Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal

of Computer Science and Technology: H

Information & Technology

Probability of Semantic Similarity

Graphic Interface Applied

Highlights

High Speed AES Algorithm

Fast Stereo Images Compression

Discovering Thoughts, Inventing Future

VOLUME 17 ISSUE 2 VERSION 1.0

Global Journal of Computer Science and Technology: H
Information & Technology

Global Journal of Computer Science and Technology: H
Information & Technology

Volume 17 Issue 2 (Ver. 1.0)

Open Association of Research Society

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
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
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 Pvt. Ltd.
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)

Editorial Board

Global Journal of Computer Science and Technology

Contents of the Issue

Global Journal of Computer Science and Technology: H Information & Technology
Volume 17 Issue 2 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Probability of Semantic Similarity and *N-Grams* Pattern Learning for Data Classification

By V. Vineeth Kumar & Dr. N. Satyanarayana
Jawaharlal Nehru Technological University

Abstract- Semantic learning is an important mechanism for the document classification, but most classification approaches are only considered the content and words distribution. Traditional classification algorithms cannot accurately represent the meaning of a document because it does not take into account semantic relations between words. In this paper, we present an approach for classification of documents by incorporating two similarity computing score method. First, a semantic similarity method which computes the probable similarity based on the Bayes' method and second, n-grams pairs based on the frequent terms probability similarity score. Since, both semantic and N-grams pairs can play important roles in a separated views for the classification of the document, we design a semantic similarity learning (SSL) algorithm to improves the performance of document classification for a huge quantity of unclassified documents.

Keywords: *semantic similarity, classification, naive bayes, n-grams pattern.*

GJCST-H Classification: *G.3 I.5, I.5.2*

Strictly as per the compliance and regulations of:

Probability of Semantic Similarity and *N-Grams* Pattern Learning for Data Classification

V. Vineeth Kumar [α] & Dr. N. Satyanarayana [σ]

Abstract- Semantic learning is an important mechanism for the document classification, but most classification approaches are only considered the content and words distribution. Traditional classification algorithms cannot accurately represent the meaning of a document because it does not take into account semantic relations between words. In this paper, we present an approach for classification of documents by incorporating two similarity computing score method. First, a semantic similarity method which computes the probable similarity based on the Bayes' method and second, *n*-grams pairs based on the frequent terms probability similarity score. Since, both semantic and *N*-grams pairs can play important roles in a separated views for the classification of the document, we design a semantic similarity learning (SSL) algorithm to improves the performance of document classification for a huge quantity of unclassified documents. The experiment evaluation shows an improvisation in accuracy and effectiveness of the proposal for the unclassified documents.

Keywords: semantic similarity, classification, naive bayes, n-grams pattern.

I. Introduction

Web mining is facing an important problem in measuring the semantic similarity among the words in the process of information retrieval and language processing. The most semantic based application requires the accurate measuring of semantic similarity among the document concepts and words. In information search, one of the most important problems is to semantically to get a number of documents correlated to a user's request. Semantic similarity between the words such as "word sense disambiguation" (WSD) can be an efficient assessment for the text entailment and automatic document classification, it is also important for the variety of natural language processing tasks. Automatic classification of documents is an important part of the research in the vision, and an enormous prospective for numerous applications around the text, such as search and analysis. Its purpose is to allocate a document given to the group of default to which it is in the right places. So far, applications have different types of algorithms based on the study or automatic calculation in this process and showed how much work [2], [3], [5]. However, mainly of the work functional to this task used aneffortless word-collection representation where each attribute communicates to a particular word. That is, assume that words are independent and utilize only the distribution of content words.

Over the past few years, we've seen the Web evolve into a semantic Web. The amount of information posted with linked data has consistently increased. With this increase, annotation and classification systems have created new opportunities to reuse this data as a semantic knowledge base and can be interconnected and structured to increase the accuracy and recovery of annotation and classification mechanisms. The Semantic web aims to explain the meaning of the information posted on the Web in order to make it possible to search by understanding the meaning of the information accurately. In this regard, document text learning and classification is most common, by assigning text to one or more existing class. This development determines the class membership of a text document that has a separate set of classes with profiles and different features. Criteria for deciding appropriate features for classification are important and are determined by the priority of the classifier. Semantic classification occurs when the target document element or term of the classification represents the meaning of the document.

Measuring the semantic similarity among texts is a basic task and can be capable of being utilized for a variety of applications, together with "text clustering" [1] and "text classification" [2]. The challenge in evaluation similarities among texts is infrequent, that is, there will be no coincidence of terms between the two texts. For example, two texts "Apple's New Product" and "iPhone-6" refer to related topics, even though they do not use similar terms.

To overcome scarcity, we need to use external data or knowledge to enrich the semantic representation of text. The semantically associated words of a particular word are listed in amanually created universal dictionary vocabulary ontology such as "Word Net". In this, a synset includes a set of synonyms for a specific word sense. However, semantic similarities among individual transform more than time and across domains. For example, apples are often associated with computers on the web. However, this apple sensation is not listed in most universal thesauri or dictionaries. Users searching for apples on the web may be concerned in the meaning of "apple" and "not apple" as a fruit. Innovative words are stably generated and new

Authors α: Research Scholor, JNTU Hyderabad.
e-mail: vineethvyas@gmail.com
Author σ: Principal, NGITS, Hyderabad.

senses are dispensed to existing words. Preserving ontology manually to confined these innovative words and senses is costly, if not impracticable.

In this paper, we contribute an automated semantic similarity learning (SSL) move towards to compute the probability of semantic similarity among terms or entities of documents with the class knowledge set entities. Here, we define two probabilistic scores, a semantic similarity (SS) score and *N-grams* pair similarity (GS) score enhancing Naive Bayes probabilistic method to aggregate the relation between document and class entities. Semantic Similarity method relates the trained class entities terms with the extracted document key terms to compute the document probable SS score against each class entities, and *N-grams* pair similarity method relate a document with each trained class entity with the constructed *N-grams* pairs, which is constructed using most frequent terms extracted from the document and the probable GS score is the summation of all individual *N-grams* pairs, i.e., $sum(GS_1, GS_2, .. , GS_n)$.We perform an experiment evaluation on Reuters-21578 Datasets to demonstrate the effectiveness of the proposal.

This papers organized in 6 sections. Section-1 above describes the introduction, section-2 discuss the background works, section-3 presents the proposed works outline, probabilistic semantic and N-gram pairs pattern learning, section-4 discuss the semantic similarity classification approach, section-5 present experiment methodology and results and finally section-6 presents the conclusion of the work.

II. Background Study

Semantic similarity plays an significant responsibility in "natural language processing", "information retrieval", "text summarization", "text classification", and "text clustering". Particularly, "Explicit Semantic Analysis" (ESA) [6] is extensively utilized because of its accessibility and diversity. ESA was build up to calculate word relationship as well as text comparison in natural language. ESA creates a "weighted index" that maps each phrase to the listing of articles that appears and calculates the similarity among the two words or a vector of text.

Naive Bayes [1] classification performance using semantic similarity has made various efforts. An approach that is often used to mitigate naive indepe-ndent assumptions is to express attribute addiction in a graph-based model called a "Bayesian network", where nodes correspond to attributes. Oriented arch is weighted by the circumstances probability for each node specified a close relation. Because "Bayesian network learning" is NP-hard [6], numerous approaches recommend imposing model constraints to formulate it easier to deal with learning problems.

Subsequent approaches in [8], [9], [17], [18] have brought considerable improvements. For example, in [21], an ensemble of Tree Augmented Naive-Bayes (TANs) was be trained, each rooted in a dissimilar attribute. It then compiles the classifications of all eligible TANs to predict class labels. In [8], we assume that the entire Bayesian network structure is learned first and all attributes are dependent. Unlike [18], the "Markov network model" is utilized to express characteristic dependencies that are estimated similar to [39] by taking advantage of the conditional log probability intention purpose. However, performing andtake advantage operation can be computationally demanding. Many methods are used to inherit the structural simplicity of Naive Bayes classifiers to keep away from the complication of the construction learning process [9],[10],[12],[13]. While the "Naive Bayes classification" is functional at the "decision tree leaves level" and is act upon on a subset of the training data, the data set properties are divided into two collections as in [11],where one group is assigned a class probability based on "Naive Bayes", and the other is supported on a "decision table".

Despite its effortlessness, the previously point out the classifier still shows a few constraints in handling very much related data. In [12], [13], the features are weighted dissimilarly depending on the involvement to the classification. A comparable approach was applied to the most effective "Bayesian Network classifier" and " Hidden Naive Bayes" [9]. In [9], the authors recommended generating a hidden close qualified that correspond to the effect of everything else on each property. The effect is computed as a linear arrangement of circumstance common information among attribute pairs, similar to [8]. Therefore, the parent correlation is ignored.

Dissimilarity like [10], [11], [19], "En Bay" [2] implements a new, uncomplicated, and useful approach that unites the generation of conditionally independent decision models and the reliable probability approximation by class. En Bay is a pattern-based Bayesian classifier that frequently uses a set of items frequently to estimate Bayesian probabilities. En Bay uses new and effective probabilistic approximation estimates that adhere to the conditional independence model. The set of extended, normal and separate items to be comprised in a class-based approximation is chosen by entropy-based heuristics, and the set of properties is conditionally mutually independent, depending on the class being evaluated. We extend En Bay probability computation methods to computes the semantic similarity probability score based on the terms dependency over the trained class terms entities, as discussed in section 3.2 below.

The "Large Bayes classifier" [11] performed the primary challenge to mitigate well-built independent

assumptions using a lengthy and frequent set of items to estimate the probability through product form approximation [12]. However, all preceding pattern-based Bayesian advance create inimitable product approximations for all test cases. Thus, estimations are only tied to the considered grade. Moreover, since it is necessary to extract animmense number of long and redundant repeated item sets, the superiority of the approximation is sensitive to changes in the "support threshold", and the classification algorithm cannot cope with a large data set. We extend this constructing *N*-grams pairs using frequent items to estimates the *N*-grams similarity probability score, as discussed in section 3.3 below.

III. Proposed Approach

a) Outline

The Semantic Similarity Learning (SSL) method, which uses probabilistic performances to describe probabilistic scores and put together scores supported on Bayes' method for accurate document classification to measure the robust discovery and semantic similarity of related entities to document.

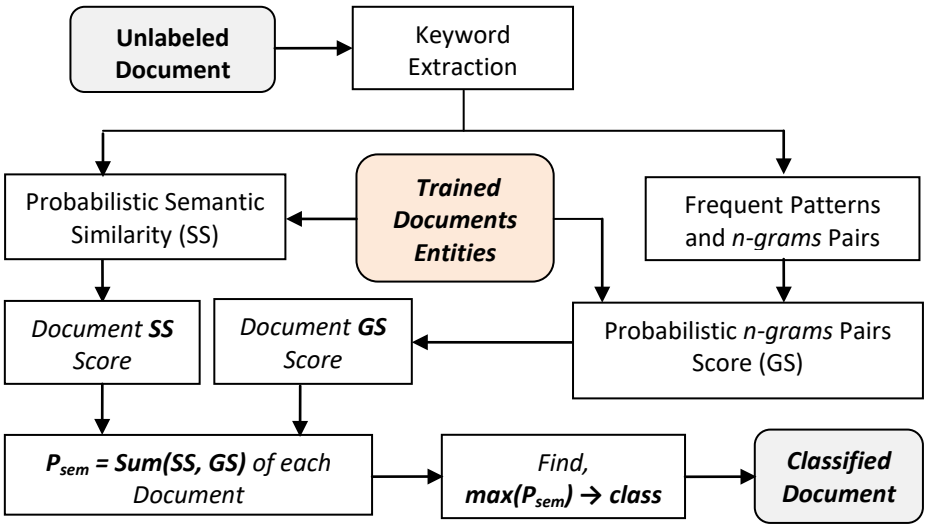


Figure 1: Outline of the proposed Approach

Fig.1. outlines our the proposed approach method. Our method obtains the main points of the probabilistic analysis of associations and related documents on the basis of trained document entities. The approach performs two probabilistic score computation method. First, Semantic Similarity Method which measures the similarity of their associated entity of a document with the list of trained class entity terms by $SS_k = P(d_k(t) \mid C_m)$, *i.e.,* probability of a document $d_k(t)$terms associated with a set of class C_m terms by means of cosine similarity.

The second method extracts the most frequent terms *F* from the extracted document terms using term frequency (*tf)* and using *F* we construct *N-grams* pairs. In general, an *N-gram* method slice a longer text into *n-characters*, but we customized this to slice a pattern into number words pairs (*V-Pair*) based on *n* which we term as *N-gram* pattern, an illustration is shown in Fig. 2.Using the constructed pairs we compute, $GS_k = \sum_{i=1}^{n} W_i$, where *n* is the number of pairs and $W_i = P(\ V\text{-}Pair_n \mid C_m\ )$ *i.e.,* probability of N-gram pair terms related to the set of class C_m terms using cosine similarity.

Now, we compute the final probability of semantic similarity $P_{sem} = sum\ (SS_k GS_k\ )$ for each document against each trained class. To classify the document we find the max P_{sem} among the computed probability of semantic similarity of each class. The class which has the max P_{sem} will be considered as the document class. We describe each method mechanism in the aspect in the following sections.

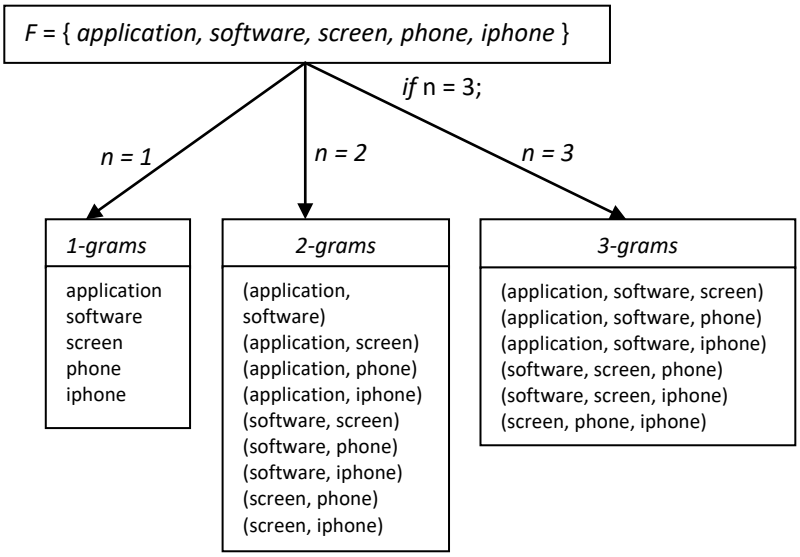


Figure 2: An illustration of *N-gram* pairs

b) Probabilistic Semantic Similarity

Classification of classifiers named a set of classes that train classifiers built from sets of the abstract model defined aims. Then use the categorizer to properly classify new data whose class labels are unknown. Various approaches have been proposed to make accurate classifiers such as, "Bayesian classifiers" [1], "Decision Trees" [2], "SVMs"[3], "Rule-based" [4], and "Associative classifiers" [5].

Bayesian classification methods recognized a classification supported on the of "Bayes theorem" [1].It predicted that a class based on test documents previously un seen $T = \{ a_1, a_2, \ldots, a_n \}$by opting the class c_i that make the most of the subsequent formula:

$$P(c_i \mid T) = \frac{P(T, c_i)}{P(T)} = \frac{P(c_i) \cdot P(T \mid c_i)}{P(T)}, \qquad (1)$$

Where $P(T \mid c_i)$indicates the provisional possibility of the test document T of a given class c_i. Probability is approximate commencing from the training set. Since classification focuses on choosing the class that takes advantage based on the equation (1), relatively than assigning an unambiguous probability to each class, denominator $P(T)$ in (1) can be misplaced because it does not influence the comparative class instruct.

Despite the simplicity, the Bayesian approach is calculation intractable without compelling a powerful model simplification [1], [6], [7]. The most important instance of simplification is the "Naive Bayes classifier" [1], which solves the problem by assuming that all attributes are conditionally self-determined and given as the class c_i. Therefore, the join probability of (1), is based on the generated Naive Bayes model, which can be approximated as,

$$\begin{aligned} P(T, c_i) &= P(a_1, a_2, \ldots, a_n, c_i) \\ &\simeq P(c_i) P(a_1 \mid c_i) P(a_2 \mid c_i) \cdots P(a_n \mid c_i) \\ &= P(c_i) \prod_{j=1}^{n} P(a_j \mid c_i). \end{aligned} \qquad (2)$$

Based on the approximation we combine the probabilistic semantic similarity (SS) scores extracted from the training data to find the appropriate entities for the document. Let's assume that multiple key terms are entered as input. That is, we compute $P(c \mid T')$for the set of core key terms $T' = \{t_1, t_2, \ldots, t_k\}$, where T' is a key term, which are derived using traditional Naive Bayes for any related class c_i.

One possible approach to this task is a two-step method of determining the key terms first and then applying the existing Naive Bayes. However, this approach raises the question of how key terms are established. We have developed a probabilistic similarity method for finding related entities. It can be functional to a set with probability determined members.

For a particular, a set of key terms *T*, *P (c|T')* is calculated for all probable states *T'*.Fig.3,summarizes an illustration of the probabilistic semantic similarity method for a set of key terms of a document $d_k$as $t_1, \ldots, t_k$. SS method is utilized to calculate $P(t_K|C_m)$, which is the probability score SS_k of the set of key terms, *T* for the class C_m.

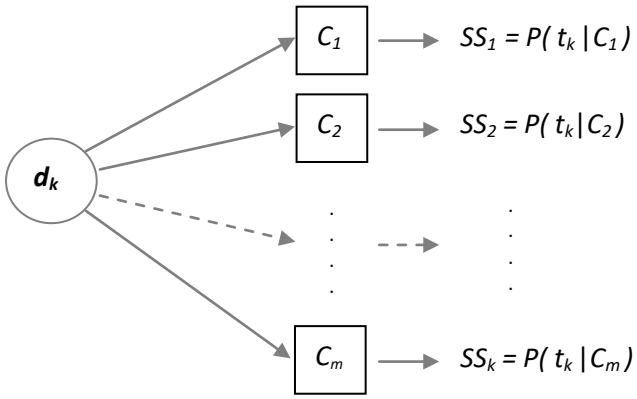


Figure 3: Probabilistic Semantic Similarity Method

Unfortunately, the circumstances of self-determination supposition prepared by Naive Bayes may not true always, to obelieves high-order associations for the period of the probability estimate, a parallel proposal is made based frequent pattern learning in *T,* and constructing a *N-grams* pairs to support accurate classification.

c) N-grams Pattern Learning

The *N*-gram is defined as a sequence of terms, the length is *n*, and the words taken are called terms. In the literature, we can see the definition of an *N*-gram as a concurrent set of terms, but only consecutive term sequences were used in this study. One word in the document is represented by a set of overlapping *N*-grams as shown in Fig. 2. The *N*-gram model can be fictional by introduction a small window over a sentence or text, where only *n* words can be seen at the same time. So the effort less *N*-gram model is the so-called "unigram model". This is a one-word model at a time. For example, the "Latest application and iPhone released." sentence contains five unigrams as, "Latest", "application", "and", "iPhone" and "released" Of course, this is not very beneficial information. It is just a word that makes up the sentence. In fact, *N*-grams are interesting when *n* is greater than 2 (bigram) or more.

