ISSN 2313-1527 (PRINT)
ISSN 2313-1535 (ONLINE)

IJEIE

International Journal of Electronics and Information Engineering

Vol. 10, No. 1 (Mar. 2019)

INTERNATIONAL JOURNAL OF ELECTRONICS & INFORMATION ENGINEERING

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Electronics and Information Engineering is published both in traditional paper form (ISSN 2313-1527) and in Internet (ISSN 2313-1535) at http://ijeie.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

23-75, P.O. Box, Taichung, Taiwan 40199, R.O.C.

International Journal of Electronics and Information Engineering

Vol. 10, No. 1 (Mar. 1, 2019)

Mode Conversion, Topology Preservation and Symmetry Of Filter Circuit and New Tunable Circuit Example

Sudhanshu Maheshwari

(Corresponding author: Sudhanshu Maheshwari)

Department of Electronics Engineerings, Aligarh Muslim University
Aligarh, Uttar Pradesh 202001, India
(Email: sudhanshu_maheshwari@rediffmail.com)

(Received Sept. 21, 2018; revised and accepted Oct. 28, 2018)

Abstract

This paper presents interesting mode conversion and topology preserving property of a current conveyor based circuit topology, with simultaneous symmetry property, enabling wider application domain. The mode of operation choice without topology change and symmetry aspects are explored. The circuit topology is further used to realize an electronically tunable filter circuit, employing a single active building block, with inherent tuning property. The presented theory is validated through simulation results. This study will provide further exploration of such topologies and the advantages owing to their versatile usage for voltage and current mode without alterations.

Keywords: Analog Circuits; Current Conveyors; Current-mode Circuits

1 Introduction

There has been continuous effort to transform the traditional voltage mode circuits into their current-mode counterparts, owing to the inherent benefits of current mode signal processing. Network transposition method has been effectively used for the purpose in the available literature [1]. Use of adjoints for the purpose has also been well covered in the open literature. As a result, the voltage-mode circuits have been successfully transformed into current-mode ones [2–5]. It has been proven in the literature that some active building blocks preserve their identity, even on transposition. The circuits realized using such active building blocks may possess the advantage of preserving their topology, even after transformation, a feature which is strongly topology-dependent. On the other hand, the symmetry of networks has been another interesting aspect, which allows interchange of input and output ports without changing port voltages and currents.

The above two mentioned features, namely preservation of active building block identity and the concept of symmetrical network, when combined together becomes powerful circuit design tool, giving rise to interesting circuits and their applications. Recently, a current conveyor with additional X-terminal was proposed and employed for realizing compact analog signal processing functions [6]. Conjoining the preceding, it becomes an interesting problem to investigate a circuit topology, which exhibits the two features, namely topology preservation on transformation and symmetry, followed by a new circuit

proposal based on the use of an extra-X current conveyor. The proposed theory is verified through simulation results. The topic of study on transformation in current conveyor based circuits, along with the applications of recent current conveyor variants continue to receive attention in technical literature [7–11]. As far as the recent coverage on EXCCCII is concerned, some voltage mode analog circuits have appeared in literature [12].

The subsequent section investigates a filter circuit topology in Section 2, and the possible functions realized from the same. The symmetry property and mode preserving property of the topology are investigated therein. A new filter circuit with electronic tuning is realized from the topology of section 2, and presented in Section 3. The results on the theory of sections 2 and 3 are presented in Section 4, followed by the concluding discussion in Section 5.

2 A Circuit Topology

The mode transformation is used to convert a voltage-mode circuit to its current mode counterpart. For a current conveyor of second generation, with negative current transfer gain from X to Z, the transformation results in interchange of Y and Z-terminals, while leaving X-terminal un-altered. Thus, a CCII- is transformed to CCII- itself. Any circuit employing CCII- and operating in voltage-mode may permit mode transformation from voltage to current, without topology change. For instance, the circuit of Figure 1 is shown, which is useful for realizing a number of electronic functions. The transfer function for the same (ratio of OUT to IN) is given below.

$$T(s) = 1 - \frac{Z_2}{Z_1}. \tag{1}$$

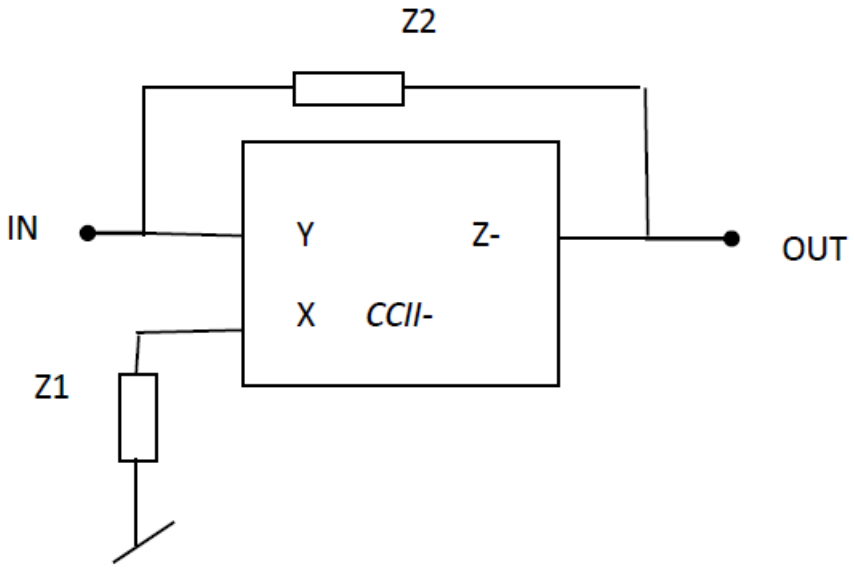


Figure 1: Circuit topology suited for VM and CM operation without change

The functionality of the topology of Figure 1 is listed in Table 1, showing various specialization of two impedances and the functions realized. The transformation of the topology (from voltage to

current-mode) amounts to Y and Z- interchange, and the interchange of IN and OUT marked nodes, which in turn yields the same topology, as in Figure 1. Thus the topology of Figure 1 is equally suited for voltage and current mode operation without changes, by inputting and outputting the desired mode signals at IN and OUT nodes respectively. However, it may be noted that for current-mode operation, the OUT node is to be referenced to ground. Therefore, it is to be concluded that the topology of Figure 1 realizes all the functions listed in Table 1, both in voltage-mode and current-mode without any topology change. It is attributed to the fact that a CCII- based circuit is transformed from voltage-mode to current-mode by interchange of Y and Z- terminals. It is worth noting the circuit obtained at #7 is already available in literature [7]. The functional versatility and mode preserving features of the topology of figure 1 makes it a promising candidate for being used as a configurable analog block for field programmable analog arrays.

Table 1: Functionality of Figure 1 for various impedance specialization

Sr. No.	Z_1	Z_2	Condition	T(s)	Function
1	R_1	R_2	$R_1 > R_2$	$1 - \frac{R_2}{R_1}$	Attenuator
2	R_1	R_2	$R_1 < R_2$	$1 - \frac{R_2}{R_1}$	Inverting amplifier
3	R_1	R_2	$R_2 = short/2R_1$	± 1	Bi-phase amplifier
4	R_1	Open	—	I_{out}/V_{in} $= 1/R_1$	Voltage to Current converter
5	R_1	1/sC	—	$1 - \frac{1}{sR_1C}$	Proportional-Integral circuit
6	1/sC	R_2	—	$1 - sR_2C$	Proportional-Derivative circuit
7	R_1	$R_2//1/sC$	$R_1 = R_2/2$; $R_2 = R$	$\frac{s-1/RC}{s+1/RC}$	All-pass filter
8	$R_1//1/sC_1$	$R_2 + 1/sC_2$	$R_1 = R_2 = R$; $C_1 = C_2 = C$	$-[1 + sRC$ $+1/sRC]$	Proportional Integral Derivative circuit

Next study is performed on the circuit of Figure 1 for its h-parameters. The circuit topology of Figure 1 is next shown as two port network in Figure 2, with port voltages and current shown marked. The port relationships and h-parameters expressions and for the circuit are found as below.

$$\begin{aligned} V_1 &= h_{11}I_1 + h_{12}V_2; \\ I_2 &= h_{21}I_1 + h_{22}V_2, \end{aligned}$$

where

$$\begin{aligned} h_{11} &= Z_2; \\ h_{12} &= 1; \\ h_{21} &= \frac{Z_2}{Z_1} - 1; \\ h_{22} &= \frac{1}{Z_1}. \end{aligned}$$

From the above equations, it is found that the topology of Figure 1 (hence Figure 2) exhibits the

following relation of h-parameters (Equation 2), which holds (Equation 3) for a symmetrical network.

$$h_{11}h_{22} - h_{21}h_{12} = 1. \quad (2)$$

$$(Z_2 \times \frac{1}{Z_1}) - (\frac{Z_2}{Z_1} - 1) = 1. \quad (3)$$

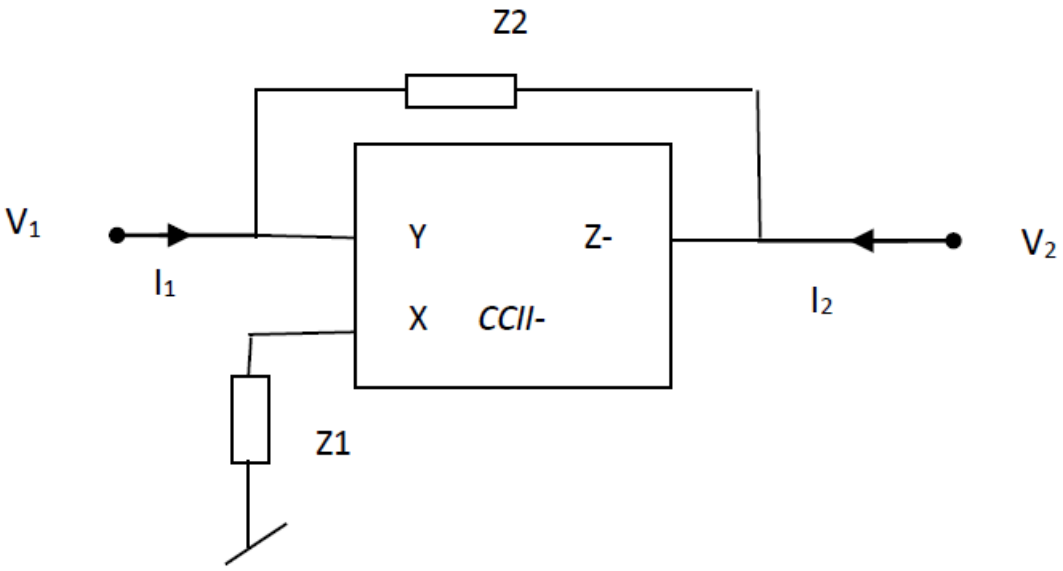


Figure 2: Circuit topology of Fig. 1 shown as two-port network

Thus the topology also exhibits symmetry property, which states that interchange of input and output ports does not change port voltages and currents.

3 New Electronically Tunable Filter Circuit

As the second part of this study, a new filter circuit keeping in view the topology of Figure 1 is proposed, especially for obtaining a tunable counterpart of the circuit #7 of Table 1. It is important to note that the preceding section presented the topology with symmetry and versatility for both voltage and current mode operation with topology preservation. Now, a circuit example of the same topology is drawn from Table 1, circuit #7, which will be used further. It is worth noting that the same is made electronically tunable by employing an extra-X current controlled current conveyor (EXCCCII), and the resulting circuit is shown in Figure 3. It employs a single EXCCCII with following terminal characteristics.

$$\begin{aligned} i_y &= 0; \\ v_{x1} &= v_y + i_{x1}R_{x1}; \\ v_{x2} &= v_y + i_{x2}R_{x2}; \\ i_{z1-} &= -i_{x1}; \\ i_{2z2-} &= -2i_{x2}. \end{aligned}$$

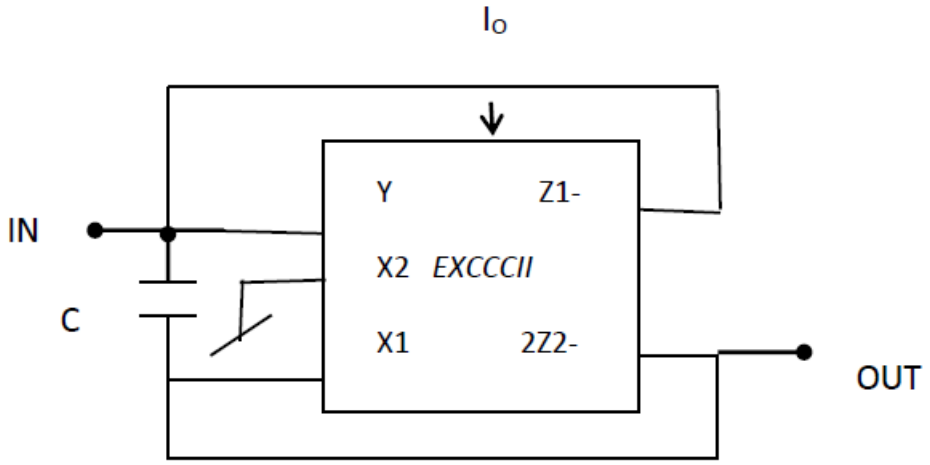


Figure 3: Proposed VM/CM filter circuit

It may be noted from the above equation that the Z2- stage is designed for a current gain of '2' from X2 stage. This implements the resistive ratio of '2' as required in the circuit listed at #7 of Table 1, which is converted to the tunable version. The generalized transfer function for the circuit of Figure 3 is given as below.

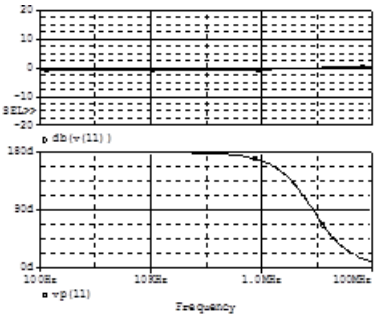
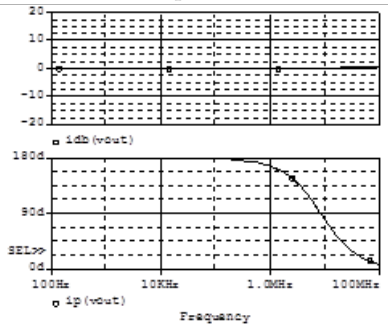
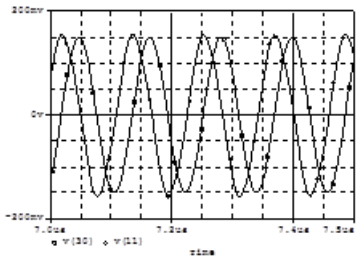
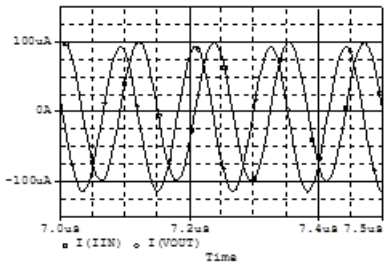
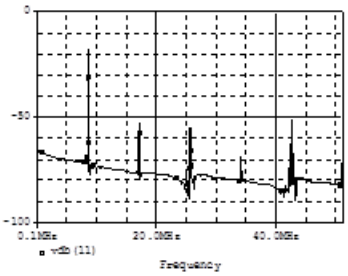
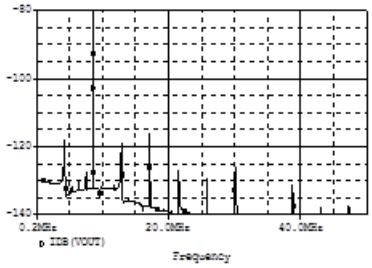
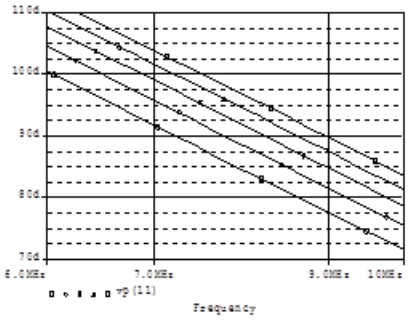
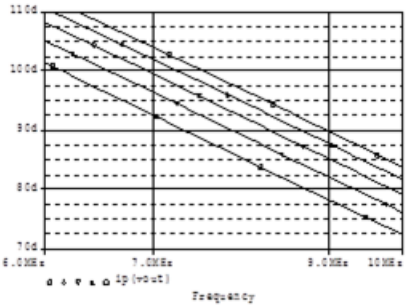
$$T(s) = \frac{OUT}{IN} = \frac{s - 1/R_xC}{s + 1/R_xC} \tag{4}$$

The transfer function (4) is general in the sense that the circuit can operate both in VM and CM, without any change in the circuit. For CM operation, the output is to be referenced to ground. The circuit is electronically tunable through the bias current of EXCCCII. It may be noted that EXCCII/EXCCCII based realizations have recently been reported as alternative choice, keeping in view their low circuit complexity [8, 9]. It is worth pointing that the recent circuit reported in literature can operate only in voltage mode, whereas the circuit of Figure 3 is more versatile with both voltage and current mode operation [12].

4 Simulation Results

The circuit of Figure 3 is next simulated using the CMOS circuitry and 0.25 μm parameters [8, 9]. The circuit is designed with C=20 pF, and various aspects of the simulation studies are summarized in Table 2, where, frequency response, time domain response, and electronic tuning graphs are presented. The results for both voltage and current-mode operation are included. The gain and phase plots show the pole-frequency as 8.55 MHz, with unity gain at all frequencies, while a phase shift of 90^o at the pole-frequency. The input and output waveforms for both modes of operation are shown, where the input of 8.55 MHz yields the output signal, which is phase-shifted by 90^o. The spectrum of the output shows the suppression of harmonics by -35 dB in either of the two modes. The electronic tuning of pole-frequency is further shown, where the bias current of EXCCCII is varied from 50-90 μA, is steps of 10 μA, so as to vary the pole-frequency from 9 MHz to 7.2 MHz respectively. Thus the proposed circuit of Figure 3 is verified for its operation.

Table 2: Results for the proposed circuit of Figure 3 for VM and CM operation

Characteristic	VM operation	CM operation
Frequency response showing gain in dB and phase in degrees respectively		
Time-domain response showing input and output at pole-frequency (8.55 MHz)		
Fourier spectrum of output showing elimination of harmonics by at least -35 dB		
Phase plot showing tuning of pole-frequency (9 to 7.2 MHz) through bias current (50-90 µA), in 10 µA step		

5 Conclusion

This work is devoted to the study of a CCII based circuit topology, which is useful for realizing many electronic functions and exhibits the properties of (i) preserved topology, when transformed from VM to CM and (ii) symmetry. All these features make the topology a potential configurable analog block for field programmable analog arrays. A related but tunable filter circuit, with the first property is further proposed, which employs an EXCCCII, and a single capacitor, for realizing an electronically tunable all-pass filter of first order. The new proposed circuit's workability, both in VM and CM is shown through simulation studies. This study adds to the known theory on mode transformation and symmetry aspects of circuits, while providing novel all-pass filtering circuit with phase-shifting applications, both for voltage and current mode signals and electronic tuning ability for adoption in modern electronics and information systems.

References

[1] B. B. Bhattacharyya, M. N. S. Swamy, "Network transposition and its applications in synthesis," *IEEE Transactions on Circuit Theorem*, vol. CT-18, pp. 394-397, 1971.

[2] T. Dostal, D. Biolek, K. Vrba, "Adjoint voltage-current mode transformation for circuits based on modern current conveyors," in *IEEE Int. Caracas Conference*, T034(1-4), 2002.

[3] C. M. Chang, P-C Chen, "Realization of current-mode transfer function using second generation current conveyors," *International Journal of Electr.*, vol. 71, no. 5, pp. 809-815, 1991.

[4] A. M. Soliman, "Theorems relating to port interchange in current-mode circuits," *International Journal of Electr.*, vol. 82, no. 6, pp. 585-604, 1997.

[5] E. T. Cuautle, C. Sanchez-Lopez, D. Moro-Frias, "Symbolic analysis of (MO)(I) CCI(II)(III) based analog circuits," *International Journal of Circuit Th. and Appls*, vol. 38, no. 6, pp. 649-659, 2010.

[6] S. Maheshwari, "Current conveyor all-pass sections: brief review and novel solution," *The Scientific World Journal*, 2013. DOI. 10.1155/2013/429391.

[7] S. Maheshwari, "New voltage and current mode APS using current controlled conveyor," *International Journal of Electr.*, vol. 91, no. 12, pp. 735-773, 2004.

[8] D. Agrawal, S. Maheshwari, "Current-Mode Precision Full-Wave Rectifier Circuits," *Circuits Syst Signal Process*, vol. 36, pp. 4293-4308, 2017.

[9] S. Maheshwari, "Tuning approach for first order filters and new current-mode circuit example," *IET: Circuits Devices & Systems*, 2018. DOI: 10.1049/iet-cds.2017.0431.

[10] A. Kumar, B. Chaturvedi, "Dual-X current conveyor transconductance amplifier realization with current-mode multifunction filter and quadrature oscillator," *Circuits Syst Signal Process*, 2017. (`https://doi.org/10.1007/s00034-017-0680-9`)

[11] M. N. S. Swamy, "Mutators, generalized impedance converters and inverters, and their realization using generalized current conveyors," *Circuits Syst Signal Process*, vol. 30, 2011. (`https://doi.org/10.1007/s00034-010-9208-2`)

[12] S. Maheshwari, "Analog circuit design using a single EXCCCII," *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 61-69, 2018.

