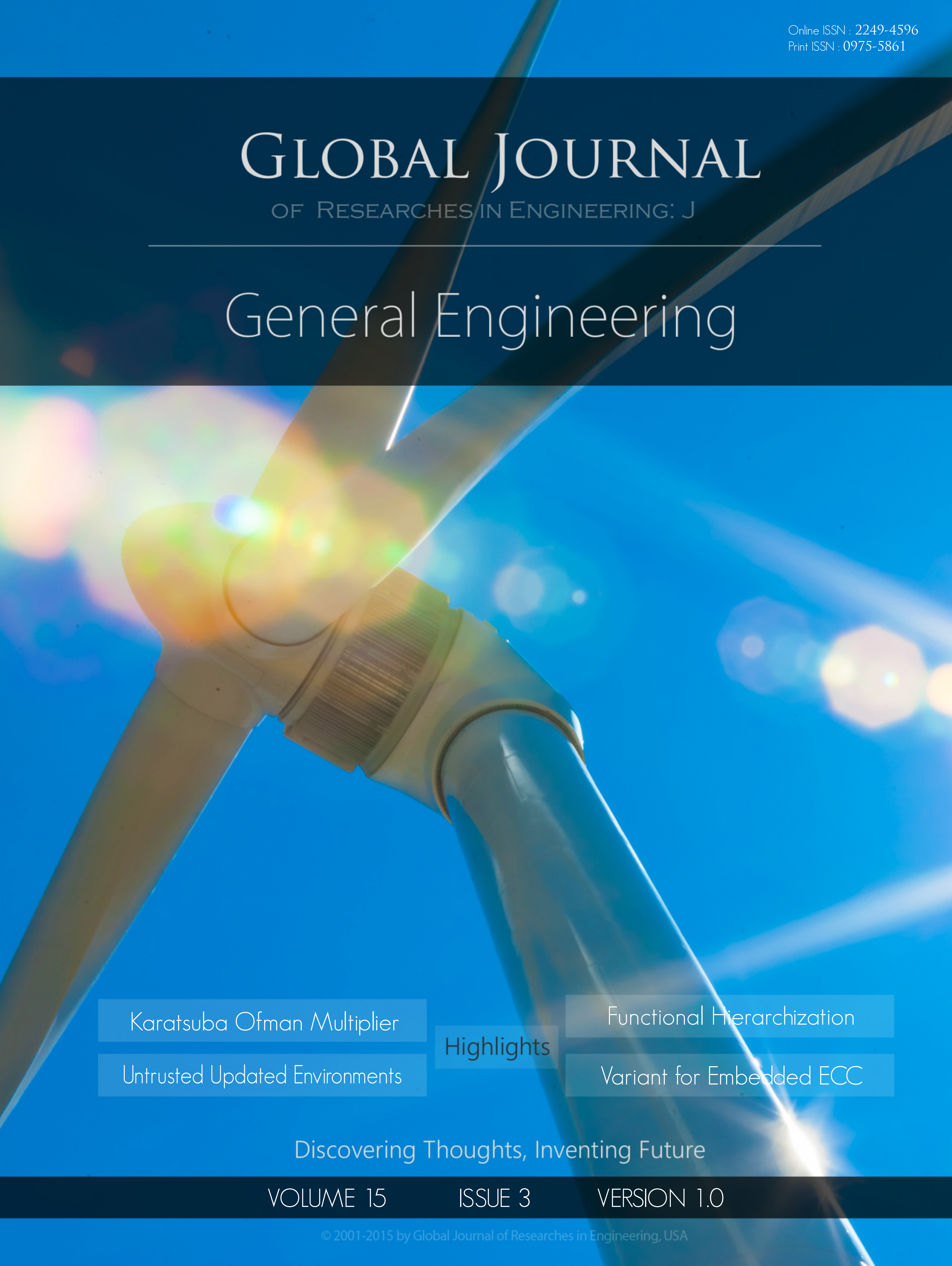
Online ISSN : 2249-4596
Print ISSN : 0975-5861

Global Journal

of Researches in Engineering: J

General Engineering



Karatsuba Ofman Multiplier

Untrusted Updated Environments

Highlights

Functional Hierarchization

Variant for Embedded ECC

Discovering Thoughts, Inventing Future

VOLUME 15 ISSUE 3 VERSION 1.0

Global Journal of Researches in Engineering: J
General Engineering

Global Journal of Researches in Engineering: J
General Engineering

Volume 15 Issue 3 (Ver. 1.0)

Open Association of Research Society

The opinions and statements made in this book are those of the authors concerned. Ultraculture has not verified and neither confirms nor denies any of the foregoing and no warranty or fitness is implied.

Engage with the contents herein at your own risk.

The use of this journal, and the terms and conditions for our providing information, is governed by our Disclaimer, Terms and Conditions and Privacy Policy given on our website http://globaljournals.us/terms-and-condition/menu-id-1463/.

By referring / using / reading / any type of association / referencing this journal, this signifies and you acknowledge that you have read them and that you accept and will be bound by the terms thereof.

All information, journals, this journal, activities undertaken, materials, services and our website, terms and conditions, privacy policy, and this journal is subject to change anytime without any prior notice.

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals Headquarters
301st Edgewater Place Suite, 100 Edgewater Dr.-Pl,
Wakefield MASSACHUSETTS, Pin: 01880,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

For Authors:
22 USD (B/W) & 50 USD (Color)
Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 250 USD (Color)

Integrated Editorial Board
(Computer Science, Engineering, Medical, Management, Natural Science, Social Science)

Contents of the Issue

i. Copyright Notice
ii. Editorial Board Members
iii. Chief Author and Dean
iv. Contents of the Issue

1. Proposal for a Methodology based on Functional Hierarchization for Product Development. *1-11*
2. Area Optimized Low Latency Karatsuba of man Multiplier Variant for Embedded ECC. *13-18*
3. Security in Untrusted Updated Environments. *19-21*

v. Fellows and Auxiliary Memberships
vi. Process of Submission of Research Paper
vii. Preferred Author Guidelines
viii. Index

Global Journal of Researches in Engineering: J
General Engineering
Volume 15 Issue 3 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4596 Print ISSN:0975-5861

Proposal for a Methodology based on Functional Hierarchization for Product Development

By Adriana Yumi Sato Duarte, Marilia Colozio Favaro, Fabio Mazzariol Santiciolli & Franco Giuseppe Dedini

State University of Campinas, Brazil

Abstract- This research aims to permit a simultaneous visualization of primary and secondary functions, sub-functions and subsystems in order to establish, according to its position in the plane, the influence on the overall function and how it can be inserted into the product design. The methodology described consists of an in depth-study of the functional deployment starting from a basic need. Since it is a conceptual study with a philosophical approach, three hypotheses underlie this methodology: the union of two techniques of functional deployment is not possible since there is no correlation; the union of two functional deployment techniques provides similar result if applied separately or the union of two functional deployment techniques provides better results since it allows a comprehensive view of the project. Until this point, this research suggests the union of the two functional deployment techniques provides better results since it allows a comprehensive view of the project.

Keywords: *function; functional deployment; design methodology; design tools; product design.*

GJRE-J Classification : *FOR Code: 091599*

Proposal for a Methodology based on Functional Hierarchization for Product Development

Adriana Yumi Sato Duarte [α], Marilia Colozio Favaro [σ], Fabio Mazzariol Santiciolli [ρ]
& Franco Giuseppe Dedini [ω]

Abstract- This research aims to permit a simultaneous visualization of primary and secondary functions, sub-functions and subsystems in order to establish, according to its position in the plane, the influence on the overall function and how it can be inserted into the product design. The methodology described consists of an in depth-study of the functional deployment starting from a basic need. Since it is a conceptual study with a philosophical approach, three hypotheses underlie this methodology: the union of two techniques of functional deployment is not possible since there is no correlation; the union of two functional deployment techniques provides similar result if applied separately or the union of two functional deployment techniques provides better results since it allows a comprehensive view of the project. Until this point, this research suggests the union of the two functional deployment techniques provides better results since it allows a comprehensive view of the project.

Keywords: function; functional deployment; design methodology; design tools; product design.

I. Introduction

The key factor for the product development is design methodology: an innovative and iterative process to design a product by relating functional requirements and customer needs [4]. A technique that encompasses the study and the systematization of a function is the Functional Analysis, which allows the transcription of consumers' needs in a semantic structure that, afterwards, may be broken down into sub-functions until the most basic and simple level is achieved.

Authors such as [2,3, 6,9, 16, 17, 21] describe function and functional analysis from different points of view. However, there is a consensus among these authors that the function deployment technique must be inserted into the stage of concept generation, in which consumers' needs are described and broken down in order to apply creativity tools later.

The functional analysis can be classified in two groups: the function structure and the function tree. Some authors [9, 16, 21] proposed studies on the function structure:a chart that encompasses the functions and their connecting flows. The function tree based on "why-how" approach was a consequence of the Value Analysis/Value Engineering described by Lawrence D. Miles[6]. The most widespread function tree is the Function Analysis System Technique (FAST) by Charles By the way.

Although both functional analysis are well established and supported a great number of projects around the world [1] asserts that function structures demand a high level of abstraction from the designer that can result in ambiguous or redundant functions. Moreover, the function trees do not reflect the connecting flows between the functions and the correlation between the functions and the product components.

Two functional basis to reduce the cases of redundancy and ambiguity were proposed by [9, 18]. However, even if the functional deployment is guided by a functional basis or taxonomy, some cases of redundancy and ambiguity will still remain [1].

On the other hand, some efforts have been made to correlate the function trees to the product components. [25] Proposed the intersection between the FAST diagram and the components by means of the "Removal and Operation" technique. [13] implemented the integration between the Function Analysis System Technique and the Axiomatic Design Theory to boost the capacity of defining the functional requirements and correlate the functions with others design domains.

The debate regarding different approaches for functional deployment is encouraged by [7], who explains that the function definitions are complementary and the coexistence of various techniques is beneficial to the design process and design teaching.

The present paper contributes to the debate about the coexistence of the design methodologies. Assuming that both function tree and function structure start from the product overall function, it is proposed a technique that merges the function structures to the function trees. Thus, it allows a simultaneous visualization of primary and secondary functions, sub-functions, and sub-systems aiming to establish, according to their position, their influence upon an overall function.

Author α σ ρ Ѡ: Laboratory of Integrated Systems (LabSIn), Faculty of Mechanical Engineering, State University of Campinas, Sao Paul, Brazil. e-mail: dri@fem.unicamp.br

The design methodology described in this research consists of an in-depth and conceptual study of two functional deployment techniques, based on By the way [3] and Pahland Beitz[16]. Section 2 describes different function definitions as well as establishes the function definition adopted in this paper. Section 3 is a literature review about functional analysis. Are search gap is reported in Section 4.The main goal of this paper, which is the proposal of a design methodology based on the literature review and the research gap, is presented in Section 5. Section 6 exemplifies the use of the proposed design methodology by analyzing a Hot Air Popper. Section 7 presents concluding remarks and discusses directions for future research.

II. Function Definition

There is an intense academic debate regarding the function definition. One example of function definition is proposed by[18] and states that a function is the operation to be performed by an artifact or a device. According to [23], function is the relation between the inputs and the output of a system or particular solution, in overall or local positions. Moreover, [9] emphasize that the functions are performed by the products in order to fulfill customer needs.

There are several other definitions for the term function in literature. [24] Explains this fact as a conceptual anomaly: function is a key term but there is no general agreement about its definition. However, it is indicated that the function definitions usually refers to “goals of the device”, “actions with the device”, “behavior of the device” and/or “structure of the device”. Finally, [7] investigated the awareness about the functional concepts among the designers and engineers who worked in product development in industry. As a result, it was noticed that they misused the word “function” for behavior, purpose or performance of a product. Furthermore, when these professionals were asked to describe a functional deployment of a product, many of them neglected the methodologies proposed by literature.

In order to avoid this type of misuse, we will adopt the definition of function as a description of desired or necessary capabilities that make the product accomplish its objectives by using a semantic structure of a verb that indicates an action, and a noun which is the object of the action.

III. Functional Analysis Methods

Functional analysis may be applied to the different stages of product development, but it is usually associated with the concept generation stage, before the feasibility study stage [2, 16, 17, 21, 22]. Due to the ease of measuring, behavior and performance are two terms associated with functions [21].