Each word happens in a document with a dissimilar frequency. The main thought of categorization utilized by Trenkle and Cavnar [5] is that they should have similar *N*-gram frequency distributions when comparing documents of the same category. We performan*N*-gram pattern learning through creating *n* pairs using frequent document terms.

For a given document *d* having a *T* terms. Let's assume the frequent terms represent as *F*. Using the *F* terms we construct *N-grams* pairs as *V-Pair.* To learn the probability of *V-pair* pattern associationW_n of a document with a class c_m we calculate $P(V\text{-}Pair_n|c_m)$as shown in Fig .3. Here, the class must contain all the pair terms to match the association. To compute the N-grams probable similarity *GS,* we done the summation of all W_n as,

$$GS_1 = \sum_{i=1}^{n} W_i$$

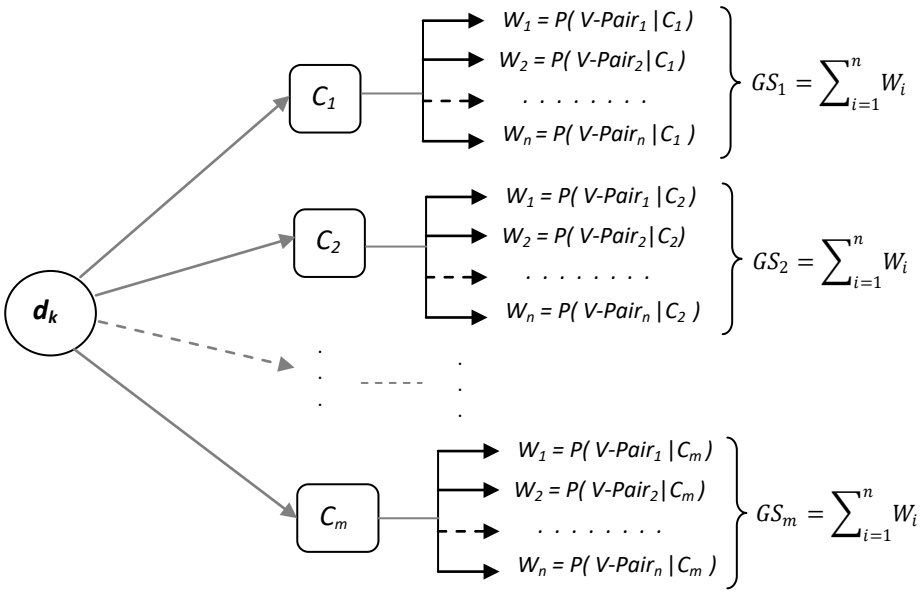


Figure 4: Probabilistic *N-grams* Similarity Method

IV. SSL based Classification

a) *Training*

In order to efficiently search for class-specific patterns, in the SSL training phase, an FP-growth data pattern representation [18] is separately created to store training data belonging to each class in a compressed form. The FP-growth pattern is a single-tree data structure for the minimum support (*min_sup*) frequent item set used in the class pattern learning context. Algorithm-1 shows the pseudo-code in the SSL training phase. Minimum supported thresholds were applied to remove infrequently used items. In this case, items that do not meet the necessitated minimum support threshold are not consisted of in the FP-growth pattern.

Algorithm 1. SSL Training Phase (*D, min_sup*)

Input: The training set *D* and the minimum support threshold *min_sup*
Output: FP-G = { T_i } ∀ $c_i \epsilon$ *C*, a FP-Tree for each class belonging to the training class set *C*

for all c_i in *C* **do**
    ac_i = set of all items belonging to class c_i
    FT_i = *ExtractPattern* (ac_i, *min_sup*)
    FP-G = *FP-T* ∪ { FT_i }
end for
return *FP-G.*

The obtained *FP-G* of each individual class c_i, will be used as a trained knowledge for the SSL classifier.

b) *SSL Classification*

The SSL classification approach is one of the accomplished algorithms managing unlabeled documents. It applies two probability computation as semantic similarity SS and N-gram Similarity G Son the dataset to perform the classification using the trained FP-growth pattern knowledge as shown in Fig.1. The SSL classifier initialized with anonly some trained class item sets. At each iteration, it chose an unlabeled document and perform the computation to compute the SS and GS score. It learns separate similarity score over each class pattern learning, and support a set of class labels for the unlabeled documents. For each class c_i belonging to the training data set is corresponding to FP-growth is visited to construct the class-centric product estimation and calculated the probability $P(T,c_i)$.

Its ultimate prediction is through by coming together both SS and GS score, $P_{sem} = sum(SS_k, GS_k)$ which decline classification error spredictions. The massive is the P_{sem} of the class will be predicated as the

closer association. This predictionim provises the performance of the algorithm classification accuracy. Since SSL classification uses two probability computation score with the FP-growth pattern, its presentation is better than any particular classifier.Algorithm-2briefly summarizes the SSL classification algorithm.

Algorithm 2.SSL Classification

Input: Document Terms *D* and the class set *FP-G* = { FT_i}

*Output:*Classified class of *D.*

for all*d*in *D*do
//-- For all document in D --
// -- Probability of Semantic Similarity(SS) Score
d_k= {T_k} ∀D_k ;
//-- For all class in FP-G vector --
for all c_i *in FP-G*do
c_i= {FT_i } ∀*FP-*G_i ;
SS_i = *P* (d_k ϵ c_i);
V_SS[i] = SS_i ;
end for
VD_s*[k]* = *V_SS;*
// -- Probability of N-grams Similarity(GS) Score
//-- Most frequent terms--
F = frequent_Terms (d_k, *min_sup);*
//-- Builds N-grams Patterns --
NP = BuildPattern(F, n);
//-- For all n-grams patterns --
for all ng_pin*NP* do
ng_terms = ng_p;
//-- For all class in FP-G vector --
for all c_i *in FP-G*do
c_i= {FT_i } ∀*FP-*G_i ;
GS_i = *P (ng_terms* ϵ c_i*);*
V_GS[i] = GS_i ;
end for
end for
VD_g*[k]* = *V_GS;*
// -- Summation Probability --
for all c_i *in FP-G*do
SS_P_{sem} = VD_s*[i];*
GS_P_{sem} = VD_g*[i];*
P_{sem} =*sum*(SS_P_{sem}, GS_P_{sem});
VP_{sem} *[i]* = P_{sem} ;
end for*pmax* = *findMax* (VP_{sem});
d_k*_class* = *getClass (pmax, C);*
end for

The obtained d_k*_class* class from *C*is determined by the summation of two probabilities scores. It classifies the most excellent class *c*of document *d* is set to the individual with the maximum probability:

V. Experiment

a) Datasets

The "Reuters-21578 corpus" is the mainly common utilized benchmark corpus in text classification. It consists of over 20,000 Reuters news stories from 1987 to 1991, and 135 subject classes are used in the experiment. This version contains "9603 training documents", "3299 test documents", and "27,863 inimitable words" after stopping stemming and word removal. We consider only 10 topics as classes of Reuters-21578 data for experimental evaluation measurements.

b) Performance Measure

To estimate the classification performance of the proposed method, we utilize the precision, recall, and accuracy. Let considered *P* is all relevant documents and *N* is all negative document. PC_+ as a positively classified, NC_+ as negatively classified documents. PC_- as a positively classified for an incorrect document, NC_- as negatively classified for correct documents. By constructing a confusion matrix for the above evaluation measure we compute the classifier performance.

To measure the classifier precision rate *CP*, the classifier recall rate *CR* and the classifier accuracy rate *CA* the following equation are used.

$$CP = \frac{PC_+}{PC_+ + NC_+} \quad (4)$$

$$CR = \frac{PC_+}{PC_+ + NC_-} \quad (5)$$

$$CA = \frac{PC_+ + NC_+}{P + N} \quad (6)$$

c) Evaluation Results

In the Reuters-21578 datasets we do consider both labeled and unlabeled documents, the effect of using two probabilistic semantic similarity learning is given in Table 1. We initially evaluate with Semantic Similarity Score (SS), then with N-grams patterns pairs Score (GS) and finally with both. The classification performance using both the Semantic Similarity and the N-gram pattern pairs learning outperforms over the one using any single learning for most classes.

Table 1: The accuracy enhancement by using semantic similarity learning on "Reuters-21578 corpus".

Class	Relevant documents	Semantic Similarity	N-gram pattern pairs	Both
Acq	1650	1591	861	1629
Corn	181	93	92	168
Crude	389	328	146	354
Earn	2895	2765	1621	2825
Grain	433	396	208	426
Interest	347	284	159	341
Money-fx	538	327	179	493
Ship	197	106	68	188
Trade	369	235	97	355
Wheat	212	184	102	206

We found that the greater the number of related documents in the training set, the higher the accuracy of using *N*-gram pattern pair learning. This is because Naive Bayes has a low error rate and high accuracy when there are many documents in the class. The classification comparison result is shown in Fig.4.

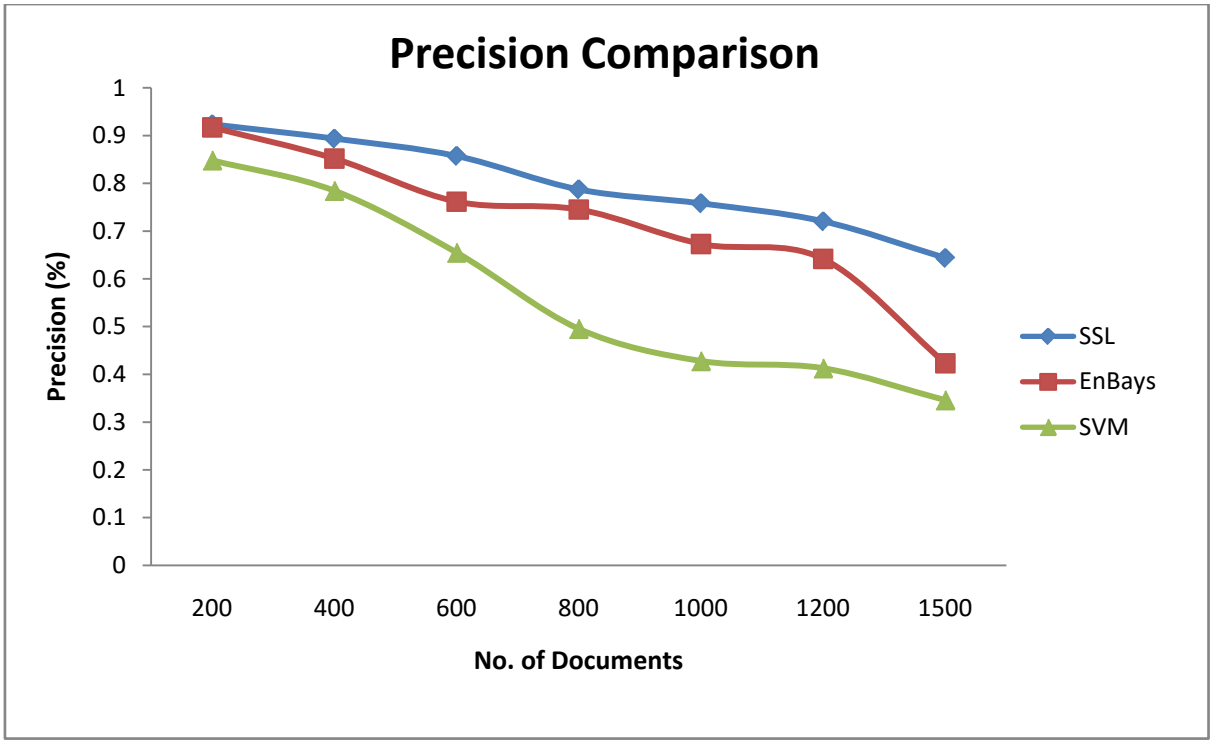


Figure 4: Classification Comparison

Accuracy measures the capability of a taxonomy to correctly classify unlabeled data. The ratio of the number of correctly categorized data to the number of given data, including accurate and incorrect classification. Experimental results show that average SSL outperforms other classified segments. The statistical significance of improving SSL accuracy is discussed below.

At first, we performed comparisons with state-of-the-art Bayesian classifiers. And because our approach is pattern-based, we compare it with the well-known associative classifiers SVM and the new improved Bayesian approach known as En Bays [2]. Finally, we performed a comparative assessment of precision, recall, and accuracy rates as a classifier for classifiers.