Biography

Sudhanshu Maheshwari works as full Professor in the Department of Electronics Engineering, AMU, Aligarh, India and has published more than 100 referred International journal papers, a large number of Conference papers and several books chapters in the area of Analog Current mode circuits.

Meta-Search Engine for Universiti Kebangsaan Malaysia Patent: UKM Patent

Rosilah Hassan[1], Abdullah A. Al-khatib[1], Wan M. Hussain[2], and Mohammed A. Hassan[3]
(Corresponding author: Abdullah A. Al-khatib)

Research Centre for Software Technology and Management, University Kebangsaan Malaysia (UKM)[1]
Graduate School of Business, Universiti Kebangsaan Malaysia (UKM)[2]
43600 UKM Bangi Selangor, Malaysia
Department of Information Systems, Seiyun Community College[3]
Seiyun, Yemen
(Email: khteb2003@gmail.com)
(Received Oct. 4, 2018; revised and accepted Nov. 4, 2018)

Abstract

A Meta-Search engine is an optimal tool that uses search words and phrases and transmits them away to multiple search engines. It then comes back with the categorized results to the user. One example is, we created a Universiti Kebangsaan Malaysia (UKM) Patent meta-search engine that takes patents from a number of search engines, such as Google patent and Patent Mall. This website enables UKM students to investigate patents inside Patent Mall, the UKM database and the Google patent search engine. This paper aims at web design and its development using different tools and programming languages, such as open source ASP.Net and SQL Server Database. Some of these are used to retrieve information from search engines such as the Google patent application programming interface (API) and Post Query to Patent Mall. In this project, we set up a new framework for the first meta-search engine specialised in patents, which will reduce worthless pages in search results. Additionally, the UKM database contains private university UKM patents. The UKM patent meta-search will extract (or retrieve) these patents based on Language-Integrated Query (LINQ) which is used for conveniently extracting and processing patents from the UKM database. Finally, the UKM meta-search is a new solution to the problem of obtaining requested information quickly.

Keywords: API; Google Patent; LINQ; Meta-Search Engine; Patent Mall; UKM Database

1 Introduction

Searching for information is currently an activity of great importance. It searches large volumes of documents available to find those that best fit our needs in the shortest time possible. To this end, information search tools are implemented to help find information in a large corpus of documents. Therefore, several questions arise about these tools; especially about their performance and relevance of the results that they return. A meta-search engine is a search engine whose main feature is that it forwards a query to several other search engines simultaneously as demonstrated in Figure 1 and collects and processes the results. The results can be easily arranged one after the other [6]. In other words, meta-search is software that draws its information from several other search engines. This

allows users to enter the subject of their research once and access multiple responses from different search engines [2]. Some meta-search engines don't use an algorithm, but still present the resulted information of the sources found. The UKM patent meta-search is a friendly website that gives all similar patent information from other search engines. To achieve this goal, we need to be able to connect to it from this website. In this paper, the reason why the UKM patent adopts this meta-search engine is because it assists in generating results accurately and conveniently from an increasing number (millions) of patents and from many different search engines. Finally, the UKM patent meta-search engine allows researchers to quickly get accurate information from different search engines.

A preliminary work of this project was presented in a conference [10] where the implementation of the framework and the results have not been addressed and analyzed due to limited space in Conference Proceedings. The remainder of this paper is organized as follows. In Section 2 the meta-search engine concept is simply introduced. The proposed framework for UKM patent meta-search engine is described in Section 3. Section 4 analyzes the interaction between components of framework. The implementation of the proposed framework is presented in Section 5. Section 6 discusses the experimental results. Finally, Section 7 draws the conclusions and future work.

2 Meta-Search Engine

A meta-search engine is an internet search tool that collects search results using many different search engines, indexes, and clusters, and organizes them using cutting-edge technology. It then uses Latent Semantic Analysis to quickly discover the relevant results. It saves time using intelligent indexing to quickly focus only on the results of interest. Meta-search engine has been classified for several types of searching queries. Some of meta-search engines are used for general purpose of searching based on Google, Yahoo, and Bing search engines. Other meta-search engines are used for specific search query like searching based on country, file type and site type, as shown in Figure 1.

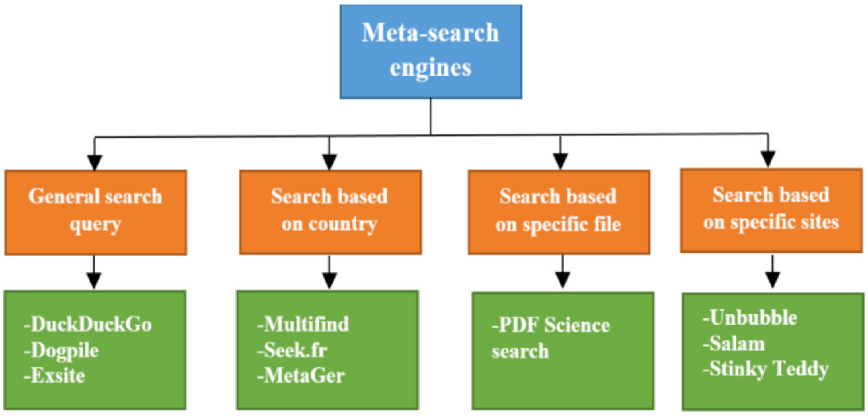


Figure 1: Classifications of meta-search engine

Search engines have become a daily tool for Internet users and the educational process. However, an increasing number of pages per day (in the millions) make it difficult for researchers to find information. Therefore, they require an easier method to obtain information quickly. The UKM meta-search engine is a new solution for these problems. The architecture standard of meta-search engines is shown in Figure 2.

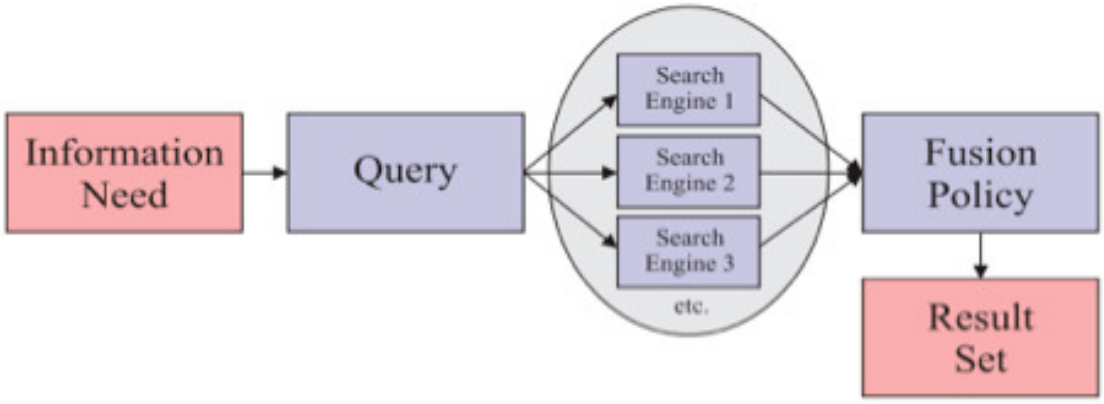


Figure 2: The architecture standard of meta-search engine [7]

2.1 Limitations of Search Engines

According to [16], most existing web pages are not indexed. Each search engine captures a different percentage of the total; but no one can say exactly what proportion has been captured. The estimated size of the World Wide Web is at least 5,000 million pages; however, there is a much greater depth; estimated at about 500,000 million pages within databases whose contents are not captured by the search engines. These dynamic web pages take shape within a web server when a user asks for it; therefore, a conventional search engine cannot access them. Page United States Patent and Trademark Office (Patent Office and registered US marks) is an example: if a search engine can find your homepage, one can only search their database of individual patents by searching for the site itself. [13] The study result of a search engine query can sometimes give ambiguous results:

- Confusion between the part and the whole: Google can index some of the knowledge that is published on the web; but what is indexed by Google is not the entire Web, or all of the knowledge present worldwide.
- Confusion between quality and quantity: the countdown is preferred answers to the evaluation of the argumentative quality.
- Confusion between information and reality: the information provided by Google reflects reality without an intermediary.

2.2 Benefits of Meta-Search Engine

In [19], authors conducted an explicit study on the benefits of Meta-search engines:

- For access to multiple retrieval systems, the user must learn to work with only one interface. This may not take into account the differences in various search systems.
- Eliminate duplications in the search.
- From the user?s perspective, it is more efficient if every query is entered only once. The query is evaluated in parallel and does not need to be entered for each system separately.

- Meta-search systems contribute to higher search completeness. Individual systems are not measured by the amount of indexed files only; but also by the content focus of the database. By utilizing meta-search engines so the user has a higher chance that their query will get more relevant documents.

2.3 Meta-Search Engine Architecture

Traditionally, the meta-search engine?s server has to wait for responses from all search services to which it has forwarded the search, in order to start with the results representation [7]. This result faces delays compared to a normal search engine. In order to counter this, a display that has been updated in each case, upon the arrival of different search results, can be carried out; or slow-response search engines can be excluded from the search. The current generation of meta-search engines also allows syntax translations; so that even more complex search queries can be sent to the respective search engines [14]. Two investigations on the problem of recovery of similar documents are identified [21], [12]. These works proposed fingerprint processes to represent the input document sets of relevant terms. Both architectures make use of meta-search engines to retrieve large lists of candidates for similar documents. In [21], authors use cosine similarity of the vector model to compare the search query with the documents snippets. In [12] text similarity algorithms such as Patricia and k-grams are used to compute the similarity. The following will study the standard architecture of a meta-search engine.

2.4 Standard Architecture

Apart from basic search engines, meta-search engines consist of four main software components; User Interface, Dispatcher, Display, and Personalization & Knowledge [11]. The software component architecture of a meta-search engine is shown in Figure 3.

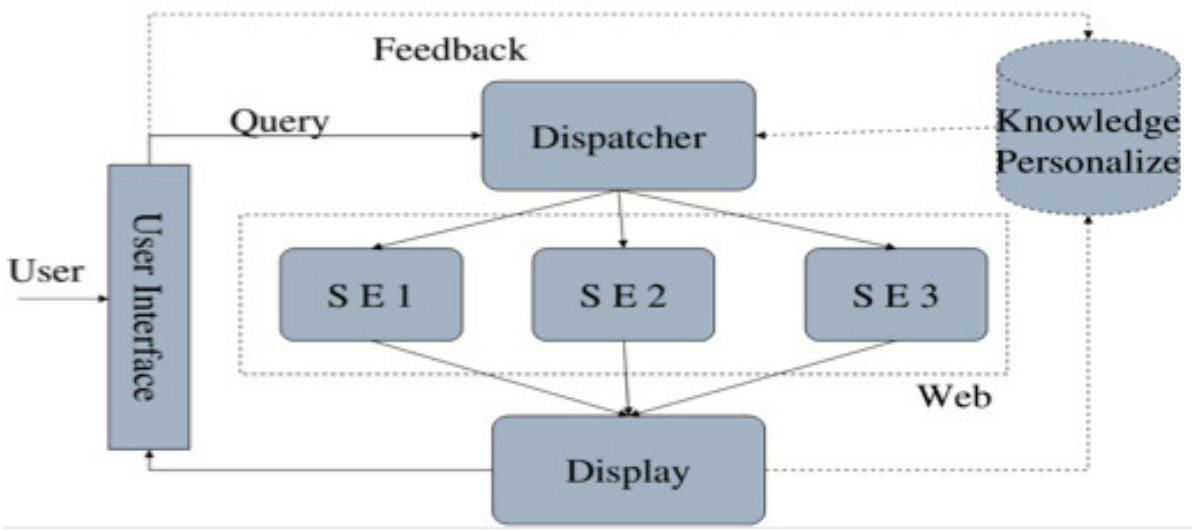


Figure 3: Components of a meta-search engine [11]

1) *User Interface:* should be very easy to use. However, this makes no difference in providing a unification of the various interfaces of various search engines.

2) *Dispatcher:* deals with consultations that interact with different modules related to search engines. It is responsible for sending adequate consultations for each search engine and then collecting the returned results.

3) *Display:* generates a results page from the replies received. This may involve ranking, parsing and clustering of the search results or just plain stitching.

4) *Personalization/Knowledge:* may contain either or both. Personalization may involve weighting of search results/query/engine for each user.

3 Proposed Framework for UKM Patent Meta-Search Engine: System Architecture

The system framework as shows in Figure 4 consists of components based on design layers developed in the UKM patent meta-search engine framework. Each component has proposed control of the tasks necessary to solve the problem of retrieving similar patents from the search engines. In this system, we have design-oriented services based on Web Services. In this system, the service can combine results from other search engines. In this case, the services allow users to deal with the web interface to retrieve similar patents. The interaction between the components is explained as follows. The process begins with text input at the user-interface and ends with a list of patents that are similarity ranked. The input is converted into a set of queries generated by the user-interface process that assigns greater probabilities of occurrence to the most relevant terms. Then, the queries are sent in parallel to a customizable list of search engines.

Finally, the patents are retrieved, merged and ranked by the strategy proposed in the model and returned to the users; which, in this case, is the user interface. The following sections will describe the overview of the main components of the UKM patent meta-engine framework; which consists of four layers; front-end GUI, Middle-end meta-search, back-end search engines, and back-end UKM patent database. These components are illustrated in Figure 4.

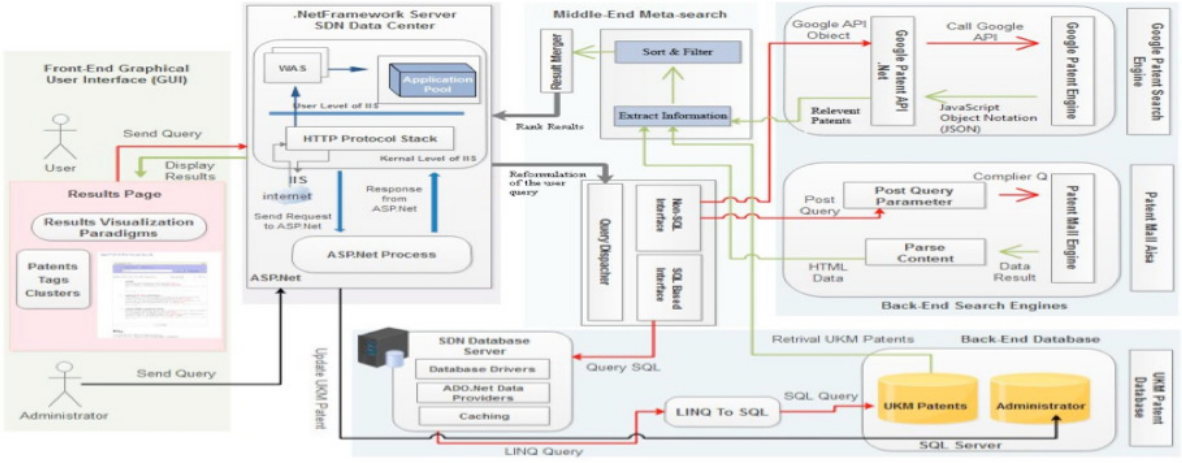


Figure 4: UKM patent meta-search engine framework

3.1 Front-End GUI

The front-end GUI is the first layer in the system architecture of the UKM patent meta-search engine that interacts directly and transparently to the user with webpage interfaces. It is therefore merely a front-end that collects, organizes and manages information collection. However, it also translates user interaction in order to provide a text interface that is in charge of performing specific operations on the website, such as sending queries and displaying results on the front page of the website. This layer consists of two main components: results visualization Para-diagram and reformulation query. The results visualization is responsible classified by patents search engine, each in a tab. On each tab title patents documents are highlighted with a color for easy identification, the URL has a color that stands out, and left tab show the images of patent display in picture box. The user can click to image to get the URL of patents. The other component, reformulation the query provide a reformulation user query that generates a new query and initial request, in order to achieve more relevant documents from those provided by a non-reformulated query.

3.2 Middle-End Meta-Search

The Meta-search layer is the layer between the front-end GUI and the back-end. The interaction flow of this layer is either with the dispatcher or retrieved data that is saved from these search engines and the UKM database. The main task of the Meta-search in this system architecture is to distribute queries and merge the results retrieved from the search engines and the UKM database; all of the retrieved data that needs clustering and format conversion. There are five main components found in this layer; query dispatcher, result rank and merger, information extractor and sorting with filtering. The Query Dispatcher consists of two main components; SQL Based Interface and Non-SQL Interface. It is responsible route query to either Non-SQL or SQL, depend on it attribute. Each attribute processed by the Dispatcher to pass the query. The algorithm for rank and merge results use the Top Document search engine score (TopD) [11]. It allows classification and sorting of the retrieved patents. The extractor results from different search engines that need to be merged and stored either in a database or in xml format. This layer also sorts and filters the obtained results, based on the distance of cosines (commonly used in the vector model of information retrieval) [20], and neatly shows three tabbed results (Google patents, Mall Patents and UKM Patents).

3.3 Back-End

Back-end is comprised of two components, namely search engines and UKM patent database as shown in Figure 4. The search engine module in this system?s architecture interacts with the middle-end layer through the query dispatcher, either directly to UKM database or indirectly retrieving information, like Google patents API and post query that supported by Patent Mall. However, there is no direct interaction from the back-end to the GUI layer.

The search engine back-end module indirectly serves the front-end services; usually by being closer to the required resource or by having the capability to communicate with the required resource. For example, the resource in this system?s architecture are the Google patent search engine and Patent mall databases. The main task of this layer is to collect patents from search engines using tools like API and Post query. API is a JavaScript library that allows inserting Google Patents into the UKM Patent meta-search website. It also obtains requests and query strings for patents that appear in URLs from Patent Mall. These patents consist of title, URL, images, and the description of the patent. The UKM Patent database represents the established connection between the SDN Server and the databases. It is a standard that defines Microsoft SQL Server interfaces between middle-end and back-end servers on databases. The main task of this layer is to establish gateways that allow users to access different

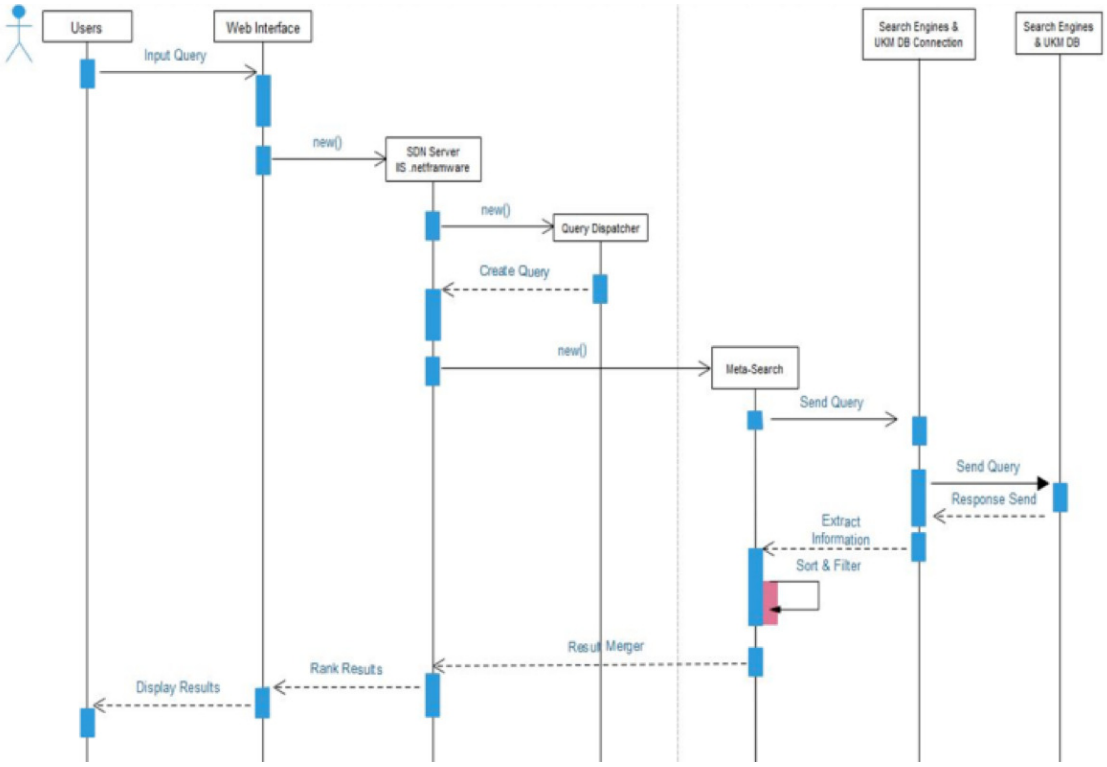


Figure 5: Sequence diagram of UKM patent meta-search engine

databases within a distributed environment using translation methods. It is also the administrative centre of the UKM patent meta-search engine website. The construction and implementation of the web, managing editing and insertion patent's content, are made through this elegant and intuitive interface. However, there is no direct interaction from the back-end to the GUI layer, but an indirect interaction through accessing the administration panel; either from the "Administration" menu item on the homepage.

4 Analysis Model

In this section the flows of detailed interaction between components of framework analysis by developing a sequence diagram as shown in Figure 5. The process begins when the user enters a term of query in the Web Interface. Then the web interface creates an instance of Query which returns the set of queries created from the terms. After that established connection to server Software Defined Network (SDN). The queries are sent to external search engine which in turn sends them to the corresponding external search engine by query dispatcher. The external search engines are returned the patents to Meta-search which in turn extract information, filtering, sorting, and merge the results to SDN server then performs ranking the results or give the scoring for patents. Final after ranking return to the Web interface to displaying for users a final result with similar patents are retrieved.