The functional analysis of a product is described in different ways by literature. According to [21], firstly, one must find the overall function to be carried out so as to describe it in a black box, in which the input and the output of material, energy and signal are considered. The second stage of this technique is to describe the sub-functions involved in the system, so as to guide the search for solutions in order to achieve a better understanding of the problem and to make the correlation between components and function easier.

Following the same line of reasoning [17] describe function modeling starting with the determination of an overall function so as to structure, afterwards, a function tree, with black boxes and establishing boundaries. Also, according to the authors, function modeling allows the creation of alternative structures to meet the overall function by means of (a) division or combination of functions, (b) alteration in specific dispositions, (c) alteration in the type of connection, and (d) alteration in the limit of the system.

A method of function deployment in five steps is described by [22] and [5], so as to divide a complex issue into sub-issues. The first step is based upon the clarification of the issue, including mission, consumer needs and product specification. After that, the issue is subdivided and described in black boxes. At this point, the author emphasizes that the objective is to describe the functional elements of the product without involving a specific technological principle [22]. The second step is to research external information, by means of interviews with users, consulting specialists, patents and the literature. The third step presents the same technique, but the search is internal, based on both individual and collective knowledge. The fourth step is exploring systematically. At this point, the function analysis is developed to generate benefits related to the identification of a solution that may seem irrelevant at first glance, to the adequate allocation of resources, and to refinement upon dividing the issue. Next, it is necessary to combine solutions in a systematic manner. Finally, the fifth step consists of reflection and the identification of opportunities for improvement [5, 22].

The axiomatic design proposes that the design is composed of four domains: the customer domain, the functional domain, the physical domain and the process domain. The customer domain contains the customer needs and/or the attributes the customer requires from the product. The requested needs and attributes are translated into functional requirements inside the functional domain. Design parameters are set in the physical domain in order to satisfy the functional requirements. Finally, the process variables are established in the process domain to accomplish the design parameters set in the physical domain [19]. The correlation between the members of each domain is verified in a “zigzagging” process that requires attention and experience from the design team because it defines the product coupling and the hierarchies for the functional requirements, the design parameters and the process variables [11]. It is stated that products with minor coupling present superior design. The couplings can be organized in a matrix base, making possible the design of large systems such as cargo/public transport [20].

a) Value Analysis (VA)

The functions of a product are classified according to their hierarchy or purpose. The classification of functions according to their purpose allows the determination of use value, which enables the functioning of the product, and esteem value, a characteristic that makes the product attractive to consumers. Besides, use function must be measurable, while esteem function is, in most cases, immeasurable [15].

Regarding the hierarchy, there are the overall functions, the basic functions and the secondary. The overall function explains itself the existence of a product. The primary functions are placed above the overall function and are the ones responsible for making the product work. Without them the product will have its value decreased and may lose the identity. Finally, the secondary functions support or enhance the basic functions [2].

As value analysis (VA) is a systematic analysis of the characteristics of a product, it requires the knowledge of its functioning [2]. Thus, VA is executed by a group of designer selected taking into account their expertise in specific domains related to the product on development process; this group is coordinated by a VA expert [4]. The first step of VA is to generate the functions of the product, asking what the product "does", and not only what the product "is". After determining the functions, it is necessary to organize them systematically in a function tree.

The Function Analysis System Technique organizes functions schematically, emphasizing their relations and hierarchy. Upon developing a FAST diagram, the designing team is questioned regarding (a) the reasons for the existence of the product, (b) the critical path between functions and, (c) the definition of the functions. This happens by using the terms "Why?" and "How?"[3] as shown in figure 1.

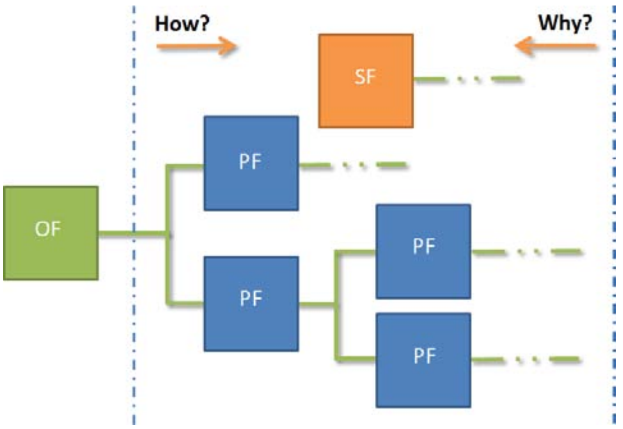


Fig. 1 : FAST Diagram

The functions expanded to the "How Direction" answer how the major function can be performed. In the opposite way, the functions expanded to the "How Direction" answer the reason why the inferior minor functions are performed. The first step in this top-down functional decomposition is the determination of the Overall Function of the product. Going through the "How direction", the Basic Functions are found, than the sub-functions are defined. At the same level of abstraction, Secondary Functions may arise. They may contribute with the performance of the Overall and Primary Functions and/or with the product value, but they also can be harmful or undesired but necessary functions [10].

b) Function Deployment According to Pahland Beitz

The Pahl and Beitz'sFunction Deployment is established above functional structures. It is widely accepted all over the world because it is closer to industrial practice and human thinking system [14]. [16] Define overall function as the overall relation between the input and output of a plant, a machine or assembly. Therefore, input and output, which consist of material, signal, and energy flow, are represented by different types of line in a block diagram. If the overall function is complex, it is necessary to divide it into sub-functions, so as to seek simple and unequivocal solutions.

First of all, the authors indicate that sub-functions must be structured around a main flow. When the function structure reaches the lowest level of complexity, the next step is to detail auxiliary flows and their sub-functions. Thus, function deployment continues until a simpler level is reached, such as described in figure 2. For didactic reasons, these functions are named as Pahl and Beitz functions in this paper.

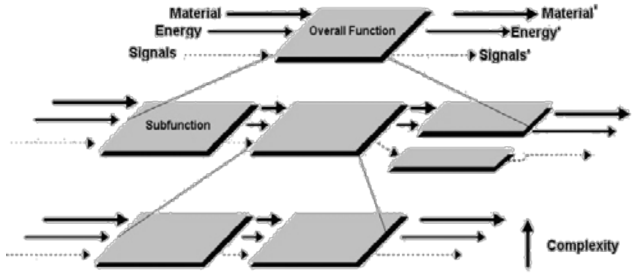


Fig. 2 : Function Structure. Adapted from [16]

IV. Research Gap

The literature presents well established tools and methodologies for the functional deployment in function trees or in function structures. On the other hand, there is a debate about the different kinds of functional analysis, and their possible complementary relations. Also some studies have proposed kinds of hybrid methodologies, however there is a lack of proposals on the explicit merge of a functional tree with a functional structure. The present article intends to contribute to the academic debate by investigating this gap with the proposal in the next section.

V. Proposal for a Design Methodology based on Function Deployment

The methodology described below consists of an in-depth study of function deployment starting from a basic need. This study derives from functional analyses described by Bytheway [3] and Pahland Beitz [16]. As this is a conceptual study with a philosophical approach to these two classical authors in this field, three hypotheses permeate this research: (a) the combination of both function deployment techniques is not possible because they do not present a correlation; (b) the combination of both function deployment techniques presents a similar result if they are applied separately; (c) the combination of both function deployment techniques presents a superior result because it enables an encompassing view of the design.

For didactic purposes, the proposed methodology is divided as figure 3 shows.

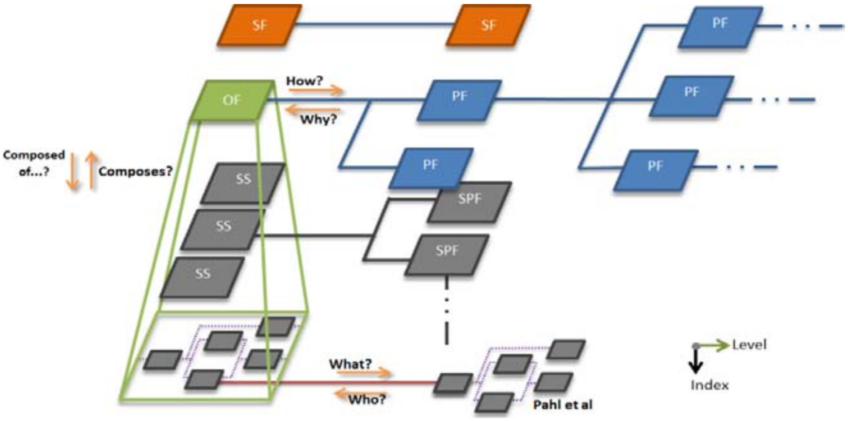


Fig. 3 : Design Methodology based on function deployment

This methodology starts from an Overall Function (OF) and goes on to function deployment with the determination of Primary Functions (PF) and/or Secondary Functions (SF), which, afterwards, are divided into Primary Sub-functions (PSF) and/or Secondary Sub-Functions (SSF), which are related to Sub-systems (SS) that, in turn, make up the Overall Function (OF).

Based on this information, the proposed methodology consists of the following steps:

Step 1: The basic need is described by an Overall Function (OF), which consists of an overall and desired relation between the input and the output of a product, with a view to accomplishing an overall task. In this context, the black box is of most importance so as to indicate the input and output parameters of the system, as in figure 4.

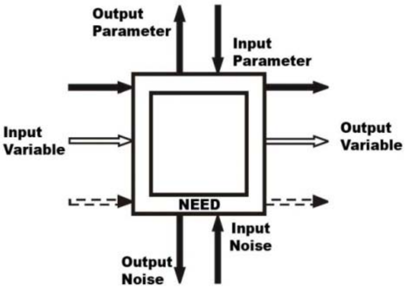


Fig. 4 : Step 1: The overall function and its input and outputs

Step 2: The Overall Function (OF) is divided into sub-systems, which correspond to the components that constitute the overall task. Moreover, each sub-system may be divided into new sub-systems so as to reach the basic sub-system, as [16] propose. Given that, as mentioned before, there is no consensus among authors regarding nomenclature and terms, this proposal indicates that sub-systems should be obtained by means of asking “Composes?” and “Composed Of?”, as shown in figure 5. Nomenclature at this stage follows the pattern “sub-system n.x”, in which “n” is the level of deployment and “x” is the index of the sub-system at an “n” level.

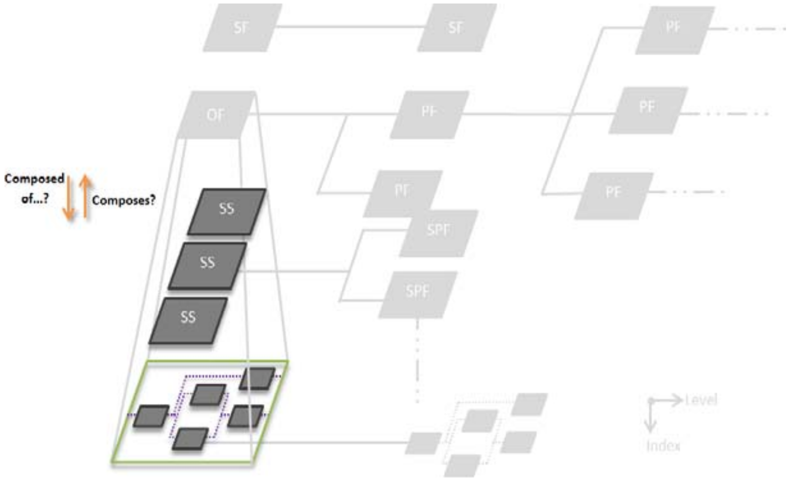


Fig. 5 : Step 2: Sub-systems and components deployment

Step 3: The Overall Function (OF) is divided into Primary Functions (PF), which correspond to how the OF is carried out, as in figure 6. Moreover, each primary function may be divided into new primary functions so as to reach the basic primary function, as [6] proposes. In this case, the terms “How?” and “Why?” are used for deployment. The nomenclature at this stage follows the pattern “primary function m.y”, in which “m” is the level of deployment and “y” is the index of the primary function at an “m” level.

