet Transform Embedding	
	WBS	BBS	WBS	BBS
2000	56	55	49	48
5000	58	59	51	50
10000	62	61	55	53

We created three stego databases with payloads of 2000, 5000 and 10000 bits for each steganography algorithm (DWT, Contourlet). Size of each stego database is 800. So, each pair of stego-cover databases includes 1600. We selected 1000 images for training phase and 600 images for testing, randomly. To evaluate the robustness of our proposed method against steganalyses, random subsets of images are selected; percentage of its average true detection (both stego and cover) over these random subsets is named accuracy of each method. The average detection accuracy of Wavelet-based and Block-based steganalyses over steganography techniques are represented in Tables 8 and 9. The results show that the proposed cover selection algorithm improved the robustness of DWT and Contourlet steganography against steganalysis attacks.

6. Conclusions

We proposed a new Cover selection approach for secure steganography using textural features of run-length matrix and structural similarity metric. According to textural features of run length matrix, suitable images are extracted as candidate covers. Through using SSIM, algorithm selects one image as the best cover among suitable images. This quality assessment method, SSIM, takes advantage of known characteristics of the human visual system.

New proposed cover selection algorithm results on preserving higher quality in stego with equal payload in comparison with traditional steganography methods. Additionally, we applied our suggested cover selection method to steganography methods such as DWT and Contourlet embedding. The results showed the robustness of our composed method against steganalysis attacks in comparison with DWT and Contourlet steganography methods.

References

[1] Abbas Cheddad, Joan Condell, Kevin Curran, PaulMcKevitt, "Digital imag steganography: Survey and analysis of current methods", Signal Processing, 2010, 727-752.

[2] M. Kharrazi, H. T. Sencar, and N. Memon, Image steganography: Concepts and practice,. to appear in Lecture Note Series, Institute for Mathematical Sciences, National University of Singapore, 2004.

[3] Walter Bender, Daniel Gruhl, N. Morimoto, A. Lu, "Techniques for Data Hiding", IBM Systems Journal, Vol.35, 1996.

[4] Chin-Chen Chang, Ju-Yuan Hsiao, Chi-Shiang Chan, "Finding optimal least-signicant-bit substitution in image hiding by dynamic programming strategy", Pattern Recognition 36, 2003, 1583-1595.

[5] K.B. Raja, C.R. Chowdary, K.R. Venugopal, L.M. Patnaik, "A secure image steganography using LSB, DCT and compression techniques on raw images", in: Proceedings of IEEE 3rd International Conference on Intelligent Sensing and Information Processing, ICISIP'05, Bangalore, India, 14-17 December 2005, pp.170-176.

[6] S. K. Muttoo, Sushil Kumar, "Data Hiding in JPEG Images", BVICAM'S International Journal of Information Technology, 2008.

[7] Chin-Chen Chang, Tung-Shou Chen, Lou-Zo Chung, "A steganographic method based upon JPEG and quantization table modification", Information Sciences 141 (2002) 123-138.

[8] R.T. McKeon, "Strange Fourier steganography in movies", in: Proceedings of the IEEE International Conference on Electro/Information Technology, 17-20 May 2007, pp.178-182.

[9] M.F.Tolba, M.A.Ghonemy, I.A. Taha, and A.S. Khalifa, "using integer wavelet transform in colored image-steganography", IJICIS Vol.4 No.2, July 2004.

[10] RajaVikas, VenugopalPatnaik., High capacity lossless secure image steganography using wavelets, Proceedings of International Conference on Advanced Computing and Communications (2006), pp.230-235.

[11] Arthur L. da Cunha, Jianping Zhou, The Non Subsampled Contourlet Transform Theory, Design, and Applications, IEEE Transactions On Image Processing, Vol.15, No.10, OCTOBER 2006, pp.3089-3101.

[12] Duncan D. Y. Po and Minh N. Do, Directional Multiscale Modeling of Images using th e Contourlet Transform, IEEE Transactions on Image Processing (2006), Volume: 15, Issue:6, pp.1610-1620.

[13] Hedieh Sajedi, Mansour Jamzad, Using Contourlet Transform and Cover Selection for Secure Steganography, International Journal of Information Security (2010), Vol.9, Issue:5, Publisher: Springer, pp.1-16.

[14] Z. Kermani, M. Jamzad, "A Robust Steganography Algorithm Based On Texture Similarity Using Gabor Filter", In: IEEE Symposium on Signal processing and Information Technology, pp.578-582, 2005.

[15] H. Sajedi, M. Jamzad, "Cover Selection Steganography Method Based on Similarity of Image Blocks". In: IEEE CIT, Sydney, Australia, 2008.

[16] M. Kharrazi, M. Sencar, H. Memon, "Cover Selection for Steganographic Embedding", In ICIP, pp.117-121, 2006.

[17] Hedieh Sajedi, Mansour Jamzad, "Secure Cover Selection Steganography", J.H. Park et al. (Eds.): ISA 2009, LNCS 5576, pp.317-326, 2009.

[18] Xiaoou Tang, "Texture Information in Run-Length Matrices", IEEE Transction on image processing, Vol.7, No.11, November 1998.

[19] S.Theodoridise, K. koutroumbas, pattern Recognition, Elsevier 2009.

[20] B. Girod, "What's wrong with mean-squared error", in Digital Images and Human Vision, A. B. Watson, Ed. Cambridge, MA: MIT Press, 1993, pp.207-220.

[21] Z. Wang, A. C. Bovik, and L. Lu, "Why is image quality assessment so difficult", in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol.4, Orlando, FL, May 2002, pp.3313-3316.

[22] Z. Wang, A. C. Bovik, and L. Lu, "Image Quality Assessment: From Error Visibility to Structural Similarity", IEEE transaction on image processing, Vol.3, No.4, April 2004.

[23] Z. Wang and E.P. Simoncelli, "Translation insensitive image similarity in complex wavelet domain", in Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing, Mar. 2005, pp.573-576.

[24] X. Shang, "Structural similarity based image quality assessment: pooling strategies and applications to image compression and digit recognition" M.S. Thesis, EE Department, The University of Texas at Arlington, Aug. 2006.

[25] Lyu., Farid, Detecting hidden messages using higher-order statistics and support vector machines, in: Proceedings of 5th International Workshop on Information Hiding (2002).

[26] Seongho Cho, Byung-Ho Cha, Jingwei Wang and C.-C. Jay Kuo, Block-Based Image Steganalysis: Algorithm and Performance Evaluation, IEEE International Symposium on Circuits and Systems (ISCAS) (2010), Paris, France.

[27] *USC*-SIPI Texture Database, *http://sipi.usc.edu /database /database.cgi*.

[28] Washington Database, *http://www.cs.washington.edu /research/imagedatabase.*