5 Implementation of the Framework

This section is going to present the implementation of the proposed framework presented in Figure 4. First we will presents the development environment used to implement the system including .Net framework platform, and Microsoft SQL server. This is followed by detail explanation on the implementation of the graphical user interface (GUI) for the service provider and the service student sides and for middle layer (meta-search). The following Figure 6 shows the implantation steps of framework of UKM patent meta-search engine.

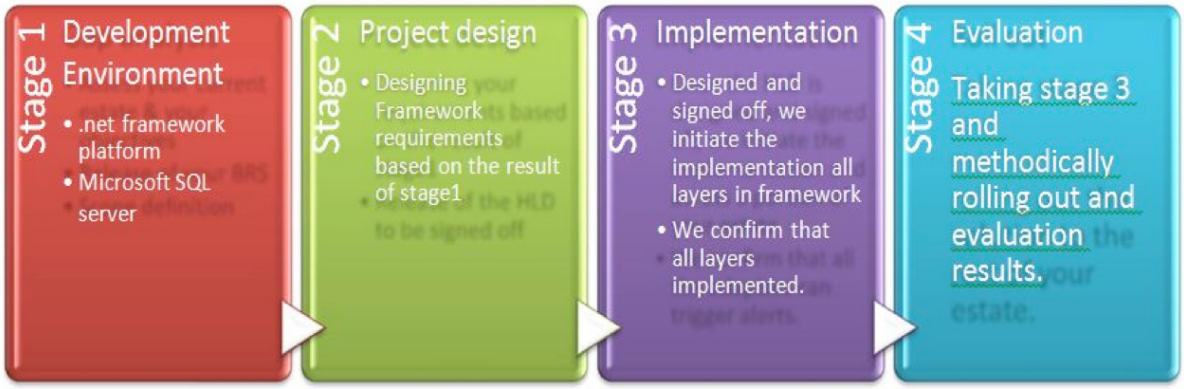


Figure 6: Implementation steps

Figure 7 shows the tool consisting of components based on its design layers developed in Figure 4. Each proposed component controls the tasks necessary to solve the problem of recovery similar patents from different search engines.

The interaction between these components is explained below; The process begins with input query terms delivering user-interface, and ends with a list of Web patents by similarity rank output. The input is converted into a set of queries generated by reformulation query that assigns greater probabilities of occurrence to the most relevant terms. Then queries are sent in parallel to a customisable list of search engines. Finally, patents are retrieved and returned to the user interface which also allows the user to evaluate the quality of the results.

5.1 Front-End GUI

This subsection provides the graphical interface developed for user interaction with the website, and the relationship between the different pages, and also, elaborate on the graphical user interface (GUI) of the system implementation. The web interfaces are designed and developed by Microsoft visual studio 2013 that allows the development of web pages with a customisable design to the size of the device, using ASP.Net, visual C#.Net, HTML, CSS and JavaScript. According to the Graphical User Interface (GUI) design, this interface is comprised of two webpage interfaces:

5.1.1 Primary Form (Main Window)

The primary form is allocated for users to enter, post query and display results. That appears after accessing the UKM Patent meta-search engine. It is a very simple screen, similar to the home screens of many commercial search engines like Google patent or Mall patent. The Main window screen of UKM patent meta-search engine can be seen in Figure 8.

This form was created using a combination of ASP.NET, HTML, and CSS. It is a part of the index.aspx webpage, which links to meta2.css where the overall design of the site is defined. It consists of a search text box, search button, and option buttons (button menu-drop) for aggregation or clustering search (All patent, UKM patent, Google patent, and Mall patent). The search text box being the area where the user enters their query and submits the entire form using the Search button. Also, all pages have a common menu at the top of the screen for navigation between different webpages. This menu implemented in masterpage.master page it is the back layout of the website.

The option buttons (button menu-drop) allow the user to decide whether they would like results returned as aggregated like all Patent options, clustered regardless of that which option they pick (UKM patent, Google patent, and Mall Patent). Aggregated is selected by default and the user cannot select more than one of these options at a time. They are located to the left of the search text box. The final four radio buttons are used to allow the user to specify the number of results they would like returned. The options are 10, 20, 50, or 100, with 10 selected by default.

5.1.2 Secondary Form (Administration Webpage)

The second interface is allocated for administrator page (control panel) the person responsible for the maintenance and operation of the computer system call (website master or Administrator). The administrator module enables administrator to control meta-search engine databases to manage UKM patents like adding a new patent to UKM database and modifying the patents in the following form as show in Figure 9.

5.2 Middle-End Layer

This section provides interaction flow with this layer either dispatcher or retrieval data that are saved in these search engines and UKM databases. In addition, we will describe the meta-search components layer system implementation. In rank and merge results design Figure 4, the result arrays collected

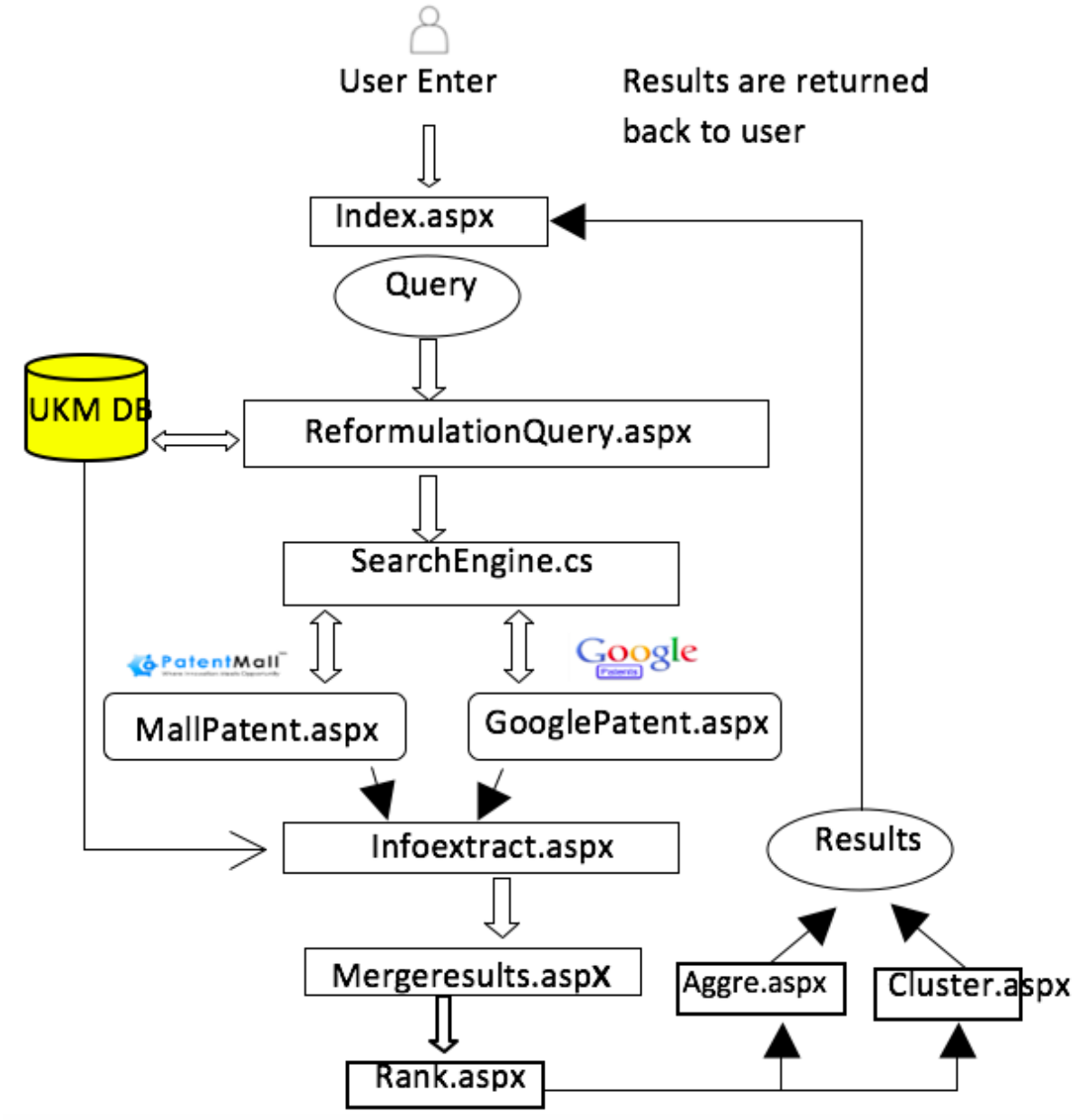


Figure 7: Navigation diagram of UKM patent meta-search engine

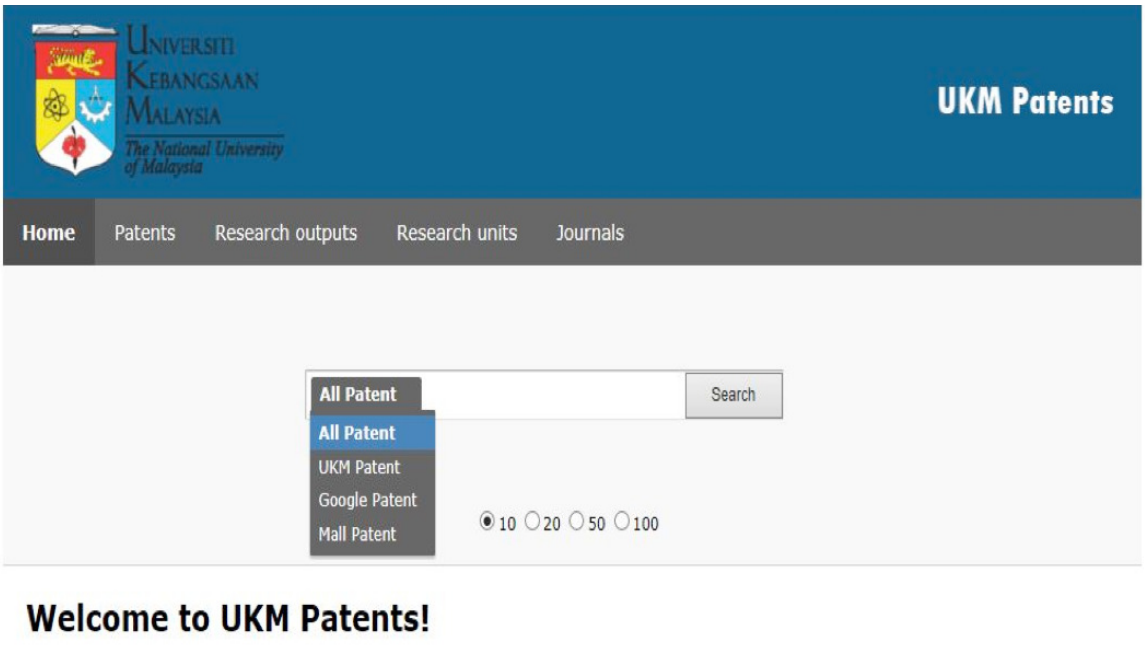


Figure 8: Main window screen

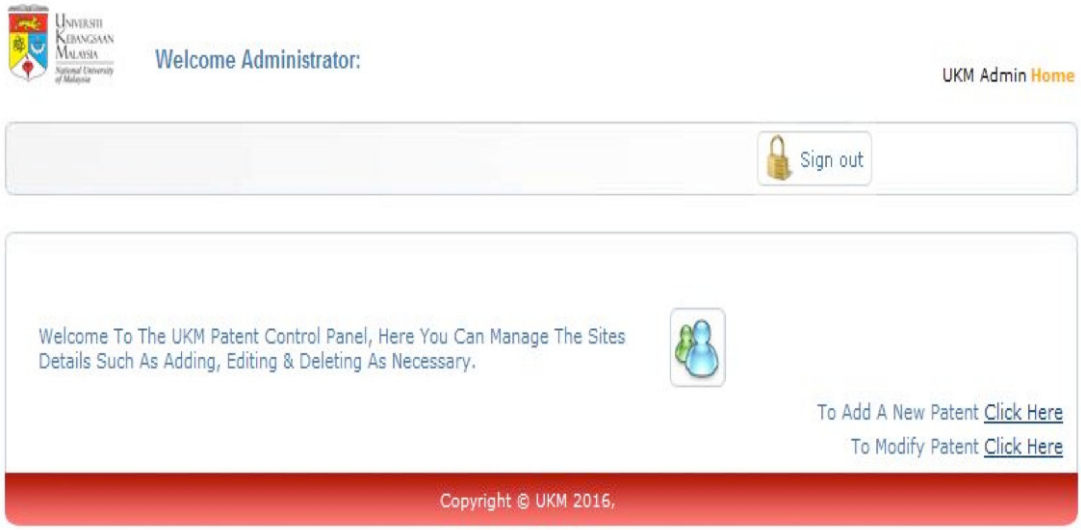


Figure 9: UKM admin home webpage screen

Table 1: Response time of queries

No.	Query Terms	Response Time		
		Google P.	P. Mall	UKM P.
1	Motor	0.48	0.52	0.27
2	Computer	0.32	0.39	0.24
3	Network	0.44	0.62	0.21
4	Communication	0.56	0.52	0.18
5	Mobile	0.62	0.58	0.28
6	Laptop Computer	0.73	0.62	0.25
7	Barcode	0.45	0.48	0.19
8	System	0.49	0.68	0.21
9	Information	0.52	0.47	0.18
10	Information System	0.48	0.59	0.28

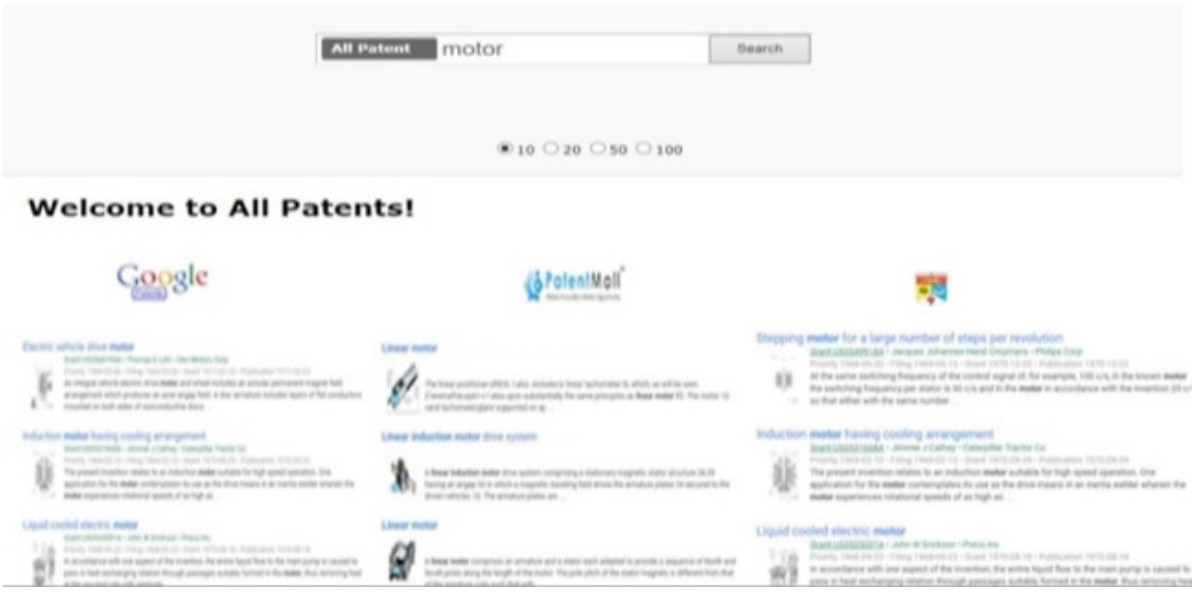


Figure 10: Snapshot of UKM patent meta-search engine

from each engine are sent to rank.aspx where they are compared and combined into a single array and displayed as a single list of results (aggregation). Each patent is listed in the order it was retrieved. As well as a rank patent is to a sub-array. The algorithms used to define the order in which these results are listed are distance of Cosines and Borda-Count [5,17]. Distance of Cosines merges patents returned into a unified list using only the rank positions of retrieved documents to assign a simple score, which are essentially determined by the underlying search engines themselves [15]. The order in which arrays are combined together using the *add_to_total_array*() function in rank.aspx allows one to implement a slight bias towards one engine over another. In this case, UKM patent results take preference, followed by Google patent, and finally Mall Patent. Therefore, if two patents from different engines have the same score, one patent from Google, and the second from Mall patent. The Google patent will precede the Mall patent within the list of returned results.

The aggregated array using the C# function *asort*() in rank.aspx webpage, which sorts the associative array in ascending order; i.e. sorts the array such that patents with the lowest reciprocal rank score are displayed first. A new array is then initialised to hold only the top return number of results in the aggregated array, using the C# function *arrayslice*(). The array is then sent to index.aspx webpage to be displayed to the user.

The clustering refers to the partitioning of data into number of groups, or clusters. Clustering of patents was performed using a number of steps. The first step is to create a vector space model of the entire aggregated results set. Each patent is represented by a vector of n-dimensions if it contains n amount of terms. Terms were identified for each document by tokenisation [4] the strings a document contained. Each term was then assigned a numeric value or weighting using a method known as Term Frequency-Inverse Document Frequency [18]. After which, the K-means clustering method could then be applied. Once the entire document vector space [3] is assigned to a cluster, vectors are then recombined with their matching patents and sent to index.aspx to be displayed. Though originally, one had iterated the clustering process over the entire document vector space multiple times, it seemed to inhibit rather than enhance the clustering results. For each iteration placing are more and more patents into the same cluster. As such, it was reverted back to assigning vectors to clusters just once.

6 Results and Discussions

In order to assess the framework presented in Figure 4, a prototype system is developed and implemented using virtual C# and ASP.net. The front-end user interface as shown in Figure 10 displays the results obtained when running a query looking for "motor" in left side. The results obtained from Google patent search engine is depicted and the middle the results from Patent Mall display. In the right side, the query results database is from UKM. The figure shows that the system is able to execute retrieving, processing, filtering and arrangement of the patents obtained have been performed. This interface displays classified patents from search engines, each in a tab. On each tab, the patent's title is highlighted in colour for easy identification and a snippet (or text summary) is clearly displayed. We also test the query dispatcher to distribute the query to give quickly retrieved patents. We note that the queries to external server take 0.4 second more time to execute. The connection through Google patent API take 0.2 longer time compare to access our local database patents. We have met the chairman of UKM patents in order to ensure usability of our proposed framework. The user is satisfied with the system performance and usability since it gives quick access to UKM patent database. In addition, it was able to retrieve patent result from Google patent online service as well as mall patent. We hosted this project in the server support SDN to enable quick searches, above using a traditional hosting server.

In addition, we run 10 terms queries as shown in Table 1. The results prove that local query takes less time to perform compared to external source.

7 Conclusions and Future Work

The UKM patent meta-search engine has become a necessity for students, professors and researchers in order to give them patents easily and quickly. The goal is to enable users to find patents whose content meets their information needs. However, we found that the idea of relevance depends on the user's satisfaction on one hand, and different meanings carried by the terms of the application on the other. This finding is a weak point of looking for traditional information. It also represents the starting point for new research paradigms. After proposing this architecture, our future work will improve the rank and merge results algorithm. In addition, we will implement our framework with new mechanism using optional filed on Internet Protocol Security (IPSec's) Encapsulating Security Payload (ESP) frame [1,8]. Based on [9] and use of Distributed Alternative Binding Cache mechanism (DABC), we will apply this system to accelerate retrieval results.

Acknowledgments

The authors would like to acknowledge the assistance provided by the Network and Communication Technology Research Group, FTSM, and UKM in providing facilities throughout the research. This project is partially supported under the ETP-2014-008.

References

[1] A. S. Ahmed, R. Hassan, and Z. Md Ali, "Eliminate spoofing threat in ipv6 tunnel," in *8th International Conference on Information Science and Digital Content Technology (ICIDT'12)*, vol. 1, pp. 218–222, 2012.

[2] B. M. Bassiouni, "Meta search engines," *Meta Search Engines*, vol. 4, no. 2, 2008.

[3] P. Castells, M. F. Sánchez, and D. Jordi, V. Weadon, "An adaptation of the vector-space model for ontology based information retrieval," *IEEE Transactions on Knowledge and Data Engineering*, 2007.

[4] C. I Chang, *Hyperspectral imaging: techniques for spectral detection and classification*, vol. 1, Springer Science & Business Media, 2003.

[5] R. L. Cilibrasi and P. M. B. Vitanyi, "The google similarity distance," *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, no. 3, 2007.

[6] N. Garman, "Meta search engines.," *Online*, vol. 23, no. 3, pp. 74–78, 1999.

[7] E. J. Glover, S. Lawrence, W. P. Birmingham, and C. L. Giles, "Architecture of a metasearch engine that supports user information needs.," in *CIKM*, pp. 210–216, ACM, 1999.

[8] K. Grewal, G. Montenegro, and M. Bhatia, "Wrapped encapsulating security payload (esp) for traffic visibility.," *RFC 5840*, pp. 1–15, Apr. 2010.

[9] S. S. Hasan, R. Hassan, and F. E. Abdalla, "A new binding cache management policy for nemo and mipv6," *Journal of Theoretical and Applied Information Technology*, vol. 36, no. 1, pp. 113–117, 2012.