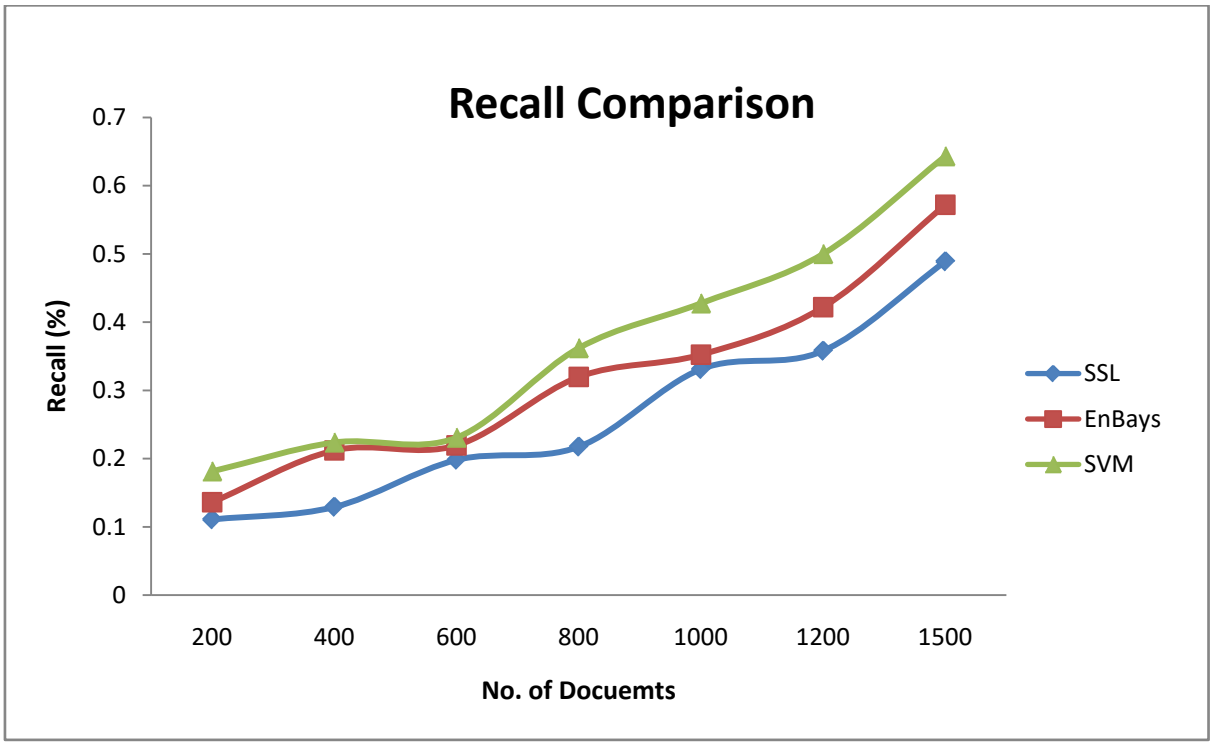


Figure 5: Precision Comparison

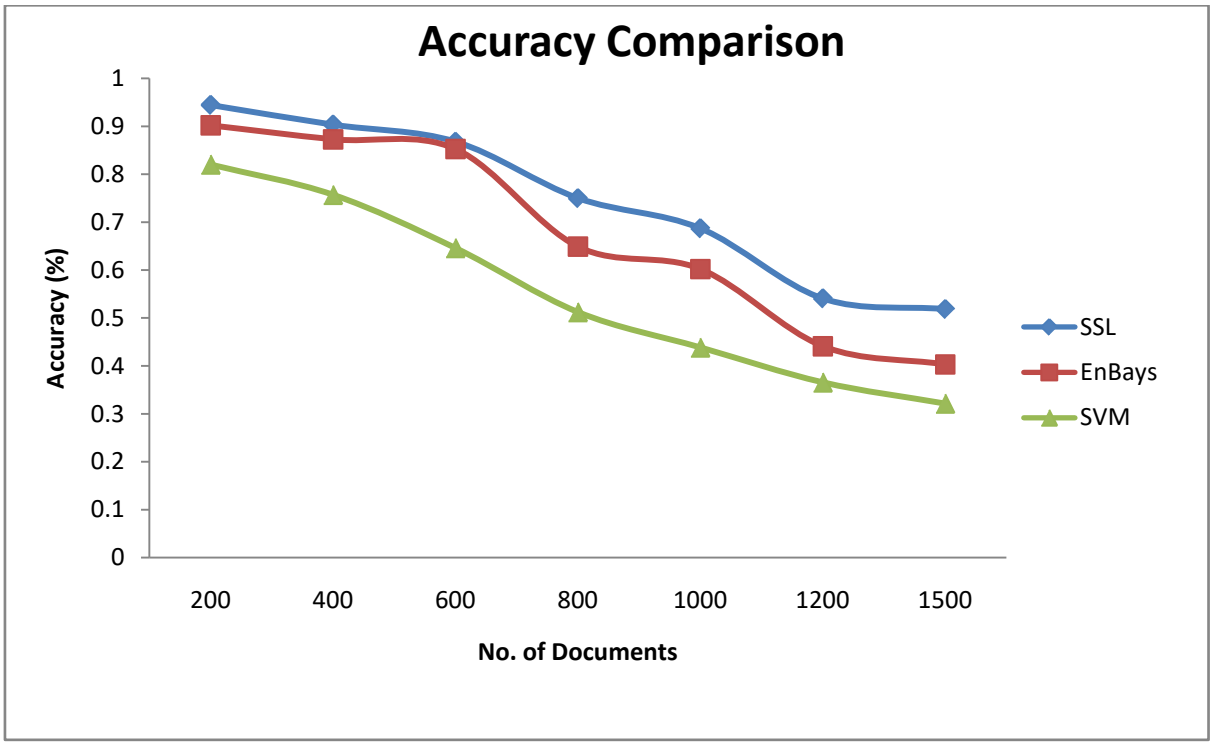


Figure 6: Recall Comparison

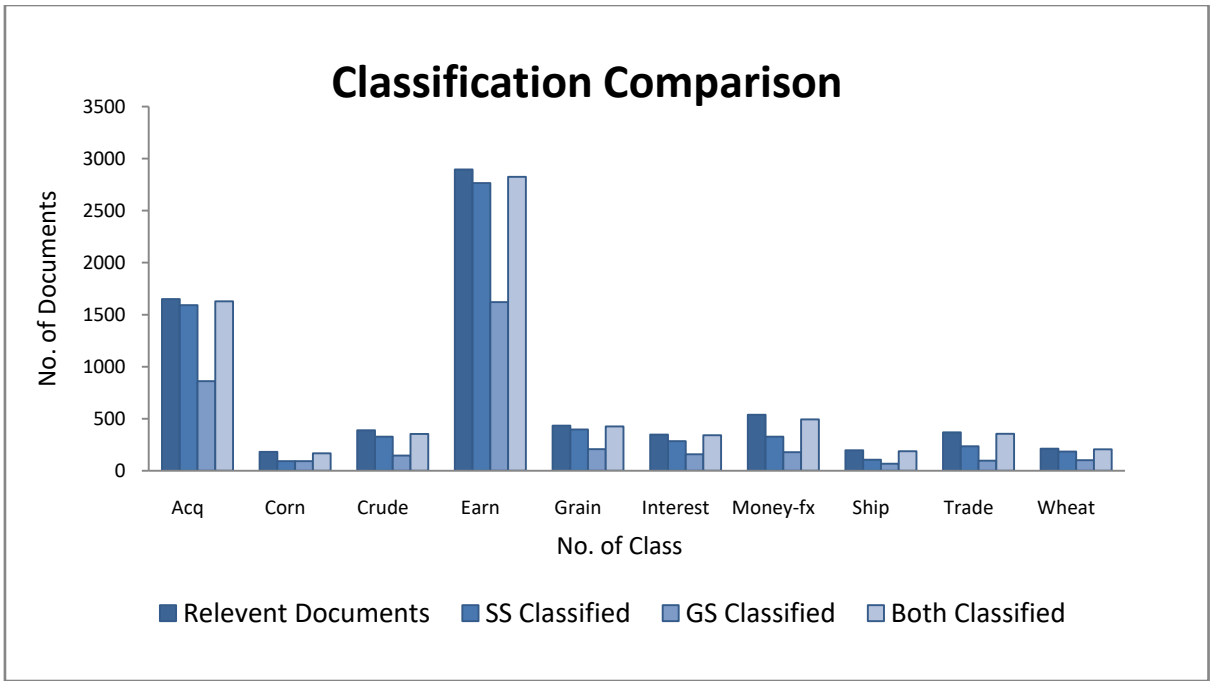


Figure 7: Accuracy Comparison

The rate of precision and recall in Fig. 5 and 6 shows an improvisation in compared to SVM and En Bays method. The effects of both SS and GS score in probability similarity measure shows SSL precision improvisation. Fig. 7 shows the classifier accuracy measures comparison. It also shows an improvisation of SSL approach in compare to others. The falling of accuracy with increasing of the document due to the limitation of trained class knowledge. As both the method has a dependency on the trained data knowledge for performing probability similarity computation cause the falling of the rate.

VI. Conclusion

In this paper, we propose a semantic similarity and *N*-gram pattern learning method based on the Bayesian classifier, which approximates Bayesian probability using frequent itemsets. It utilized new and more efficient probability approximations that adhere to the conditional independence model. A long, frequent, and separate set of items to be included in a class-based approximation is selected. It is based on the Baye's theorem and semantic similarity computation approach. Our method is a sort of probabilistic semantic similarity learning (SSL) that uses vectors to generate vectors of related entities as semantic representations of specific text and to measure semantic similarities. SSL combines vectors using expanded Naive Bayes, while SSL simply adds up the vectors for each term occurring in the text based on the majority of rules. This method uses both Semantic Similarity Learning for SSL algorithms and *N*-gram pattern learning and applies algorithms to unstructured document classification. Experiments on the Reuters-21578 document show that the SSL approach improves classification performance, and unlabeled documents are a good resource to overcome documents with a limited number of labels.

Future developments in this work will address the integration of generalized item aggregation mining algorithms to further improve classification and accuracy in noise-prone areas of data where there liability of probability estimation is particularly important.

References Références Referencias

1. Masumi Shirakawa, Kotaro Nakayama, Takahiro Hara, and Shojiro Nishio, "Wikipedia-Based Semantic Similarity Measurements for Noisy Short Texts Using Extended Naive Bayes", IEEE Transactions On Emerging Topics In Computing, Volume 3, No. 2, June 2015.
2. Elena Baralis, Luca Cagliero, and Paolo Garza, "En Bay: A Novel Pattern-Based Bayesian Classifier", IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 12, December 2013.
3. D. Grossman and P. Domingos, "Learning Bayesian Network Classifiers by Maximizing Conditional Likelihood," Proc. 21st Int'l Conf. Machine Learning (ICML '04), http://doi.acm.org/10.1145/1015330.1015339, p. 46, 2004.
4. R. Kohavi, "Scaling up the Accuracy of Naive Bayes Classifiers: A Decision-Tree Hybrid," Proc. Second Int'l Conf. Knowledge Discovery Data Mining (KDD '96), pp. 740-743, 1996.
5. M. Hall and E. Frank, "Combining Naive Bayes and Decision Tables," Proc. 21st Int'l Florida Artificial

Intelligence Research Soc. Conf., pp. 318-319, 2008.
6. J.T.A.S. Ferreira, D.G.T. Denison, and D.J. Hand, "Weighted Naive Bayes Modelling for Data Mining," 2001.
7. M. Hall, "A Decision Tree-Based Attribute Weighting Filter for Naive Bayes," Research and Development in Intelligent Systems XXIII, M. Bramer, F. Coenen, and A. Tuson, eds., pp. 59-70, Springer, 2007.
8. R. Agrawal, T. Imielinski, and A. Swami, "Mining Association Rules between Sets of Items in Large Databases," ACM SIGMOD Record, vol. 22, pp. 207-216, 1993.
9. R. Johnson and J. Shore, "Axiomatic Derivation of the Principle of Maximum Entropy and the Principle of Minimum Cross Entropy," IEEE Trans. Information Theory, vol. IT-26, no. 1, pp. 26-37, Jan. 1980.
10. E. Baralis, L. Cagliero, T. Cerquitelli, V. D' Elia, and P. Garza, "Support Driven Opportunistic Aggregation for Generalized Itemset Extraction," Proc. Fifth Int'l Conf. Intelligent Systems, 2010.
11. [1]S. Banerjee, K. Ramanathan, and A. Gupta, "Clustering short texts using Wikipedia", in Proc. Int. ACM SIGIR Conf. Res. Develop. Inf. Retr. (SIGIR), Jul. 2007, pp. 787-788.
12. X. Sun, H. Wang, and Y. Yu, "Towards effective short text deep classification", in Proc. Int. ACM SIGIR Conf. Res. Develop. Inf. Retr. (SIGIR), Jul. 2011, pp. 1143 - 1144.
13. Preethi, Ms. N., and Devi, Dr. T., Case and Relation (CARE) based Page Rank Algorithm for Semantic Web Search Engines. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.
14. Lee, T. B., Hendler, J., and Lassila, O., "The semantic web". Scientific American, vol. 284(5), May 2001.
15. Ch.-Qin Huan, Ru-Lin Duan, Y. Tang, Zhi-Ting Zhu, Y.-Jian Yan, and Yu-Qing Guo, ."EIIS: an educational information intelligent search engine supported by semantic services". international Journal of Distance Education Technologies, January 1, 2011.
16. Robin Sharma, Ankita Kandpa, and Priyanka Bhakuni, Rashmi Chauhan, R.H. Goudar and Asit Tyagi." Web Page Indexing through Page Ranking for Effective Semantic Search". Proceedings of7'h International Conference on Intelligent Systems and Control (ISCO 2013).
17. Yuan LIN, Hongfei LIN, and Li HE." A Cluster-based Resource Correlative Query Expansion in Distributed Information Retrieval ".Journal of Computational Information Systems 8: 1, 2012, 31–38.
18. W. W. Chu, Z. Liu and W. Mao."Textual document indexing and retrieval via knowledge sources and data mining". Commun. Inst. Inf. Comput. Mach. (CIICM), Taiwan, 2002, 5, (2), pp. 135–160
19. A. Vizcaíno, F. García, I. Caballero, J.C. Villar, M. Piattini."Towards an on tology for global software development". IET Softw., 2012, 6, (3), pp. 214–225
20. N. Tyagi and S. Sharma."Weighted Page Rank Algorithm Based on Number of Visits of Links of Web Page". In International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.
21. N. Duhan, A. K. Sharma and K. K. Bhatia."Page Ranking Algorithms: A Survey". In proceedings of the IEEE International Advanced Computing Conference (IACC), 2009.
22. Vishal Jain, Dr. Mayank Singh."Ontology Based Information Retrieval in Semantic Web: A Survey ", I.J. Information Technology and Computer Science, 2013, 10, 62-69.

This page is intentionally left blank

Global Journal of Computer Science and Technology: H Information & Technology
Volume 17 Issue 2 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Comparative Study of Symmetric Key Algorithms-Des, AES and Blowfish

By H. Fathima, K.S.R. Matriculation & K.S.R. Kalvi nagar
KSRMHSS

Abstract- This paper presents a peer analysis in the field of encryption algorithms, concentrating on private key block ciphers which are generally used for bulk data and link encryption. We have initially surveyed some of the popular and efficient algorithms currently in use. This paper focuses mainly on the different kinds of encryption techniques that are existing, and comparative study together as a literature survey. This study extends to the performance parameters used in encryption processes and analyzing on their security issues. Cryptography is the practice and study of hiding information. Prior to the modern age, cryptography was almost synonymous with encryption i.e. the conversion of information from a readable state to unreadable state. In order to avoid unwanted persons being able to read the information, senders retain the ability to decrypt the information. There are three types of Cryptography.

Keywords: encryption, decryption, cipher text, permutation, symmetric, subsitution bytes.

GJCST-H Classification: B.7.1, I.1.2

Strictly as per the compliance and regulations of:

Comparative Study of Symmetric Key Algorithms-Des, AES and Blowfish

H. Fathima [α], K.S.R. Matriculation [σ] & K.S.R. Kalvi nagar [ρ]

Abstract- This paper presents a peer analysis in the field of encryption algorithms, concentrating on private key block ciphers which are generally used for bulk data and link encryption. We have initially surveyed some of the popular and efficient algorithms currently in use. This paper focuses mainly on the different kinds of encryption techniques that are existing, and comparative study together as a literature survey. This study extends to the performance parameters used in encryption processes and analyzing on their security issues. Cryptography is the practice and study of hiding information. Prior to the modern age, cryptography was almost synonymous with encryption i.e. the conversion of information from a readable state to unreadable state. In order to avoid unwanted persons being able to read the information, senders retain the ability to decrypt the information. There are three types of Cryptography. They are Asymmetric-key cryptography, symmetric key cryptography and hashing. Encryption methods in which both the sender and receiver share the same key are referred to as symmetric key cryptography. This paper provides a comparison between symmetric key algorithms such as DES, AES, and Blowfish. The comparison is made on the basis of these parameters such as block size and key size.

Keywords: encryption, decryption, cipher text, permutation, symmetric, subsitution bytes.

I. Introduction

Symmetric-key algorithms [1] are algorithms that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.[2] This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption).[3]Symmetric-key encryption can use either stream ciphers or block ciphers.[4]Stream ciphers encrypt the digits (typically bytes) of a message one at a time.

Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size. Blocks of 64 bits have been commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001 uses 128-bit blocks.

Author α σ ρ: M.Sc (IT)., M.Phil (CS), Hss, Thokkavadi (p.o), Thiruchengode-637215.
e-mails: Fathimahussain_mscit07@rediffmail.com, Fathi.fathimahussain@gmail.com

II. Data Encryption Standard

Data Encryption standard (DES) adopted in 1997 by the National Bureau of Standards. For DES data are encrypted in 64 bit blocks using a 56- bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output.

III. Des Encryption

There are two inputs in the encryption function: the plaintext to be encrypted and the key. In this case, the plaintext must be 64 bits in the length and the key is 56 bits in length. The 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input. This is followed by a phase consisting of 16 rounds of the same function, which involves both permutation and substitution functions.

The output of the last (sixteenth) round consists of 64 bits that there are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the preoutput. Finally the preoutput is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation function, to produce the 64-bit cipher text.

IV. Initial Permutation

The input to a table consists of 64 bits numbered from 1 to 64. The 64 entries in the permutation table contain a permutation of the numbers from 1 to 64. Each entry in the permutation table indicates the position of a numbered input bit in the output which also consists of 64 bits.

V. Details of Single Round

The round key Ki is 48 bits. The R input is 32 bits. This R input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the R bits. The resulting 48 bits are XORed with Ki. This 48 bit result passes through a substitution function that produces a 32-bit output.

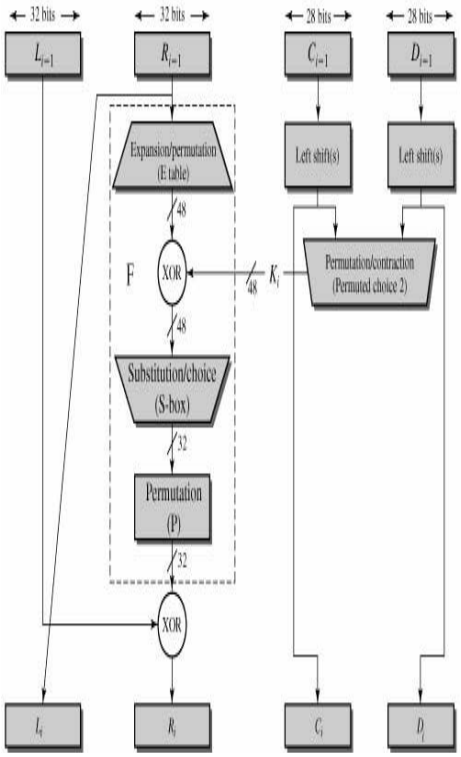


Figure 1: Single Round DES

The substitution consists of a set of eight S_ boxes, each of which accepts 6 bits as input and produces 4 bits as output. The first and last bits of the input to box Si from a 2-bit binary number to select one of four substitutions defined by the four rows in the table for Si the middle four bits select one of the sixteen columns.

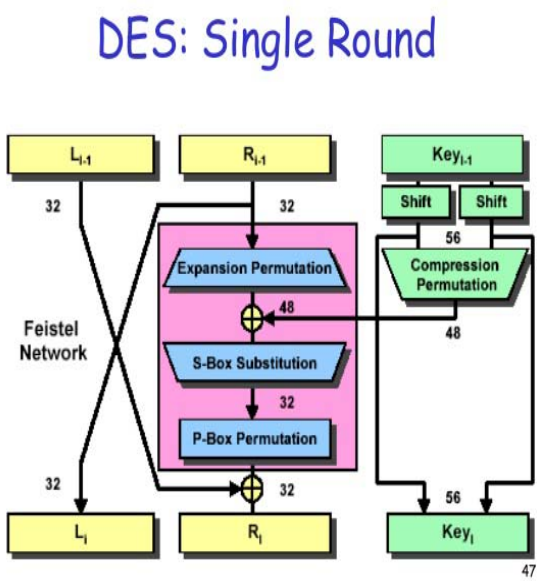


Fig 2: Single Round DES

The decimal value in the cell selected by the row and column is then converted to its 4-bit representation to produce the output. The outer two bits of each group select one of four possible substitutions (one row of an s- box). Then a 4 bit output value is substituted for the particular 4-bit input (the middle four input bits). The 32-bit output from the eight S-boxes is then permuted.

VI. Avalanche Effect

A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text. I particular, a change in one bit of the plain text or one bit of the key should produce a change in many bits of the cipher text. If the change were small, this might provide a way to reduce the size of the plaintext or key space to be searched.

VII. Advanced Encryption Standard

NIST in 1997 issued a call for proposals for a new Advanced Encryption Standard (AES). NIST specified that AES must be a symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits. The AES specification uses the same three key size alternatives but limits the block length to 128 bits. A number of AES parameters depend on key length. Substitute byte uses an S-box to perform a byte-by-byte substitution of the block.

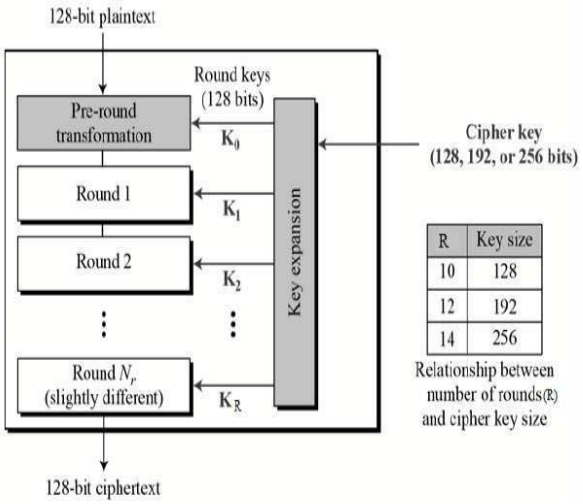


Fig 3: AES

VIII. Substitute Bytes Transformation

AES defines a 16×16 matrix of byte values called an S-box that contains a permutation of all possible 256 8-bit values. The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value serve as indexes into the S-box to select a unique 8-bit output value.

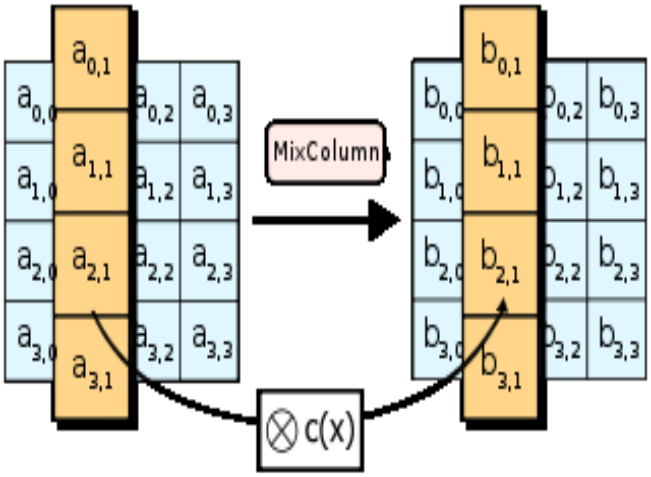


Figure 4: substitute bytes transformation

IX. Shift Row Transformation

a) Forward and Inverse transformations

The forward shift row transformation, called shift rows. The Inverse shift row transformation called Inv shift Rows, Perform the circular shifts in the opposite direction for each of the last three rows, with one- byte circular right shift for the second row.