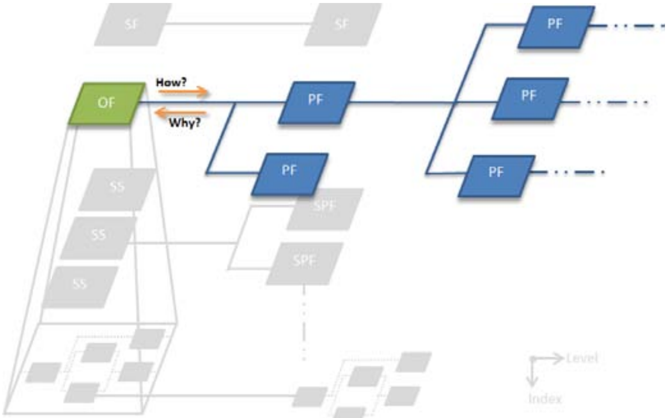


Fig. 6 : Step 3: Primary Functions deployment

Step 4: Secondary Functions (SF) are related to the overall function (OF) and, as it is a combined value, their deployment is indicated by the authors of this research. By doing this, SFs can be divided into new secondary functions so as to reach the basic secondary function, forming the basis for the questions recommended by[3], as indicated in figure 7. Nomenclature at this stage follows the pattern "secondary function m.y", in which "m" is the order of deployment and "y" is the index of the primary function in an "m" order.

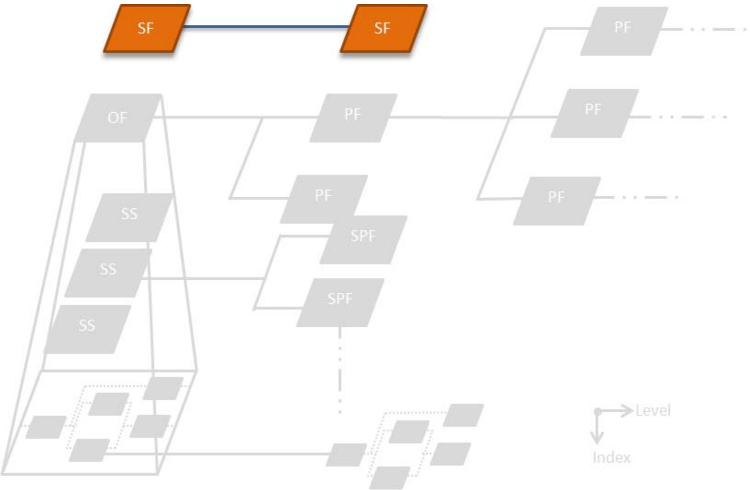


Fig. 7 : Step 4: Secondary Functions deployment

Step 5: Both primary and secondary functions may still be divided into sub-functions using Pahl and Beitz [16] deployment, as in figure 8. Thus, nomenclature at this stage follows the pattern "primary sub-function n.y" and "secondary sub-function n.y", in which "n" is the level of deployment and "y" is the index of the primary or secondary function at an "n" level.

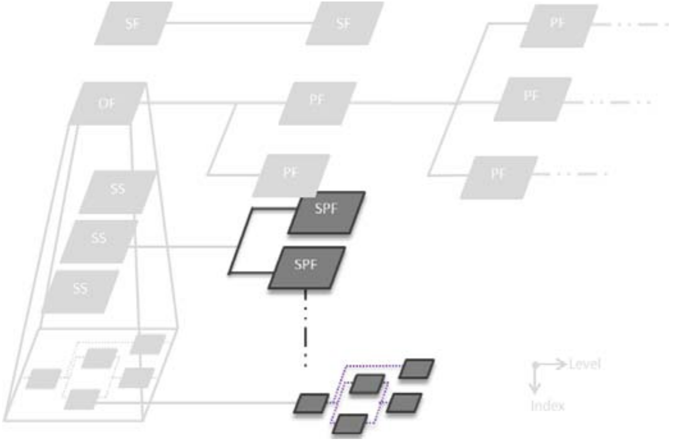


Fig. 8 : Step 5: Sub-functions deployment based on Pahl and Beitz[16] technique

Step 6: After describing the functions, sub-functions, and sub-systems, the last step is to relate basic sub-functions to basic sub-systems. In the end, it is still necessary to eliminate redundancies or repeated elements so as to make the design uncoupled and modular, a design in which each sub-function relates only to a single sub-system.

This methodology shows the sequence of functions, according to levels and order, and their respective relations to sub-systems. Thus, upon generating the complete design, it is possible to distinguish two initial approaches: by presenting alternative solutions to new products and/or by looking for faults in existing products. In a new product, there is the possibility of adding auxiliary tools during the design development, mainly at the concept generation stage, with creativity tools. By doing this, exploring alternative solutions makes innovation and the generation of patents easier. As for existing products, when there are faults in the design, the sequence of the divisions of functions makes the identification of the origin of the error easier. At this point, this research, of a philosophical and conceptual nature, suggests that the combination of both techniques of function deployment produces superior results since they enable an encompassing view of the design.

intrinsically related to functional basis. Once the Hot Air Popper requires little technical knowledge for functioning and operating, we decided to adopt this product as a didactic example to illustrate the proposed methodology.

First of all, it is necessary to define the overall function as described in Step 1. By studying the product and the user manual [8], the main objective of the Hot Air Popper is to "pop corn kernels". After that, the inputs and the outputs indicated by [18] were organized in "energy flow" and "material flow" as shown in figure 9.

The Step 2 connects the flows and the components in order to relate every subfunction to a component. Thus, the product components (pictured in figure 11) were inferred from the functional model adapted from [18] (illustrated in figure 10).

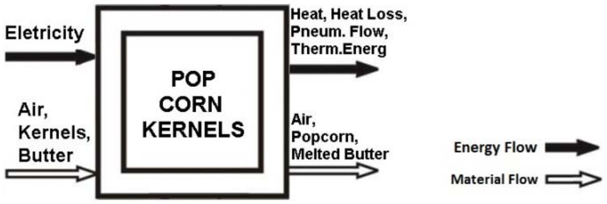


Fig. 9 : Hot Air Popper overall function black box

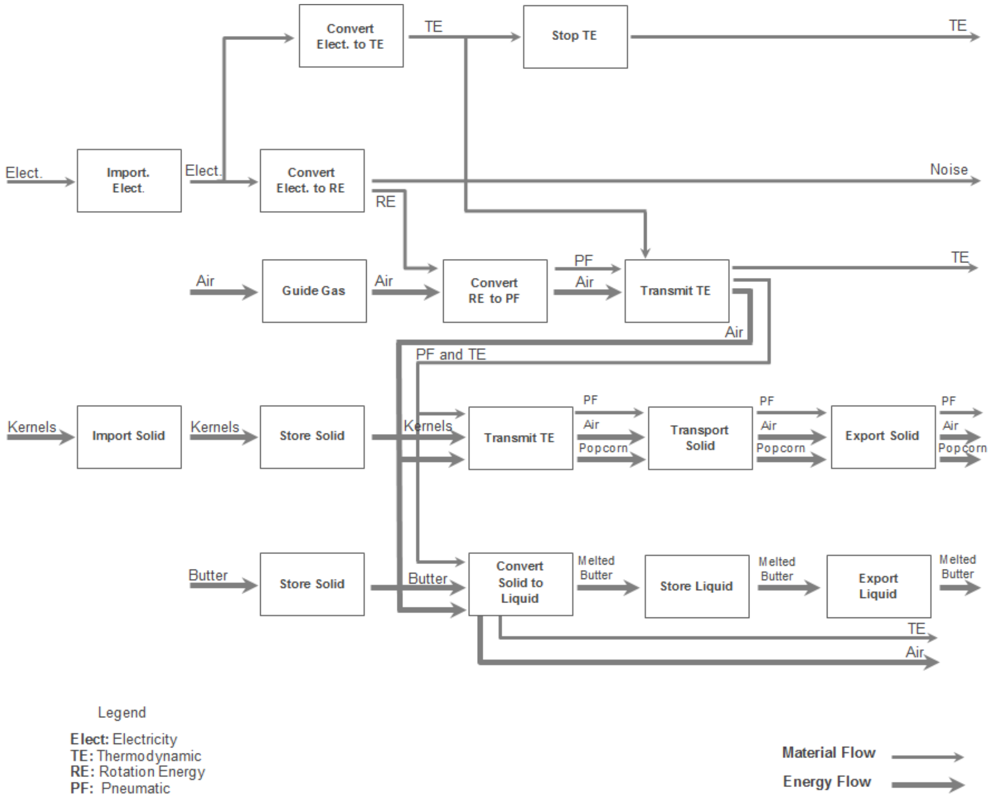


Fig. 10 : The Hot Air Popper functional deployment adapted from [18]

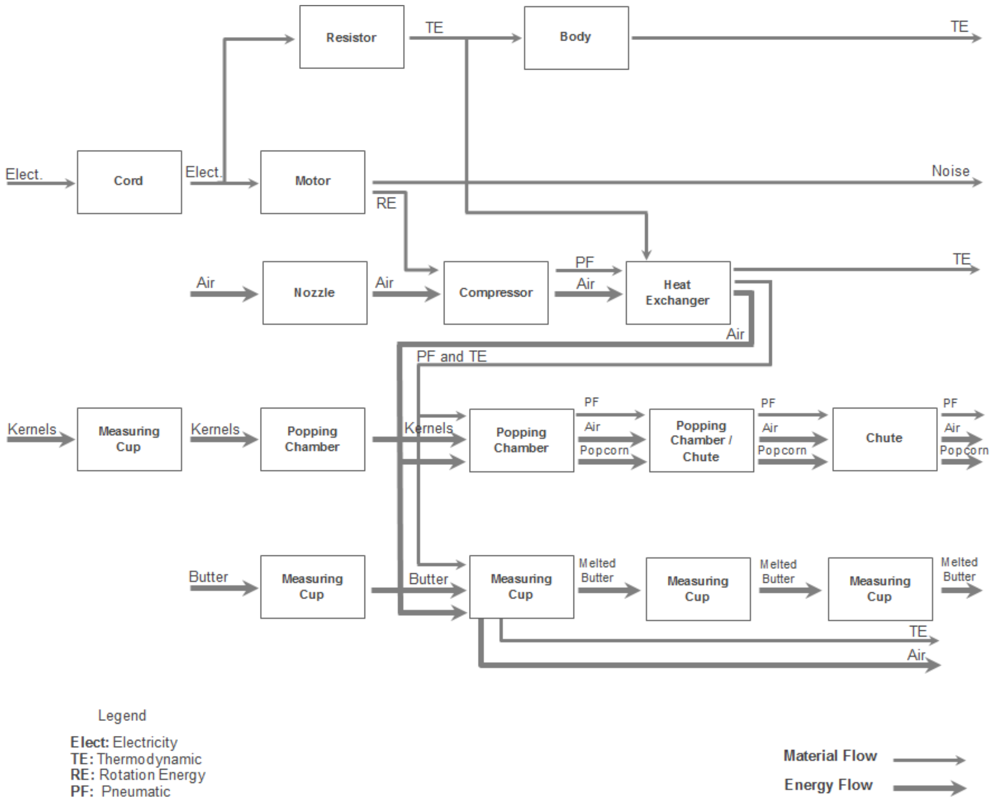


Fig. 11 : The Hot Air Popper components and the respective flows

The third step consists in the deployment of the primary functions based on the "why-how" approach, and the forth step is related to the deployment of the secondary functions. With these two steps, the FAST diagram is completed. To achieve the overall function – pop corn kernels – it is necessary to heat kernels by moving or storing kernels. With the hot air stream it is possible to move kernels, and in the end the air is heated and pumped to form a circuit. The secondary functions are related to melt butter and remove the popcorn. Figure 12 shows the complete diagram.