[10] R. Hassan, A. A. Al-Khatib, and W. M. H. W. Hussain, "A framework of universiti kebangsaan malaysia patent: Ukm patent," in *19th International Conference on Advanced Communication Technology (ICACT'17)*, pp. 232–236, IEEE, 2017.

[11] H. Jadidoleslamy, "Introduction to metasearch engines and result merging strategies: a survey," *International Journal of Advances in Engineering & Technology*, vol. 1, no. 5, pp. 30–40, 2011.

[12] . R. Pereira Jr. and N. Ziviani, "Retrieving similar documents from the web.," *Journal of Web Engineering*, vol. 2, no. 4, pp. 247–261, 2004.

[13] A. N. Langville and C. D. Meyer, "A reordering for the pagerank problem," *SIAM Journal on Scientific Computing*, vol. 27, no. 6, pp. 2112–2120, 2006.
[14] W. Meng, *Metasearch Engines*, Department of Computer Science, State University of New York at Binghamton; Binghamton, 2008.
[15] R. Nuray and F. Can, "Automatic ranking of information retrieval systems using data fusion," *Information Processing & Management*, vol. 42, no. 3, pp. 595–614, 2006.
[16] I. S. Oberoi and M. Chopra, *Web Search Engines - A Comparative Study, Mälardalen University*, 2010.
[17] C. A. Perez, L. A. Cament, and L. E. Castillo, "Methodological improvement on local gabor face recognition based on feature selection and enhanced borda count," *Pattern Recognition*, vol. 44, no. 4, pp. 951–963, 2011.
[18] S. Robertson, "Understanding inverse document frequency: on theoretical arguments for IDF," *Journal of Documentation*, vol. 60, no. 5, pp. 503–520, 2004.
[19] W. Sander-Beuermann, "Internet information retrieval: The further development of meta-searchengine technology," in *the Internet Summit*, pp. 22–24, 1998.
[20] G. Sidorov, A. Gelbukh, H. Gmez-Adorno, and D. Pinto, "Soft similarity and soft cosine measure: Similarity of features in vector space model," *Computacin Sistemas*, vol. 18, no. 3, pp. 491–504.
[21] B. Zaka, "Empowering plagiarism detection with a web services enabled collaborative network," *Journal of Information Science and Engineering*, vol. 25, no. 5, pp. 1391–1403, 2009.

Biography

Dr. Rosilah Hassan is an Associate Professor at Universiti Kebangsaan Malaysia (UKM) in the Faculty of Information Science and Technology. She received her PhD in Mobile Communication from the University of Strathclyde, United Kingdom in May 2008. She obtained her Master of Electrical (M.E.E) Engineering in Computer and Communication from the Universiti Kebangsaan Malaysia, Malaysia in 1999. Her first Degree was BSc. in Electronic Engineering from Hanyang University, South Korea. Rosilah Hassan worked as an Engineer with Samsung Electronic Malaysia in Seremban, Malaysia before joining UKM in 1997. She is the head of Network Communication Technology Lab in her Faculty. Her research interests are in Mobile Communications, Networking, IoT, Big Data, and Academic Entrepreneurship. She has had experince as an external examiner for PhD and Master for both national and international level. She is also an active member of IEEE, MySET, and IET.

Abdullah Abdulrahman graduated from Al-Ahgaff University Hathramout in 2009. He works in communtiy college from 2009. He enrolled to study Master in University Kebangsaan Malaysia (UKM) in Computer Sceince (Network Technology) in 2015. His research interests are in Software Defined Network (SDN) and IP Security (IPSec), Computer Security.

Dr. Wan M. Hussain, Ph.D, is a university researcher at Graduate School of Business, UKM and internet marketing entrepreneur. He also specializing in technology transfer, commercialization technology and law. He has been involved in technology transfer activity and commercialization technology from university to the industry. He has published numerous articles in international conference and journal publication. Specialties: Technology Transfer, Commercialization University Research, Innovation Technology, Internet Marketing Strategy. Having over 8 years experience in internet marketing, search engine marketing (SEM), search engine optimization (SEO), business development, product, service and commercialization technology.

Dr. Mohammed A. Hassan is assistant Professor at Department of Information Systems, Seiyun Community College, Yemen. He received the B.S. degree in Mathematics and Computer Science from the University of Al-Ahgaff, Yemen, in 2002, the M.S. degree in Computer Science from The University

of Hamdard, India, in 2008 and Ph.D. degree in Computer Science from The Central University of Hyderabad, India, in 2014. His research interests include human visual system models for solving image and video processing problems.

A New Modular Multiplication Method and Its Application in RSA Cryptosystem

Maheshika W.D.M.G. Dissanayake

(Corresponding author: Maheshika W.D.M.G. Dissanayake)

Department of Computer Engineering, Faculty of Engineering, University of Peradeniya, Sri Lanka.
135/1, Inner Harbour Road, Trincomalee, Sri Lanka.
(Email: maheshi14d@gmail.com)

(Received Jan. 28, 2018; revised and accepted Oct. 26, 2018)

Abstract

Modular multiplication is a very important fundamental operation in exponentiation based cryptography. Any problem of security, high cost or speed of a cryptosystem is based on modular exponentiation. Modular exponentiation is realized by a series of modular multiplications. Therefore the performances of an exponentiation based cryptosystem can be increased by using a fast modular multiplication algorithm. In this paper a new modular multiplication algorithm is presented with showing the algorithm is faster than the previous algorithms. The proposed algorithm is based on the following two ideas. The remainder in regard to n can be constructed from the remainder with modulus $(n+1)/2$ and the remainder with modulus $(n-1)/2$. It often happen that $(n+1)/2$ and $(n-1)/2$ can easily be factorized, even if n is a prime number or difficult to be prime factorized. Then, the Chinese Remainder Theorem can be applied to the remainder calculation with those numbers as the modulus.

Keywords: ElGamal Cryptosystem; Modular Exponentiation; Modular Multiplication; Public Key Cryptosystems; RSA Cryptosystem

1 Introduction

Modular multiplication is used in many cryptographic schemes, especially in the RSA public key cryptosystem and the El-Gamal public key cryptosystem. The most important and time-costly part in exponentiation based cryptosystems is modular exponentiation. The speed of an algorithm is one of key research areas of public key cryptosystems, and in order to improve the computation efficiency of modular exponentiation, it is necessary to improve the performance of modular multiplication. It is well known the modular arithmetic is usually performed on integers and in the context of cryptography, we assume all the variables used to perform modular arithmetic are integers unless and otherwise mentioned.

For an example, $c \equiv m^e \bmod n$ and $m \equiv c^d \bmod n$ are the most important operations in RSA public key cryptosystem. Here, m is the message, c is the ciphertext, e is the public key, d is the private key and n is generated by multiplying two large prime numbers, are all considered to be integers. When using RSA, we transform the plaintext into sequence of integers according to certain rule and then divide the sequence into many integer groups. In this case, calculating the modular exponentiation takes extremely large time and space. This case limits the wide use of RSA to some extent. In security, there

are opportunities to attack the public key cryptosystems from a brilliant attacker. So, it is clear that finding a better modular multiplication algorithm to speed up modular exponentiation is an important research area in exponentiation based cryptography.

The proposed method in this paper is based on the idea that the remainder for modulus n is constructed by the remainder with moduli different from n. In the already known method [1] the remainder with modulus $n+1$ and the remainder with modulus $n+2$ was introduced by Akira Hayashi and the method [9] the remainder with modulus $2n+1$ and the reminder with modulus $2n+2$ was introduced by G.A.V. Rama Chandra Rao, P.V. Lakshmi, and N. Ravi Shankar. Ren-Junn Hwang, Feng-Fu Su and Sheng-Hua Shiau [16] also were introduced an efficient method that the moderate factors of $p+1$ and $p-1$ by assuming $p+1$ and $p-1$ can be decomposed into products of mutually prime factors. The proposed method in this paper differs from those methods. In this paper, the modulus n is constructed from the remainder with modulus $(n+1)/2$ and the remainder with modulus $(n-1)/2$. It may be possible to set n so that $(n+1)/2$ and $(n-1)/2$ can easily be prime factorized although the prime factorization of the modulus n is difficult or impossible.

In RSA cryptography, the modulus n is not a prime number, but its prime factorization is not known except for the decipherer. In El-Gamal cryptosystem, the modulus is a prime number. If $(n+1)/2$ and $(n-1)/2$ can easily be prime factorized then the remainder operation can be sped up by applying the Chinese Remainder Theorem.

In Section 2, some definitions and some theorems which are important to understand the proposed method, RSA cryptosystem and El-Gamal cryptosystem are briefly described. The proposed method with proof, numerical examples and the related algorithm are presented in Section 3. Sections 4 gives the estimation of computational complexity of the proposed algorithm and comparing computational complexity and the security of proposed algorithm with the direct method and with the algorithms are introduced in [1], [8] and [14].

2 Remainder Computations

2.1 Chinese Remainder Theorem

Suppose that m_1, m_2, $\cdots$ m_r are pairwise relatively prime positive integers, and let a_1, a_2, $\cdots a_r$ be integers. Then the system of congruences, $X \equiv a_i \bmod m_i$ for $1 \le i \le r$, has a unique solution modulo $M = m_1 m_2 \cdots m_r$, which is given by: $X = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r \bmod M$, where$M_i = M/m_i$ and $y_i \equiv (M_i - 1_)) \bmod m_i$ for $1 \le i \le r$.

2.2 RSA Public Key Cryptosystem

This public key cryptosystem was introduced by R.L. Rivest, A. Shamir and L. Adleman in 1978. This cryptosystem was the first practical public key cryptosystem. Following is the RSA scheme.

1) Two large prime numbers are generated. Let p and q.
2) Modulus n is generated by multiplying p and q.
3) The totient of n is $\Phi(n) = (p-1).(q-1)$ is calculated.
4) Public Key: A prime number e is selected. Where $3 \le e \le \phi(n)$ and gcd $[e, \phi(n)] = 1$; gcd means greatest common divisor.
5) Private Key: The inverse of e with respect to mod $\phi(n)$ is calculated. The RSA function for message m and key k is, $F(m,k) \equiv m^k \bmod n$. Encryption: $m^e \bmod n \equiv c$; Decryption: $c^d \bmod n \equiv m$.

2.3 El-Gamal Cryptosystem [13]

This public key cryptosystem was introduced by Taher Elgamal in 1985.

Step 1: Global elements: Let any large prime number p and a primitive root g of p.

Step 2: Decryption key: x is private, Calculate $g^x \bmod p$; where $x \in Z$. Publish $(p, g, g^x \bmod p)$.

Step 3: Encryption: Let the message is m;$(0 < m < p)$ and choose y - private $(0 < y < p)$. Compute $b = g^y \bmod p$. Then, $c \equiv m.a^y \bmod p$. Send (b, c).

Step 4: Decryption: Compute $b^x \bmod p \equiv a^y$. Then, $m \equiv a^{y^{-1}} \bmod p$.

3 The Proposed Modular Multiplication Method

A new modular multiplication method is presented in this section.

3.1 The Theorem:

Let $y = X \bmod n$, where $0 \leq X \leq (\frac{n-1}{2})^2$. Let

$$y_1 = X \bmod (\frac{n+1}{2}) \quad (1)$$

$$y_2 = X \bmod (\frac{n-1}{2}). \quad (2)$$

Then y can be expressed as follows: If $y_1 > y_2$ and $y_1 + y_2, (n-1)/2$ both are even or both are odd, then

$$y \equiv \frac{(2y_1 + 2y_2 - 1 + n)}{4} (\mathrm{mod} n) \quad (3)$$

Otherwise

$$y \equiv \frac{(2y_1 + 2y_2 - 1 + 3n)}{4} (\mathrm{mod} n) \quad (4)$$

If $y_2 \geq y_1$ and y_1, y_2 both are even or both are odd, then

$$y \equiv \frac{(y_1 + y_2)}{2} (\mathrm{mod} n) \quad (5)$$

Otherwise

$$y \equiv \frac{(y_1 + y_2 + n)}{2} (\mathrm{mod} n) \quad (6)$$

3.2 Proof

From Equation (1) we can get $2y_1 = 2X \bmod (n+1)$, there exists an integer p such that

$$X = (\frac{n+1}{2})p + y_1 \tag{7}$$

From Equation (2) we can get $2y_2 = 2X \bmod (n-1)$, there exists an integer q such that

$$X = (\frac{n-1}{2})q + y_2 \tag{8}$$

From Equation (7),

$$2X = (n+1)p + 2y_1 \tag{9}$$

From Equation (8),

$$2X = (n-1)q + 2y_2 \tag{10}$$

Multiplying Equation (9) by (n-1),

$$2(n-1)X = (n+1)(n-1)p + 2(n-1)y_1 \tag{11}$$

Multiplying Equation (10) by (n+1),

$$2(n+1)X = (n+1)(n-1)q + 2(n+1)y_2 \tag{12}$$

From Equation (11) and Equation (12) we can get

$$2X = (n+1)y_2 - (n-1)y_1 + (q-p)\frac{(n^2-1)}{2} \tag{13}$$

$$4X = 2(n+1)y_2 - 2(n-1)y_1 + (q-p)(n^2-1). \tag{14}$$

First assume that $q - p < 0$. From Equation (2), $y_2 \leq \frac{(n-3)}{2}$ and from Equation (1), $y_1 \geq 0$ it follows the inequality:

$$\begin{aligned} \frac{(n+1)}{2}y_2 - \frac{(n-1)}{2}y_1 + (q-p)\frac{(n^2-1)}{4} &\leq \frac{(n+1)}{2}.\frac{(n-3)}{2} - \frac{(n^2-1)}{4} \\ \frac{(n+1)}{2}y_2 - \frac{(n-1)}{2}y_1 + (q-p)\frac{(n^2-1)}{4} &\leq -\frac{1}{2}(n+1) < 0. \end{aligned}$$

It is concluded that $X < 0$, a contradiction. Since$X \geq 0$, from Equation (13), $q-p$ cannot be negative. Then assume that $q - p > 1$. From Equation (2), $y_2 \geq 0$ and from Equation (1), $y_1 \leq \frac{(n-1)}{2}$, it follows the inequality:

$$\begin{aligned} \frac{(n+1)}{2}y_2 - \frac{(n-1)}{2}y_1 + (q-p)\frac{(n^2-1)}{4} &\geq -\frac{(n-1)}{2}.\frac{(n-1)}{2} + 2.\frac{(n^2-1)}{4} \\ \frac{(n+1)}{2}y_2 - \frac{(n-1)}{2}y_1 + (q-p)\frac{(n^2-1)}{4} &\geq \frac{(n^2+2n-3)}{4} \\ \frac{(n+1)}{2}y_2 - \frac{(n-1)}{2}y_1 + (q-p)\frac{(n^2-1)}{4} &\geq \frac{(n-1)(n+3)}{4} > \frac{(n-1)(n-1)}{4} \end{aligned}$$

It is concluded that $X \geq (\frac{n-1}{2})^2$ a contradiction. Since $X \leq (\frac{n-1}{2})^2$, from Equation (13), q-p cannot be greater than one. Therefore q-p cannot be either negative or greater than one. Now it is clear that $q-p=0$ or $q-p=1$. That is, $q=p$ or $q=p+1$. From q=p and using Equation (13). If $y_2 \geq y_1$ and y_1, y_2 both are even or both are odd, then, $y \equiv \frac{y_1+y_2}{2} (\mathrm{mod} n)$. Otherwise $y \equiv \frac{y_1+y_2+n}{2} (\mathrm{mod} n)$. From $q=p+1$ and using Equation (14). If $y_1 > y_2$ and $y_1+y_2, (n-1)/2$ both are even or both are odd, then $y \equiv \frac{2y_1+2y_2-1+n}{4} (\mathrm{mod} n)$. Otherwise $y \equiv \frac{2y_1+2y_2-1+3n}{4} (\mathrm{mod} n)$.

Example 1. *Let* $n=31$ *and* $X=x^2$ *When* $x=7$, $y_1 \equiv X \mathrm{mod}\ (n+1)/2 \equiv 49 \bmod 16 \equiv 1$ *and* $y_2 \equiv X \bmod (n-1)/2 \equiv 49 \bmod 15 \equiv 4$. *In this case* $y_2 > y_1$; y_1 *odd and* y_2 *even. Applying Equation (6),* $y \equiv \frac{(y_1+y_2+n)}{2} \bmod n = \frac{(1+4+31)}{2} \bmod 31 = \frac{36}{2} \bmod 31 = 18$, *is obtained and it is agreed with the direct calculation of* $49 \bmod 31 \equiv 18$.

Example 2. *Consider the RSA example in the original paper [15]. Let* $n=2773$ *and* $X=x^2$. *When* $x=920$, $y_1 \equiv X \bmod (n+1)/2 \equiv 846400 \bmod 1387 \equiv 330$*and* $y_2 \equiv X \bmod (n-1)/2 \equiv 846400 \bmod 1386 \equiv 940$. *In this case* $y_2 > y_1$; y_1 *and* y_2 *both are even. Applying Equation (5),* $y \equiv \frac{(y_1+y_2)}{2} \bmod n = \frac{(330+940)}{2} \bmod 2773 = \frac{1270}{2} \bmod 2773 = 635 \bmod 2773 = 635$ *is obtained and it is agreed with the direct calculation of* $920^2 \bmod 2773 \equiv 635$. *According to above examples, computation of mod* $\frac{(n+1)}{2}$ *and mod* $\frac{(n-1)}{2}$ *are used instead of the computation mod n.*

3.3 New Remainder Multiplication Algorithm

This algorithm is based on the theorem in Section 3. In this algorithm the Chinese Remainder Theorem is used to derive y_1 and y_2. This helps to improve the speed of calculations.

Preliminary Computation For The Algorithm:

As the preliminary computation, $(n+1)/2$ and $(n-1)/2$ are decomposed into products of mutually prime factors. This needs not be the prime factorization.

$$\frac{(n+1)}{2} = \prod_{i=1}^{k}(p_i) \tag{15}$$

$$\frac{(n-1)}{2} = \prod_{i=1}^{m}(q_i). \tag{16}$$

Assume that the modulus $(n+1)/2$ and $(n-1)/2$ are decomposed as above, the next algorithm receives x such that $0 \leq X \leq ((n-1)/2)^2$, and outputs $y = x^2 \bmod (p_1.p_2.\cdots.p_k)$.

Algorithm 1 Algorithm $newmod(x,p,y)$

1: 1 **Input:** x, $0 \leq x \leq (n-1)/2, p=(p_1, p_2 \cdots p_k)$
2: 2 **Output:** $y = x^2 \bmod (p_1 p_2 \cdots p_k)$
3: 3 **Calculate** $x_i = x \bmod p_i, i = 1, \cdots, k$
4: 4 **Calculate** $a_i = x_i^2, i = 1, \cdots, k$
5: 5 **Calculate** $a_i = a_i \bmod p_i, i = 1, \cdots, k$
6: 6 **Calculate** y by Chinese Remainder Theorem (a,p,y)

Here, $y_1 = x^2 \bmod (n+1)/2$ and $y_2 = x^2 \bmod (n-1)/2$ are obtained by $newmod(x,p,y_1)$ and $newmod(x,q,y_2)$ respectively. The remainder xu can calculate similarly.

Example 3. *Consider the RSA example in the original paper [15]. Let* $n = 2773$. *As preliminary computations,* $(n+1)/2$ *and* $(n-1)/2$ *are decomposed:*

$$\frac{(n+1)}{2} = \frac{2774}{2} = 1387 = 19 \times 73$$
$$\frac{(n-1)}{2} = \frac{2772}{2} = 1386 = 2 \times 3^2 \times 7 \times 11.$$

Let $p_1 = 19$ *and* $p_2 = 73, q_1 = 126$ *and* $q_2 = 11$. *Assume that* $x = 920$ *and* $y = x^2$ *mod* n *is to be calculated. Using the newmod algorithm, Algorithm newmod*$(920, (19 * 73), y_1)$ *is shown in the following: Calculate* $x_1 = 920 \bmod 19 = 8$ *and* $x_2 = 920 \bmod 73 = 44$. *Calculate* $a_1 = 8^2 = 64$ *and* $a_2 = 44^2 = 1936$. *Calculate* $a_1 = 64 \bmod 19 = 7$ *and* $a_2 = 1936 \bmod 73 = 38$. *Solving the following system of congruence equations* $y_1 = 330$ *is obtained. Similarly, using the newmod algorithm, Algorithm newmod*$(920, (126 * 11), y_2)$ *is shown in the following: Calculate* $x_1 = 920 \bmod 126 = 38$ *and* $x_2 = 920 \bmod 11 = 7$. *Calculate* $a_1 = 38^2 = 1444$ *and* $a_2 = 7^2 = 49$. *Calculate* $a_1 = 1444 \bmod 126 = 58$ *and* $a_2 = 49 \bmod 11 = 5$. *Solving the following system of congruence equations* $y_2 = 940$ *is obtained. Since* $y_2 > y_1$; y_1 *and* y_2 *both are even. Applying Equation (5),* $y \equiv (y_1 + y_2)/2 \bmod (2773) = (330 + 940)/2 = 1270/2 = 635$ *is obtained.*

4 Computational Complexity

In this section, the computational complexity of the proposed method is compared with the following 4 methods.