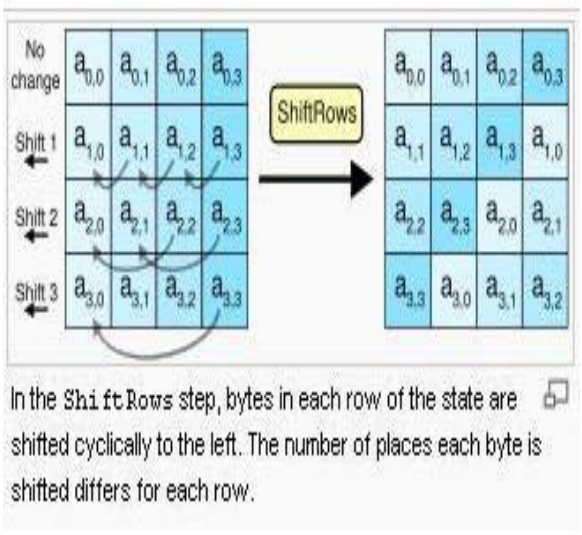


Figure 5: shift row transformation

The Forward mix column transformation, called Mix columns, operates on each column individually. Each byte of a column is a mapped into a new value that is a function of all four bytes in the column. The Inverse add round key transformation is identical to the forward add round key transformation, because the XOR operations its own inverse.

X. Blow Fish

Blowfish is a symmetric cipher developed by Bruce Schneier [SCHM93, SCHN94]. Blowfish was designed to have the following characteristics such as Fast, Compact, Simple and variably secure. The key length is variable and can be as long as 48 bits. This allows a tradeoff between higher speed and higher security.

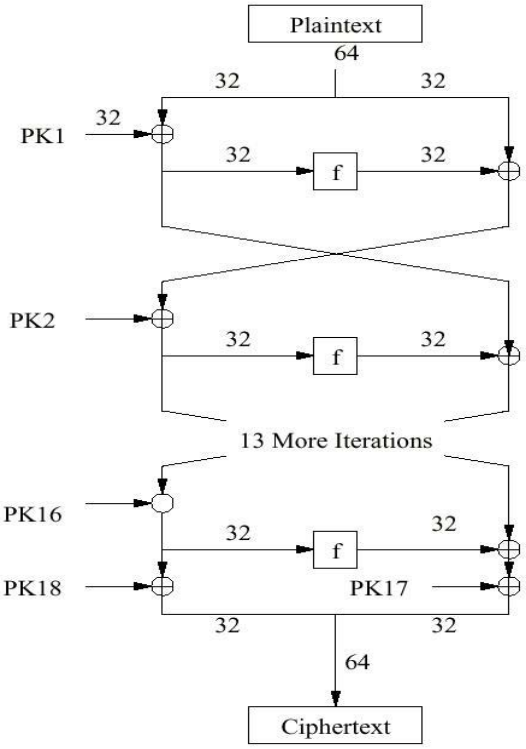


Figure 6: Blow fish

Blow fish encrypts 64-bit blocks of plaintext into 64-bit blocks of cipher text. Blowfish is implemented in numerous products and has received a fair amount of scrutiny.

XI. Encryption and Decryption

a) Blowfish uses two primitive operations

Addition: Addition of words, denoted by +, is performed by modulo 2 ^{32} .Blowfish decryption involves using the sub keys in reverse order. However, unlike most block ciphers, Blowfish decryption occurs in the same algorithmic directions as encryption, rather than the reverse.

Blowfish is a formidable symmetric cipher. Unlike DES, the S-boxes in Blowfish are key dependent. The blowfish design is that operations are performed on both halves of the data in each round, compared to performing an operation on just half the data in each round in the classic Feistel cipher. This should provide greater cryptographic strength, even though the additional operation is linear (XOR).

XII. Experimental Results

Table1: Block Size

ALGORITHM	BLOCK SIZE
DES	64
AES	128
BLOW FISH	64

Graph1: Block size

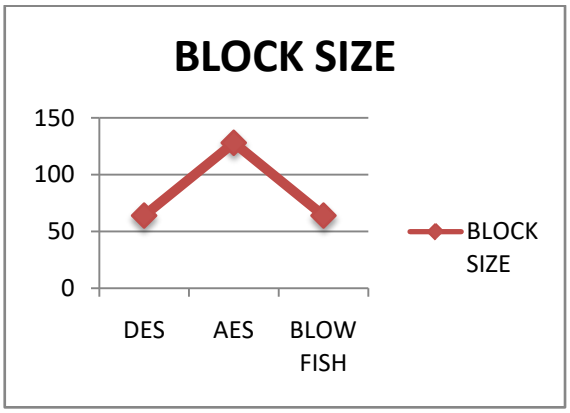
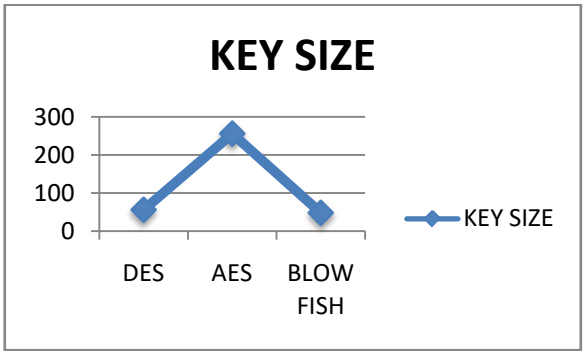


Table 1: Key Size

ALGORITHM	KEY SIZE
DES	56
AES	256
BLOW FISH	48

Graph 2: Key Size



XIII. Conclusion

This paper gives a detailed study of the popular symmetric key encryption algorithms such as DES, AES and Blowfish. Further, symmetric key encryption provides more security. This paper presents the performance evaluation of selected symmetric algorithms. From the presented simulation we can conclude that AES has better performance than other algorithms. Secondly, AES has advantage over the DES in terms of throughput & decryption time except Blowfish. In future the work may be extended by including the schemes and techniques over different types of data such as image, sound and video and developing a stronger encryption algorithm with high speed and minimum energy consumption.

References Références Referencias

1. "Cryptography: Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) – Schneier on Security". www.schneier.com Retrieved 2015-12-31.
2. Karthikeyan Bhargavan, Gaëtan Leurent (August 2016). "On the Practical (In-) Security of 64-bit Block Ciphers — Collision Attacks on HTTP over TLS and OpenVPN". ACM CCS 2016.
3. Schneier, Bruce (2004-09-27). "Saluting the data encryption legacy". *CNet*. Retrieved 2015-07-22.
4. *Biaoshuai Tao & Hongjun Wu (2015).* "Improving the Biclique Cryptanalysis of AES".
5. *SPIEGEL ONLINE, Hamburg, Germany (28 December 2014).* "Inside the NSA's War on Internet Security". *SPIEGEL ONLINE*. Retrieved 4 September 2015.

Global Journal of Computer Science and Technology: H Information & Technology
Volume 17 Issue 2 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Fast Stereo Images Compression Method based on Wavelet Transform and Two Dimensional Logarithmic (TDL) Algorithm

By Marwah Kamil Hussien
University of Basrah

Abstract- In this paper, a fast stereo images compression method has been proposed. In proposed method, Firstly, stereo images were transformed using Discrete Wavelet Transform (DWT) in order to reduce computation time. The disparities between these images were estimated by Two Dimensional Logarithmic (TDL) algorithm. The result of the Motion Vector (MV) was encoded into a bit stream by Huffman encoding while the remaining part is compressed like the compression that is used in still image. The proposed method produced good results in terms of Peak Signal-to-Noise Ratio (PSNR), CR, and computation time.

Keywords: *stereo imaging, stereoscopy, discrete wavelet transform, motion estimation, two dimensional logarithmic.*

GJCST-H Classification: *E.4, I.4.2, I.4.8*

Strictly as per the compliance and regulations of:

Fast Stereo Images Compression Method based on Wavelet Transform and Two Dimensional Logarithmic (TDL) Algorithm

Marwah Kamil Hussien

Abstract- In this paper, a fast stereo images compression method has been proposed. In proposed method, Firstly, stereo images were transformed using Discrete Wavelet Transform (DWT) in order to reduce computation time. The disparities between these images were estimated by Two Dimensional Logarithmic (TDL) algorithm. The result of the Motion Vector (MV) was encoded into a bit stream by Huffman encoding while the remaining part is compressed like the compression that is used in still image. The proposed method produced good results in terms of Peak Signal-to-Noise Ratio (PSNR), CR, and computation time.

Keywords: stereo imaging, stereoscopy, discrete wavelet transform, motion estimation, two dimensional logarithmic.

الخلاصة

في هذا البحث , تم اقتراح طريقة سريعة وبسيطة لضغط زوج من الصور المسجلة, الخطوة الاولى في الطريقة المقترحة , استخدام التحويل المويجي لغرض تحويل اشارة الصور المستخدمة الى مستويات بهدف تقليل وقت المعالجة المطلوب. ثم استخدام خوارزمية البحث (Two Dimensional Logarithmic) لغرض ايجاد متجه الحركة (Motion Vector) والذي يمثل الفرق (الاختلاف) بهدف تقدير الحركة ومن ثم تعويضها. اما الجزء المتبقي فيتم ضغطه كصورة ثابتة (ضغط الصور). الطريقة المقترحة اعطت نتائج جيدة من حيث قمة الاشارة الى الضوضاء (PSNR) ونسبة الضغط وكذلك من حيث وقت المعالجة المستغرق في عملية الضغط .

الكلمات الدالة: الصور المسجلة , التحويل المويجي المنفصل, تخمين الحركة , خوارزمية لوغارتيم ثنائي البعد.

I. Introduction

A pair of stereo images is very similar each other as they are the images of a stationary object taken from two different angles. This is why compressing both images independently is an in-efficient way of compressing stereo images [1].

In this research, has been selected a pair of stereo images which are very similar to each other are taken from two different angles (and this is why the pressure of each of the images independently, which means in the efficiency of the stereo image compression).We can get the sequence of these images by film cameras or generated by demand sequentially. Compress these pictures is the foundation necessary to reduce this data through the difference between the two images Account (matching), also known as disparity estimation, then squeeze one image independently. This is known as image as a reference, and can either is the right image or the left image, then use the reference image and vector disparity to rebuild the second image.

The work aims to propose an efficient technique for stereo images compression by transformed using Discrete Wavelet Transform technique (DWT) in order to reduce computation times, we show that in Section 2.The disparity vectors between them (The left and right image after transform in to DWT levels) were estimated by *Two Dimensional Logarithmic (TDL).*The remaining image is compressed as still image; we show that in Section 3. The two images are very similar to each other; so that the disparity vectors between the two images are estimated. Section 4 and Section 5 are gives the proposed method and evaluation criteria. Experimental results show in Section 6. Finally, the paper has been concluded in Section 7.

II. Discrete Wavelet Transform (DWT)

Wavelet transform is one of important and useful computation tools for a variety of signal and image processing applications. In image processing field, the main process in wavelet transform is to filter signal of image by two filters, namely, low pass filter (L) and high pass filter. Then, it will down sampled by factor of two leading to compose transform of one level. Repeating of one level transform on the part of low pass output only, results multiple level transform. Two dimensional (2-D) wavelet transform can be obtained by applying 1-D wavelet transform, wavelet filter separately. This computation is done by carrying out 1- D transform on the rows signals one time and on the columns signal another time. As a result of that, it separates image signals into four sub-band images: LL (low frequency in horizon and vertical), LH (low frequency in horizon and high frequency in vertical),HL(high frequency in horizon and low frequency in vertical), HH(high frequency in horizon and vertical).

Therefore, it is possible to use different methods for the sake of enhancement of the details in different frequency domain [2]. LL sub-band image often contains the most important information of the original image and it is usually called approximations the three other sub-band images are named as details. HH sub-band normally includes the small coefficients which are more likely due to undesirable noise [3]. Fig. 1 shows Foreman image and its three levels DWT.

Author: Assist. Lecturer, Department of Information Systems, College of Computer Sciences and Information Technology, University of Basrah, Basrah, IRAQ. e-mails: Lava_85K@yahoo.co.uk, Lava85k@gmail.com

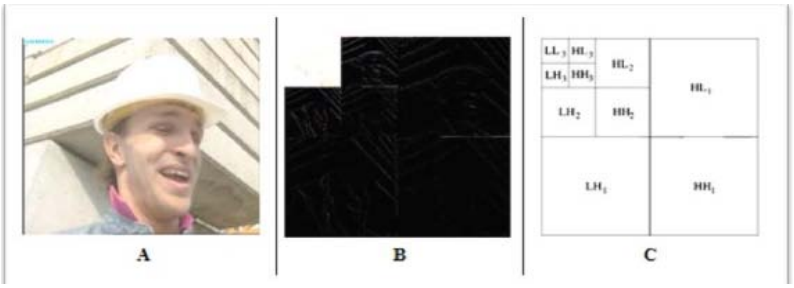


Figure 1: A) Foreman image B) Three levels Discrete Wavelet Transform of Lena image C) Low and High sub-bands resulted from three levels DWT[3].

III. Motion Estimation

Motion Estimation (ME) is the process of analyzing successive frames in any image sequence to identify objects motion. In this paper, motion estimation used to process of analyzing two stereo images using TDL.

The motion of an object is usually described by a two-dimensional motion vector, which is the placement of the co-ordinate of the best similar block in previous frame for the block in current frame. This placement is represented by the length and direction of motion [4, 5].

a) Three Step Search (TSS)

TSS is one of the earliest attempts at fast block matching algorithms and dates back to mid1980s. The TSS is the algorithm that limits the number of checking points in a search area. The general idea is represented in Fig. 2, it starts with the search location at the center and sets the „step size" S = 4, for a usual search parameter value of 7. It then searches at eight locations +/- S pixels around location (0,0). From these nine locations searched so far it picks the one giving least cost and makes it the new search origin. It then sets the new step size S = S/2, and repeats similar search for two more iterations until S = 1.At that point, it finds the location with the least cost function and the macro block at that location is the best match. The calculated motion vector is then saved for transmission. It gives a flat reduction in computation by a factor of 9 [6, 7].

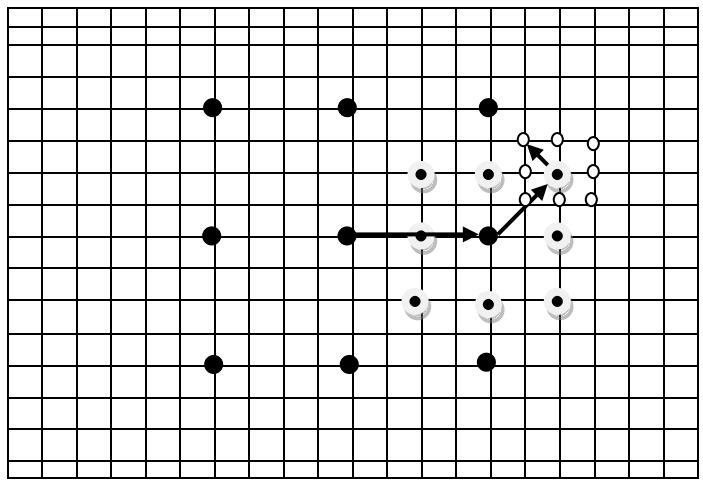


Figure 2: Example Path for Convergence of Three Step Search.

b) Disparity Estimation Using the Two Dimensional Logarithmic Algorithm

TDL Algorithm was introduced by Jain and around the same time that the Three Step Search was introduced and is closely related to it. Although this algorithm requires more steps than the Three Step Search, it can be more accurate, especially when the search window is large[2]. The algorithm may be described as:

Step1- Pick an initial step size. Look at the block at the center the search are and the four blocks at a distance of s from this one the X and Y axes. (The five positions from a + sign)

Step 2- If the position of best match is at the center, halve the step size. If however, one of the other four points is the best match, then it becomes the center and step 1 is repeated.

Step 3- When the step size becomes 1, all the nine blocks around the center are chosen for the search and the best among them is picked as the required block.

A particular path for the convergence of the algorithm is shown in the following figure:

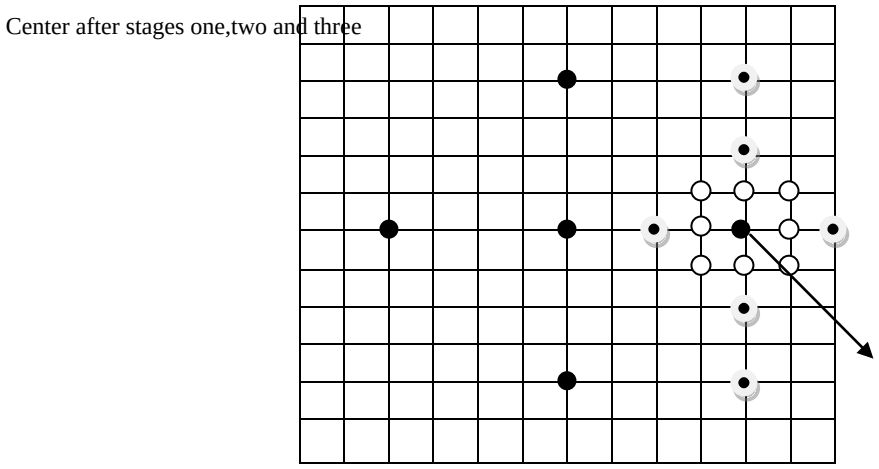


Figure 3: Example Path for Convergence of Two Dimensional Logarithmic Search.

A lot of variations of this algorithm exist and they differ mainly in the way in which the step size is changed [6, 7].

Some people argue that the step size should be halved at every stage. Some people believe that the step size should also be halved if an edge of the search space is reached. However, this last idea has been found to fail sometimes.

IV. The Proposed Method

In proposed method, there are four main steps. The first step we process the images used to convert its signal to levels using discrete wavelet Transform separately. In the second step, we match the two images the director of the first stage using TSS and TDL algorithms to find the movement between the two images and estimate the motion vector for the remaining images. Then, the remaining image will be compressed as a still image. Fig.4 shows flowchart of compression a pair of stereo images.