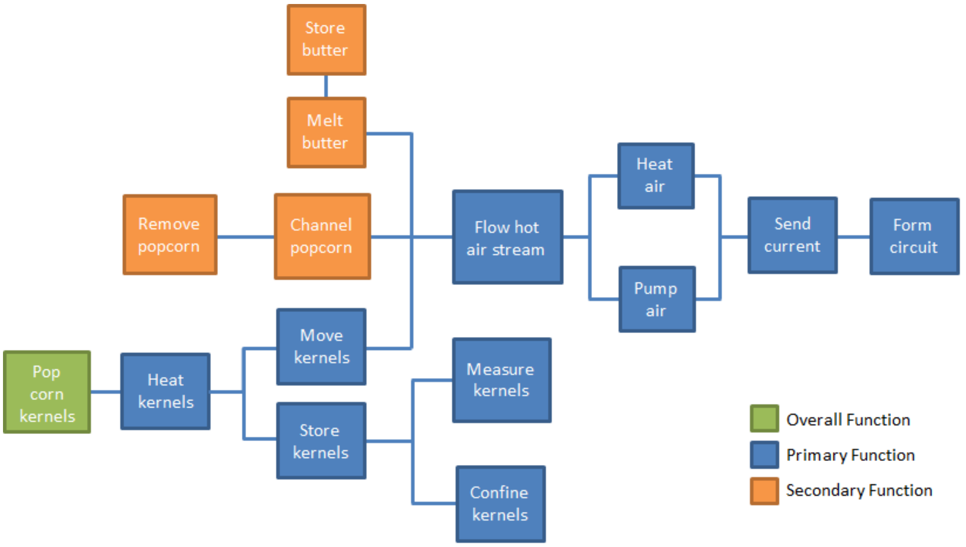


Fig. 12 : FAST diagram of the Hot Air Popper

The step 5 is the execution of the functional deployment according to [16]. As mentioned before, in this example this step is based on the deployment proposed by [18]. Finally, step 6 is the result of the superposition of the function tree and the function structure. It is possible to verify the correlation between the FAST diagram and the Pahl and Beitz functional deployment in figure 13.

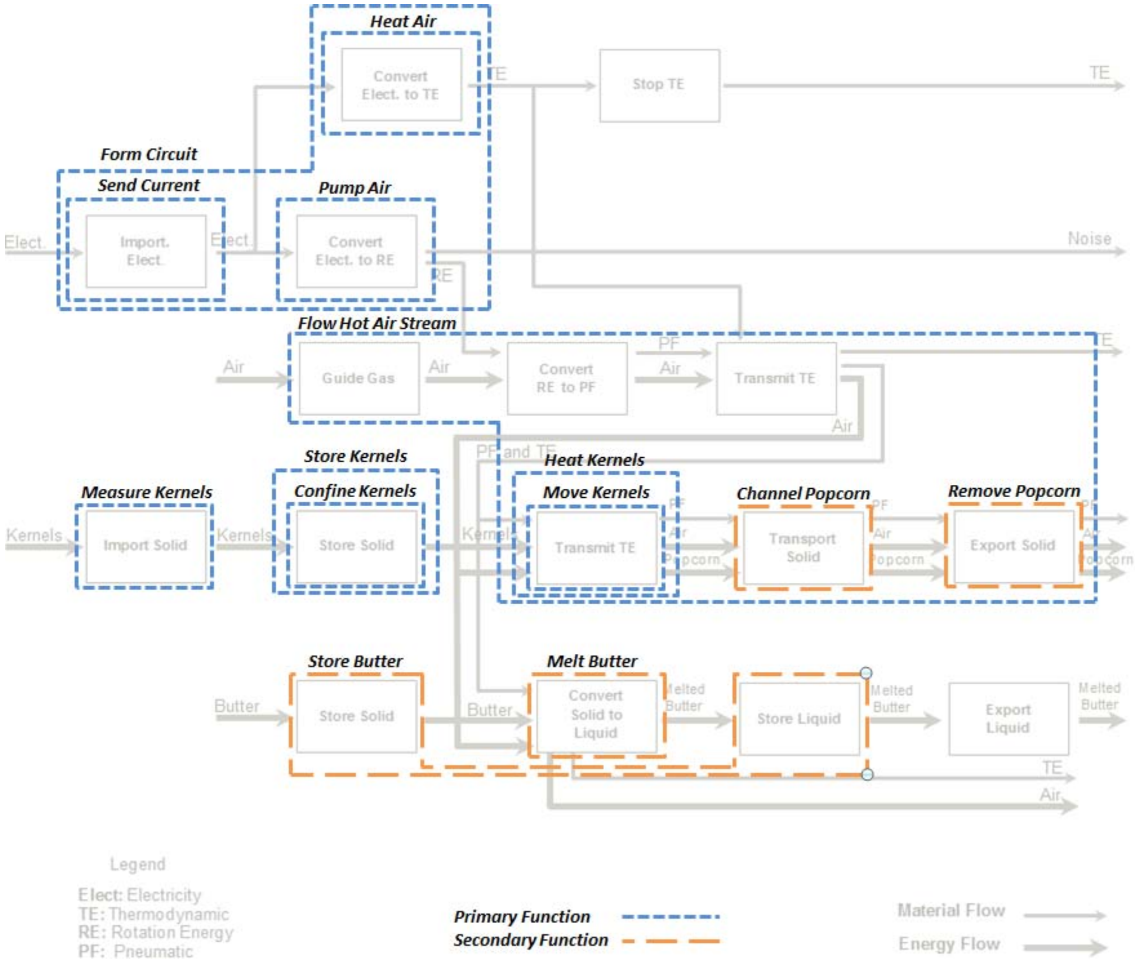


Fig. 13 : The function structure and function tree merge

This example presents a general view of how the proposed methodology correlates the functional deployments and the components. It enhances the design of products focused on the excellence of one characteristic (e.g. quality, manufacturing, cost, sustainability, etc.) because it supports the addition and/or substitution of functions. For example, in a future sustainable version of this product, a FAST function “recover heat loss” in figure 13 would be correlated to the FAST function “form circuit” and/or “heat air”. Automatically a Pahl and Beitz function “convert heat loss to electricity” would be added to the function structure, and finally a component that executes this function would be found, e.g. Peltier cell.

In Axiomatic Design the ideal product is decoupled, which means that every single part of it performs only one function [12]. The proposed methodology makes explicit the functional couplings in one single component. For example, by comparing figure 11 with figure 13, the popping chamber performs the functions “move kernel”, “heat kernels” and “flow hot air stream”; and the measuring cup executes “measure kernels”, “store butter” and “melt butter”. If it is necessary, the design team can optimize the butter melting by designing a specialized butter melting component, decoupling this function from the measuring cup. Thus, at the same time that the proposed methodology boosts the identification of couplings, it also supports the insertion of decoupling components.

During the execution of the proposed methodology, it is possible to notice some FAST functions with no correlation with Pahl and Beitz functions or vice versa. In figure 13, for example, the Pahl and Beitz functions “stop TE”, and “exportliquid” do not have a correlated FAST functions. Two hypotheses can be drawn: (a) there could be redundant or missing functions in one of the functional deployments; (b) there could be irrelevant functions in one of the functional deployments.

Finally, it is possible to link one component exclusively to primary functions, exclusively to secondary functions or both types of functions. For example, the compressor executes only a primary function (“flow hot air stream”), while the component “chute” executes one primary function (“flow hot air stream”) and two secondary functions (“channel popcorn” and “remove popcorn”). The design team can decide on splitting the components to execute exclusively primary or secondary functions, or on aggregating both types of function in one component depending on the value engineering.

VI. Concluding Remarks and Future Research

The theoretical basis allowed an analysis of the definition of the term function within the scope of design methodology. By doing that, a consensus among the several authors there were analyzed was noticed, in the semantic structure of a function based on the use of a verb and a noun. Nevertheless, these very same authors disagree over the categorization of function into hierarchical levels and purpose, and, mainly, when they transpose functions to the stages of functional analysis and function deployment. Upon dealing with tools that aim at both functional study and the classification of each function, it is possible to notice that there are conflicts regarding description and practical application stemming from the lack of clarity of the base terms. This context indicates that the study on the topic is pertinent, since it is necessary to fill in the gap left by both the definition of function and the methodology that approaches functional analysis. Therefore, the methodology proposed in this research aims at the functional study based on a need to form a representation that takes into consideration, at the same time, primary functions, secondary functions, sub-functions, and sub-systems. Considering that the proposal allows the function deployment of an Overall Function (OF), followed by the determination of Primary Functions (PF) and/or Secondary Functions (SF), divisions into Primary Sub-functions (PSF) and/or Secondary Sub-Functions (SSF) that, related to Sub-systems (SS), fulfill the Overall Function (OF), it is possible to approach alternative solutions and/or identify faults. The didactic example illustrates advantages of using the proposed methodology. The correlation between FAST functions and Pahl and Beitz functions is deeply explored, emphasizing the connection between both types of function and the product components. It allows the identification of couplings and the insertion of decoupling components. If there is one type of function with no connection, this function can be considered redundant or irrelevant or there are missing functions in the functional deployments. Thus, the proposed methodology indicates that the combination between FAST and Pahl and Beitz deployment results in a more comprehensive functional analysis by connecting function trees, function structures and components. In future researches the proposed methodology will be implemented by a multidisciplinary team on different areas of expertise such as hybrid vehicular dynamics and artisanal braiding in order to validate the procedure and contrast results.

VII. Acknowledgements

The authors thank CNPq (National Council for Scientific and Technological Development) and CAPES (the Brazilian federal agency for the support and evaluation of graduate education) for the support and for the incentive to the research.

References Références Referencias

1. Aurisicchio M, Bracewell R, Armstrong G (2013). The function analysis diagram: Intended benefits and coexistence with other functional models. Artificial intelligence for engineering design, Anal and Manuf, 27(03), 249-257.
2. Baxter M (1995) Product Design. CRC Press.
3. Bytheway CW (2007) Function Analysis Systems Technique Creativity and Innovation. J. Ross Publishing, 2007.
4. Celik HK, Lupeanu ME, Rennie AE, Neagu C, Akinci I (2013) Product re-design using advanced engineering applications and function analysis: a case study for greenhouse clips. Journal of the Brazilian Society of Mechanical Sciences and Engineering, 35 (3), 305-318.
5. Cross N (2008) Engineering Design Methods: Strategies For Product Design, 4th Edition, John Wiley And Sons Ltd., Chichester.
6. Csillag JMA (1995) Análise Do Valor. 4ed. São Paulo: Editora Atlas.
7. Eckert C (2013). That which is not form: the practical challenges in using functional concepts in design. Artificial intelligence for engineering design, Anal and Manuf, 27(03), 217-231.
8. Gopresto (2009) Hot Air Popper. Presto. https://www.gopresto.com/downloads/instructions/04820.pdf. Accessed 15 August 2014.
9. Hirtz J, Stone RB, McAdams DA, Szykman S, Wood KL (2002). A functional basis for engineering design: reconciling and evolving previous efforts. Research in Engineering Design, 13(2), 65-82.
10. Khanal YP, Buchal RO (2012). Towards an object–oriented engineering design pattern language. Journal of Design Research, 10(4): 293-306.
11. Liu, A., & Lu, S. (2013). Lessons learned from teaching axiomatic design in engineering design courses. Proceedings of the Seventh International Conference on Axiomatic Design, 99-106.
12. Mao KL (2014). Application of Axiomatic Design Theory in Multi-planetary Gear Transmission. International Journal of Mechanics and Materials in Design 536: 1306-1309.
13. Marques PA, Requeijo JG, Saraiva PM, Guerreiro FF (2013) Value-Based Axiomatic Decomposition (Part I): Theory and Development of the Proposed Method. Proceedings of the Seventh International Conference on Axiomatic Design, 18-25.

14. Mayda M, Börklü HR (2013) An integration of TRIZ and the systematic approach of Pahl and Beitz for innovative conceptual design process. Journal of the Brazilian Society of Mechanical Sciences and Engineering, 1-12.
15. Miles LD (1989) Techniques of Value Analysis and Engineering, 3rd edition.
16. Pahl G, Beitz W, Feldhusen J, Grote KH (2007) Engineering Design: a Systematic Approach. 3 Ed. Springer-Verlag London Limited.
17. Rozenfeld H, Forcellini FA, Amaral DC, Toledo JC (2006) Gestão De Desenvolvimento De Produtos: Uma Referência Para Melhoria Do Processo. São Paulo: Editora Saraiva.
18. Stone RB, Wood KL (2000). Development of a functional basis for design. Journal of Mechanical Design, 122(4), 359-370.
19. Suh NP (1998). Axiomatic design theory for systems. Research in Engineering Design, 10(4), 189-209.
20. SuhNP (2012). Fundamentals of design and deployment of large complex systems: OLEV, MH, and mixalloy. Journal of Integrated Design and Process Science, 16(3), 7-28.
21. Ullman DG (2003) The Mechanical Design Process. Boston: McGraw-Hill,
22. Ulrich KT, Eppinger, SD (2011) Product Design And Development, 5th Edition. New York: Mcgraw-Hill.
23. Verein DeutscherIngenieure (1987) Systematic approach to the development and design of technical systems and products, VDI 2221. Düsseldorf.
24. Vermaas PE (2013) The coexistence of engineering meanings of function: four responses and their methodological implications. Artificial intelligence for engineering design, 27(03), 191-202.
25. Yu F, Wang LF, Tan RH, Jin H (2012) An improved functional decomposition method based on FAST and the method of removal and operation. IEEE International Conference on System Science and Engineering, 487-492.