1) The ordinary direct method;
2) Akira Hayashi method [1];
3) G.A.V. Rama Chandra Rao, P.V. Lakshmi, and N. Ravi Shankar method [8];
4) Ren-Junn Hwang, Feng-Fu Su and Sheng-Hua Shiau method [14].

Note that the computational complexity is considered only for the multiplications and divisions and assume that the parallel computation is not used in each multiplication or division. It is assumed that the ordinary straightforward computation is applied. The computational complexity for the multiplication and the division describes as follows:

- Mul (a, b) = Computational complexity for $a \times b$ bit number $= b(a + b)$;
- Div (a, b)= Computational complexity for $a \div b$ bit number $= b(a - b)$.

The computational complexity in the preliminary computation is not included and assume that n consists of a bits and $p_1, p_2, \cdots p_k$ and $q_1, q_2, \cdots q_m$ consists of b bits at the maximum.

4.1 Ordinary Direct Method

The computational complexity of the direct method calculation of $x^2 \bmod n$ = The multiplication of two a-bit numbers + The division of $2a$-bit number by a-bit number $= Mul(a, a) + Div(2a, a) = 3a^2$.

4.2 Computational Complexity of Akira Hayashi Method [1]

In 1st step-The division of a-bit number by b-bit number; In 2nd step-The multiplication of two b-bit numbers; In 3rd step-The division of $2b$-bit number by b-bit number; Therefore the computational complexity for each i = $Div(a,b)+Mul(b,b)+Div(2b,b) = b(a+2b)$. In solving the system of congruence equations, = The multiplication of b-bit number and a-bit number + The division of $(a+b)$ bit number by a-bit number $=Mul(a,b) + Div(a+b,a) = b(2a+b)$. Therefore the computational complexity for proposed method $=b(a+2b) + b(2a+b) = 3b(a+b)$.

4.3 Computational Complexity of G.A.V. Rama Chandra Rao, P.V. Lakshmi, and N. Ravi Shankar Method [8]

In 1st step-The division of a-bit number by b-bit number; In 2nd step-The multiplication of two b-bit numbers; In 3rd step-The division of 2b-bit number by b-bit number; Therefore the computational complexity for each i = $Div(a,b)+Mul(b,b)+Div(2b,b) = b(a+2b)$. In solving the system of congruence equations, = The multiplication of b-bit number and a-bit number + The division of$(a+b)$ bit number by a-bit number $=Mul(a,b) + Div(a+b,a) = b(2a+b)$. Therefore the computational complexity for proposed method $=b(a+2b) + b(2a+b) = 3b(a+b)$.

4.4 Computational Complexity of Ren-Junn Hwang, Feng-Fu Su and Sheng-Hua Shiau Method [14]

The computational complexity of modular exponentiation $x^y \bmod z = 1.5l(y)[M(l(z))+2Mod(l(z))+1]$. Where, l(k) is denoted by the bit length of k, M(k) is denoted by the computational complexity of multiplication and Mod (k) is denoted by the computational complexity of modulus, which are associated with the bit length of k.

4.5 Computational Complexity of the Proposed Method

In 1st step-The division of $a/2$-bit number by b-bit number; In 2nd step-The multiplication of two b-bit numbers; In 3rd step-The division of 2b-bit number by b-bit number; Therefore the computational complexity for each i = $Div(a/2,b)+Mul(b,b)+Div(2b,b) = b(\frac{a}{2}-b)+2b^2+b^2 = b(\frac{a}{2}+2b)$. In solving the system of congruence equations, = The multiplication of b-bit number and $a/2$ -bit number + The division of $(a/2+b)$ bit number by $a/2$ -bit number $=Mul(\frac{a}{2},b)+Div(\frac{a}{2}+b,\frac{a}{2}) = b(\frac{a}{2}+b)+\frac{a}{2}(\frac{a}{2}+b-\frac{a}{2}) = b(a+b)$. Therefore the computational complexity of the proposed method $=b(\frac{a}{2}+2b)+b(a+b) = \frac{3b}{2}(a+2b)$.

4.6 Comparisons: Computational Complexity

The computational complexity of the calculation of $x^2 \bmod n$ (See Figure 1).

According to the Figure 1, it is clear that when $b= a/2$, the proposed new methods is better than the other three methods including the ordinary direct method. But, when $b= a$,the proposed new method is better than the Akira Hayashi Method and G.A.V. Rama Chandra Rao, P.V. Lakshmi, and N. Ravi Shankar method. But the ordinary direct method is the best.

When $b = \frac{a}{2}$		
Akira Hayashi Method	**G.A.V. Rama Chandra Rao, P.V. Lakshmi, and N. Ravi Shankar method**	**The Proposed New Method**
The computational complexity of the method $= 3\frac{a}{2}(a+\frac{a}{2})$ $= \frac{9}{4}a^2$ $= \frac{3}{4} \times (3a^2)$ $= \frac{3}{4} \times Direct\ method$	The computational complexity of the method $= 3\frac{a}{2}(a+\frac{a}{2})$ $= \frac{9}{4}a^2$ $= \frac{3}{4} \times (3a^2)$ $= \frac{3}{4} \times Direct\ method$	The computational complexity of the method $= \frac{3}{2}.\frac{a}{2}(a+2.\frac{a}{2})$ $= \frac{3}{2}a^2$ $= \frac{1}{2} \times (3a^2)$ $= \frac{1}{2} \times Direct\ method$
When $b = a$		
The computational complexity of the method $= 3a(a+a)$ $= 6a^2$ $= 2 \times (3a^2)$ $= 2 \times Direct\ method$	The computational complexity of the method $= 3a(a+a)$ $= 6a^2$ $= 2 \times (3a^2)$ $= 2 \times Direct\ method$	The computational complexity of the method $= \frac{3a}{2}(a+2a)$ $= \frac{9}{2}a^2$ $= \frac{3}{2} \times (3a^2)$ $= \frac{3}{2} \times Direct\ method$

Figure 1: Comparisons of computational complexity

4.7 Comparisons: Security

Security advantages of this method are described in briefly, here. Security is the most important feature of a cryptosystem. On the other hand, modular exponentiation is the core operation of a cryptosystem. When n and m are very large numbers, evaluating x^n mod m is an operation consuming very long time. Therefore to reduce the time and cost, small exponents are chosen. But, this case can jeopardize the cryptosystem and provides big opportunities to adversaries. Hence, to increase the security of a cryptosystem it is essential use a large exponent. The computation time problem of modular exponentiation can be reduced by using a fast modular multiplication algorithm. Therefore, the introduced new modular multiplication method is better than the other multiplication methods, to increase security of a cryptosystem.

5 Conclusion

In this paper, it is shown that the remainder for n can be determined from the remainders y_1 and y_2 with those as the modulus and also has shown that the Chinese Remainder Theorem can be applied to the calculation of y_1 and y_2. The remainder multiplication can be realized with less computational complexity. It is shown that the speed of modular exponentiation based cryptosystems like RSA cryptosystem can be improved by the proposed new method. The effectiveness of the proposed method depends strongly on whether or not $(n+1)/2$ and $(n-1)/2$ can be decomposed into small prime factors.

6 Acknowledgment

I would like to thank Dr. Sandirigama M. (Department of Computer Engineering, Faculty of Engineering, University of Peradeniya, Sri Lanka), Dr. Ishak M.I.M. (Department of Engineering Mathematics, Faculty of Engineering, University of Peradeniya, Sri Lanka) and Dr. Alawathugoda J. (Department of Computer Engineering, Faculty of Engineering, University of Peradeniya, Sri Lanka) for providing helpful feedback and advice in this research. I also gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] G. Alia, E. Martinelli,Fast modular exponentiation of large numbers with large exponents, *Journal of System Architecture, Elsevier, 47*, pp.1079-1088, 2002.

[2] M. Bansal, A. Kumar, A. Devrari, A. Bhat, Implementation of modular exponentiation using Montgomery algorithms, *International Journal of Scientific and Engineering Research*, Vol.6, Issue 11, pp. 1272-1277, Nov.2015.

[3] E. F. Brickell,D. M. Gordon, K. S. McCurley, D. B. Wilson, Fast exponentiation with precomputation, *Proceeding of Eurocrypt92, Springer-Verlag*, pp. 200-207, 1993.

[4] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms",*IEEE Transactions on Information Theory*,31, pp. 469-472, 1985.

[5] D. M. Gordon, "A survey of fast exponentiation methods", *Journal of Algorithms*, pp. 129-146, 1998.

[6] A. Hayashi,"A new fast modular multiplication method and its application to modular exponentiation based cryptography", *Electronics and Communications in Japan*, Part 3, Vol.83, No.12, pp. 88-92 2000.

[7] S. M. Hong, S. Y. Oh, H. Yoon, New modular multiplication algorithm for fast modular exponentiation", *Advances in Cryptography- Eurocrypt96, LNCS 1070, Springer-Verlag*, pp. 166-177, 1996.
[8] R. J. Hwang, F. F. Su, and S. H. Shiau, An efficient modulo P multiplication algorithm with moderate factors of P+1 and P-1, *Communication of Mathematics Science*, vol. 5, no. 2, pp.383-389, 2007.
[9] M. E. Kaihara, N. Takagi, A hardware algorithm for modular multiplication/division, *Computers, IEEE Transactions on 54.1*, pp. 12-21, 2005.
[10] C. K. Koc, "High-speed RSA implementation",*RSA Laboratories*, Ver.2.0, pp.9-51, Nov. 1991.
[11] S. P. Kumar, K.J.J. Kumar, B. Partibane, Efficient modular exponentiation architectures for RSA algorithm, *International Journal of Engineering Research in Electronic and Communication Engineering*, Vol.03, Issue 05, pp. 230-234, 2016.
[12] A. U. Maheshwari, P. Durairaj, A new modulo n multiplication algorithm with moderate factors of (2n+2) and (2n+6), *International Journal of Computer Science Engineering and Information Technology Research*, Vol.4, Issue 2, pp. 177-184, 2014.
[13] M. Moayedi, A. Rezai, Design and evaluation of novel effective Montgomery modular multiplication architecture, *International Journal of Security and Its Application*, Vol.10, No.10, pp.261-270, 2016.
[14] C. T. Poomagal, G. A. S. Kumar, Modular multiplication algorithm in cryptographic processor: A review and future directions, *International Journal of Advances in Computer and Electronics Engineering*, Vol. 02, Issue 02, pp. 28-33, 2017.
[15] G. A. V. Rama Chandra Rao, P. V. Lakshmi, N. Ravi Shankar, "A new modular multiplication method in public key cryptosystem", *International Journal of Network Security*, Vol.15, No.1, pp.23-27, 2013.
[16] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signature and public key cryptosystems",*Communications of the ACM*, Vol.21, pp. 120-126, 1978.
[17] M. Styugin, Establishing systems secure from research with implementation in encryption algorithms, *International Journal of Network Security*, Vol.20,No.1, pp.35-40, Jan.2018.
[18] N. Thampi, M. E. Jose,Montgomery multiplier for faster cryptosystems, *Procedia Technology 25, Elsevier*, pp. 392-398, 2016.
[19] S. Vollala, N. Ramasubramanian, Energy efficient modular exponentiation for public-key cryptography based on bit forwarding techniques, *Journal Information Processing Letters*, Vol. 119, Issue C, pp. 25-38, 2017.

Biography

Maheshika W.D.M.G. Dissanayake received her BSc degree in Computer Science, Mathematics and Applicable Mathematics from University of Ruhuna, Sri Lanka. Now, she is an MPhil candidate at Department of Computer Engineering, Faculty of Engineering, University of Peradeniya, Sri Lanka. Her research interests include Cryptography and Network Security.

Survey on Machine Learning Techniques: Concepts and Algorithms

Diaa Salama Abdul Minaam[1] and Eslam Amer[2]

(Corresponding author: Diaa Salama Abdul Minaam)

Information Systems department , Faculty of Computers and Informatics, Benha University, Egypt[1]

Faculty of Computers and Informatics, Misr International University, Egypt[2]

(Email: diaa.salama@fci.bu.edu.eg)

(Received Aug. 1, 2018; revised and accepted Nov. 3, 2018)

Abstract

Machine Learning is an application of artificial intelligence that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. The main idea of any machine learning application is that we have data set about any topic we try to make prediction for it and apply this data set on machine learning algorithm to get intelligence app. So in this paper we try to discover machine learning algorithm with some data sets if we can apply all machine learning algorithms on any data set or some data set need specific machine learning algorithm.

Keywords: Classification; Clustering; Prediction

1 Introduction

The primary goal of technology is helping people to improve their quality of life. Technology can assist us with our limitations. So we can use it to improve our Communication, Work and Learning [6].

Machine Learning focus on the development of computer programs that can access data and use it learn for themselves. The main idea of what are going to do in this paper we have some data set apply on it some of machine learning algorithms and discover if we get intelligence app or not the steps is as shown in (Figure 1)

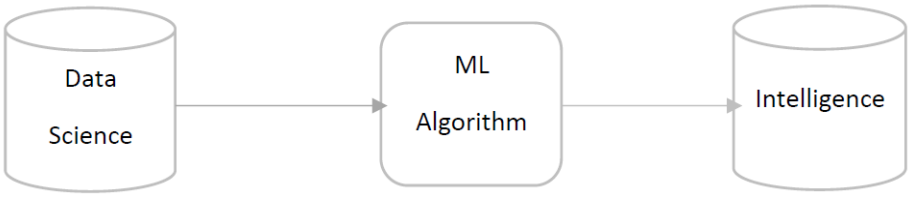


Figure 1: Machine learning steps

In this paper we try to discover if machine algorithm working with any data set or can work fine with data set and others not give good result. So we are going to use some data sets called amazon_baby,

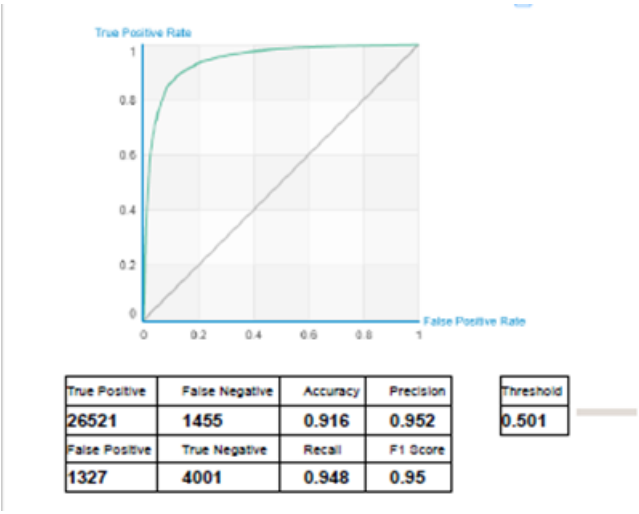
people_wiki and home_data and these data sets is working fine in predictions with specific machine algorithms (Classification, Clustering and Regression) [3,8,13,14] so we are going to use all algorithms with each data sets and discover if is all algorithm working fine with all data set or not [4,7,10,12].

2 Classification Algorithm

The definition of classification algorithm is assigning objects to predefined classes. And classification algorithm is supervised algorithms this mean that training set of pre-defined examples [1,2,5,9,11,15].

2.1 Classification with Classification

The data set working with classification called amazon_baby. So we are going to use tools to use it to help us in predications of coursera course with cloud technology called ipython juypter. At first we are going to discover the data set to know how to working on It to make predication. These data set have 183531 record to make predication and have three columns called name, review and rating so we are going to make predication through rating so at first we are going to use count_words algorithms to count words in the same review so we are going to add new column in the data set called word_count after doing this we are going to test on training sentence to discover its review so we are going to predict for specific rating that more than rate 3 and create new column called sentiment for prediction present if 1 or less than this and we are going to test with 80 percentage training data and others for testing data and apply on these data logistic classifier on the column word_count and after apply this we get this graph as show in (Figure 2)



True Positive	False Negative	Accuracy	Precision
26521	1455	0.916	0.952
False Positive	True Negative	Recall	F1 Score
1327	4001	0.948	0.95

Threshold
0.501

Figure 2: Result of applying logistic classifier on data set

So now we success with classification algorithm with these data set and now can predict with any data.

2.2 Classification with Clustering

The data set working with classification called amazon_baby we try to use it with clustering algorithm. So we are going to use tools to use it to help us in predications of coursera course with cloud technology called ipython juypter. At first we are going to discover the data set to know how to use these data set with cluster algorithm. The main idea of clustering is grouping data depend on distance between these data by the similarity between them and in this data set and when we try to apply classification algorithm on these data and add new column called word_count to count the words in review column and we try to give more weight to informative words we weight them by their tf_idf scores and apply k nearest techniques on data set and after that we can apply classification on these data set.

2.3 Classification with Regression

The data set working with classification called amazon_baby we try to use it with regression algorithm. So we are going to use tools to use it to help us in predication of coursera course with cloud technology called ipython juypter. At first we are going to discover the data set to know how to use these data set with regression algorithm. The main idea of regression is to predict the output of data based on relationship between a dependent variable and one or more independent variables and when we try to apply regression algorithm on these data set we use the regression on the rate column only as a feature we find that max error is 3.2852451 so we can apply regression algorithm on these data set.

3 Clustering

The definition of clustering algorithm is dividing the data points into a number of groups such that data point in the same groups are more similar to other data points in the same group. And clustering algorithm is an unsupervised machine learning approach. No labels provided.

3.1 Clustering with Clustering

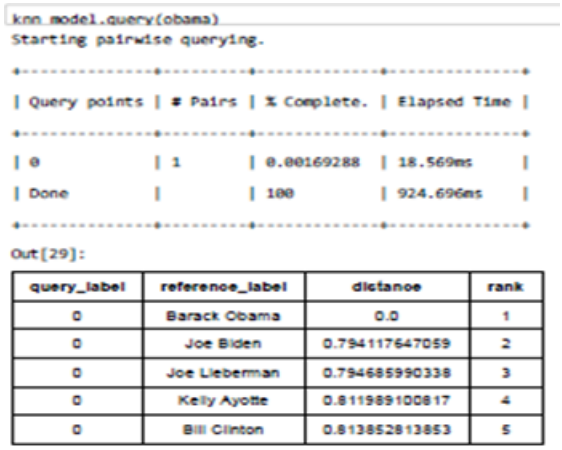
The data set working with Clustering called people_wiki. So we are going to use tools to use it to help us in predications of coursera course with cloud technology called ipython juypter. At first we are going to discover the data set to know how to working on It to make predication. These data set have 59071 record to make predication and have three columns called Uri, name and text so we are going to make predication through text so at first we are going to use count_words algorithms to count words in the text so we are going to add new column in the data set called word_count after doing this we are going to use technique of tf_idf on the word_count column and we are going to use the cosine similarity to consists these data to groups depend on the similarity between them and this happen by using nearest neighbor model for document retrieval to the distance between words and we are going to test on it by passing any text to know if this success or not and actually we success as shown in (Figure 3).

3.2 Clustering with Classification

We cannot apply classification on these data set.

3.3 Clustering with Regression

The data set working with clustering called people_wiki we try to use it with regression algorithm. So we are going to use tools to use it to help us in predication of coursera course with cloud technology called ipython juypter. At first we are going to discover the data set to know how to use these data



```
knn_model.query(obama)
Starting pairwise querying.
+--------------+---------+-------------+--------------+
| Query points | # Pairs | % Complete. | Elapsed Time |
+--------------+---------+-------------+--------------+
| 0            | 1       | 0.00169288  | 18.569ms     |
| Done         |         | 100         | 924.696ms    |
+--------------+---------+-------------+--------------+
Out[29]:
```

query_label	reference_label	distance	rank
0	Barack Obama	0.0	1
0	Joe Biden	0.794117647059	2
0	Joe Lieberman	0.794685990338	3
0	Kelly Ayotte	0.811989100817	4
0	Bill Clinton	0.813852813853	5

Figure 3: Result of testing text

set with regression algorithm. The main idea of regression is to predict the output of data based on relationship between a dependent variable and one or more independent variables and when we try to apply regression algorithm on these data set by adding new column called rating with constant value is 1 but we find that there is a problem and may not provide accurate predictions for validation on testing data set.

4 Regression

The definition of regression used to predict the output of data based on relationship between a dependent variable and one or more independent variables.

4.1 Regression with Regression

The data set working with Regression called home_data. So we are going to use tools to use it to help us in predications of coursera course with cloud technology called ipython juypter. At first we are going to discover the data set to know how to working on It to make predication. These data set make predication and have more columns called id, date, price, bedrooms, bathrooms, sqtfit_live, view, condition, grade, sqft_above, sqft_basement, yr_built, yr_review, long, sqft_living15 and sqft_lot15 so we are going to make predication through price with sqft_living and we discover on the data set to know the result and we got the result as show in (Figure 4).

Now we are going to apply regression model on the result above with training data set with 80 percentage and other 20 percentage for testing and after applying this we got the result as show in (Figure 5).

And after we applying regression model on data set and try to testing it we have success in applying it to prediction.