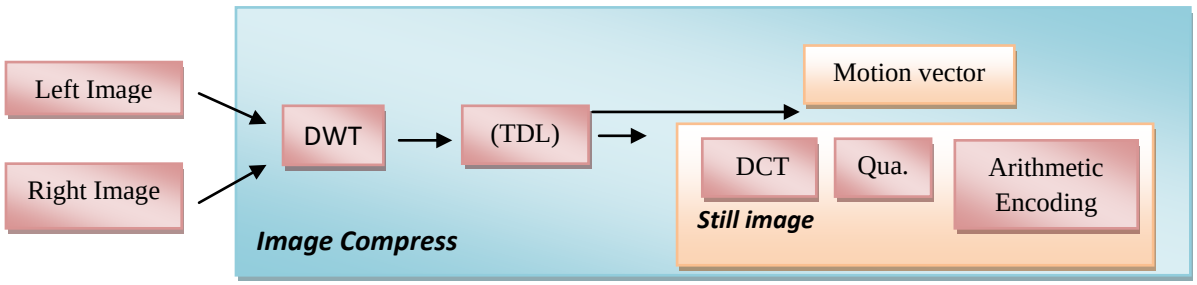


Figure 4: Flow chart of proposed method.

V. Evaluation Criteria

Peak signal-to-noise ratio (PSNR) is the standard method for quantitatively comparing a compressed image with the original. For an 8-bit grayscale image, the peak signal value is 255. Hence, the PSNR of an M×N 8-bit grayscale image C_{ij} and its reconstruction R_{ij} is calculated as [8,9]:

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \quad (2)$$

where the Mean Square Error (MSE) is defined as [10]:

$$MSE = \frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left[C_{ij}(m,n) - R_{ij}(m,n)\right]^2 \quad (3)$$

PSNR is measured in decibels (dB), M: height of the image, N: width of the image.

VI. Experimental Results

This section explains the experiments which have been implemented on two stereo images, Aloe, child and chosen image from personal camera as test images; each one of them is in size of 256*256 and of JPEG format. MATLAB version 7.4.0.287 (R2007a) was

used as a work environment to carry out these experiments.

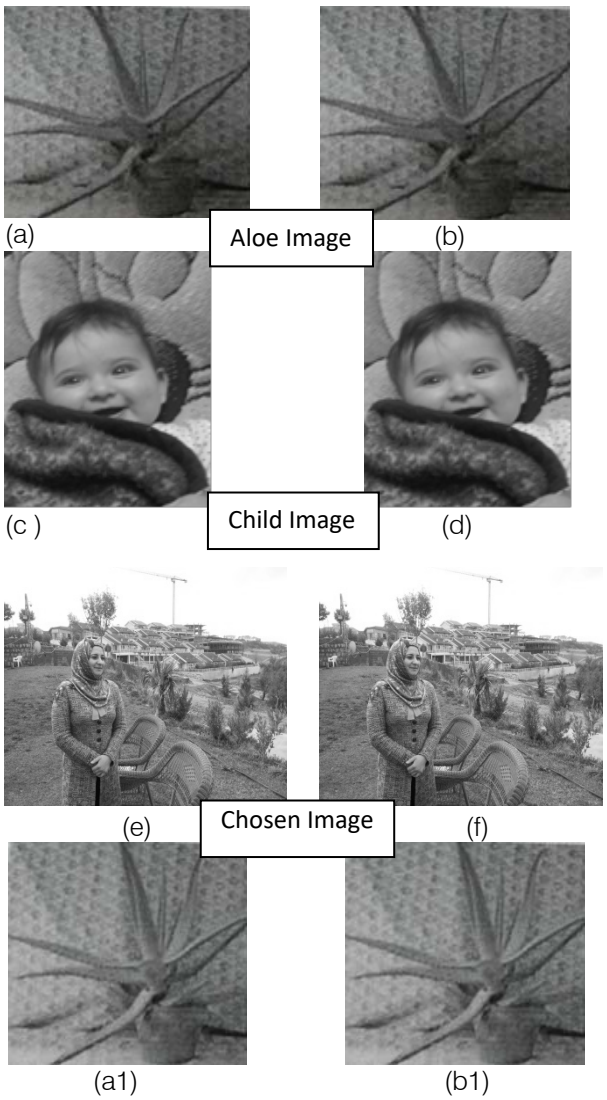
Table (1): display the results of data (PSNR, CR and computation Time) for the TSS algorithm of stress selected three images recorded after using discrete wavelet transform.

Table 2: display the results of data (PSNR, CR and computation Time) for the proposed method of stress selected three images recorded after using discrete wavelet transform.

The decoded left and right images were compared with the original left and right images. The Mean Square Error (MSE) between the original and decoded left and right images was referred in Equ. (3). The MSE of the image is the average of the MSE of the left image and the MSE of the right image as show in Equ. (4)[10].

$$MSE = (MSE_L + MSE_R) / 2 \quad (4)$$

a) Results of Images



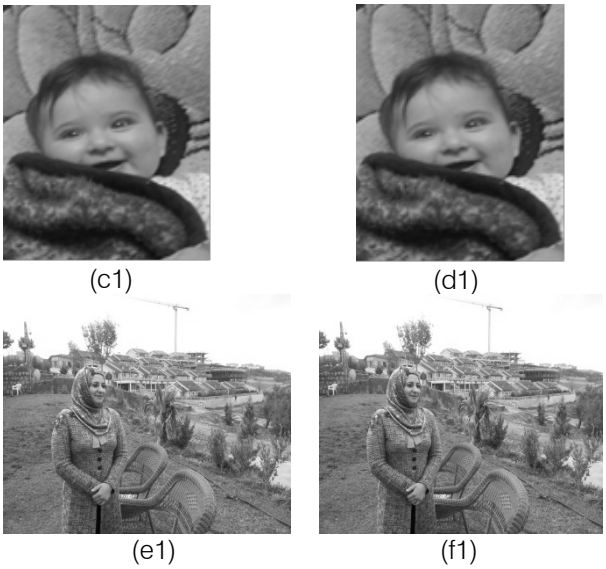


Figure 5: (a), (b), (c), (d), (e) and(f) Original Left and Right Images.
(a1), (b1), (c1), (d1), (e1) and(f1) Reconstructed Left and Right images.

Table1: Data for TSS Algorithm.

Images	PSNR (db)	CR	Time (sec)
Aloe	32.222	0.432	66.51
Child	33.321	0.522	72.22
Chosen Image	34.411	0.643	100.33

Table 2: Data for the Proposed Method.

Images	PSNR (db)	CR	Time (sec)
Aloe	45.32	0.566	50.32
Child	47.45	0.6.98	59.44
Chosen Image	50.28	0.789	88.76

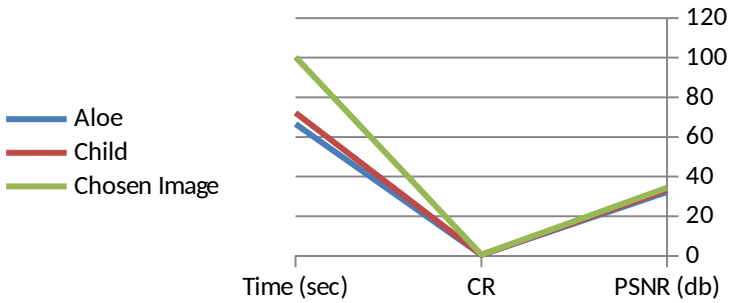


Figure 6: PSNR vs Bitrate for TSS Algorithm.

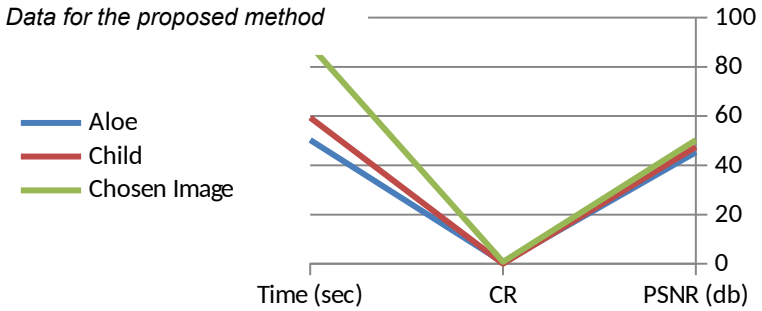


Figure 7: PSNR vs Bitrate for the Proposed Method.

VII. Conclusions

In this paper, a method for stereo images has been proposed to decrease the computation time without much influence on PSNR and compression ratio. Referring to the results that are shown in Table 1, and Table 2, it is obviously that the values of PSNR, CR, and computation time are affected by the length and the resolution of each pair from the images.

Additionally, we can notice clearly that the use of DWT minimized the processing time approximately 45%.

Three pair of images were compressed and then reconstructed by reversing the steps followed to compress the images.

The reconstructed images were then compared with the original images.

References Références Referencias

1. Beil W. and Carlsen I., "Surface reconstruction from stereoscopy and "shape from shading" in SEM images in Machine Vision and Applications, pp281-295, 2010.
2. Q. Yan, and R. Li, "Novel Image Enhancement Algorithm based on Wavelet Multiscale", 3rd International Conference on Intelligent Networks and Intelligent Systems, 01 - 03 November, pp. 39-42, 2010.
3. L. Passrija, A. Virk, and M. Kuar, "Performance Evaluation of Image Enhancement Techniques in Spatial and Wavelet Domains", International Journal of Computers and Technology, Vol. 3, No. 1, pp. 162-166, 2012.
4. Karthik A., Chandra S. and Das S.,"3D Tool Wear Measurement and Visualization Using Stereo Imaging" in International Journal of Machine Tools and Manufacture, pp 1531-1522, 2005.
5. Fisch M. M., Stg. ner H., Uhl A., "Layered Encryption Techniques for DCT-Coded Visual Data", In Proceedings (CD-ROM) of the European Signal Processing Conference, EUSIPCO '04, Vienna, Austria, September 2004.

6. J. Ratnottar, et al., "Review towards the Fast Block Matching Algorithms for Video Motion Estimation," in International Conference on Communication Systems and Network Technologies (CSNT), pp. 153-156, 2012.
7. C. Cheong Seong, et al., "Review of energy efficient block-matching motion estimation algorithms for wireless video sensor networks," in IEEE Symposium on Computers & Informatics (ISCI), pp. 241-246, 2012.
8. *Hameed A. Y.,* "New Techniques for Partial Encryption of Wavelet-based Compressed, May 2012.
9. Beegan A. P., "Wavelet-based Image Compression Using Human Visual System Models" M.Sc. Thesis, Electrical Engineering Department, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, May 2001.
10. Marwa K., " Video Compression by Wavelet Technique", M.Sc. Thesis, *Department of Information Systems, College of Computer Sciences and Information Technology, University of Basrah, IRAQ*, April 2013 .

Global Journal of Computer Science and Technology: H Information & Technology
Volume 17 Issue 2 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

High Speed AES Algorithm to Detect Fault Injection Attacks and Implementation using FPGA

By Prof. Dr. S. S Chorage & Somwanshi V. A.
Bharati vidyapeeths college of engg for women

Abstract- Information security is an essential issue in communication system. Advance Encryption Standard (AES) is utilized as a part of many embedded applications to give data security. Different counter measures are present in AES against fault injection attacks. Plain text and key of 128-bit is given as an input to the system and encryption and decryption operations are performed. Flag error shows the status of fault. Fault is produced randomly during encryption and decryption. For this reason, round transformation is broken into two sections and a pipeline stage is inserted in between. After fault detection one operation is performed that is redundancy check. Detected error or fault is corrected using redundancy check. The scheme is implemented using FPGA.

Keywords: *security, fault injection, confidential, wncryption, decryption, redundancy.*

GJCST-H Classification: *B.2.4, B.7.1*

Strictly as per the compliance and regulations of:

High Speed AES Algorithm to Detect Fault Injection Attacks and Implementation using FPGA

Prof. Dr. S. S Chorage [α] & Somwanshi V. A. [σ]

Abstract- Information security is an essential issue in communication system. Advance Encryption Standard (AES) is utilized as a part of many embedded applications to give data security. Different counter measures are present in AES against fault injection attacks. Plain text and key of 128-bit is given as an input to the system and encryption and decryption operations are performed. Flag error shows the status of fault. Fault is produced randomly during encryption and decryption. For this reason, round transformation is broken into two sections and a pipeline stage is inserted in between. After fault detection one operation is performed that is redundancy check. Detected error or fault is corrected using redundancy check. The scheme is implemented using FPGA.

Keywords: security, fault injection, confidential, wncryption, decryption, redundancy.

I. Introduction

Cryptography is used in the data communication system to secure the information. The national institute of standards and technology (NIST) finalized the advance encryption standard in October 2000. AES is introduced after the data encryption standard (DES). AES algorithm is most frequently used due to its high frequency and simplicity.

In AES during encryption it accepts a plain text input. Plain text input is limited to 128 bits and a key that can be specified to be 128 bit (AES-128) 192 or 256 bits to generate the cipher text. Round transformations are performed in AES. The four transformations includes sub bytes shift rows, mixed columns and add round keys.

The objective of AES is to secure the information being transferred from a user and only the desired receiver with a secret key would retrieve the original data. But sometimes some malicious faults injected during the implementation of AES algorithm. Due to these faults AES does not ensure that the information is transferred reliably. There are several fault attacks on AES. To obtain the confidential information the differential fault analysis (DFA) attacks are based on injecting faults into the structure of AES.

Author α σ: Department of Electronics and telecommunication Bharati Vidyapeeths College of Engineering for Women Pune, 43. Savitribai Phule Pune University.
e-mails: suvarna.chorage@bharatividyapeeth.edu, somwanshivishakha60@gmail.com

II. Related Work

Mestiri et al. [1] introduced a fault detection scheme, which is based on modified temporal redundancy for AES round it is used to detect transient single and multiple faults occurring at rub time. Round transformations are performed to detect the faults. The authors give the new scheme for fault detection in sub bytes and the inverted sub bytes using the relation between the input and output of S-box and inverted S-box.

Chu et al. [2] focused on the new method called as polynomial residue number system (PRNS) that is error detection method to secure the AES implementation. This scheme yields very good coverage and the distribution and parallelism characteristic of a PRNS error detecting system yields intrinsic resistance to some side channel attacks.

Rajendran et al. [3] proposed a new mechanism called as CED which is based on the slide attacks. This mechanism is independent of the S-box scheme. It is applicable to all symmetric block ciphers.

A. Reyhani -Masoleh et al. [4] proposed a structure independent low cost fault detection scheme for implementation of AES. The authors introduced new formulations for the fault detection in sub bytes and inverted sub bytes using arithmetic relations. The arithmetic relations are in between the input and the output of the S-box and inverted S-box. These schemes are independent of the way the S-box and the inverted S-box are implemented.

From this related search, it is observed that the new fault detection scheme is used for AES implantation. This scheme gives reliable implementation with new architecture of AES for checking sub bytes, inverted sub bytes and the other transformation in the inscription and the decryption process.

III. Advance Encryption Standard

Advance encryption standard (AES) is a non-feistel block cipher that encrypts and decrypts a data block of 128, 192 and 256 bits each data blocks consist of 4×4 array of bytes this array of bytes is called as states. AES is a round-based algorithm. The number of round is 10, 12 or 14. These rounds use key length of 128,192 and 256 bits respectively.

The different operations are performed in AES like sub bytes, shift rows, mix columns and add round keys. But in the final round doesn't have the mix column transformation. The separate key scheduling module help to initial key to generate the round key which is used in each round.

1. In this process, each byte is replaced with another based on LUT in non-linear substitution step called as Sub bytes.
2. Each row of the state is shifted cyclically a certain number of steps which happens in the transposition step that operation is called as rows called as Shift rows.
3. Combining the four bytes in each column by linear transformation during column interchange that is called Mix column operation.
4. The cipher key generates a round key by using the key schedule and the round combines each byte of state. This process is known as Add round key.

Fig.1 shows the general structure of AES which includes the different round transformation that is sub bytes, shift rows and mix columns.

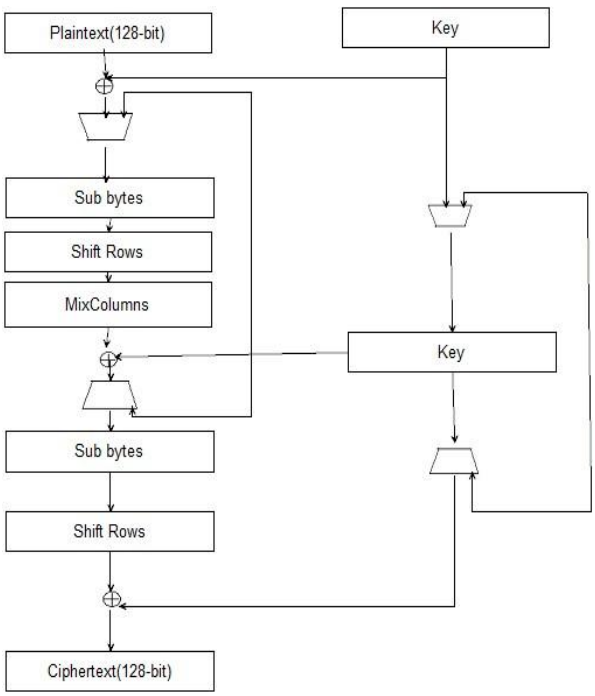


Figure 1: General Structure of AES [1]

For generating key schedule AES algorithm takes the cipher key and performs a key expansion routine. In the decryption process the inverse of corresponding transformation in encryption is performed i.e. Inv_shiftRows, Inv_SubBytes and Inv_MixColumns.

IV. AES Implementation

In AES 32-bit implementation, it takes four32bit words for the input data and four 32-bit words for the cipher key. Then it performs the encryption or decryption process and the output data it as four32-bit words. The architecture of AES is composed of six modules:

1. *Input interface*- It is used to load and store the input blocks for encryption and decryption process.
2. *Controller*- It generates the control signals for all other units in the implementation.
3. *AES round*- It is used to perform the round operations in encryption and decryption of the input data.
4. *Key Expander*- To compute the set of internal cipher keys based on single external key one block is used called as key expander.
5. *Output interface*- It takes the output with 128-bit length and then it converts into the four 32-bit words.
6. Input data buffer and Input key buffer are used to load the data and key.
7. *AES library*- To perform the basic operations one library is used called AES library which contains the basic function used in implementation of AES.