This page is intentionally left blank

Global Journal of Researches in Engineering: J
General Engineering
Volume 15 Issue 3 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4596 Print ISSN:0975-5861

Area Optimized Low Latency Karatsuba of man Multiplier Variant for Embedded ECC

By Sunil Devidas Bobade & Dr.Vijay R. Mankar
S.G.B. Amravati University Amravati, India

Abstract- Due to resource constrains, implementation of secure protocols for securing embedded systems has become a challenging task. System designers are advised to design and install area efficient versions of existing, proven security protocols. System designers are finding ways and means to compress existing security protocols without compromising security and without tampering with basic security structure of algorithm. Modular multiplication, point multiplication, point doubling are few critical activities to be carried out in ECC algorithm. By optimizing Modular Multiplier, area efficiency in ECC algorithm can be achieved. In this paper, we propose Area optimized and low latency multiplier that implements the efficient KOA algorithm in altogether novel style to be used in ECC architecture. The proposed algorithm uses a novel technique of splitting input operands based on exponent's parity and it eventually helps in reducing FPGA footprint and offers low latency by avoiding overlapping, prime concern for any embedded system. The complete modular multiplier and the crypto processor module is synthesized and simulated using Xilinx ISE Design suite 14.4 software. We have investigated area occupancy of proposed multiplier and crypto processor and concluded that proposed scheme occupies relatively reduced percentage area of FPGA as compared to the one using traditional KOA multiplier.

Keywords: *ECC, double point multiplication, karatsuba ofman multiplication, area optimization.*

GJRE-J Classification : *FOR Code: 291899*

Area Optimized Low Latency Karatsuba ofman Multiplier Variant for Embedded ECC

Sunil Devidas Bobade [α] & Dr.Vijay R. Mankar [σ]

Abstract- Due to resource constrains, implementation of secure protocols for securing embedded systems has become a challenging task. System designers are advised to design and install area efficient versions of existing, proven security protocols. System designers are finding ways and means to compress existing security protocols without compromising security and without tampering with basic security structure of algorithm. Modular multiplication, point multiplication, point doubling are few critical activities to be carried out in ECC algorithm. By optimizing Modular Multiplier, area efficiency in ECC algorithm can be achieved. In this paper, we propose Area optimized and low latency multiplier that implements the efficient KOA algorithm in altogether novel style to be used in ECC architecture. The proposed algorithm uses a novel technique of splitting input operands based on exponent's parity and it eventually helps in reducing FPGA footprint and offers low latency by avoiding overlapping, prime concern for any embedded system. The complete modular multiplier and the crypto processor module is synthesized and simulated using Xilinx ISE Design suite 14.4 software. We have investigated area occupancy of proposed multiplier and crypto processor and concluded that proposed scheme occupies relatively reduced percentage area of FPGA as compared to the one using traditional KOA multiplier.

Keywords: ECC, double point multiplication, karatsuba ofman multiplication, area optimization.

I. Introduction

Integrating security protocols in embedded systems is not an easy proposition. Embedded system designers have so far failed to install required levels of security in embedded systems, due to unusual design constraints like storage limitation, restricted processor performance and easy power drain in embedded devices. Regular cryptography algorithms are not suitable for Embedded systems due to wide footprint.

Due to resource constrains in the design and implementation of secure protocols, system designers are well advised to use area efficient versions of existing, proven security protocols, rather than developing their own protocols or implementations. This call for refined, area and space optimized; easy to deploy versions of original cryptography algorithms tailor made for resource constrained Embedded system.

Of the available choices, AES is the most powerful, most secured encryption algorithm with a key size ranging from 128 to 256. RSA is another well established and most preferred public key cryptography algorithm. To provide security equivalent to AES, RSA public-key sizes would have to range between 3,072 and 15,000 bits long, too big for embedded implementation. One appealing solution to the key size problem is the promising family of asymmetric algorithms known as Elliptic Curve Cryptography, or ECC.

Victor Miller and Neal Koblitz proposed the concept of elliptic curve cryptography in the mid of 1980's as an advancement in public key cryptographic systems such as DSA and RSA. The main advantage of ECC is the usage of shorter key helping compact implementations, resulting in faster cryptographic operations, running on smaller chips or more compact software. For hardware-based implementations of security functions, the benefits of ECC are more in comparison to RSA and AES. Optimized ECC chip designs have been designed and are as much as 37 times faster than its software counterparts. ECC offers other advantages of small software footprint, low hardware implementation costs, low bandwidth requirements, high device performance. Due to these many advantages of ECC a number of hardware implementations have been proposed, and included in many standards such as IEEE 1363and NIST.

Modular multiplication is the most primitive and critical operation in ECC. The design of Finite field multipliers is the complex design issue in the implementation of the ECC processor. A number of multipliers with different area and time complexity are reported in the available literatures. The Karatsuba Ofman algorithm is agreed upon as a most efficient multiplication algorithm and is widely adopted in VLSI implementation. Here input operands are processed as the "most significant half" and the "least significant half".

In proposed multiplier, instead of splitting input operands into the "most significant half" and the "least significant half", our method split operands according to the parity of multiplicands's exponent. Both the space and time complexities of the resulting multiplier are found to be much better than that of traditional multiplier. Here we have concentrated and investigated on area optimization. This is a significant achievement if we intend to use this multiplier in FPGA implementation of elliptical curve cryptography for embedded systems.

The basic step of Karatsuba Ofman's algorithm is a formula that computes the product of two large

Author α: Research Scholar, S.G.B. Amravati University Amravati, India. e-mail: sunilbobade73@gmail.com

Author σ: Deputy Secretary, R.B.T.E. Pune Region, Pune, India.

numbers using three multiplications of smaller numbers, each with about half as many digits as operands, plus some additions and digit shifts. Karatsuba Ofman method of multiplication is a faster way of multiplying two integers of length n. For the first step of the algorithm, it initially requires the breaking of multi digit integers into parts. These parts can then be used in three multiplications to produce a solution.

The Karatsuba algorithm is an effective multiplication algorithm. It diminishes the multiplication of two ***n*** -digit numbers to at most single-digit multiplications in general (and exactly when n is a power of 2). It is along these lines quicker than the traditional algorithms, which requires n^2 single-digit products. If n = 2^{10} = 1024, in particular, the precise counts are 3^{10} = 59,049 and $(2^{10})^2$ = 1,048,576, respectively. Here the operands α and β can be divided into two equal-size parts α_L and α_H , β_L and β_H respectively, which represent the $l/2$ higher and lower order bits of α and β . We can split them in two parts as follows:

$$\alpha(x)=\sum_{i=0}^{l-1}a_i x^i=\sum_{i=\frac{l}{2}}^{l-1}a_i x^i+\sum_{i=0}^{\frac{l}{2}-1}a_i x^i$$

$$=\alpha^{\frac{l}{2}}\sum_{i=0}^{\frac{l}{2}-1}a_{i+\frac{l}{2}}x^i+\sum_{i=0}^{\frac{l}{2}-1}a_i x^i$$

$$\alpha(x)=x^{\frac{l}{2}}\alpha_H+\alpha_L$$

Likewise,

$$\beta(x)=x^{\frac{l}{2}}\beta_H+\beta_L$$

The product $\gamma(x)*$ can be computed as

$$\gamma(x)*=\alpha(x).\beta(x)$$

By using above equation output can be represented as,

$$\gamma(x)*=\alpha_L\beta_L+\alpha_H\beta_H x^l+(\alpha_H\beta_L+\alpha_L\beta_H)x^{\frac{l}{2}}$$

To further improve the computation of the product $\gamma(x)*$ equation can be modified as,

$$\gamma(x)*=\alpha_L\beta_L+\alpha_H\beta_H x^l+(\alpha_L\beta_L+\alpha_H\beta_H+(\alpha_H+\beta_L)(\beta_H+\beta_L)x^{\frac{l}{2}}$$

II. Related Work

Several modular multiplication algorithms have been proposed. Of them all, Karatsuba- Ofman algorithm, KOA is widely used for performing modular arithmatic. In [1] a variant of Karatsuba multiplier of the type GF $((2^n)^8$ is presented and is highly area efficient. Kimmo U. Järvinen *et.al* [2] adopted an efficient implementation of point multiplication on Koblitz curves and was designed for extremely-constrained, secure applications. In that approach a new technique was introduced for point addition which required fewer registers and small processor. In [3] Hossein Mahdizadeh and Massoud Masoumi built elliptic curve cryptographic processor by organizing multipliers in parallel.

In [4], hybrid multiplier was proposed that intelligently switches between two variants of multiplier depending on the size of multiplicands. The Karatsuba multiplier is efficient algorithm ensuring fewer LUTs and stable number of Flip-flops for the smaller bit multiplications, while the systolic variant ensures fewer LUTs count for the bigger size multiplicands. This hybrid multiplier does the initial recursion using the systolic algorithm while final small sized multiplications are accomplished using the Karatsuba algorithm. Area analysis report suggested that by using a hybrid multiplier instead of just traditional Karatsuba Multiplier, eventually helps in reducing FPGA footprint. This hybrid multiplier exhibits a savior of 7.56 % in terms of Flip flop slices. Involves 52 % fewer LUTs and utilizes 47% fewer slices as compared to traditional Karatsuba multiplier for 256 bit multiplication.

In [5], FPGA based area efficient ECC processor was built using Digit multiplier. Instead of processing vector (polynomial) bit by bit or parallelly, operands are process in 16-bit word format. This Modular multiplier exhibits a savior of 23.88% in terms of Flip flop slices. Proposed Multiplier involves 62 % fewer LUTs and utilizes 59% fewer slices as compared to traditional Karatsuba multiplier for 256 bit multiplication. Further reduction was achieved in ECC processor by employing efficient double point multiplication algorithm.

Area and speed efficient 163 bit Scalar multiplier with improved area and speed was designed by Sujoy Sinha Roy *et.al* [6]. Scalar multiplication was performed on Xilinx Virtex V platforms over GF (2^{163}). The implementation used a novel three stage pipelined bit-parallel Karatsuba multiplier with subquadratic complexity. Scalar multiplication algorithm, optimized field primitives, balanced pipeline stages, and enhanced scheduling of point arithmetic all contributed to a high-speed architecture with a significantly small area Hybrid binary-ternary number system for elliptic curve cryptosystems was designed by Jithra Adikari *et.al* [7]. In their newly designed system three novel algorithms for both single and double scalar multiplication were implemented. The first algorithm is w-HBTF and the other two algorithms, namely, HBTJF and RHBTJF. The output results showed that hybrid algorithms are almost always faster than classical w-NAF methods or JSF. Kazuo Sakiyama et.al [8] implemented modular multiplication algorithm that integrates three different existing algorithms, based on Barrett reduction and

Montgomery reduction. This modular multiplier is highly speed efficient.

III. Proposed Area Optimized Low Latency Multiplier

Proposed multiplier is based on Karatsuba Ofman Algorithm. Two operands A and B in KOA can be represented in polynomial format as

$$\mathrm{A} = \sum_{i=0}^{n-1} \mathrm{a_i X^i}$$

$$= X^m \sum_{i=0}^{m-1} a_{m+i} X^i + \sum_{i=0}^{m-1} a_i X^i$$

$$= \mathrm{X^m A_H + A_L}$$

Similarly,

$$\mathrm{B} = \sum_{i=0}^{n-1} \mathrm{b_i X^i}$$

$$= X^m \sum_{i=0}^{m-1} b_{m+i} X^i + \sum_{i=0}^{m-1} b_i X^i$$

$$= \mathrm{X^m B_H + B_L}$$

Where

$$\mathrm{A_H} = \sum_{i=0}^{m-1} a_{m+i} X^i \text{ and } \mathrm{A_L} = \sum_{i=0}^{m-1} a_i X^i$$

$$\mathrm{B_H} = \sum_{i=0}^{m-1} b_{m+i} X^i \text{ and } \mathrm{B_L} = \sum_{i=0}^{m-1} b_i X^i$$

The product of A and B can be written as

$$\mathrm{AB = A_H B_H X^{2m} + \{[(A_H + A_L)(B_H + B_L)]}$$

$$\mathrm{- [A_H B_H + A_L B_L]\}Xm + A_L B_L}$$

In Modulo 2 domain, addition and subtraction operation can be accomplished using XOR Gate and product using AND gate. Total gates involved for implementing above expression will be five AND gates for accomplishing five multiplication activities and four XOR gates for performing modulo 2 addition. Further, it is a three level realization, as input operand has to pass through maximum of three levels of XOR gate before reaching output line because of overlapping. Therefore, total XOR gate delay for implementing the above expression will be $3T_D$ besides the cost of the recursive computation of the three partial products. Thus basic KOA multiplier utilizes five AND gates and four XOR gates to accomplish the basic multiplication activity.