4.2 Regression with Classification

The data set working with Regression called home_data we try to use it with classification algorithm. So we are going to use tools to use it to help us in predications of coursera course with cloud technology

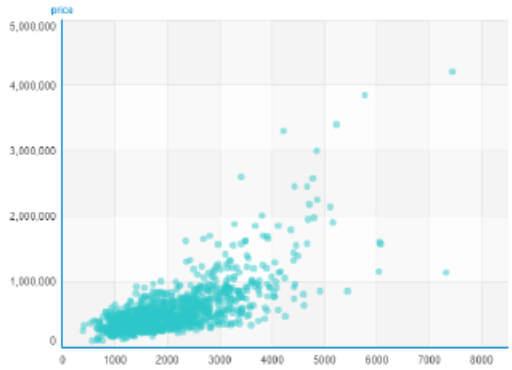


Figure 4: Result of discover home price depend on the sqft_living

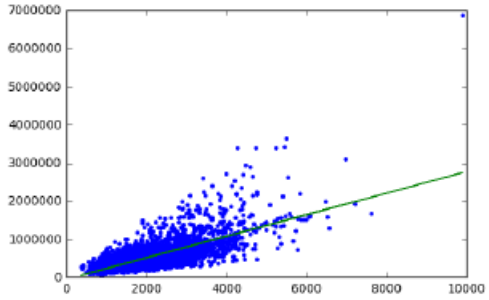


Figure 5: Result of applying regression model on data set

called ipython juypter. At first we are going to discover the data set to know how to use these data set with classification algorithm. The main idea of classification is to predict data depend on predefined data and in this data set we try to apply classification algorithm on it and after applying it on data set we find that give predications of data with max error 3.285

4.3 Regression with Clustering

The data set working with Regression called home_data we try to use it with clustering algorithm. So we are going to use tools to use it to help us in predications of coursera course with cloud technology called ipython juypter. At first we are going to discover the data set to know how to use these data set with cluster algorithm. The main idea of clustering is grouping data depend on distance between these data by the similarity between them and in this data set we try to apply clustering algorithm on it and after applying it on data set we find that give low predications of data with max error 1.34176.

5 Code Sample

1) DB Classification using Classification Algorithm: See Figure 6;

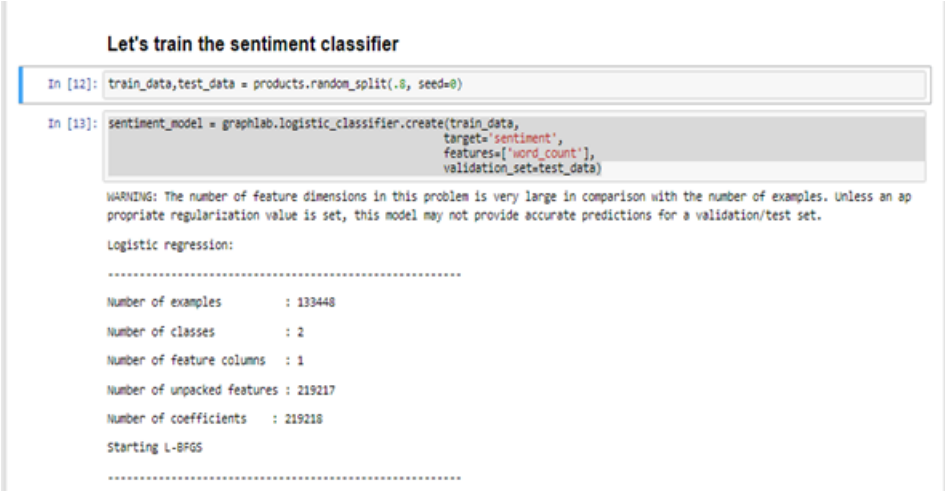


Figure 6: DB Regression using Regression Algorithm

2) DB Classification using Clustering Algorithm: See Figure 7;

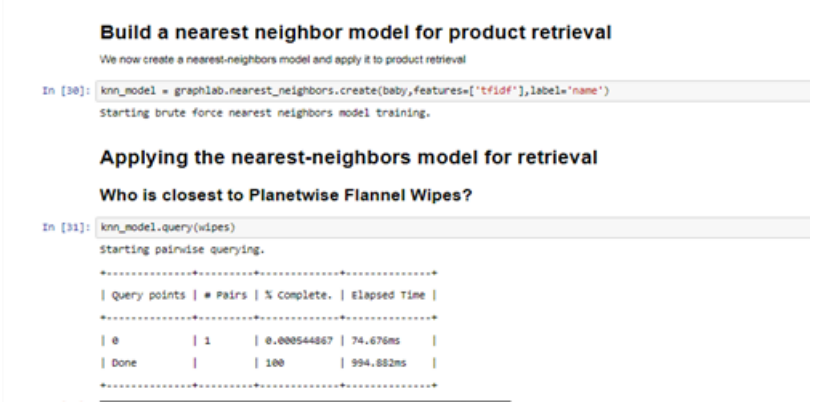


Figure 7: DB Regression using Regression Algorithm

3) DB Classification using Regression Algorithm: See Figure 8;

4) DB Clustering using Regression Algorithm: See Figure 9;

5) DB Clustering using Clustering Algorithm: See Figure 10;

6) DB Clustering using Classification Algorithm: We cannot apply classification algorithm on this dataset because it isn't contains any column to do calculations of algorithm on it.

7) DB Regression using Classification Algorithm: See Figure 11;

8) DB Regression using Clustering Algorithm: See Figure 12;

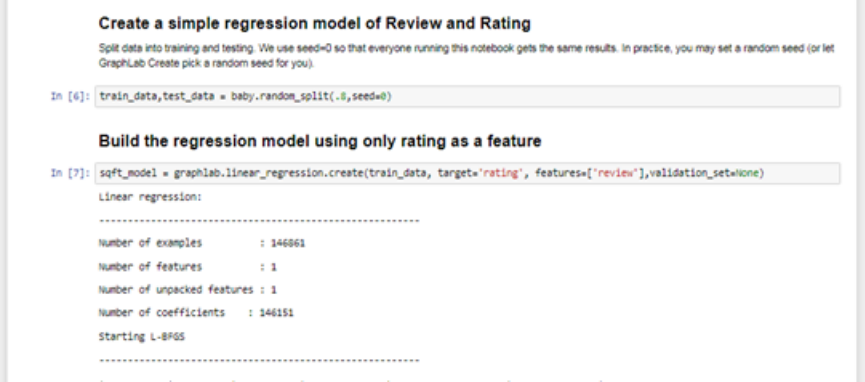


Figure 8: DB Regression using Regression Algorithm

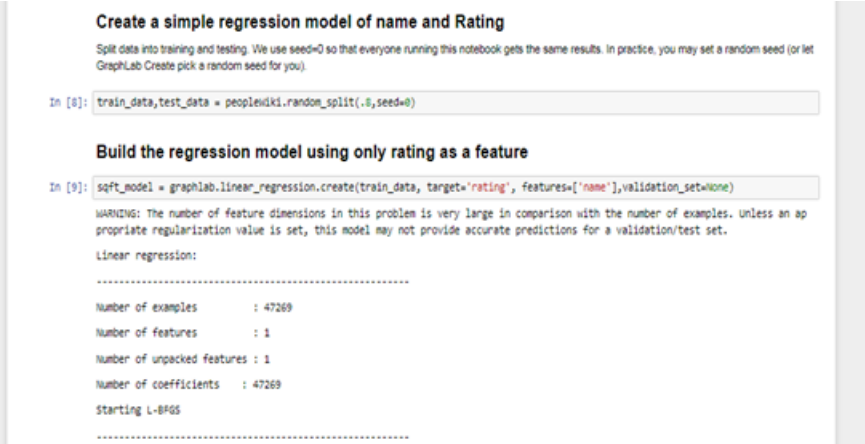


Figure 9: DB Regression using Regression Algorithm

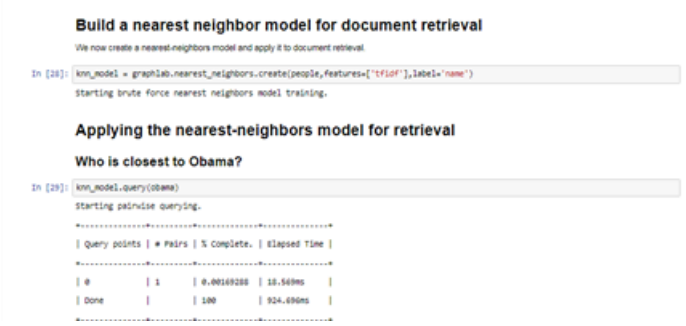


Figure 10: DB Regression using Regression Algorithm

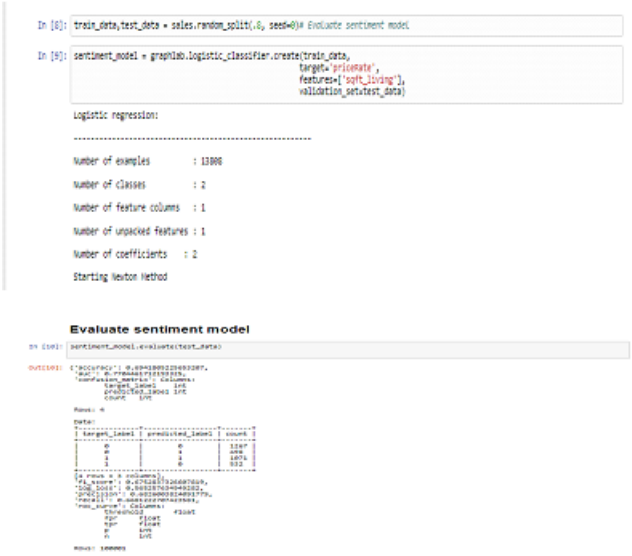


Figure 11: DB Regression using Regression Algorithm

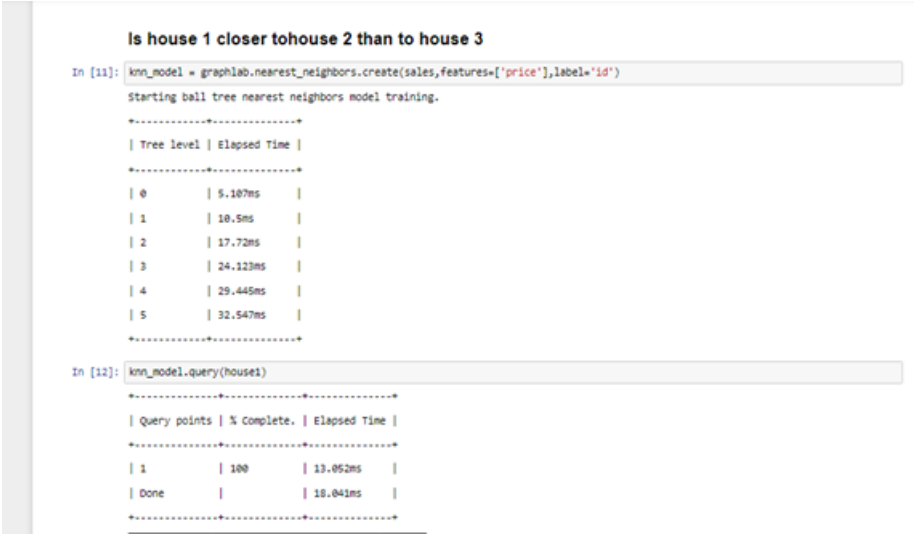


Figure 12: DB Regression using Regression Algorithm

9) DB Regression using Regression Algorithm: See Figure 13.

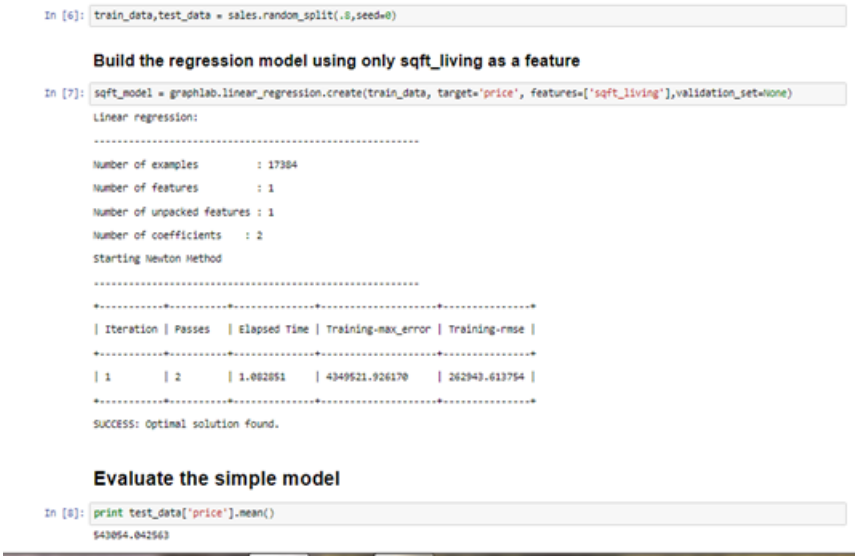


Figure 13: DB Regression using Regression Algorithm

6 Conclusion

In this paper we try to discover if machine learning algorithm working with any data set or each algorithm will work fine with some data set and with other not working fine. And in this paper with the data sets we discover that some algorithm will work with data set and others cannot achieve our goal as show in Table 1.

Table 1: Some algorithm will work with data set

Algorithm/Database	Classification	Clustering	Regression
Classification	Max error: Rmse:	— —	Max error: 3.285 Rmse: 2.4189
Clustering	Max error: Rmse:	Max error: Rmse:	Max error: 1.34176 Rmse: 1.34711921
Regression	Max error: 3.28524518 Rmse: 2.41897763	Max error: 1.34717629 Rmse: 1.34711922	Max error: 4143550.888 Rmse: 256191.028

References

[1] R. Boada, R. Borkowski, and I. T. Monroy, "Clustering algorithms for Stokes space modulation format recognition," *Optics Express*, vol. 23, no. 12, pp. 521-531, June 2015.

[2] R. Borkowski, D. Zibar, A. Caballero, V. Arlunno, and I. T. Monroy, "Stokes space-based optical modulation format recognition for digital coherent receivers," *IEEE Photonics Technology Letters*, vol. 25, no. 21, pp. 2129-2132, Nov. 2013.
[3] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153-1176, Oct. 2015.
[4] D. S. A. Elminaam, and N. R. Mohammed, "Flower Classification and Its Physiological and Psychological Relaxing Effects of Viewing Flowers for Sportive," in *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 124-134, June 2018.
[5] F. N. Khan, K. Zhong, W. H. Al-Arashi, C. Yu, C. Lu, and A. P. T. Lau, "Modulation format identification in coherent receivers using deep machine learning," *IEEE Photonics Technology Letters*, vol. 28, no. 17, pp. 1886-1889, Sep. 2016.
[6] S. Marsland, *Machine learning: An algorithmic perspective*, CRC press, 2015.
[7] J. Mata, I. de Miguel, R. J. Durn, N. Merayo, S. K. Singh, A. Jukan, and M. Chamania, "Artificial intelligence (AI) methods in optical networks: A comprehensive survey," *Optical Switching and Networking*, vol. 28, pp. 43-57, 2018.
[8] T. J. O'Shea, T. Erpek, and T. C. Clancy, "Deep learning based MIMO communications," in *arXiv preprint arXiv:1707.07980*, July 2017.
[9] T. Panayiotou, S. Chatzis, and G. Ellinas, "Performance analysis of a data-driven quality-of-transmission decision approach on a dynamic multicast-capable metro optical network," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 9, no. 1, pp. 98-108, Jan. 2017.
[10] I. Sartzetakis, K. Christodoulopoulos, C. Tsekrekos, D. Syvridis, and E. Varvarigos, "Quality of transmission estimation in WDM and elastic optical networks accounting for space-spectrum dependencies," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 8, no. 9, pp. 676-688, Sep. 2016.
[11] T. Tanimura, T. Hoshida, J. C. Rasmussen, M. Suzuki, and H. Morikawa, "OSNR monitoring by deep neural networks trained with asynchronously sampled data," in *OptoElectronics and Communications Conference (OECC'16)*, IEEE, pp. 1-3, 2016.
[12] J. Thrane, J. Wass, M. Piels, J. C. M. Diniz, R. Jones, and D. Zibar, "Machine learning techniques for optical performance monitoring from directly detected PDM-QAM signals," *IEEE/OSA Journal of Lightwave Technology*, vol. 35, no. 4, pp. 868-875, Feb. 2017.
[13] H. Ye, G. Y. Li, and B. H. Juang, "Power of deep learning for channel estimation and signal detection in OFDM systems," *IEEE Wireless Communications Letters*, Sep. 2017.
[14] D. Zibar, M. Piels, R. Jones, and C. G. Schaeffer, "Machine learning techniques in optical communication," *IEEE/OSA Journal of Lightwave Technology*, vol. 34, no. 6, pp. 1442-1452, Mar. 2016.
[15] D. Zibar, J. Thrane, J. Wass, R. Jones, M. Piels, and C. Schaeffer, "Machine learning techniques applied to system characterization and equalization," in *Optical Fiber Communications Conference (OFC'16)*, pp. 1-3, Mar. 2016.

Biography

Diaa Salama Abdul-Minaam was born on November 23, 1982, in KafrSakr, Sharkia, Egypt. He received the B.S from Faculty of Computers &Informatics, Zagazig University, Egypt in 2004 with grade very good with honor, and obtains the master degree in information system from the faculty of computers and information, menufia university, Egypt in 2009 specializing in Cryptography and network security. He obtained his Ph.D. degree in information system from the faculty of computers

and information, menufia university, Egypt in 2015. He is currently a Lecturer in Information systems department, Faculty of Computers and Information, Benha University, Egypt since 2011. He has worked on a number of research topics.Diaa has contributed more than 30+ technical papers in the areas of wireless networks, wireless network security, Information security and Internet applications , Cloud Computing , Mobile Cloud Computing, Internet of Things, Machine learning in international journals, international conferences, local journals and local conferences. He majors in Cryptography, Network Security, IoT, Big Data, Cloud Computing. (Mobile: +201019511000 ; E-mail: ds_desert@yahoo.com)

Eslam Amer working as associate professor of computer science at Misr International University. His main research interests are mainly related to Information retrieval, natural language processing. He published several publications in the field of NLP and information retrieval. He is passionate to work in different domains where can apply NLP, IR, and machine learning.

A New Sinusoidal Quadrature Oscillator for Electronics Engineering

Kushaagra Maheshwari
(Corresponding author: Kushaagra Maheshwari)

G.L. Bajaj Institute of Technology & Management
Plot No.2, Knowledge Park III, Greater Noida, Uttar Pradesh 201306, India
(Email: kushaagramaheshwari02@gmail.com)
(Received Aug. 25, 2018; revised and accepted Nov. 3, 2018)

Abstract

This paper presents new sinusoidal oscillator employing operational amplifiers and six passive components with the advantage of easy tuning of oscillator frequency. Separate resistive elements control the frequency and the condition of oscillation. The easy control over the frequency and condition of oscillation through separate resistors makes the circuit practically feasible. The new proposed circuit provides three outputs with progressive quadrature relationship. Simulation results are presented using TINA software. The circuit is further experimentally tested for workablity by using different set of components. The new proposed circuit is verified using low cost general purpose operational amplifier.

Keywords: Circuit Design; Operational Amplifier; Quadrature Oscillators

1 Introduction

Voltage controlled voltage source operational amplifiers, also referred to as voltage operational amplifiers are the most versatile analog building block for voltage mode circuits and systems. The voltage operational amplifiers (simply operational amplifiers) find applications in a wide range of linear and non linear applications. Sinusoidal oscillators form the basic block of a large number of electronic instrumentation and communication systems. The oscillators providing more than one sinusoidal signals are known as quadrature and multi phase oscillators, the former providing a 90^o phase separated signals, while the latter generates multiple outputs for designed phase shifts separation. The quadrature and multiphase sinusoidal oscillators find wide ranging applications as standard test signals, in measurement and instrument systems and in communication systems. For instance, a quadrature oscillator providing 90^o separated signals is an integral part of a large number of communication circuits. Similarly two phase inverted sine waves may be used for phase shift keying, Another example of four quadrature signals application could be in quadrature phase shift keying, Some of these applications and many other such applications have been the motivating factor for a large number of circuits being proposed in open literature [4, 8, 10, 11].

The available oscillator circuits employing operational amplifiers (opamps) are based on the use of two or three opamps. The circuits provide quadrature signals while employing different passive component count [4, 8, 10]. The proposed circuit in this work is based on the use of four opamps while

providing three signals. However, the new proposed circuit benefit from an easy tuning of oscillation frequency, which is fully independent from the oscillation condition. The proposed circuit employs six passive components: two capacitors and four resistors. Whereas the two resistors control the oscillation frequency, the other two resistors control the oscillation condition. The subsequent sections deliberates on the proposed circuit description, comparison with existing circuits, simulations results, experimental results and concluding discussion.