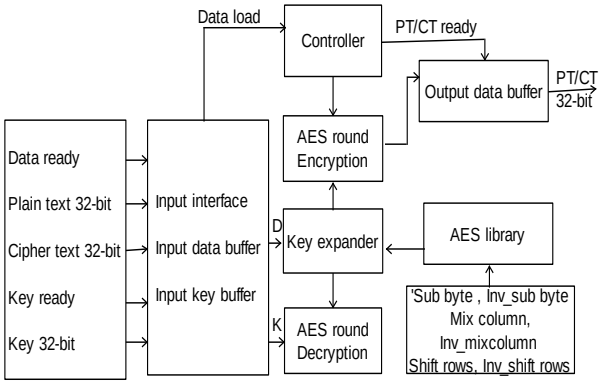


Figure 2: Block diagram of AES 32-bit [1]

V. Fault Injection Attacks

The errors that are introduced during implementation of cryptographic algorithms are called as fault injection attacks. During implementation of AES one or several faults are injected and faulty output is used to obtain information on the secret key stored in secured component.

Many authors introduced series of simulation for evaluation of robustness of unprotected AES algorithm against fault injection attacks. After a certain numbers of fault injection those attacks can retrieve the secret key of AES. So it is necessary to protect AES from those fault injection attacks. To protect AES from the faults different techniques are introduced.

VI. Fault Detection Scheme for AES

In related work, it shows that, no. of fault detection schemes against fault injection attacks are based on some sort of redundancy. The redundancies are hardware, temporal, and information redundancy.

In case of AES basic temporal redundancy is used it is related to hardware. Fig.6 is used to perform both the normal encryption and re-encryption using same input. The results are compared and every discrepancy is considered as an error at the end of encryption execution.

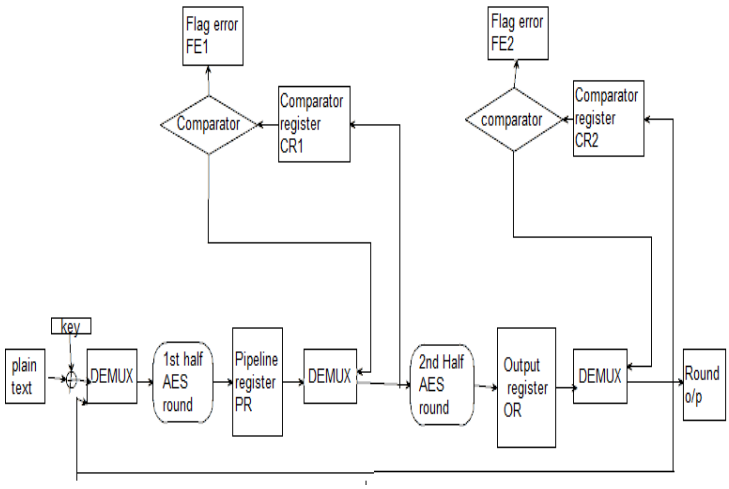


Figure 3: AES round with fault detection scheme [1]

In the proposed fault detection scheme modified temporal redundancy technique used for the AES round to detect transient single and multiple faults occurring at runtime. So, for this purpose the AES round transformation is broken into two parts and pipeline register inserted in between. In that the first-round operation is checked against errors while second half round is performed and vice versa. Every round is required two clock cycles: the first cycle is to perform normal encryption while second is to realize the re-encryption of the same input and to compare the results. The registers are loaded in each clock cycle to perform the round operation and the fault detection process is shown in table1

In first clock cycle, the plain text is XORed with the initial key, round 0 is processing. In the second clock cycle (k=2, 3) the state message goes through the first half of the first AES round ($R1,1$). The $R1,1$starts with the second clock cycle. In third clock cycle, while the second half round is processing the second half of the

first AES round $R2,1$, the first half round perform the re-encryption of $R1,1$ using the same input [1]. The $R1,2$of the AES encryption starts at the fourth clock cycle, at the same clock cycle the second half round is reprocessing the second half of the first round $R2,1$. The $CR1$and $CR2$registers are used to store the output value of each round to be compared with PR and OR registers, respectively. It should be noted that although the encryption is performed at second clock cycle, the result is not used till the third clock cycle where the output of the first half round is available for error checking [1].

Table 1: Sequence of operations for proposed architecture [1].

Clock cycle (k)	Register operation	1st half round	2nd half round
k = 1	PT ⊕ Key	----	---
k =2, 4, 6,…	CR2 ← PR FE2 ← CR2⊕ OR	Encryption	Re-encryption
k = 3,5,7,…	CR2 ← OR FE1 ← CR1⊕ PR	Re-encryption	Encryption

VII. Implementation Details of Rounds

a) Implementation of first half AES ($R1,j$)

In first half AES round to implement the S-box operation two methods are present, first is using LUT and second is by mathematical equations. LUT method is more suitable. All operations are in infinite Galois field. In first half sub byte and shift row operations are performed. For sub byte /inv_subbyte operation 16 S-box/inv_S-box are required.

The Shift row operation is a circular shifting operation on the rows of state having different no. of bytes.

b) Implementation of second half AES ($R2,j$)

In second half mix column and add round key operations are performed. Mix column operation is performed using following equations [1].

$$S'0,j = (02\cdot S0,j) \oplus (03\cdot S1,j) \oplus S2,j \oplus S3,j$$
$$S'1,j = S0,j \oplus (02\cdot S1,j) \oplus (03\cdot S2,j) \oplus S2,j \oplus S3,j$$
$$S'2,j = S0,j \oplus S1,j \oplus (02\cdot S2,j) \oplus (03\cdot S3,j)$$
$$S'3,j = (03\cdot S2,j) \oplus S1,j \oplus S2,j \oplus (02\cdot S3,j)$$

Considering 03= 02 ⊕ 01 this rule the equations can be re-written as:

$$S'0,j = 02\cdot(S0,j \oplus S1,j) \oplus S1,j \oplus S2,j \oplus S3,j$$
$$S'1,j = S0,j \oplus 02\cdot(S1,j \oplus S2,j) \oplus S2,j \oplus S3,j$$
$$S'2,j = S0,j \oplus S1,j \oplus 02\cdot(S2,j \oplus S3,j) \oplus S3,j$$
$$S'2,j = S0,j \oplus S1,j \oplus S2,j \oplus 02\cdot(S3,j \oplus S0,j)$$

The Add round key is XOR operation that adds round key to the mix column output state and the round keys are generated during key expansion [1].

VIII. Simulation Results

In AES algorithm some operations are performed. For these operations one look up table is used to assign values to the register that look up table is shown in table 2.

In AES algorithm, the encryption and decryption operations are performed. Plain text of 128-bit and key also of 128-bit are given as a input. During encryption sub byte, shift rows. mix column and add round key operations are performed. During decryption inv_sub byte, inv_shift row and inv_mixcolumn, operations are performed. The faults are generated randomly during the encryption and decryption process. Flag error in fig.3 shows the status of fault that is present or not.

Table 2: AES S-box look-up-table [12]

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	A	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	B	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	C	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	D	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	E	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	F	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 4: shows the simulation result of round1 operation.

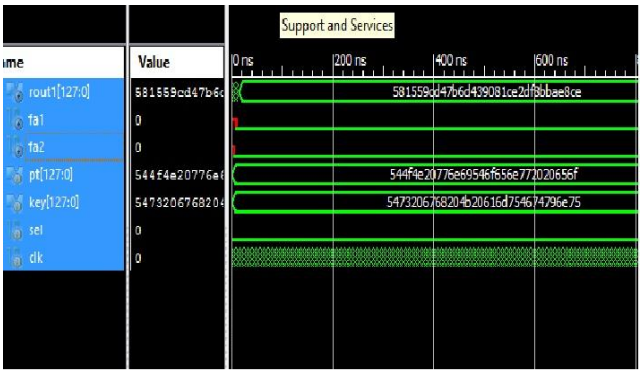


Figure 4: Simulation result of Round1 operation

This result shows the round1 operation, in which Sub byte, Shift rows, Mix column and add round key operations are performed. Similarly, all 10 rounds are performed in AES encryption and decryption. Fa1 and Fa2 shows the status of fault in fig.4. If Fa=0, then no fault and if Fa=1, then fault is present. Fig.5 and Fig.6 shows simulation result of encryption and decryption operation.

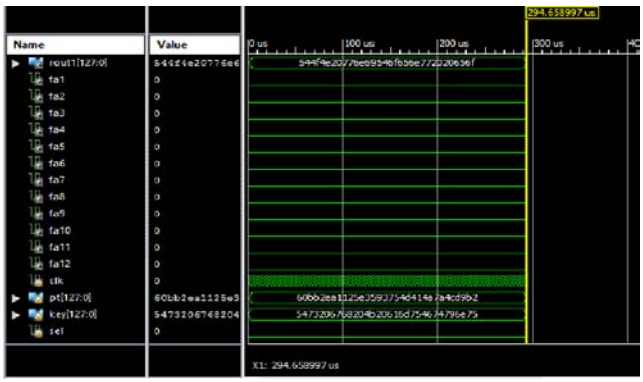


Figure 5: Simulation result of Encryption

Figure 6: Simulation result of Decryption.

IX. Conclusion

In communication system information security is most important. AES algorithm, can resist any kinds of password attacks with a strong practicability and reliability. The AES algorithm can be efficiently implemented by using FPGA platform. During implementation of AES some natural and malicious faults are injected. It is necessary to resist those faults for better performance of AES algorithm.

In fault detection scheme critical path of the AES round operation is divided into two halves and a pipeline register is inserted in between them and normal encryption and re-encryption operations are performed. Simulation results show the round1, encryption and decryption operations. During encryption and decryption

process faults are injected and the flag error shows the status of fault. This scheme can be implemented using Xilinx and Spartan-6 FPGA platform. Compared to some previous works, this method achieves 99.99% fault coverage. In future work text input, can be replaced with audio or video input.

References Références Referencias

1. Hassen Mestiri, FatmaKahri, Belgacem Bouallegue, Mohsen Machhout, "A high speed AES design resistant to fault injection attacks", *Microprocessors and Microsystems journal,2016 Elsevier,* pp.47-55.
2. J. Chu, M. Benaissa, "Error detecting AES using polynomial residue number systems", *Microprocessor and Microsystem journal*" , 37(2) (2012), pp. 228–234.
3. J. Rajendran, H. Borad, S. Mantravadi, R. Karri, "SLICED: Slide-based concurrent error detection technique for symmetric block ciphers," *IEEE International Symposium on Hardware-Oriented Security and Trust*, 2010, pp. 70-75.
4. M. Mozaffari - Kermani, A. Reyhani - Masoleh, "Concurrent structure independent fault detection schemes for the advanced encryption standard", *IEEE Transaction on computers*. 59 (2010), pp.608–622.
5. L. Lan, "The AES encryption and decryption realization based on FPGA," *Seventh International Conference on Computational Intelligence and Security* (CIS 2011), 2011, pp. 603-607.
6. H. Mestiri, N. Benhadjyoussef, M. Machhout, R. Tourki, "High performance and reliable fault detection scheme for the advanced encryption standard", *International Rev. on Com. Soft. (IRECOS)8(3),* 2013,pp.730–748.

A. Moh'd, Y. Jararweh and L. Tawalbeh, *"*AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation*," 7th International Conference on Information Assurance and Security (IAS 2011),* 2011, pp. 292-297*.*

7. Hoang Trang, Nguyen Van Loi "An efficient FPGA implementation of the Advanced Encryption Standard algorithm" *IEEE Symposium on Industrial Electronics & Applications (ISIEA),* 2012, pp. 696-699.
8. H. Mestiri, N. Benhadjyoussef, M. Machhout, R. Tourki, "A Robust fault detection scheme for the advance decryption standard", *International journal of Computer Network and Information Security(IJCNIS),*2013,pp.49–55.
9. M. Joye, P. Manet, and J.B. Rigaud, "Strengthening hardware AES implementations against fault attacks," *IET Information Security*, pp. 106-110, Sept, 2007.
10. Guo, D. Mukhopadhyay, and R. Karri, "Provably Secure Concurrent Error Detection Against Differential Fault Analysis," IACR Cryptology ePrint Archive, Available from:eprint.iacr.org/2012/552.pdf, 2012.
11. William Stallings, "Cryptography and Nework Security", *Third Edition, Pearson Education,* 2003.

Global Journal of Computer Science and Technology: H Information & Technology
Volume 17 Issue 2 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Graphic Interface Applied to Automated System to Manage the use of Tools in Machine

By Francisco C. P. Bizarria, José W. P. Bizarria, Luis F. de Almeida & Fernando M. R. S. e Santos

Taubaté University (UNITAU)

Abstract- The processing industry has to find ways to reduce manufacturing costs, as a way to survive in the market with increasing competition. This competition has become increasingly driven by globalization, that is, an industry has to share the consumer market with other industries that are installed worldwide. One of the possible ways to reduce manufacturing costs is related to the efficient use of basic inputs. Among the main inputs used in the manufacture, some are specifically related to the tools that are installed on machines such as lathes, grinding machines, presses and others. Typically, the tools developed by the industry in the process engineering sector have dedicated characteristics that must be maintained to perform the appropriate transformation of the product being manufactured. The preservation of these characteristics is linked mainly with the specified service life for the use of each tool, in order to make the substitution before the product is affected by non conformities arising from the manufacturing process.

Keywords: tool replacement, eccentric press, graphical interface, automation.

GJCST-H Classification: B.7.2, D.2.6

Strictly as per the compliance and regulations of:

Graphic Interface Applied to Automated System to Manage the use of Tools in Machine

Francisco C. P. Bizarria [α], José W. P. Bizarria [σ], Luis F. de Almeida [ρ] & Fernando M. R. S. e Santos [ω]

Abstract- The processing industry has to find ways to reduce manufacturing costs, as a way to survive in the market with increasing competition. This competition has become increasingly driven by globalization, that is, an industry has to share the consumer market with other industries that are installed worldwide. One of the possible ways to reduce manufacturing costs is related to the efficient use of basic inputs. Among the main inputs used in the manufacture, some are specifically related to the tools that are installed on machines such as lathes, grinding machines, presses and others. Typically, the tools developed by the industry in the process engineering sector have dedicated characteristics that must be maintained to perform the appropriate transformation of the product being manufactured. The preservation of these characteristics is linked mainly with the specified service life for the use of each tool, in order to make the substitution before the product is affected by non conformities arising from the manufacturing process. The tool replacement at the right time becomes essential, but to perform this task should be considered aspects related to the early and late replacement, both of which can lead to increased costs for the purchase of tools or rework parts produced with different characteristics what was envisaged in the specification. In this context, this paper proposes a graphical interface to be integrated into the physical architecture of the automated system that makes managing the use of tools for industrial eccentric press. All virtual components designed for the windows of the graphical interface are significant and related to the procedures set out to make the replacement of each of the press tool. The validation of the functionality of the interface is obtained by means of tests on the prototype that adopts the basic elements provided in said architecture. The positive results observed in practical tests suggest that graphical interface is appropriate for the purpose which it is intended.

Keywords: tool replacement, eccentric press, graphical interface, automation.

I. Introduction

In the last decades the global consumer market is demanding products with competitive cost, minimum assured quality, configuration options, ease of maintenance, durability, ergonomic advantages, sustainability ecological characteristics consistent with diversified social values, and free of exploitation with human labor and/or animal in the manufacturing process [1].

In order to meet these characteristics, national and international industries are investing in the improvement of their manufacturing facilities and adopting the use of automation in their production lines as the main resource to: i) maximize the control performed at the various levels of the process, ii) to integrate production lines, iii) to reduce losses in the process, iv) to increase manufacturing capacity, v) to meet seasonal variations in production demands, vi) to minimize the number of production cycles, vii) to meet national and/or international standards; and viii) to reduce or even eliminate the use of human and/or animal labor in repetitive tasks and/or environments that are hostile and/or dangerous [2].

In this sense, the manufacturing industry also has to look for effective ways to reduce manufacturing costs as a way to survive in a market with growing competition. This competition has become increasingly stimulated by globalization, as an industry has to divide its consumer market with others installed in different parts of the world.

One of the possible ways to reduce manufacturing costs is related to the efficient and effective use of basic inputs. Among the main inputs used in manufacturing are those related to the tools that are installed in machines, such as: lathes, grinders, presses and others related. Typically, tools developed by an industry's process engineering sector have dedicated features that must be maintained to perform the proper transformation of the product being manufactured.

The preservation of these characteristics is mainly related to the useful life that is specified for the use of each tool, in order to replace them before the product is affected by non-conformities from the manufacturing process. The replacement of tools at the right moment becomes essential, but in order to perform this task, the aspects related to premature and late replacement must be considered, both of which may generate cost increases for tool acquisition or rework in parts that were produced with divergent characteristics.

In this context, this work proposes the use of a graphical interface to be integrated in the physical architecture of the automated system that performs management in the use of tools for an eccentric industrial press. The virtual components elaborated to

Author α: Asst. Professor in Electrical Engineering Department - Taubaté University (UNITAU), Brazil. e-mail: fcpbiz@gmail.com
Author σ: Asst. Professor in Computing Department - Taubaté University (UNITAU), Brazil. e-mail: jwpbiz@gmail.com
Author ρ: Asst. Professor in Computing Department - Taubaté University (UNITAU), Brazil. e-mail: luis.almeida@unitau.br
Author ω: Master student in mechanical engineering-Taubaté University (UNITAU), Brazil. e-mail: f_mario@terra.com.br

meet the windows of the graphical interface are expressive and related to the procedures defined to carry out the replacement of each tool of the press. The validation of the functional efficacy of this interface is obtained through tests carried out in prototype which adopts the basic elements provided for in architecture.

II. Objectives of The Work

This work has as main goal to propose the windows and their respective virtual components for a graphical interface to be integrated in the architecture of automated system that performs the management in the use of eccentric press tools, in order to minimize the premature or late replacement of these tools.

To present the most expressive results obtained in the practical tests carried out with the prototype that was developed to validate the virtual resources contained in the windows of the mentioned interface.

III. Reference Architecture

The basic blocks provided in the physical architecture that is considered as reference to integrate the resources established in each window of the Graphical Interface (GI) in order to interact with the automated system that manages the use of tools in eccentric press are presented in Figure 1.

The acronyms defined for the blocks contained in the reference architecture, which is shown in Figure 1, have the following meanings: i) HC: Process Engineering Host Computer or Tool Preparation Room, ii) GI: Graphic Interface of Process Engineering or Tool Room, iii) TDB: Tool Database, iv) DCL: Data Communication Line, v) DPC: Dedicated Press Control, vi) CMP: Control and Monitoring Panel, and vii) EP: Eccentric Press.

The block called Host Computer (HC), which belongs to the Process Engineering Sector, has the following main functions: i) host, at the application layer, the window of the Graphical Interface (GI) that allows the system user to register the codes of the products that will be manufactured by the press, the codes of the tools available to meet the processes and the useful life times established for operations under nominal press conditions, in Tool Database (TDB), and ii) perform data communication with the Dedicated Press Control (DPC) and Host Computer (HC) of the Tool Preparation Room.