Instead of splitting input operands into the "most significant half" and the "least significant half", the method split operands according to the parity of X's exponent.

Accordingly, Operands A and B may be rewritten as

$$\mathrm{A} = \sum_{i=0}^{n-1} \mathrm{a_i X^i}$$

$$= \sum_{i=0}^{m-1} a_{2i} X^{2i} + \sum_{i=0}^{m-1} a_{2i+1} X^{2i+1}$$

$$= \sum_{i=0}^{m-1} a_{2i} X^{2i} + X \sum_{i=0}^{m-1} a_{2i+1} X^{2i}$$

Similarly,

$$\mathrm{B} = \sum_{i=0}^{n-1} \mathrm{b_i X^i}$$

$$= \sum_{i=0}^{m-1} b_{2i} X^{2i} + \sum_{i=0}^{m-1} b_{2i+1} X^{2i+1}$$

$$= \sum_{i=0}^{m-1} b_{2i} X^{2i} + X \sum_{i=0}^{m-1} b_{2i+1} X^{2i}$$

Now let us define

$$\mathrm{A_E} = \sum_{i=0}^{m-1} a_{2i} X^{2i} \qquad \mathrm{A_O} = \sum_{i=0}^{m-1} a_{2i+1} X^{2i}$$

$$\mathrm{B_E} = \sum_{i=0}^{m-1} b_{2i} X^{2i} \qquad \mathrm{B_O} = \sum_{i=0}^{m-1} b_{2i+1} X^{2i}$$

Let i=2 and X^2=Y,

Then product AB can be written as

$$\mathrm{AB = (A_E(y) + XA_O(y))\ (B_E(y) + XB_O(y)) = \{A_E(y)B_E(y) + X^2A_O(y)B_O(y)\} + X\{A_E(y)B_O(y) + A_O(y)B_E(y))\}}$$

Applying KOA formula to above expression,

$$\mathrm{= \{[A_E(y)B_E(y) + YA_O(y)B_O(y)]\} + X\{[(A_E(y) + A_O(y))(B_E(y) + B_O(y))] - [A_E(y)B_E(y) + A_O(y)B_O(y)]\}}$$

In VLSI implementation of above expression multiplying a polynomial by x or y = x^2 is equivalent to shifting its coefficients left, and no gate is required. For implementing this revised expression four AND gates and three XOR gates are required. The expressions in the three square brackets can be computed concurrently, and these addition operations require one XOR gate delay $1T_D$. We conclude that computing product AB needs only a total delay of $2T_D$ besides the cost of the recursive computation of the three partial products.

Compared to the $3T_D$ gate delays required in traditional formula, one XOR gate delay $1T_D$ is saved for each recursive iteration. Thus compared to the four EXOR gates delays required in traditional formula, one XOR gate and also one AND gate is saved for each recursive iteration, which is a significant achievement considering embedded systems are highly resource constrained. . Thus this variant of KOA multiplier utilizes four AND gates and three XOR gates to accomplish the basic multiplication activity.

Table 1 : Resource Utilization Comparison of Two Multipliers

	Karatsuba Ofman Multiplier				Proposed New Version Multiplier			
Multiplicand Size	Flip flops	LUTs	Occupied Slices	IOBs	Flip flops	LUTs	Occupied Slices	IOBs
2 bit	17	25	16	9	15	16	13	9
4 bit	32	75	43	17	21	31	19	13
8 bit	46	150	79	33	29	57	32	21
16 bit	54	162	87	65	45	78	42	37
32 bit	102	315	168	129	81	142	78	69
64 bit	266	665	411	257	145	270	143	133
128 bit	646	1782	1000	513	273	526	272	261
256 bit	1118	13761	7008	913	530	1038	529	517

From the above basic concept, it is observed that by splitting the operand polynomials, based on the parity, results in reduction of hardware (fewer AND and XOR gates) and latency time (fewer levels due to little overlapping). By extending this very concept of splitting the operands based on parity to FPGA implementation, we have explored and implemented FPGA based finite field multiplier and compared FPGA footprint with that of traditional KOA multiplier. Also we have incorporated the proposed multiplier in ECC processor and investigated its impact on the footprint of entire processor. In this paper, we have only concentrated on area occupancy of proposed multiplier, its impact on processor footprint but haven't investigated quantum of latency improvement, which forms the future scope of investigation.

IV. Results and Discussion

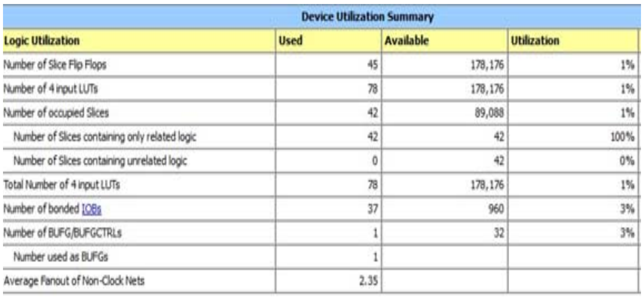
In this section, we focus on the FPGA implementation of the proposed multiplier. The proposed architecture is coded in verilog HDL and is synthesized using Xilinx ISE version 14.4 design software and is implemented on Xilinx Virtex-4 xc4vlx200ff1513 FPGA. The RTL schematic for the proposed Finite Field multiplier is shown in figure 1.

Fig. 1 : RTL Diagram of Proposed multiplier

a) *Area Report of Proposed Multiplier*

Since the area of the complete processor mainly depends on the incorporated GF multiplier, most of the slices in the target device are utilized by it. From table 2, for 16 bit multiplicands, proposed modular Multiplier needs 42 slices out of 89,088 available slices in the target device. Among the 178,176 available four input LUTs only 78 are used. The multiplier also needs only 45 out of 178,176 Flip Flops.

Table 2 : Resource Utilization By Multiplier For L=16



Device Utilization Summary			
Logic Utilization	Used	Available	Utilization
Number of Slice Flip Flops	45	178,176	1%
Number of 4 input LUTs	78	178,176	1%
Number of occupied Slices	42	89,088	1%
Number of Slices containing only related logic	42	42	100%
Number of Slices containing unrelated logic	0	42	0%
Total Number of 4 input LUTs	78	178,176	1%
Number of bonded IOBs	37	960	3%
Number of BUFG/BUFGCTRLs	1	32	3%
Number used as BUFGs	1		
Average Fanout of Non-Clock Nets	2.35		

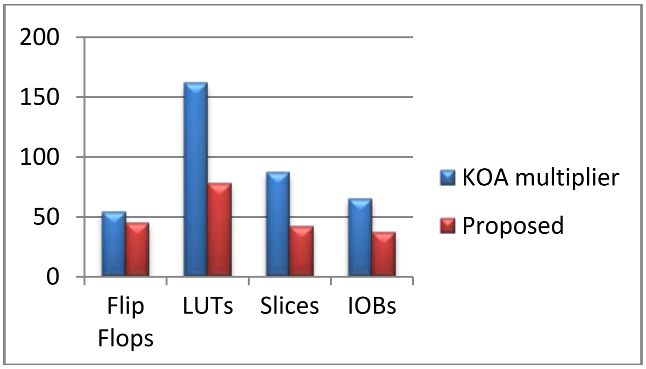
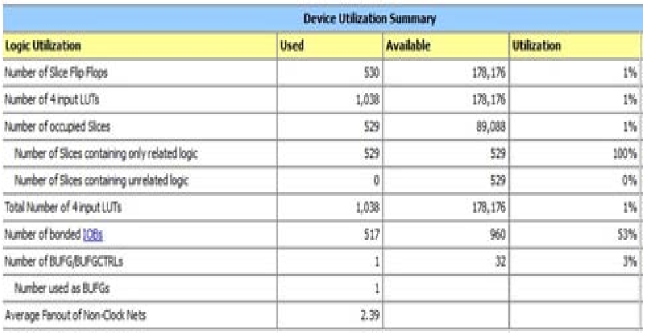


Fig. 2 : Resource utilization comparison of two KOA variants for L=16

A bar chart representation shown in figure 2 compares the resource utilization of Proposed multiplier with traditional Karatsuba Ofman Multiplier for L =16. Thus proposed multiplier exhibits a savior of 20 % in terms of Flip flop slices. Proposed Multiplier involves 53 % fewer LUTs and utilizes51.72% fewer slices as compared to traditional Karatsuba Ofman multiplier for 16 bit multiplication. This helps in bringing down the footprint of modular multiplier on FPGA while building cryptography schemes.

Table 3 : Resource Utilization By Multiplier For L=256



Device Utilization Summary			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Flip Flops	530	178,176	1%
Number of 4 input LUTs	1,038	178,176	1%
Number of occupied Slices	529	89,088	1%
Number of Slices containing only related logic	529	529	100%
Number of Slices containing unrelated logic	0	529	0%
Total Number of 4 input LUTs	1,038	178,176	1%
Number of bonded IOBs	517	960	53%
Number of BUFG/BUFGCTRLs	1	32	3%
Number used as BUFGs	1		
Average Fanout of Non-Clock Nets	2.39		

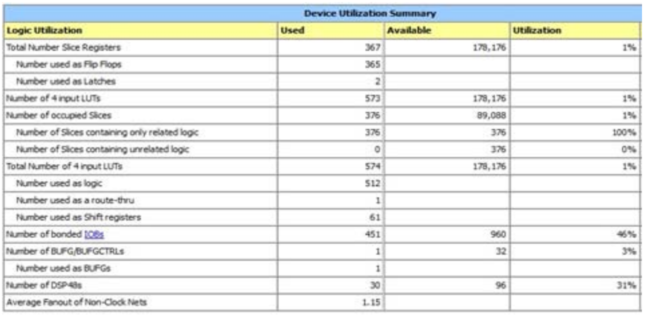
This saviour is more significant for L= 256. Proposed multiplier exhibits a savior of 52.49 % in terms of Flip flop slices. Proposed Multiplier involves 92 % fewer LUTs and utilizes 92% fewer slices as compared to traditional Karatsuba multiplier for 256 bit multiplication as indicated in table 3.

b) Area Report of Crypto Processor

The ECC processor implementation uses a double point multiplication algorithm proposed in [9]. We have adapted revised and area optimized version of Montgomery's PRAC algorithm [10]. The area comparision is carried out for crypto processors using proposed multiplier the one proposed in [11].

Table 4 below shows device utilization summary of Crypto processor, when the above proposed multiplier is employed for performing modular multiplications. Processor needs 376 slices out of 89,088 available slices in the target device. Among the 178,176 available four input LUTs only 573 are used. The multiplier also needs only 451 out of 178,176 Flip Flops.

Table 4 : Resource Utilization by Ecc Processor



Device Utilization Summary			
Logic Utilization	**Used**	**Available**	**Utilization**
Total Number Slice Registers	367	178,176	1%
Number used as Flip Flops	365		
Number used as Latches	2		
Number of 4 input LUTs	573	178,176	1%
Number of occupied Slices	376	89,088	1%
Number of Slices containing only related logic	376	376	100%
Number of Slices containing unrelated logic	0	376	0%
Total Number of 4 input LUTs	574	178,176	1%
Number used as logic	512		
Number used as a route-thru	1		
Number used as Shift registers	61		
Number of bonded IOBs	451	960	46%
Number of BUFG/BUFGCTRLs	1	32	3%
Number used as BUFGs	1		
Number of DSP48s	30	96	31%
Average Fanout of Non-Clock Nets	1.15		

We have investigated area occupancy of cryptoprocessr built using proposed variant of Karatsuba Ofman multiplier and compared it with similar ECC work. Bar chart representation shown in figure 3 compares the resources utilized by proposed ECC with a similar work [11]. The comparison of implemented ECC processor employing proposed modular multiplier and the crypto Processor using traditional Karatsuba Multiplier with respect to the area occupied (Slice registers, Slices, LUTs and IOBs) is tabulated in Table 5 and compared in figure 3. Proposed implementation utilize about 23.93 % reduced slices and 62.65 % fewer LUTs. This is a significant achievement as we intend to put this ECC hardware for providing security services in embedded system which is known to be highly resources thirsty.