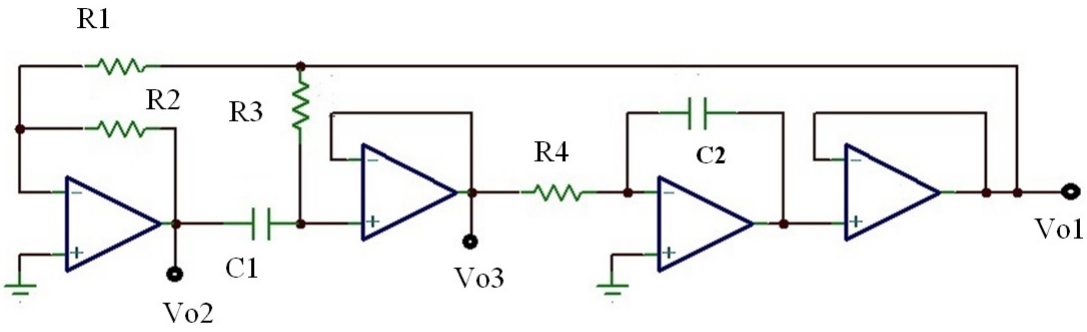


Figure 1: Proposed opamp based quadrature oscillator circuit

2 The Proposed Circuit

The proposed circuit which realizes an oscillator with three 90^o progressive phase shift is shown in Figure 1. The circuit employs four opamps and six passive components. It may be noted that two of the opamps are used as voltage followers, one opamp is configured as an inverter and one opamp is configured as integrator. The circuit is characterized by the following characteristic equation.

$$s^2 + s(\frac{1}{R_3C_1} - \frac{R_2}{R_1R_4C_2}) + \frac{1}{R_3R_4C_1C_2} = 0. \tag{1}$$

Equation (1) yields the following frequency of oscillation (FO) and condition of oscillation (CO) respectively.

$$FO: \qquad \omega_0 = \frac{1}{\sqrt{R_3R_4C_1C_2}} \tag{2}$$

$$CO: \qquad R_4C_2 \leq \frac{R_2R_3C_1}{R_1} \tag{3}$$

As a simple design, involving equal resistors (R_3 and R_4) and equal capacitors simplifies the CO expression as below.

$$CO: R_2 \geq R_1. \tag{4}$$

From the above equations it is evident that the frequency of oscillation can be independently controlled without affecting the condition of oscillation. For example, the CO can be adjusted through R_1 and

R_2 whereas the FO can be independently adjusted through R_3 and R_4. This feature makes the circuit specially attractive, because it allows easy and independent control over the frequency and condition of oscillation. The three outputs of oscillator V_{o1}, V_{o2} and V_{o3} are related as below.

$$v_{o3} = -sR_4C_2v_{o1} \quad (5)$$

$$v_{o2} = -v_{o1}. \quad (6)$$

Equations (5) and (6) imply that v_{o1} leads v_{o3} by 90^o and v_{o2} is phase inverted with respect to v_{o1}. Therefore, the proposed circuit generates three outputs with a progressive 90^o phase shift. Next, the sensitivity of FO to various resistive components is analyzed and found as below.

$$S^{FO}_{R_3,R_4} = -1 \quad (7)$$

$$S^{FO}_{R_1,R_2} = 0. \quad (8)$$

Equations (7) and (8) show that the sensitivity of FO to R_1 and R_2 is zero, the property that makes the circuit easily tune-able through R_3 and R_4. The new proposed circuit is now compared with the existing quadrature oscillators based on operational amplifiers. The Table 1 shows the comparative study, which clearly suggests that the proposed circuit benefit from easy and completely independent control over the oscillator frequency and condition of oscillation, while providing three outputs. It is further seen that the new circuit requires fewer passive components for the available features. The new proposed circuit based on opamps is low cost solution as compared to higher frequency oscillators based on modern active elements [1–3, 5–7, 9].

Table 1: Comparative study

Ref.	Number of opamps	Passive element count	No. of 90^o shifted outputs	FO and CO control complete independence
[10]	2	7	2	No
[4]	3	8	2	No
[8] Fig. 8	2	6	2	No
[8] Fig. 9	4	10	2	No
Work	4	6	3	Yes

3 Simulation and Experimental Studies

The new proposed quadrature oscillator circuit with three outputs is next simulated using UA741 model in the TINA software. The circuit is designed using capacitor values as 0.01 μF. The resistors controlling the FO ($R_3 = R_4$) are varied to obtain different frequency of oscillation, while the resistors controlling CO are chosen as 2.2 kΩ, with R_2 made variable for sustained oscillation in the vicinity of the mentioned value. The results for varying frequency of oscillation are shown in Figure 2, where the FO affecting resistors are varied. It is observed that the FO can be independently tuned without involving CO affecting resistors. Moreover, the simulated results are also in good agreement with the theoretical values calculated using FO expression. Another result in form of three outputs are further shown in Figure 3, where the FO is found as 10 KHz, and the three outputs are evidently spaced 90^o apart in phase.

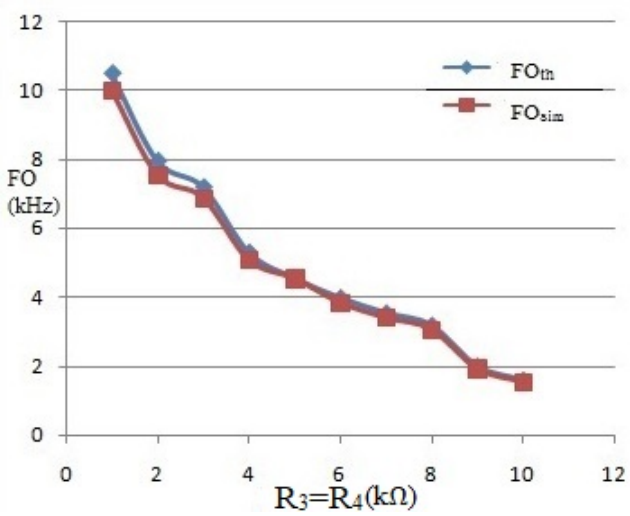


Figure 2: Frequency of oscillation (FO) tuning

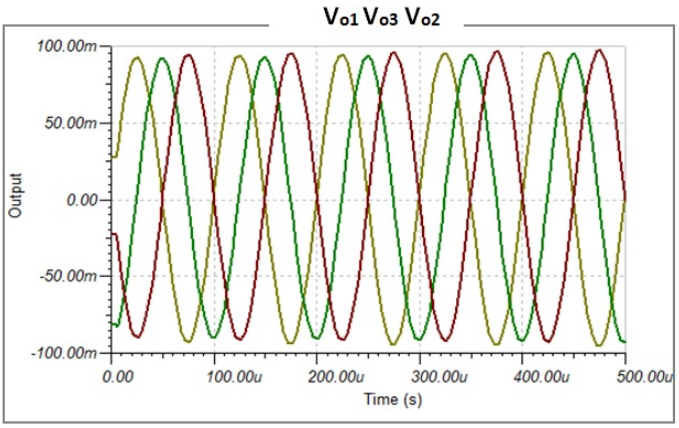


Figure 3: Three simulated outputs (volts) of proposed circuit at 10 kHz

To further verify the practicality of the proposed oscillator, commercially available low cost general purpose opamp IC 741 are used to breadboard the new proposed circuit. The values of capacitor are again chosen as 0.01 μF. The FO controlling resistors ($R_3 = R_4$) are varied, while CO controlling resistors are realized using a 10 kΩ POT. The first set of results for 4.7 kΩ resistive elements is shown in Figure 4. It may be noted that the measured value of resistors was 4.62 kΩ, thus resulting the theoretical value of FO as 3.4 kHz. As seen from Figure 4, the experimental FO is 3.34 kHz which is in good agreement with theoretical value. Furthermore the quadrature relationship of the two shown outputs is also evident. Next set of experimental results for 2.2 kΩ resistors are shown in Figure 5. The measured value of resistors is found as 2.15 kΩ, thus resulting in theoretical FO as 7.4 kHz, whereas the experimental FO from Figure 5 is found as 6.54 KHz.

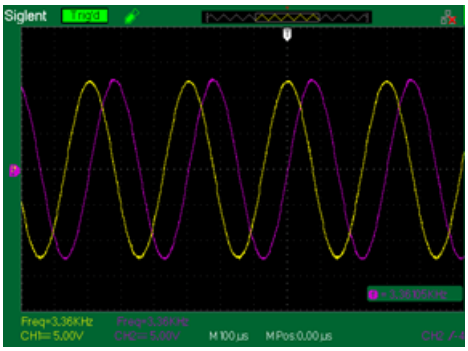


Figure 4: Experimental results for 4.7 kΩ resistors

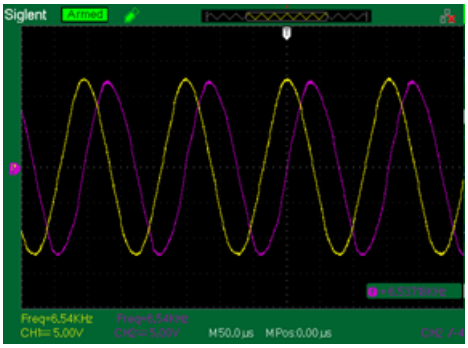


Figure 5: Experimental results for 2.2 kΩ resistors

4 Conclusion

This work presents a new quadrature oscillator circuit using operational amplifiers and six passive elements. The new circuit benefits from easy control over FO through independent resistive elements, which are not involved in CO control. The circuit provides three outputs and is verified both through

simulation studies as well as experimental results using low cost commercial opamps. The proposed circuit may further be extended to four phase outputs by augmenting an inverting stage.

Acknowledgement

This work was carried out during summer break June-July 2018, under academic support of Prof. S. Maheshwari, AMU, Aligarh, India.

References

[1] S. Avireni, C. S. Pittala, "Grounded resistance/capacitance controlled sinusoidal oscillator using operational transconducatnce amplifier," *WSEAS Transactions on Circuits and Systems*, vol. 13, pp. 145-152, 2014.
[2] V. Biolekovo, J. Bajer, D. Biolek, "Four-phase oscillator employing two active elements," *Radio-engineering*, vol. 20, no. 1, pp. 334-339, 2011.
[3] B. Chaturvedi, J. Mohan, "Single acitive element based mixed mode quadrature oscillator using grounded components," *IU-JEEE*, vol. 15, no. 1, pp. 1897-1906, 2015.
[4] J. W. Horng, "Quadrature oscillators using operational amplifiers," *Active and Passive Electronic Components*, vol. 2011, no. 2, 2011.
[5] A. Kumar, J. Mohan, B. Chaturvedi, S. Maheshwari, "Single active element based orthogonally controllable MOSFET-C quadrature oscillator," in *IMPACT*, India, 2017.
[6] S. Maheshwari, "Analog circuit design using a single EXCCCII," *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 61-69, 2018.
[7] S. Maheshwari, I. A. Khan, "Novel single resistor controlled oscillator using two CDBAs," *Journal of Acitve and Passive Electronic Devices*, vol. 2, no. 2, pp. 137-142, 2007.
[8] R. Mancani, "Design Of opamp sine wave oscillators," *Analog Application Journal*, pp. 33-37, Aug. 2000.
[9] J. Mohan, B. Chaturvedi, S. Maheshwari, "Low voltage mixed-mode multi phase oscillator using single FDCCII," *Electronics*, vol. 20, no. 1, pp. 36, 2016.
[10] A. S. Sedra, K. C. Smith, *Microelectronic Circuits*, 5th edition, Oxford University Press, 2004.
[11] A. M. Soliman, "Two integrator loop quadrature oscillators: A review," *Journal of Advanced Research*, vol. 4, pp. 1-11, 2013.

Biography

Kushaagra Maheshwari is pursuing B. Tech in Electronics and Communication Engineering from GLBITM, G. Noida, India.

Modified RSA Algorithm Using Two Public Key and Chinese Remainder Theorem

Rasha Samir Abdeldaym, Hatem Mohamed Abd Elkader, Reda Hussein
(Corresponding author: Rasha Samir Abdeldaym)

Faculty of Computers and Information Benha Qalubia, El menufia
Faculty of Computers and Information Shebein El kom, El menufia
Faculty of Computers and Information Kafr Elshiekh
(Email: rashasamir661@yahoo.com, hatem6803@yahoo.com, reda_mabrouk@fci.kfs.edu.eg)
(Received Oct. 29, 2018; revised and accepted Jan. 6, 2019)

Abstract

Network security is an activity which is designed to protect the integrity and usability of the data and network. In network security [14], the branch of cryptography is which one can save and transmit data in format particular so that only the user intended can read and process it, the text encrypted is the cipher text which is then decoded on the receiver side. The algorithm of RSA is an asymmetric cryptography technique, this is working on two keys i.e. public key and private key. The proposed model takes four prime numbers in RSA. Instead of sending one public key directly, send two public keys to the receiver. But there is problem of the speed, so that in RSA decryption used Chinese remainder theorem to enhancement the speed of RSA decryption.

Keywords: Chinese Remainder Theorem (CRT); Cryptography; Network Security; RSA

1 Introduction

Cryptography is defined as the study of techniques for ensuring the secrecy and authenticity of information. It is the science and study of secret writing which concerns the ways of communication and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers and other methods, so that only certain people can see the real message. With regards to confidentiality, cryptography is used to encrypt data residing on storage devices or travelling through communication channels to ensure that any illegal access is not successful [15].

The branch of Network Security and cryptography which covers range wide about how to protect data in digital form and to provide security services [6]. Every day a large amount of data shared through computer networks, network security has become very important aspect of networking, to secure the data through some measures whether they are software measures or the hardware. Chinese Remainder Theorem, CRT is one of the mathematics theorems which are important in the field of cryptography [18]. Computing was the area original of the application and still important which is related to various algorithmic aspects and computations modular.

In 1978, Rivest, Shamir, and Adleman invented a method to implement the cryptosystem public-key, which is known as the RSA cryptosystem [17]. RSA cryptosystem is the most attractive and popular security technique for many applications, such as electronic commerce and secure internet access. It

has to perform modular exponentiation with large exponent and modulus for security consideration. The RSA cryptosystem takes great computational cost. In many RSA applications, user uses a small public key to speed up the encryption operation. However, the decryption operation has to take more computational cost to perform modular exponentiation by this case [15], but It provides high security and it is easy to implement, RSA is an asymmetric key algorithm (public key).

The proposed model for RSA cryptosystem contains four prime numbers [24] and by using two public key instead of sending one public key directly [23], so that if an attacker has an opportunity of hacking and getting the component of public key they cannot get the private key value by brute force search. On the other hand RSA works quite slowly when its bit size increases after 1024bits, So that to improve the speed on RSA decryption side used the Chinese remainder theorem (CRT) [15] by which the scheme is semantically secure also. The objective of this paper enhancement the performance by using Chinese [21] and increased the security by using two public keys in the encryption.

2 Existing Techniques

2.1 RSA Algorithm

The RSA cryptosystem [17] is invented by R. Rivest, A. Shamir, and L. Adleman, is widely most used public key Cryptosystem. RSA algorithm is the first algorithm suitable for encryption and decryption [27]; The RSA algorithm used the multiplication modular and exponentiation [2]. The algorithm of RSA is a cipher block which the plaintext [3] and cipher text are integers between 0 and n-1 for some n. this algorithm is one of the best cryptosystem known asymmetric key for exchange key or digital signatures or encryption block of data, which uses prime numbers.

In asymmetric cryptography or public key cryptography, two different keys are used for encryption and decryption. One key is public and another one is private. By applying some the computation mathematical of two large prime numbers, the keys are generated. Send the public key to everyone in the system, but keep secret the private key in RSA. The RSA cryptosystem security depends upon the difficulties of large prime numbers factorization. can be generated the Private Key by using information of public key, which includes n (multiplication of prime numbers), the attacker cannot get the factor prime of n and therefore the private key. And this makes the algorithm of RSA more secure.

RSA Key Generation:

1) Obtain two large numbers prime p and q of relatively same size such that their product $n = pq$ is required bit length for example 1024.
2) Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$.
3) Choose a random integer encryption such that $\gcd[e, \phi(n)] = 1$ and $1 < e < \phi(n)$.
4) Compute the exponent secret d in the range $1 < d < \phi$ such that: $ed = 1 \bmod \phi(n)$.
5) The public key is (e, n) and the private key is (d, n).

The secret values are d, p, q and ϕ.

1) n is known as the multiplication or modulus of the prime numbers.
2) e is known as the exponent public or exponent encryption or just the exponent.
3) d is known as the exponent private or exponent decryption.

RSA Encryption:

Sender does the following operations:

1) Determine the public key.
2) The plaintext message represented as a message positive as an integer positive.
3) Calculates the cipher text: $C = M^e \bmod (n)$.
4) Send to the receiver the cipher text.

RSA Decryption:

The receiver does the following:

1) Use the private key (n, d) to compute plaintext: $M = C^d \bmod (n)$.
2) Extract the plaintext from the message representative M.

2.2 Chinese Remainder Theorem

CRT, Chinese Remainder Theorem, is the one of the main theorems of mathematics. It is can be used in the cryptography field [21]. CRT continues to present itself in new contexts and open vistas for new applications types. Original field of this application is the computing, continues to be important as regards some aspects of algorithmic and computations modular. The Chinese remainder theorem (CRT) is to determine a single integer from its remainders from a set of modulos. It has applications in various areas, such as digital signal processing and cryptography. CRT allows for implementation the RSA algorithm efficiently [1].

CRT is an algorithm with many applications in mathematics, the main area of its application is the computing, and recently it is being used in cryptography. But in the field of cryptosystem, the algorithm is used for functionality for modular computation. The size of the exponent decryption, d and the modulus, n is very important because the complexity of the decryption in RSA depends directly on it. The exponent decryption specifies the numbers of multiplication modular, there are necessary to perform the exponentiation. The modulus, n play an important role in determined the size of the intermediate results. A way to reduce the size of both d and n is by using the Chinese Remainder theorem.

Theorem 1. *Let $m_1, m_2, \cdots, m_n$ be a pairwise relatively prime, i.e. $\gcd(m_i, m_j) = 1$ for all i and j less than or equal to n where $i \neq j$. Then, the system of congruencies:*

$$\begin{aligned} X &\equiv a_1(\bmod(m_1)) \\ X &\equiv a_2(\bmod(m_2)) \\ &\vdots \quad\quad \vdots \\ X &\equiv a_n(\bmod(m_n)). \end{aligned}$$

Has a solution which is unique modulo the integer $m_1, m_2, \cdots, m_n$.

The RSA decryption and signature operation can be speeded up by using the CRT, where the factors of the modulus N (i.e. and Q) are assumed to be known. By CRT, the computation of $M = CD(\bmod N)$ can be partitioned into two parts:

$$MP = CP^{DP}(\bmod P), \tag{1}$$

$$MQ = CQ^{DQ}(\bmod Q). \tag{2}$$

Where

$$CP = C(\mathrm{mod}P) \quad (3)$$
$$DP = D(\mathrm{mod}P-1) \quad (4)$$
$$CQ = C(\mathrm{mod}Q) \quad (5)$$
$$DQ = D(\mathrm{mod}Q-1). \quad (6)$$

This reduces computation time since $DP, DQ < D$ and $CP, CQ < C$. In fact, their sizes are about half the original sizes. In the ideal case, we can have a speedup of about 4 times.

2.3 RSA Using Multi-Keys

Generated multiple keys (two public and two private keys) [23] In RSA algorithm. In this algorithm the computation time is more because of multiple keys, but the security is more [7] compared to the standard algorithm (RSA). We are using two public and private keys in modified RSA algorithm [9], in which we will be used four prime number and get public key and private key [26], also using two public keys for encrypting and two private keys for decrypting [10]. It is less vulnerable to attack .there are 3 phases: Key generation, encryption, and decryption.

Key Generation : In the process of key generation we will generate multiple public key and private keys. In this algorithm the public keys are apparent to both sender and receiver. And private keys became secret. These are steps for process of key generation:

1) Select two set numbers randomly say r, s and p, q.
2) Find the value of (z, n), i.e., $z = rs$, $n = pq$.
3) Compute the value of $\phi(z) = (r-1)(s-1)$, $\phi(n) = (p-1)(q-1)$.
4) Select integer random e, g such that $1 < e < n$, $1 < g < z$ and $\gcd(e, \phi(n)) = 1$, $\gcd(e, \phi(z)) = 1$.
5) Compute the value of T, d such that $tg \equiv 1 \bmod (z)$, $de \equiv 1 \bmod (n)$.
6) Public Key $\{e, g, n, z\}$, Private Key $\{d, t, n, z\}$.

Encryption: After generated multiple public and private key in the process of key generation. Now encrypted the message with the public keys. Thus the process of encryption made two times, the reliability is became more compared to the standard RSA algorithm. We will take the message (M) and the first public key (e) then make the process of encryption and find out $C_1 = M^e \bmod (n)$. By using C_1 and the second public key (g) would be found the cipher text in process of encryption: $C = C_1^g \bmod (z)$.

Decryption : In the process of decryption, the message original decrypted by using private keys d, t. The ciphertext would be decrypted with the first private key (d) with this formula: $m_1 = C^t \bmod (z)$, then can getting the original message with second private key (t) with this formula: $M = m_1^d \bmod (n)$.

3 Related Work

1) Rivest, Adi Shamir and Adelman has invented RSA algorithm which it is widely most used public key cryptosystem, this algorithm used to encrypt the data to provide security [17].

2) Vivek Choudhary and N. Praveen has proposed Enhanced RSA cryptosystem based on three prime numbers ,which it becomes difficult for the intruder to guess the factor of n and hence the encrypted message remains safe from the hackers [5].

3) Somesh Kumar has implemented RSA algorithm with free forward artificial neural network [11].

4) Dhakar, Gupta, and Sharma provide a modify RSA algorithm based on the n-prime numbers. This technique uses n-prime numbers because large prime numbers are not easily factorized [7].

5) Saurabh *et al.* evaluated three famous encryption algorithms, ECC, RSA, AES [19].

6) Abdulameer K. Hussain has proposed a method to eliminate the redundant messages occurred in the RSA method by applying the K-Nearest Neighbor values of either p or q or both [8].

7) Bhumi and Patel provide a modify RSA algorithm and Chinese remainder theorem which this algorithm enhancement the performance only not increased the security [15].

8) Sony, Shaik, Ski, and Anitha have Improvised Asymmetric Key Encryption Algorithm Using MATLAB by using two public keys and two private keys to increase the security but slow performance [23].

All of them have a problem about security, efficiency and performance. So that we will be tried to solve this problem through a proposed approach.