The Dedicated Press Control (DPC) block has features that allow: i) to execute the Eccentric Press (EP) operational control algorithm, ii) to parameterize the Eccentric Press (EP) operating modes, iii) to control, monitor and interrupt the operation of the Eccentric Press (EP), through the local Control and Monitoring Panel (CMP), iv) send signals to control the actuators installed in the physical structure of the Eccentric Press (EP), v) receive signals from the installed sensor systems in the physical structure of the Eccentric Press (EP); vi) to perform data communication with the Process Engineering Sector and the Tool Preparation Room.

The resources contained in the Host Computer (HC) of the Tool Preparation Room are directed to: i) host, at the application layer, the Graphical Interface (GI) window that allows the user to access the records that are registered in the Tool Database (TDB) for up-to-date information on the quantities of tools available, product codes, tool codes, and service life of each tool, ii) selecting and loading specific tool data in the Dedicated Press Control (DPC) to be used in the current manufacturing process, and iii) to perform data communication with the Process Engineering and Dedicated Press Control (DPC).

The Data Communication Line (DCL) is the physical means established to perform data communication, in a bidirectional way, with the Host Computer (HC) that belongs to the Sector of Process Engineering, Computer Host (HC) from the Tool Preparation Room, and Dedicated Press Control (DPC). It should be mentioned that this line is provided with galvanic separation and protection against electromagnetic interference.

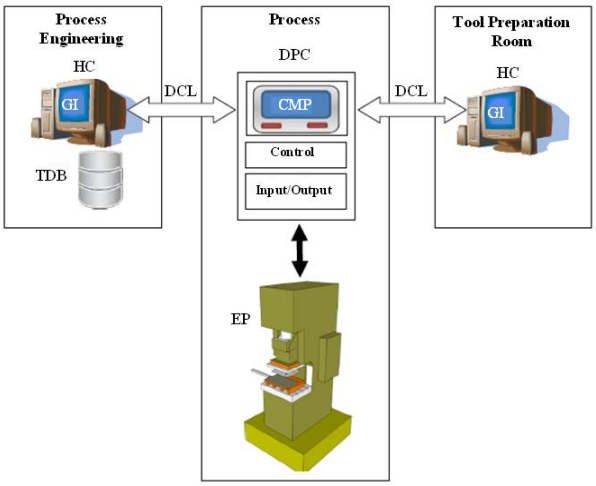


Figure 1: Reference Architecture Blocks.

In the Eccentric Press (EP), each production tool is installed, which should have its life cycle monitored to identify the appropriate moment of substitution, in order to avoid the negative consequences related to premature or late exchange.

IV. Prototype

A view of the components contained in the prototype that was assembled to evaluate the features established in the Graphical Interface (GI) windows, which is intended to be integrated into the physical architecture of the automated system that performs the management in the use of tools for an industrial eccentric press, is shown in Figure 2. In this prototype

the practical tests were carried out to validate the operational efficiency of the blocks of the reference architecture shown in this work, with special attention being given to the elaboration, operation and use of the virtual components that are contained in the windows of said interface.

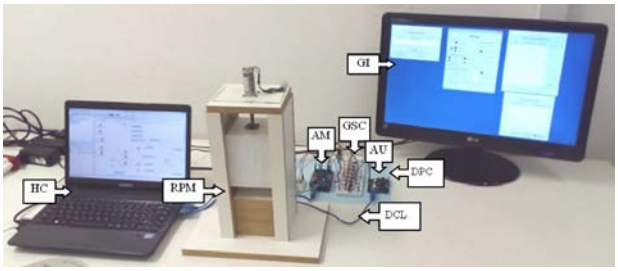


Figure 2: Prototype view.

As shown in Figure 2, the components established for the prototype are: i) Graphical Interface (GI), ii) Host Computer (HC), iii) Data Communication Line (DCL), iv) Dedicated Press Control (DPC), and v) Representative Press Model (RPM). It should be mentioned that the number of modules defined in the prototype is lower than that predicted in the reference architecture shown in Figure 1, but this condition is not limiting to prevent the validation of the virtual resources that are present in the Graphical Interface (GI) windows.

The Host Computer (HC), used in the prototype, is a portable (notebook) type, with Intel® 64-bit architecture and Windows 8.1™ operating system. The Graphical Interface (GI), installed on this computer, has been developed with the resources available in the integrated development environment that is called by MyOpenLab, build: 3.0.4.1, under license: GNU - general public license [3].

In the physical layer, the Data Communication Line (DCL) adopts the EIA (Electronic Industries Alliance) 232, and in the logic the protocol denominated by Firmata [4].

The Dedicated Press Control (DPC) consists of: i) microcontrolled unit (AU) of the Arduino type UNO [5], ii) Galvanic Separation Circuit (GSC), and iii) micro-controlled unit (AM) of the Arduino type MEGA 2560 [6]

The Arduino UNO unit (AU) performs the bidirectional data communication interface between the Galvanic Separation Circuit (GSC) and Host Computer (HC), through the protocol Firmata.

The Galvanic Separation Circuit (GSC) is a mean established to perform bidirectional communication of electrical signals between the Arduino UNO (AU) and Arduino MEGA 2560 (AM) unit in an irradiated way. It should be mentioned that the use of this circuit is intended to minimize possible incompatibilities and/or electrical faults of one unit affecting the operation of the other.

The purpose of the Arduino MEGA 2560 (AM) unit is to: i) execute the dedicated operation control of the Representative Press Model (RPM) from the command signals sent by the Galvanic Separation Circuit (GSC), and ii) send signals related to the state of the sensors installed in the Representative Press Model (RPM) for the Galvanic Separation Circuit (GSC). This unit is equipped with a specific circuit to control the motor installed in the model, which is the Motor Shield L293D Driver H-Bridge [7].

a) Management software

In the development of the prototype, a version of the tool management program was developed for an eccentric industrial press in order to evaluate the virtual resources that were established for each Graphical Interface (GI) window. In this sense, the analytical flowchart that represents a specific sequence of actions foreseen in this management program, and that was used in the accomplishment of the practical tests of this work is presented in Figure 3.

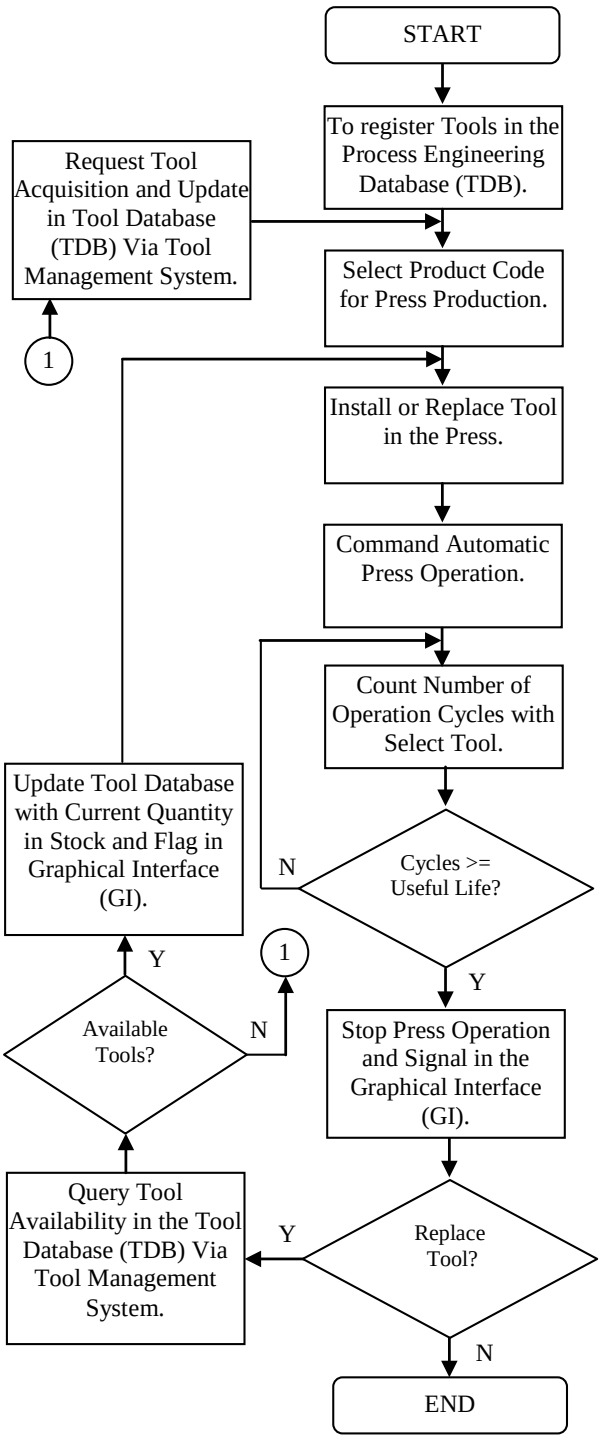


Figure 3: Flowchart of the management system.

b) Graphical interface

In the windows of the Graphical Interface (GI) that was elaborated for the prototype are present the resources that allow to the user of the system to make the registrations of the codes of the products, codes of the tools, times of useful life and also, to carry out the control, the monitoring and the interruption of the operation of the Representative Press Model (RPM).

In this sense, Figure 4 presents the virtual resources that were established for the Tool Registry Window, which specifically serves the Process Engineering Sector.

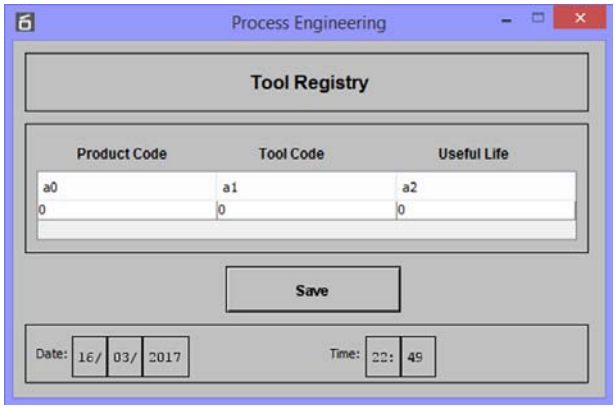


Figure 4: Process engineering tool registry window.

The virtual components contained in the Tool Registry Window, shown in Figure 4, allow the Process Engineering user to perform the following tasks:

- Enter each product code number in the field labeled "Product Code", where this field establishes the product that will be manufactured in a specific production process by the press.
- Register each tool code in the field called "Tool Code", this field contains the code defined by the company for each tool that is used by the press in its various manufacturing processes.
- Register each tool life in the field called "Useful Life", this field establishes the useful life for each tool that is used in the press in nominal use condition.
- Save in the Process Engineering Sector Database (TDB) the information that has been registered through the Tool Registry Window.
- View the current date (Date) and time (Time), which are provided by the Host Computer (HC).

The Figure 5 presents the virtual resources that were developed to attend the Press Window, which is dedicated to the production process. In this window there are regions with virtual components that allow the production user to perform the following tasks:

- Set the automatic mode (Automatic) or manual mode (Manual) of the press by means of the virtual key contained in the region that is called Press Condition. The manual mode is basically used to carry out tool replacement in the press or set the initial state of the actuator (Ready Press) to set the reference in the automatic operation.
- Execute the production cycle for the press using the button labeled "On/Off Cycle", which is present in the region called "Auto Mode Functions". When this button is activated the visual signaling that is called "On Cycle" will be activated (red color) and the one called "Cycle Off" will be inactive (black color), and the button in the not activated state will occur vice versa. It should be mentioned that in this region

visual signals are also present to indicate that the actuator of the press is in the condition of maximum retracted (Press on top) or maximal expanded (Press on bottom), since the set formed with the sequences of activations of these signals defines the Cycle of the tool.

- Establish a reference to start the operation of the press (Referencing Press) with the resources contained in the region called "Manual Mode Functions". The user can actuate the button labeled "Jog Up Press" to set the maximum condition retracted in the actuator of the press, or "Jog Down Press" for the maximum extended condition. When these buttons are activated the visual signage called "Jog" is activated.
- Manage the useful life of the tool installed in the press with the resources of the region called "Management Tool Life". The "Tool Life" display shows the current number of operating cycles that the tool installed in the press has performed, and related information is also displayed in the bar graph as another means to sensitize the user about the importance of that number to the process. The "Tool Limit" display shows the number of operations that was established by Process Engineering to use the current tool installed in the press. The "Tool Code" display shows the number assigned by the company to the tool installed in the press. The "Tool Change" signaling is triggered (red) when the current number of tool operation cycles (Tool Life) is equal to or greater than the number of operations that has been established by Process Engineering (Tool Limit), being that for this condition the operation of the press will be stopped until the replacement by a new tool, and the actuation of the button called "Tool Replaced".
- View the current date (Date) and time (Time) provided by the Host Computer (HC).

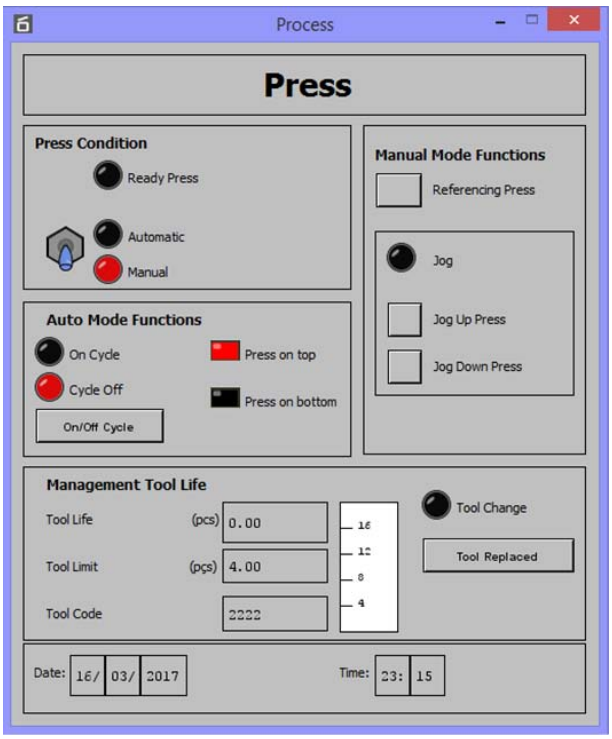


Figure 5: Press window of the production process.

The Figure 6 presents the virtual resources that have been established to serve the Tool Selection Window, which specifically serves the Tool Preparation Room.

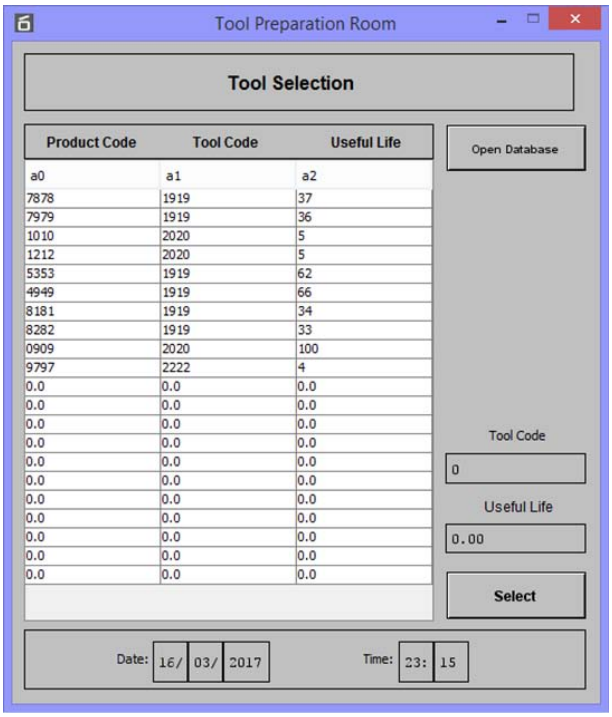


Figure 6: Tool selection window.

The virtual components contained in the Tool Selection Window, shown in Figure 6, allow the Tool Preparation Room user to perform the following tasks:

- Display the information of the product code number in the field labeled "Product Code", the tool code in the field called "Tool Code", and the tool useful life in the field called "Useful Life", which are displayed in the columns in the main part of that window.
- Update the records of tools carried out by Process Engineering, through the button called "Open Database".
- Select a particular tool to process through the button labeled "Select". It should be mentioned that the user after choosing the tool and pressing the "Select" button, the information about this tool is loaded in the respective fields of the region named "Management Tool Life", which belongs to the Press Window.
- View the current date (Date) and time (Time) provided by the Host Computer (HC).

The Figure 7 presents the virtual resources that have been developed to meet the Tool Stock Window, which is dedicated to the Tool Management System.

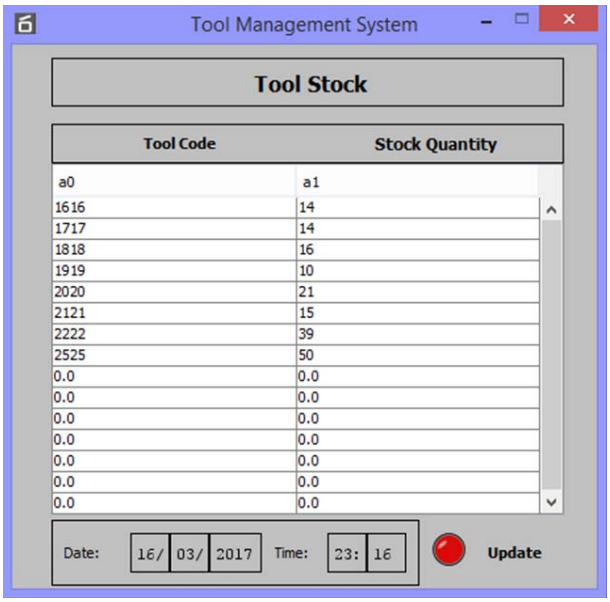


Figure 7: Tool stock window.

In the Tool Stock Window, shown in Figure 7, there are virtual components that allow the Tool Management System user to perform the following tasks:

- View information about the tool code in the field called "Tool Code", and the current number of tools available in the company stock in the field called "Stock Quantity", which are displayed in the main display columns of that window.
- View the state of the signaling that informs the update (Update) of information in the Tool Database (TDB).
- View the current date (Date) and time (Time) provided by the Host Computer (HC).

c) Practical tests

The following sequence of actions was performed to evaluate the effectiveness of the virtual components provided in the Graphical Interface (GI) windows that is proposed in this work:

- Perform the mechanical assemblies and electrical connections required to meet each of the components provided in the prototype shown in Figure 2.
- Program the Arduino UNO (AU) and Arduino MEGA 2560 (AM) units, in accordance with the respective proposals for use and the steps established in the analytical flowchart shown in Figure 3.
- Design the Graphical Interface (GI) with windows, layouts of virtual components, resources and structural hierarchy, as shown in Figure 4, Figure 5, Figure 6 and Figure 7.