Table 5 : Resource Utilization Comparison of Two Ecc Processors

Work	/	Slices	LUTs	IOBs
[11]	193	466	932	932
Proposed	233	376	573	451

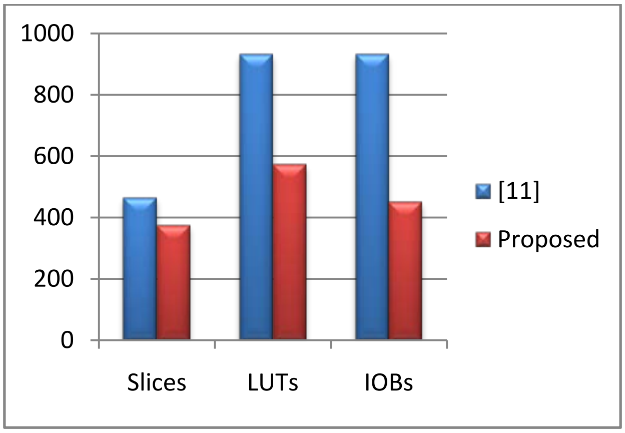


Fig. 3 : Resource utilization comparison of ECC processor using proposed multiplier and [11]

V. Conclusion

We have proposed a novel method to implement the modular multiplier for performing critical multiplication activities in ECC processor. Area occupancy of the resulting multiplier is found to be far superior than that of traditional KOA multiplier. This contributes in bringing down the footprint of entire ECC process. While injecting this modification, nowhere we have tampered with the basic flow and structure of basic ECC protocol. Just by processing the operands in different style, we have achieved area optimization of complete ECC protocol and made it suitable for embedded system with no compromise on security of ECC algorithm.

References Références Referencias

1. C. Paar A new architecture for a parallel finite field multiplier with low complexity based on composite fields. IEEE Transactions on Computers, 45(7): 856- 861, July 1996.
2. Azarderakhsh. R, Jarvinen K.U and Mozaffari-Kermani. M, "Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications", IEEE Transactions on circuits and systems- I, Vol. 61, No. 4, April 2014.

3. Hossein Mahdizadeh and Massoud Masoumi, "Novel architecture for efficient FPGA implementation of elliptic curve cryptographic processor over GF(2^{163})", IEEE Transactions on very large scale integration (vlsi) systems, Vol. 21, NO. 12, pp: 2330- 2333, Dec.2013.
4. Sunil Devidas Bobade and Dr. Vijay R. Mankar," Low footprint Hybrid Finite field multiplier for Embedded cryptography", International Journal of Computer Science and Information Security(IJCSIS), Vol. 13, No. 3, pp: 28- 32, March 2015.
5. Sunil Devidas Bobade and Dr. Vijay R. Mankar," Space optimized Multiplier Architecture for Embedded cryptography", International Journal of Computer and Applications (IJCA), Vol. 113, No. 14, pp: 26- 32, March 2015.
6. Roy. S.S, Rebeiro, C and Mukhopadhyay D, "Theoretical modeling of elliptic curve scalar multiplier on LUT-based FPGAs for area and speed", IEEE Transactions on Very Large Scale Integration (VLSI) systems, Vol. 21, No. 5, May 2013.
7. Azarderakhsh. R, Jarvinen K.U and Mozaffari-Kermani. M,"Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications", IEEE Transactions on circuits and systems- I , Vol. 61, No. 4, April 2014.
8. Kazuo Sakiyama, Miroslav Knezevica, Junfeng Fana, Bart Preneela, and Ingrid Verbauwhedea, "Tripartite modular multiplication", Integration, the VLSI Journal, Vol. 44, No.4, pp: 259–269, September 2011.
9. Roy. S.S, Rebeiro, C and Mukhopadhyay. D, "Theoretical modeling of elliptic curve scalar multiplier on LUT-based FPGAs for area and speed", IEEE Transactions on Very Large Scale Integration (VLSI) systems, Vol. 21, No. 5, May 2013.
10. R. Azarderakhsh and K. Karabina, "A New Double Point Multiplication Algorithm and its Application to Binary Elliptic Curves with Endomorphisms", IEEE Transactions on Computers, to appear: pp, 2013.
11. A. Kaleel Rahuman and G. Athisha, "Reconfigurable Architecture for Elliptic Curve Cryptography Using FPGA", Hindawi Publishing Corporation Mathematical Problems in Engineering, 2013.

Global Journal of Researches in Engineering: J
General Engineering
Volume 15 Issue 3 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4596 Print ISSN:0975-5861

Security in Untrusted Updated Environments

By Jahnavi Terva, Jaya Krishna K & K. Kondaiah
K L University, India

Abstract- At present days, technology growth was rapid and its use is very often. So the attacks were concentrated on the user systems mainly by using the network applications. Bugs in the application of a network can ruin the applications in a system that are running. When the user is in the use of internet or e-commerce sites, etc.., the applications will be considered that they are in an unsafe environment. Providing security to the network applications like web servers, mails, etc... Is very difficult because they are usually very big applications to make them free from bugs.

Now this paper describes how to provide security to the network applications which are in unsafe environment. This idea describes that all the applications were wrapped together for the security purpose and there will be no use to rewrite the network applications.

Keywords: internet security, network applications, secure environment [2], sandbox technique.

GJRE-J Classification : FOR Code: 090799

SECURITYINUNTRUSTEDUPDATEDENVIRONMENTS

Strictly as per the compliance and regulations of :

Security in Untrusted Updated Environments

Jahnavi Terva [α], Jaya Krishna [σ] K & K. Kondaiah [ρ]

Abstract- At present days, technology growth was rapid and its use is very often. So the attacks were concentrated on the user systems mainly by using the network applications. Bugs in the application of a network can ruin the applications in a system that are running. When the user is in the use of internet or e-commerce sites, etc.., the applications will be considered that they are in an unsafe environment. Providing security to the network applications like web servers, mails, etc... Is very difficult because they are usually very big applications to make them free from bugs.

Now this paper describes how to provide security to the network applications which are in unsafe environment. This idea describes that all the applications were wrapped together for the security purpose and there will be no use to rewrite the network applications.

Keywords: internet security, network applications, secure environment [2], sandbox technique.

I. Introduction

Because of the easy access of the Internet throughout the globe, many various applications can be runned on the hardware platforms, which gives any opportunities in the commercial field. Developing an application is also an issue for providing the security from the internal attacks of users system. With a correct Securitas guard, the attacks can be detected. Different security solutions should be provided to the different attacks from the network. Many applications which are developed cannot provide a guarantee that can give total security. To develop a bug free application is very complex for the network applications which can result in a security issue.

In this paper, CMW which mean Common Mode Workstation Operating system with a B1-level grade is used to secure the applications from the unsafe helper environments. In this rewriting will not be done for an existing application as the applications will be wrapped and can be upgraded safely and securely.

II. Background

There are many protocols for the network security like SHTTP, SHHP, TLS, BITCOIN Protocol, etc… to give some protection where the communication is done at the two Ends of a receiver and sender. Unwanted connections can be kept out by using the Firewall [3]. If the bugs which are hidden in the server side is connected with the data of a user that may lead to the leakage of data from user system. Because of the bugs that are present in the network applications, either internal attacks can be done to sensitive data or leakage of data will be done. Providing security to a network application is almost impossible. While providing security, rewriting of the application will be done which also leads to a security issue. Mainly while providing security to the social networking sites is a complex issue.

While opening these networking sites the data transfer should not be done from receiver to the sender. All the applications should be developed keeping the security issue in the mind.

III. Existing Techniques

The traditional technique used is called sandboxing which can prevent the vulnerable applications running in a confined environment. Protecting the data from hackers and unwanted network applications from the break ins. There are many possibilities to the hacker to develop many privileged applications to break the security policies. Let us consider an example TIS96 which depends on the physically distinguish hardware which gives us information separation. Another example GWT96 which depends on operating systems. There is a user and security check at the user level. There is still the possibilities that the hacker can make use of compromised privileged applications to alter the security policies and further his attacks.

IV. Our Approach for Security

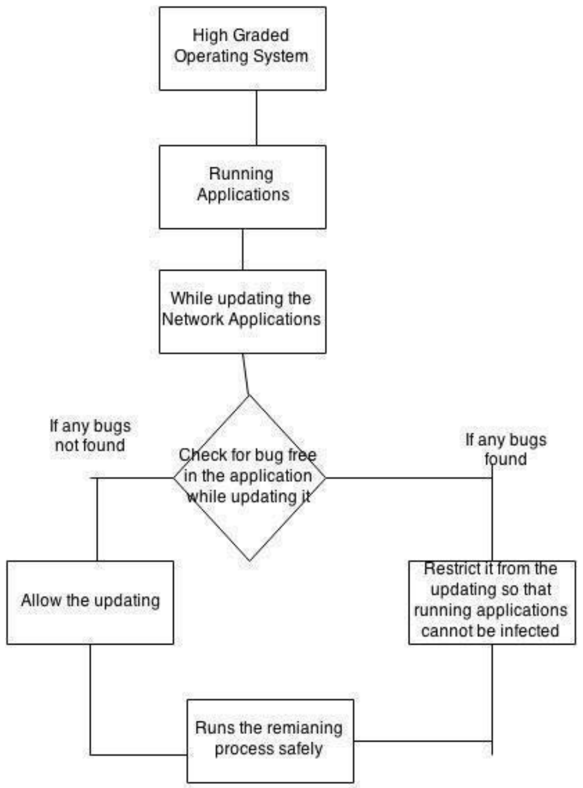
HP-UX[1] CMW can be used to combine all the untrusted network applications. In this approach we are going to design an Operating systems [5] that facilitates a group of fine grained administrative security assigns and operations to handle these assigns. Security checks should be done at each level to the Operating System in which process are running simultaneously so that it can guarantee maximum protection. Because of these features, it will be able to distinguish the network application format from security format, to provide a general platform for combining the existing untrusted dumb applications for security. For explaining how to use CMW in sandbox for untrusted applications, for serving as case studies we took two typical examples. One of those examples is the HP's Presidium Virtual Vault, which prevents the unauthorized access unauthorized modification of the data in the server by wrapping the Web server. Other example is Trusted Send mail Proxy which was developed in HP Labs[4],

Author α σ ρ: Dept. of Electronics and Computer Engineering, K L University, Guntur. e-mails: jahnaviterva@gmail.com, smile.jayakrishna@gmail.com, kondaya.kuppala@kluniversity.in

Bristol and this prevents highly privileged but vulnerable send mail that are running on the system without causing any fatal damages to the users system.

The objective of the work is to provide the network application services safely by combining untrusted applications and to have a view on the advantages of introducing CMW to solve the security issues in the commercial field.