4 Proposed Technique

The proposed technique is trying to enhancement the implementation of the RSA cryptosystem through a method that has improvement a speed [13] on the RSA decryption side by using Chinese remainder theorem [22] and increase the security of the data by using two public key pairs in place of single public key [10]. This technique avoids various possible force attacks on RSA [20]. Using the random integer if encrypted the same message more than one time it will look different every time. The general idea towards this technique is to improvement the implementation the algorithm and make it more secure and decrease the decryption time both at the same time [16]. By using four prime numbers, and two cipher texts for each message, the analysis of algorithm become more difficulty. RSA is a block cipher in which the plaintext and cipher text are integer between 0 and $n-1$.

For some n and decryption can be done by the following steps:

Key Generation of the Proposed Technique:

1) Generate four large prime numbers p, q, r and s.
2) Find the value of (n, z), i.e. $n = pq$ and $z = rs$.
3) Calculate the value of $\phi(n) = (p-1)(q-1)$ and $\phi(z) = (r-1)(s-1)$.
4) Select integer random e, g such that $1 < e < n$ and $1 < g < z$, $\gcd(e, \phi(n)) = 1$, $\gcd(e, \phi(z)) = 1$.
5) Calculate the value of d by using the formula: $ed = 1 \bmod (\phi(n))$. Nxet, calculate the value of T by using this formula: $tg = 1 \bmod (\phi(z))$.

6) Find

$$\begin{aligned} dp &= d \bmod (p-1) \\ dq &= d \bmod (q-1) \\ dr &= d \bmod (r-1) \\ ds &= d \bmod (s-1). \end{aligned}$$

Public key $KU =< (e,n),(g,z) >$ and private key $KV =< t,z,dp,dq,dr,ds >$.

Encryption for Proposed Technique: To encrypt the message M steps are as follows:

1) Represent the message M as integer form in the range [0 to $n-1$].
2) Take the message (M) and with the first public key (e) make the process of encryption by using this formula: $C_1 = M^e \bmod (n)$ then obtain ciphertext (C_1).
3) By using C_1 and the second public key (g) would be found the ciphertext-2 (C) in process of encryption: $C = C_1^g \bmod (z)$.
4) Send the ciphertext-2 value to the receiver.

Decryption for Proposed Technique: To decrypt the ciphertext-2 as follows:

1) By using first private key (t,z) with the formula: $m_1 = C^t \bmod (z)$.
2) Calculate the following:

$$\begin{aligned} C_p &= C_1 \bmod p \\ C_q &= C_1 \bmod q \\ C_r &= C_1 \bmod r \\ C_s &= C_1 \bmod s. \end{aligned}$$

3) Then calculate:

$$\begin{aligned} m_p &= C_p d_p \bmod p \\ m_q &= C_q d_q \bmod q \\ m_r &= C_r d_r \bmod r \\ m_s &= C_s d_s \bmod s. \end{aligned}$$

4) Combining M_p, M_q, m_r and m_s, we get original plaintext message.

5 Comparison

5.1 Comparison between Standard RSA and RSA Using Multiple Keys with Results

RSA using multiple keys more secure than the standard RSA but it is slower than it, so that this decrease the performance, which this algorithm used four prime numbers to generate multiple public keys and private keys which this technique provide more security compared with RSA algorithm . in this algorithm used two public and private keys, this makes him safer since he is not attacked or robbed

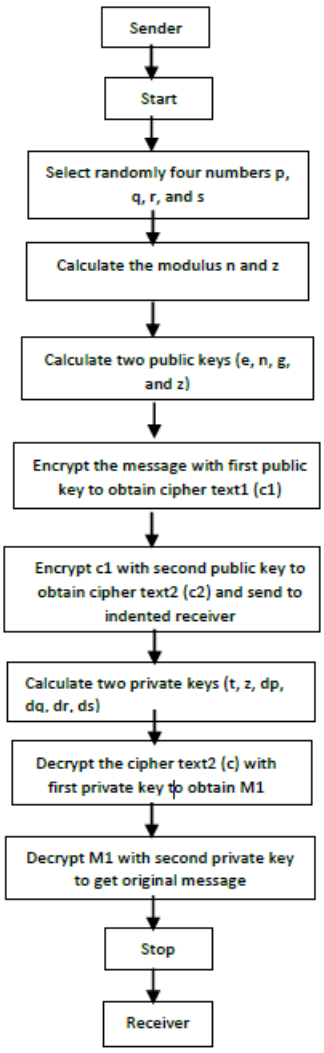


Figure 1: Block diagram of proposed RSA algorithm

by unauthorized people and improving security and efficiency in data sharing over the network, but less speed compare to RSA algorithm . Since the standard RSA used two prime numbers to generate one public key and one private key to make encryption and decryption this make it less secure which it is easily decomposed.

Following table and chart explain the comparison through the time in milliseconds with different sizes in bits, the encryption time of RSA smaller than the encryption time of RSA using multiple keys (two public keys and two private keys) because RSA using multi keys make two iteration in the encryption and decryption so that take time greater than standard algorithm (RSA), the decryption time of RSA smaller than the decryption time of RSA using multi keys (See Table 1 and Figure 2).

Table 1: Comparison between standard RSA and RSA using multiple keys with results

Size in bits	RSA		All time	RSA Uusing Multi Keys		All time
	Encryp. Time	Decryp. Time		Encryp. Time	Decryp. Time	
640	14	28	42	28	56	84
1040	15	33	48	31	62	93
1136	16	47	63	35	78	113

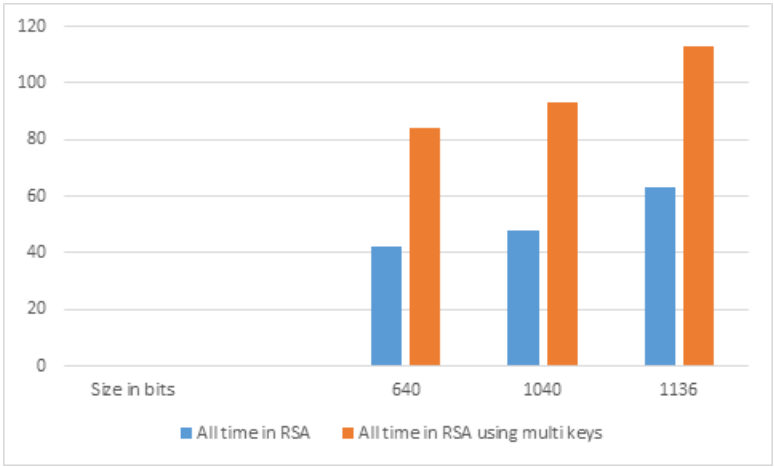


Figure 2: Comparison between standard RSA and RSA using multiple keys with results

5.2 Comparison between Standard RSA, RSA-CRT and RSA by Multi Keys with Results

In RSA by multi keys technique used four prime numbers to generate multiple public keys and private keys which this technique provide more security [12] compared with RSA algorithm and RSA_CRT [4]. In RSA by multi keys technique used two public and private keys, this makes him safer since he is not attacked or robbed by unauthorized people and improving security and efficiency in data sharing over the network, but less speed compare to RSA algorithm and RSA_CRT. Since the standard RSA used

two prime numbers to generate one public key and one private key to encrypt and decrypt, this makes it less secure which it is easily decomposed. RSA by multi keys take time to encrypt and decrypt more than RSA_CRT, by using CRT in decryption of RSA algorithm it requires less processing time and smaller amount of memory for final decoded result compared with RSA by multi keys.

Fowling table and chart explain the comparison through the time in milliseconds with different sizes in bits, all time encryption and decryption of RSA using Chinese smaller than all-time encryption and decryption of RSA and RSA using multiple keys (two public keys and two private keys) because RSA using Chinese reduce the size of both d and n, so that The CRT technique improves the throughput rate up to 4 times [25] in the best case. Where the factors of the modulus N (i.e. and Q) are assumed to be known. By CRT, the computation can be partitioned into two parts, this reduces computation time since $DP, DQ < D$ and $CP, CQ < C$. In fact, their sizes are about half the original sizes (See Table 2 and Figure 3).

Table 2: Comparison between standard RSA, RSA-CRT and RSA by multi keys with results

Size in Bits	All time encryption and decryption of RSA	All time encryption and decryption of RSA-CRT	All time encryption and decryption of RSA by multi keys
640	42	26	84
1040	48	29	93
1136	63	32	113

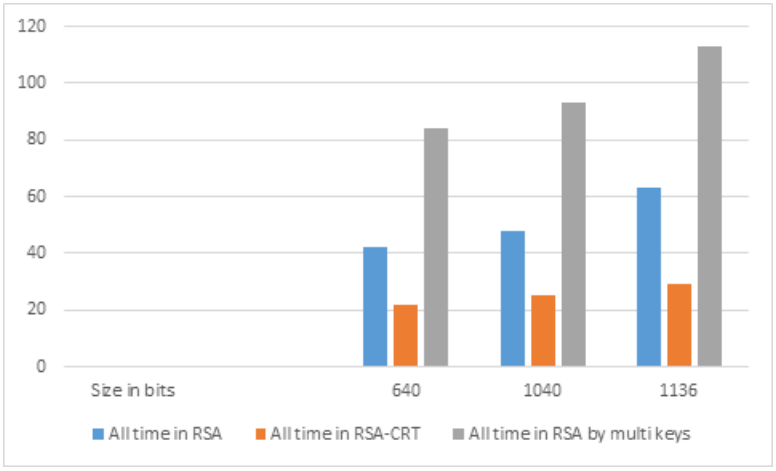


Figure 3: Comparison between standard RSA, RSA-CRT and RSA by multi keys with results

5.3 Comparison between Standard RSA, RSA-CRT, RSA by Multi Keys and Proposed Technique with Results

In proposed technique provide more security compared with RSA algorithm and RSA_CRT because the proposed technique make the encryption by two public key to increase the security to data and it

improved a speed on the RSA decryption side by using Chinese remainder theorem. Thus the proposed technique enhancement the speed and the performance compared RSA by multi keys.

Fowling table and chart explain the comparison through the time in milliseconds with different sizes in bits, all time encryption and decryption of RSA using Chinese smaller than all-time encryption and decryption of RSA, RSA using multiple keys (two public keys and two private keys) and proposed technique because RSA using Chinese reduce the size of both d and n, so that the CRT technique improves the throughput rate up to 4 times in the best case. Where the factors of the modulus N (i.e. and Q) are assumed to be known. By CRT, the computation can be partitioned into two parts, this reduces computation time since $DP, DQ < D$ and $CP, CQ < C$. In fact, their sizes are about half the original sizes. But the proposed technique increased the security (See Table 3 and Figure 4).

Table 3: Comparison between standard RSA, RSA-CRT, RSA by multi keys and proposed technique with results

Size in bits	All time encryption and decryption of RSA in MS	All time encryption and decryption of RSA-CRT in MS	All time encryption and decryption of RSA by multi keys in MS	All time encryption and decryption of proposed technique in MS
640	42	26	84	66
1040	48	29	93	71
1136	63	32	113	85

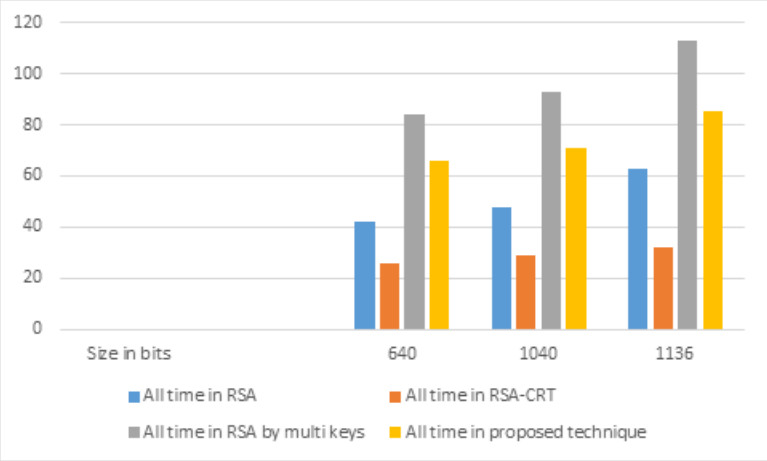


Figure 4: Comparison between standard RSA, RSA-CRT, RSA by multi keys and proposed technique with results

5.4 The Objective of this Paper

Enhancement the performance of RSA and increase the security and evaluated the security according to Randomness testing (using NIST statistical tests) has developed a package of 15 statistical tests to assure the randomness of a cryptography algorithm, The NIST Test Suite is developed to test the randomness of binary sequences produced by either hardware or software based cryptographic random number generators. These tests focus on a variety of different types of non-randomness that could exist in a sequence, the 15 tests are:

1) The Frequency (Mon obit) test;
2) Frequency test within a block;
3) The Run test;
4) Tests for the longest-Run-of-ones in a block;
5) The Binary matrix rank test;
6) The Discrete Fourier transform test;
7) The Non-overlapping template matching test;
8) The Overlapping template matching test;
9) Maurer's "Universal statistical" test;
10) The Linear complexity test;
11) The Serial test;
12) The Approximate entropy test;
13) The cumulative sums test;
14) The Random excursions test;
15) The Random excursions variant test.

After NIST tests have been run, there are some of tests with value to P-value as in Table 4.

Table 4: NIST tests

Test name	p-value	conclusion
Overlapping template matching test	0.980204	Random
Runs test	0.550989	Random
Frequency test	0.101978	Random

Since the P-value is ≥ 0.01, accept the sequence as random.

5.5 Performance

The proposed technique is more secure as compared to original RSA algorithm and RSA-CRT. And it enhanced the performance the algorithm in decryption because it used the CRT in decryption, thus the proposed technique faster than RSA by multi keys. It reduces the cost of computation. Although it takes long time to perform it as compared to original RSA.

6 Conclusion and Future Work

This paper shows study of number theory and Chinese remainder theorem (CRT) and RSA (public key cryptosystem). RSA algorithm cryptographic system generates one public key for encryption whereas, proposed technique generates two public key and sends them separately. So that to speed up the time of decryption, Chinese remainder theorem is used. This technique also improves the security of RSA algorithm by using two public key pairs. The future work would be based upon working on the attacks which are possible on RSA and therefore to give more secure RSA cryptosystem and improvement the performance.

References

[1] V. S. Balaji and R. Rengaraj, "Secure Transmission of Data Using CRT-RSA," *Journal of Global Research in Computer Science*, vol. 1, no. 1, Aug. 2010.

[2] G. R. Blakey, "A Computer Algorithm for Calculating the Product AB Modulo M," *IEEE Transaction on Computers*, vol. 32, no. 5, pp. 497-500, 1983.

[3] C. Blondeau and K. Nyberg, "On distinct known plaintext attacks," in *9th International Workshop on Coding and Cryptography*, 2015.

[4] A. Chhabra, S. Mathur, "Modified RSA algorithm: A secure approach," in *International Conference on Computational Intelligence and Communication Systems*, IEEE, pp. 545-550, 2011.

[5] V. Choudhary and N. praveen, "Enhanced RSA cryptosystem based on three prime numbers," in *International Journal of Innovative Science, Engineering & Technology*, vol. 1, no. 10, Dec. 2014.

[6] T. R. Devi, "Importance of cryptography in network security," in *IEEE International Conference, Communication System and Network Technologies (CSNT'13)*, 2013.

[7] R. S. Dhakar, A. K. Gupta, P. Sharma, "Modified RSA encryption algorithm (MREA)," in *Second International Conference on Advanced Computing & Communication Technologies*, IEEE, pp. 426-429, 2012.

[8] A. K. Hussain, "A modified RSA algorithm for security enhancement and redundant messages elimination using K-nearest neighbor algorithm," *International Journal of Innovative Science, Engineering & Technology*, vol. 2, no. 1, Jan. 2015.

[9] I. Jahan, M. Asif, L. J. Rozario, "Improved RSA cryptosystem based on the study of the number theory and public key cryptosystems," *American Journal of Engineering Research*, vol. 4, no. 1, pp. 143-149, 2015.

[10] V. Kapoor, "Data encryption and decryption using modified RSA cryptography based on multiple public keys and 'n'prime number," *International Journal of Scientific Research in Network Security and Communication*, 30 June 2013.

[11] S. Kumar, "Implementation of RSA with feed-forward neural network using MATLAB," *International Journal of Computer Applications Foundation of Computer Science*, NY, 2016.

[12] R. Minni, K. Sultania, S. Mishra, D. R. Vincent, "An algorithm to enhance security in RSA," in *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, 2013.

[13] S. A. Nagar, S. Alshamma, "High Speed Implementation of RSA Algorithm with Modified Keys Exchange," in *6th International Conference on Science of Electronics, Technologies of Information and Telecommunications*, 2012.
[14] S. Negi, M. Bhardwaj, A. Ajitsaria, "Survey of Wireless Network Security: Attacks & their Counter measures SSRG," *International Journal of Computer Science and Engineering*, vol. 3, 2016.
[15] B. J. Patel, N. J. Janwe, "To Design and Implement a Novel Method of Encryption Using Modified RSA Algorithm and Chinese Remainder Theorem," in *International Conference on Industrial Automation and Computing*, 2014.
[16] A. Rai, S. Jain, "Modified RSA Cryptographic System with Two Public keys and Chinese Remainder Theorem," *International Journal of Computer Science and Engineering*, vol. 4, no. 7, July 2017.
[17] R. L. Rivest, A. Shamir, L. Adelman, "On Digital Signatures and Public Key Cryptosystems," *MIT Laboratory for Computer Science Technical Memorandum 82*, April 1977.
[18] S. Saraireh, "A Secure Data Communication System Using Cryptography and Steganography," *International Journal of Computer Networks & Communications*, vol. 5, no. 3, May 2013.
[19] Er. K. Saurabh, *et al.*, "A Comparative Evaluation of Cryptographic Algorithms," *International Journal of Computer Technology & Applications*, vol. 3, no. 5, pp. 1653-1657, 2012.
[20] S. Sharma, P. Sharma, R. S. Dhakar, "RSA algorithm using modified subset sum cryptosystem," *2011 2nd International Conference on Computer and Communication Technology*, pp. 457-461, 2011.
[21] S. Singh, G. Agarwal, "Use of Chinese Remainder Theorem to generate random numbers for cryptography," *International Journal of Applied Engineering and Research Lucknow and Mysore*, vol. 1, no 1, 2010.
[22] N. Somani, D. Mangal, "An improved RSA cryptographic System," *International Journal of Computer Applications*, vol. 105, Nov. 2014.
[23] K. Sony, D. Shaik, B. Divya Sri, G. Anitha, "Improvised Asymmetric Key Encryption Algorithm Using MATLAB," *IOSR Journal of Electronics and Communication Engineering*, vol. 10, no. 2, 2015.
[24] W. Stein, "Elementary Number Theory," in *Primes Congruences and Secrets*, Jan. 2017.
[25] X. Tan, Y. Li, "Parallel Analysis of an Improved RSA Algorithm," in *International Conference on Computer Science and Electronics Engineering*, IEEE, pp. 318-320, 2012.
[26] B. P. Urbana Ivy, P. Mandiwa, M. Kumar, "A modified RSA cryptosystem based on 'n' prime numbers," *International Journal of Engineering and Computer Science*, vol. 1, no. 2, pp. 63-66, 2012.
[27] S. Wang, G. Liu, "File Encryption and Decryption System based on RSA Algorithm," in *International Conference on Computational and Information Sciences*, IEEE, 2011.

Biography

Rasha Samir Abdeldaym was born on Dec 8, 1980 in Benha, Qalubia, Egypt. She received the B.S from Faculty of Computers and Informatics, Zagazig University, Egypt in 2003 with grade good, and submitted for master degree from April 2017. she is working in faculty of computers and informatics benha university as Computer specialist and Certified ICDL Trainer.

Hatem Mohamed Abd Elkader is vice Dean of Faculty of Computers and Information, Menoufia university, Shebin Elkom, Egypt. Prof Hatem obtained his BSC. And M.SC. (by research) both in Electrical Engineering from the Alexandria University, Faculty of Engineering, Egypt in 1990 and 1995 respectively. He obtained his Ph.D. degree in Electrical Engineering also from Alexandria University, Faculty of Engineering, in 2001 specializing in neural networks and applications. Since 2009 he is the

Head of the department of Information Systems (IS). Prof. Hatem has published more than 100 papers in international journals, international conferences, local journals and local conferences.

Reda Hussein works in information system department at faculty of computers and information, Kafr Elsheikh, Egypt.

Guide for Authors
International Journal of Electronics and Information Engineering

International Journal of Electronics and Information Engineering (IJEIE) will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of Electronics and Information Engineering. Topics will include, but not be limited to, the following: Algorithms, Bioinformatics, Computation Theory, AI, Fuzzy Systems, Embedded Systems, VLSI/EDA, Computer Networks, Information Security, Database, Data Mining, and Information Retrieval, Digital Content, Digital Life, and Human Computer Interaction, Image Processing, Computer Graphics, and Multimedia Technologies, Information Literacy, e-Learning, and Social Media, Mobile Computing, Wireless Communications, and Vehicular Technologies, Parallel, Peer-to-peer, Distributed, and Cloud Computing, Semiconductor, Software Engineering and Programming Languages, Telecommunication, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijeie.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

Title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:
For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

2.5 Author benefits

No page charge is made.

Subscription Information

Individual subscriptions to IJEIE are available at the annual rate of US$ 200.00 or NT 6,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijeie.jalaxy.com.tw or Email to ijeieoffice@gmail.com.