V. Flow Chart for the Approach


High Graded Operating System
Running Applications
While updating the Network Applications
Check for bug free in the application while updating it
If any bugs not found
If any bugs found
Allow the updating
Restrict it from the updating so that running applications cannot be infected
Runs the remiang process safely

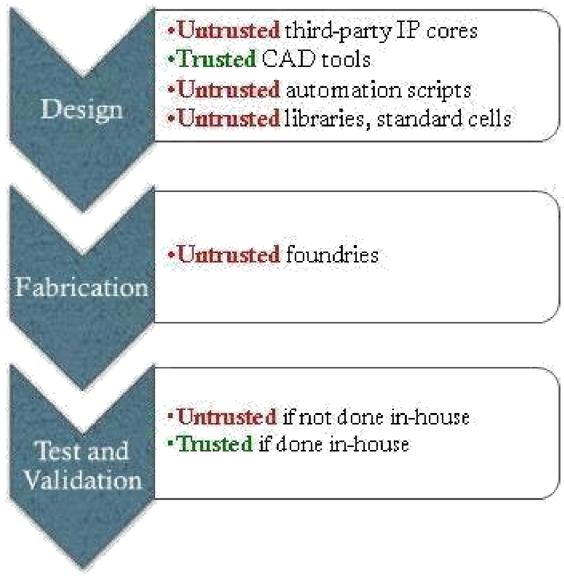

Design
•Untrusted third-party IP cores
•Trusted CAD tools
•Untrusted automation scripts
•Untrusted libraries, standard cells
Fabrication
•Untrusted foundries
Test and Validation
•Untrusted if not done in-house
•Trusted if done in-house

Fig. 1 : Example of tokens to be generated for security purpose to the network application

VI. Working of the Idea to Provide Security to Application

a) Finding an restricted process

The parent and child privileges are given to the applications which are to be updated so that safe transfer of the information can be done. Let us consider an example in which a child process cannot get access to the privileges of a parent process by inheriting, it can be restricted as inheritance is an automatic process. If it can get access from the parent process it can be given an token that it is an trusted application. So by this way we can find which process is to be restricted and which process is to be continued with security. If the child process which cannot gain access is allowed to continue further it leads to a serious issue for the internal attacks of the users system.

b) How CMWis used to combine the Untrusted Applications

As our objective is to prevent an third party gaining the access of user's system and to protect oneself from the untrusted vulnerable network applications. We use two typical network applications to wrap the application data i.e. by using the web server and send mail illustrating what is done to apply the methods to give security. A trusted mail is sent at the ending by illustrating what is done in the process.

VII. Security Analysis of the Network Application

Even if the data is broken by the bugs then the damage will be confined to only the compartment which is considered as system inside. It doesn't harm much because the data in the system inside of the operating systems cannot get access to the connections of the data which is provided from outside network.

VIII. Conclusion and Future Work

An operating system with highly grained administrative security management helps to meet many security policies while using the network applications and can protect us from an intruder accessing the gain root access of the data in a system of user. Security dumb applications can be easily found and can be issued an unsafe token to prevent access and is restricted. Depending on the various commercial applications security infrastructures should be modified according to that and should have possibility to extend the CMW for the application platform of that network.

References Références Referencias

1. Hewlett-Packard, "HP-UX Compartmented Mode Workstation key security concepts", 1996.
2. Ian Goldberg, David Wagner, Randi. Thomas and Eric A. Brewer, "A secure Environment for Untrusted Helper Applications --- Confining the Wily Hacker".

3. W.R. Cheswick, S. M. Bellovin, “Firewalls and Internet Security - Repellimg the Wily Hacker”, Addison-Wesley, 1994.
4. Andrew Berman, Virgil Bourassa, and Erik Selberg. TRON: Process-speci_c _le protection for the UNIX operating system. In Proc. 1995USENIX Winter Technical Conference, pages 165{175. USENIX Assoc 1995.}
5. Robert Wahbe, Steven Lucco, Thomas E. Anderson, and Susan L. Graham. Efficient software-based fault isolation. In Proc. of the Symp. On Operating System Principles, 1993.

Global Journals Inc. (US) Guidelines Handbook 2015

www.GlobalJournals.org

Fellows

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN ENGINEERING (FARSE)

Global Journals Incorporate (USA) is accredited by Open Association of Research Society (OARS), U.S.A and in turn, awards “FARSE ” title to individuals. The 'FARSE' title is accorded to a selected professional after the approval of the Editor-in-Chief /Editorial Board Members/Dean.

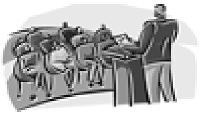
- The “FARSE” is a dignified title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FARSE or William Walldroff, M.S., FARSE.

FARSE accrediting is an honor. It authenticates your research activities. After recognition as FARSE, you can add 'FARSE' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, and Visiting Card etc.

The following benefits can be availed by you only for next three years from the date of certification:

FARSE designated members are entitled to avail a 40% discount while publishing their research papers (of a single author) with Global Journals Incorporation (USA), if the same is accepted by Editorial Board/Peer Reviewers. If you are a main author or co-author in case of multiple authors, you will be entitled to avail discount of 10%.

Once FARSE title is accorded, the Fellow is authorized to organize a symposium/seminar/conference on behalf of Global Journal Incorporation (USA).The Fellow can also participate in conference/seminar/symposium organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent.

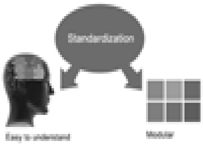


You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time.This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The FARSE can go through standards of OARS. You can also play vital role if you have any suggestions so that proper amendment can take place to improve the same for the benefit of entire research community.

As FARSE, you will be given a renowned, secure and free professional email address with 100 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders,Auto-Responders, Email Delivery Route tracing, etc.



The FARSE will be eligible for a free application of standardization of their researches. Standardization of research will be subject to acceptability within stipulated norms as the next step after publishing in a journal. We shall depute a team of specialized research professionals who will render their services for elevating your researches to next higher level, which is worldwide open standardization.

The FARSE member can apply for grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A. Once you are designated as FARSE, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria. After certification of all your credentials by OARS, they will be published on your Fellow Profile link on website https://associationofresearch.org which will be helpful to upgrade the dignity.

The FARSE members can avail the benefits of free research podcasting in Global Research Radio with their research documents. After publishing the work, (including published elsewhere worldwide with proper authorization) you can upload your research paper with your recorded voice or you can utilize chargeable services of our professional RJs to record your paper in their voice on request.

The FARSE member also entitled to get the benefits of free research podcasting of their research documents through video clips. We can also streamline your conference videos and display your slides/ online slides and online research video clips at reasonable charges, on request.

The FARSE is eligible to earn from sales proceeds of his/her researches/reference/review Books or literature, while publishing with Global Journals. The FARSE can decide whether he/she would like to publish his/her research in a closed manner. In this case, whenever readers purchase that individual research paper for reading, maximum 60% of its profit earned as royalty by Global Journals, will be credited to his/her bank account. The entire entitled amount will be credited to his/her bank account exceeding limit of minimum fixed balance. There is no minimum time limit for collection. The FARSE member can decide its price and we can help in making the right decision.

The FARSE member is eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get remuneration of 15% of author fees, taken from the author of a respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN ENGINEERING (MARSE)

The ' MARSE ' title is accorded to a selected professional after the approval of the Editor-in-Chief / Editorial Board Members/Dean.

The “MARSE” is a dignified ornament which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., MARSE or William Walldroff, M.S., MARSE.

MARSE accrediting is an honor. It authenticates your research activities. After becoming MARSE, you can add 'MARSE' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, Visiting Card and Name Plate etc.

The following benefitscan be availed by you only for next three years from the date of certification.

MARSE designated members are entitled to avail a 25% discount while publishing their research papers (of a single author) in Global Journals Inc., if the same is accepted by our Editorial Board and Peer Reviewers. If you are a main author or co-author of a group of authors, you will get discount of 10%.

As MARSE, you will be given a renowned, secure and free professional email address with 30 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders,Auto-Responders, Email Delivery Route tracing, etc.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time.This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The MARSE member can apply for approval, grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A.

Once you are designated as MARSE, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria.

It is mandatory to read all terms and conditions carefully.

Auxiliary Memberships

Institutional Fellow of Open Association of Research Society (USA)-OARS (USA)

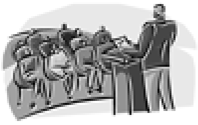
Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as "Institutional Fellow of Open Association of Research Society" (IFOARS).

The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

The IFOARS institution is entitled to form a Board comprised of one Chairperson and three to five board members preferably from different streams. The Board will be recognized as "Institutional Board of Open Association of Research Society"-(IBOARS).

The Institute will be entitled to following benefits:

The IBOARS can initially review research papers of their institute and recommend them to publish with respective journal of Global Journals. It can also review the papers of other institutions after obtaining our consent. The second review will be done by peer reviewer of Global Journals Incorporation (USA)
The Board is at liberty to appoint a peer reviewer with the approval of chairperson after consulting us.
The author fees of such paper may be waived off up to 40%.



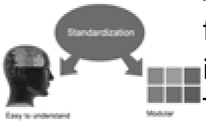
The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

The IBOARS can organize symposium/seminar/conference in their country on behalf of Global Journals Incorporation (USA)-OARS (USA). The terms and conditions can be discussed separately.

The Board can also play vital role by exploring and giving valuable suggestions regarding the Standards of "Open Association of Research Society, U.S.A (OARS)" so that proper amendment can take place for the benefit of entire research community. We shall provide details of particular standard only on receipt of request from the Board.

The board members can also join us as Individual Fellow with 40% discount on total fees applicable to Individual Fellow. They will be entitled to avail all the benefits as declared. Please visit Individual Fellow-sub menu of GlobalJournals.org to have more relevant details.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.



After nomination of your institution as “Institutional Fellow” and constantly functioning successfully for one year, we can consider giving recognition to your institute to function as Regional/Zonal office on our behalf.
The board can also take up the additional allied activities for betterment after our consultation.

The following entitlements are applicable to individual Fellows:

Open Association of Research Society, U.S.A (OARS) By-laws states that an individual Fellow may use the designations as applicable, or the corresponding initials. The Credentials of individual Fellow and Associate designations signify that the individual has gained knowledge of the fundamental concepts. One is magnanimous and proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice.

Open Association of Research Society (US)/ Global Journals Incorporation (USA), as described in Corporate Statements, are educational, research publishing and professional membership organizations. Achieving our individual Fellow or Associate status is based mainly on meeting stated educational research requirements.

Disbursement of 40% Royalty earned through Global Journals : Researcher = 50%, Peer Reviewer = 37.50%, Institution = 12.50% E.g. Out of 40%, the 20% benefit should be passed on to researcher, 15 % benefit towards remuneration should be given to a reviewer and remaining 5% is to be retained by the institution.

We shall provide print version of 12 issues of any three journals [as per your requirement] out of our 38 journals worth $ 2376 USD.

Other:

The individual Fellow and Associate designations accredited by Open Association of Research Society (US) credentials signify guarantees following achievements:

- The professional accredited with Fellow honor, is entitled to various benefits viz. name, fame, honor, regular flow of income, secured bright future, social status etc.

- In addition to above, if one is single author, then entitled to 40% discount on publishing research paper and can get 10%discount if one is co-author or main author among group of authors.
- The Fellow can organize symposium/seminar/conference on behalf of Global Journals Incorporation (USA) and he/she can also attend the same organized by other institutes on behalf of Global Journals.
- The Fellow can become member of Editorial Board Member after completing 3yrs.
- The Fellow can earn 60% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.
- Fellow can also join as paid peer reviewer and earn 15% remuneration of author charges and can also get an opportunity to join as member of the Editorial Board of Global Journals Incorporation (USA)
- • This individual has learned the basic methods of applying those concepts and techniques to common challenging situations. This individual has further demonstrated an in–depth understanding of the application of suitable techniques to a particular area of research practice.

Note :

"

- In future, if the board feels the necessity to change any board member, the same can be done with the consent of the chairperson along with anyone board member without our approval.
- In case, the chairperson needs to be replaced then consent of 2/3rd board members are required and they are also required to jointly pass the resolution copy of which should be sent to us. In such case, it will be compulsory to obtain our approval before replacement.
- In case of “Difference of Opinion [if any]” among the Board members, our decision will be final and binding to everyone.

"

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not conveninet , and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION **(Must be strictly followed)**

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, "Abstract" word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications

Research letters: The letters are small and concise comments on previously published matters.

5.STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

You must strictly follow above Author Guidelines before submitting your paper or else we will not at all be responsible for any corrections in future in any of the way.

Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

1. Choosing the topic: In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. Pick a good study spot: To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. Think technically: Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.

- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

The Administration Rules

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.
- Do not give permission to anyone else to "PROOFREAD" your manuscript.
- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

A

Artisanal · 11

C

Crypto · 14, 19

D

Deploy · 14
Didactic · 4, 5, 8, 11

E

Elliptical · 14
Encryption · 14

I

Intruder · 22

L

Latency · 14, 18

R

Recursion · 15

S

Systolic · 15

save our planet

Global Journal of Researches in Engineering

Visit us on the Web at www.GlobalJournals.org | www.EngineeringResearch.org
or email us at helpdesk@globaljournals.org

9 70116 58698 2 61427>

ISSN 9755861