The execution of the practical tests was divided in three stages, in the first one were evaluated specifically the resources related to the Tool Registry Window. This step evaluated the effectiveness of the resources provided in this window in allowing the user of the Process Engineering Sector to register the tools according to the standards adopted by the company.

In the second step it was observed whether the records registered in the Tool Registry Window were updated in the Tool Database (TDB) and available for selection in the Tool Selection Window of the Tool Preparation Room.

In the third stage the operation of the Representative Press Model (RPM) was activated, through the Press Window, in order to observe the capacity of the virtual components of this window in signaling the appropriate moment to carry out the replacement of the tool used in the current manufacturing process of the press. In this sense, Figure 8 shows the signaling activated when the current number of tool operation cycles (Tool Life = 4) is equal to the number of operations that was established by Process Engineering (Tool Limit = 4), stopping the cycle of the Representative Press Model (RPM).

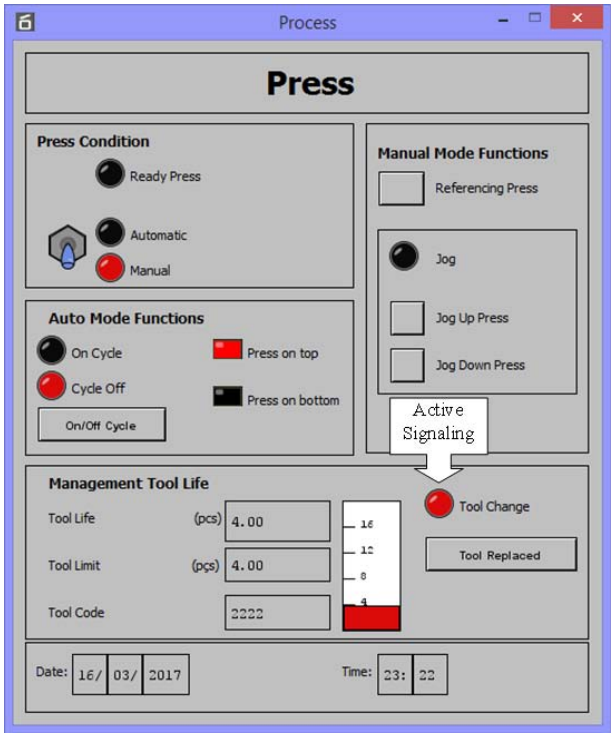


Figure 8: Signaling for tool replacement.

d) Results

The results observed in the practical tests were positive, because, with the virtual components established for the Graphical Interface (GI) windows, proposed in this work, it was possible to perform the tool registry, the selection of a specific tool to attend a given process, and the identification of the appropriate moment to perform the tool replacement, that is, the moment in which the useful life of the tool (Tool Life) is equal to the number of operations established for it (Tool Limit).

V. Conclusions

The positive results obtained in the practical tests suggest that the Graphical Interface (GI), when integrated into the real system that performs the management in the use of tools for an eccentric industrial press, may be able to aid a tool registration a selection of a specific tool to attend the process and, mainly, an identification of the appropriate moment to make the replacement of the tool in order to minimize the consequences from the premature or late tool replacement.

The virtual features contained in the Tool Selection Window and Tool Stock Window allow the user to view up-to-date information that are stored in the Tool Database (TDB), which minimize the possibility of errors in estimating available quantities of tools in the company stock.

The layout, expressiveness and details contained in the virtual components that were developed for the Graphical Interface (GI) windows provided an intuitive and informative environment for the user of the Process Engineering Sector and the Tool Preparation Room to carry out their respective activities in the company, which collaborates to minimize the occurrence of operating errors in the use of the tool management system.

References Références Referencias

1. Arun, S., Rajendra, S. and Bongale, V. "Automatic Punching Machine: A Low Cost Approach", International Journal of Advanced Mechanical Engineering. Volume 4, Number 5 (2014), pp. 509 - 517.
2. Rosário, J. M. Princípios de Mecatrônica, Editora Person Prentice Hall, São Paulo, Brasil, 2005.
3. Gutiérrez, J. M. R. MyOpenLab - Versión 3.010 - Guía de Usuário. URL: http://www.myopenlab.de/downloads/Guia_usuario_MyOpenLab_3010.pdf.Visita do em: 10 de abril de 2016.
4. Steiner, H.C. Firmata: Towards making microcontrollers act like extensions of the computer, NIME09, June 3-6, 2009, Pittsburgh, PA, 2009.
5. Banzi, M. Getting Started with Arduino, Second Edition, Published by Make: Books, an imprint of Maker Media, a division of O'Reilly Media, Inc. 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2011.
6. Oxer, J. and Blemings, H. Practical Arduino: Cool Projects for Open Source Hardware, Distributed to the book trade worldwide by Springer-Verlag New York, Inc., 233 Spring Street, 6th Floor, New York, NY 10013, 2009.
7. Margolis, M. Arduino Cookbook, Second Edition, Published by O'Reilly Media, Inc., 1005. Gravenstein Highway North, Sebastopol, CA 95472, 2012.

This page is intentionally left blank

Global Journal of Computer Science and Technology: H Information & Technology
Volume 17 Issue 2 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Technological Methods Analysis in the Field of Exaflops Supercomputers Development Approaching

By Molyakov Andrey Sergeevich & Eisymont Leonid Konstantinovich
Peter the Great St. Petersburg Polytechnic University

Abstract- In this article authors describe new supercomputing developing roadmaps, illustrate how to solve Moore's Law problem. Authors show two different ways of creating new high-productive clusters: evaluative and revolutionary. There are new era so-called "Post Moore". It means specialists all over the World should together in collaboration create new electronic components, architecture principles, design criteria and etc.

GJCST-H Classification: *B.7.1*

Strictly as per the compliance and regulations of:

Technological Methods Analysis in the Field of Exaflops Supercomputers Development Approaching

Molyakov Andrey Sergeevich [α] & Eisymont Leonid Konstantinovich [σ]

Abstract- In this article authors describe new supercomputing developing roadmaps, illustrate how to solve Moore's Law problem. Authors show two different ways of creating new high-productive clusters: evaluative and revolutionary. There are new era so-called "Post Moore". It means specialists all over the World should together in collaboration create new electronic components, architecture principles, design criteria and etc.

I. Innovative Projects of New Supercomputers Developing

Наиболее заметным явлением в начале работ по экзамасштабной и экзафлопсной тематике было проведение рабочих групп по инициативе DARPA. Далее, в 2010 году, была запущена новая программа DARPA UHPC развития экзамасштабных технологий. В этой программе участвуют четыре группы, каждая из которых, состоит из коммерческих компаний, национальных лабораторий и университетов: проект Runnemede (Intel), проект Echelon (NVIDIA/Cray), проект X-calibr (Лаборатория Sandia), проект Angstrom (MIT).

В соответствии с исторически сложившимися традициями, DARPA в своих работах заняла нишу инновационных проектов, а DOE (Министерство энергетики США) проводило большей частью эволюционную линию по созданию рекордно крупных суперкомпьютеров, прежде всего в двух ультракомпьютерных центрах в Окриджской и Аргонской лаборатории.

Тезис 1. DARPA (представляет военных и разведывательные службы США) не справилась в полной мере с задачами создания перспективных систем петафлопсного уровня реальной производительности (программа DARPA HPCS) и настолько неудачно начала работы по экзамасштабным технологиям (программы DARPA UHPC и OHPC), что можно говорить об их тупиковости и близком преждевременном закрытии. В связи с этим, ответственность за выполнение работ по экзамасштабной тематике теперь возлагается на DOE.

Тезис 2. Неудачи начала работ по экзамасштабным системам объясняются низким уровнем инновационности проектов DARPA UHPC и слабым вовлечением талантливых разработчиков в эти проекты.

Author α: e-mail: andrei_molyakov@mail.ru

Тезис 3. Инновационный стиль в виде работ инновационнного характера, от алгоритмов и прикладного программного обеспечения до элементно-конструкторской базы, противопоставляется стратегии эволюционного развития за счет постепенного введения улучшений, "инкрементному" развитию, которое считается тупиковым в долгосрочной перспективе, но выгодно экономически основным промышленным вендорам (Intel, IBM, Cray, NVIDIA и др.).

Тезис 4. В качестве ключевой темы продвижения к экзамасштабным системам ставится вопрос создания новых моделей организации и выполнения параллельных программ. Выделяются два подхода, эволюционный и инновационный.

Тезис 5. Переход инициативы по работам экзамасштабной тематики к DOI и необходимость преобладания в этих работах инновационного подхода объясняется тем, что США могут потерять мировое лидерство в данной области, а это место будет немедленно занято другими странами, вероятнее всего из Азиатско-Тихоокеанского региона. Эти страны пойдут на любые риски в выборе наиболее оптимальных стратегий, поскольку находятся в роли догоняющих. В связи с этим, подключение самой мощной в США научно-технической инфраструктуры DOE в виде не только научных национальных лабораторий, но и национальных лабораторий ядерного оружейного комплекса к решению этой ставшей важнейшей проблемы современности, которые также и скоординируют работу ведущих университетов и промышленных вендоров, – принципиально необходимо.

Тезис 6. Стремление к мировому лидерству США в области экзамасштабных систем и их приложений должно быть совмещено с международным сотрудничеством по этой линии с целью эффективного использования мировых интеллектуальных ресурсов и достижений.

Тезис 7. Разработка экзамасштабных систем и технологий их применения для решения важнейших задач к концу 2020 года рассматривается как качественный переход в области основ и технологий, организации соответствующей инфраструктуры исследований и разработок для создания систем зеттафлопса и йотафлопса, в которых будут применены новейшие достижения нанотехнологий.

Таким образом, для формирования мнения о проектах экзафлопсной тематики можно теперь рассматривать, в основном, работы DoE. Формирование крупного проекта DoE по созданию экзафлопсной машины на эволюционных или инновационных принципах задерживается. Сейчас выполняется множество небольших проектов по разным направлениям большим количеством групп.

В целом, в настоящее время в DoE имеются следующие направления работ по тематике экзамасштабных систем (это сейчас называют "exascale ecosystem", экзамасштабная экосистема, которые в 2013 году должны дополниться направлением OS/R или «Экзамасштабные операционные системы и системы поддержки выполнения программ» (Exascale Operating and Runtime Systems).

Далее приведем краткие сведения об этих программах. Эта информация специально структурирована так, чтобы в будущем вносить дальнейшие уточнения.

В части технологии создания процессора этот проект связан с работами по линии архитектуры Intel MIC (Many Integrated Core), которая в настоящее время стала называться Xeon Phi. Это микропроцессор со множеством облегченных 4-х тредовых ядер с системой команд X86 и векторными расширениями. В 2012 году вышел образец сопроцессорной платы Knight Corner с таким микропроцессором, изготовленным по технологии 22 нм, имеющим более 50 процессорных ядер. Эта плата содержит 8 Гбайт памяти GDDR5 и подключается через шину PCI Express. Производительность такого сопроцессора около 1 Тфлопс. Этот сопроцессор виден приложению как вычислительный узел, работающий под управлением ОС Linux, так что его использование ожидается более простым, чем современных графических процессоров.

В части технологии памяти Intel в этом проекте будет работать с Micron Technologies над созданием гибридного куба памяти (HMC, Hybrid Memory Cube). Это вариант технологии 3D сборки кристаллов процессоров и памяти, что должно значительно повысить пропускную способность интерфейса процессора с памятью и снизить задержки обращений к памяти.

Например, экзамасштабные приложения разрабатываются уже в настоящее время в центрах разработки, как и специальное оборудование для этих приложений. Так что вероятен и вариант появления не одного (например, в Окриджской лаборатории), а нескольких образцов экзамасштабных систем, причем в этих центрах со-разработки, т.е. в Лос-Аламосской и Аргонской лаборатории, лаборатории Сандиа.

Кстати, Лос-Аламосская лаборатория и лаборатория Сандиа образовали недавно совместный центр ASEC, причем лаборатория Сандиа также сотрудничает с Окриджской лабораторией в рамках работ образованного в DoE Института перспективных архитектур и алгоритмов. Лаборатория Сандиа и Лос-Аламосская лаборатория имеют мощный производственный комплекс, выполняющий все виды работ, включая и работы по нанотехнологиям.

В таблицах 1 и 2 приведены "дорожные карты" реализации суперкомпьютеров эволюционного направления в Окриджской и Аргонской лабораториях. Рубеж в 30 PFlops взят в 2012 году.

Таблица 1: Оценки характеристик систем, создаваемых на этапах экзафлопсного проекта с применением тяжелых" процессорных ядер

Системная характеристика	Годы внедрения системы			
	2009	2011	2015	2018
Общая пиковая производительность	2 PF	20 PF	100-200 PF	1 EF
Общий объем оперативной памяти	0.3 PB	1 PB	5 PB	10 PB
Пиковая производительность узла	125 GF	200 GF	400 GF	1-10 TF
Пропускная способность памяти узла	25 GB/s	40 GB/s	100 GB/s	200-400 GB/s
Количество ядер в узле (параллелизм узла)	12	32	0(100)	0(1000)
Пропускная способность сетевого интерфейса узла	1.5 GB/s	10 GB/s	25 GB/s	50 GB/s
Количество узлов в системе	18,700	100,000	500,000	0(Million)
Количество ядер в системе (общий параллелизм)	225,000	3 Million	50 Million	0(Billion)
Общая мощность потребления	6 MW	~10 MW	~10 MW	~ 20 MW
Объем внешней памяти	15 PB	30 PB	150 PB	300 PB
Пропускная способность ввода-вывода	0.2 TB/s	2 TB/s	10 TB/s	20 TB/s
MTTI, время между прерываниями по сбою или отказу системы	Days	Days	Days	0(1Day)

В Окриджской лаборатории потенциал модернизации суперкомпьютера XC30 до 100 Pflops, а для Аргонской лаборатории разрабатывается новый суперкомпьютер IBM BlueGene/R с производительностью до 100 Pflop/s, он будет введен в эксплуатацию в 2015 году. Кроме того, фирма IBM готовит новый вариант суперкомпьютера на базе нового микропроцессора Power 8. По информации из экспертной среды, это 256 ядер, ядра трех типов – суперкскалярные, легкие и легкие с векторнвми ускорителями, все ядра 6-тредовые.

Таблица 2: Оценки характеристик систем, создаваемых на этапах экзафлопсного проекта "легкого" направления

Системная характеристика	Годы внедрения системы				
	2004	2007	2012	2015	2019
Наименование системы/этапа	BG/L	BG/P	BG/Q (ONE)	TWO	THREE
Общая пиковая производительность	0.37 PF	1 PF	27 PF	309 PF	1127 PF (1.127 EF)
Общий объем оперативной памяти	0.034 PB	0.151 PB	2.147 PB	8.590 PB	25.770 PB
Пиковая производительность узла	5.6 GF	14 GF	205 GF	1.178 TF	4.301 TF
Пропускная способность памяти узла	5.6 GB/s	13.6 GB/s	42.6 GB/s	?	?
Объем памяти узла	0.5 GB	2-4 GB	16 GB	?	?
Количество ядер в узле (параллелизм узла)	2	4	16	32	96
Тактовая частота (GHz)	0.7	0.85	1.6	2.3	2.8
Количество запускаемых операций за такт в ядре	4	4	8	16	16
Пропускная способность сетевого интерфейса узла	2.1GB/s –3D torus 0.7GB/s – tree	5.1GB/s-3D torus 1.7GB/s-tree	40 GB/s-5D torus 4 GB/s extlinc	?	?
Количество узлов в системе	65536	73728	131072	262144	262144
Количество ядер в системе (общий параллелизм)	0.13 Million	0.3 Million	2 Million	8 Million	25 Million
Общая мощность потребления	2.5MW	4.8MW	8MW	30MW	40MW
Количество узлов в стойке	1024	1024	512	1024	1024
Количество стоек	64	72	256	256	256
Пиковая производительность стойки	5.7 TF	14 TF	105 TF	1.206 PF	4.404 PF

За 2011–2014 годы NUDT разработал новую суперкомпьютерную систему Tianhe-2 – шифр «Полет Дракона», с производительностью 30 Petaflops. Ожидается использование микропроцессоров Godson-3C или Godson-4A, мультитредовых микропроцессоров FT-1500, новой версии коммуникационной сети Arch. Эта разработка противопоставляется американскому суперкомпьютеру IBM Sequoia на 18-ядерных (4 треда в ядре) микропроцессорах PowerPC и 5-мерной сети типа тор. Ставится цель превзойти американский суперкомпьютер в 1.5 раза. Есть сведения, что этот суперкомпьютер уже практически готов, но это скрывается.

До 2016 года четырем ведущим исследовательским центрам Китая Министерства Обороны, Министерства энергетики и Министерства образования и промышленных технологий Китая (это National Air and Space Intelligence Center (NASIC), NUDT, ICT и National Applied Research Laboratories (NARL)) поставлена задача разработать и ввести в эксплуатацию вычислительный комплекс под кодовым названием «Тайваньский ястреб» производительностью 100 Petaflops. При этом важнейшую роль должна сыграть тайваньская фабрика TSMC; она на 60% принадлежит Китаю, на 20% принадлежит Японии, на 20% – иностранному капиталу США и Западной Европы (по данным конца 2011 года). По данным на сентябрь 2012 года доля Китая в TSMC составляет уже 75–80%.

Гетерогенный суперкомпьютер, включающий три типа массово-мультитредовых микропроцессоров, классические суперскалярные микропроцессоры, графические микропроцессоры и сетевые микропроцессоры. Базовый микропроцессор – СТ-2, возможны его модификации. Конструктив 4D с жидкостной системой охлаждения. Здесь будут использоваться новые микропроцессоры линейки Godson-3 и Godson-4 с тяжелыми суперскалярными ядрами, а также линейка Godson-T с легкими ядрами (типа микропроцессора Tilera).

Начиная с 2007 года Япония не имела систем, входящих в первую десятку списка Top500, т.е. систем петафлопсного класса производительности. Новые

планы развития имели цель изменить эту ситуацию, что и произошло сначала осенью 2010 года (Tsunami 2.0), а потом летом 2011 года (К-компьютер).

Tsubami 2.0 был о запущен осенью 2010 года и попал на 4-е место ноябрьского списка Top500 с пиковой производительностью 2,39 PFLOPS и производительностью на тесте Linpack около 1.2 PFLOPS. С 2013 по 2015 планируется разработать обновленную версию Tsubame 3.0 производительностью 30 PFlops, потребляемая мощность оценивается на уровне 1 MW, а стоимость – около 65 млн. долларов. Суперкомпьютеры Tsubame можно отнести к суперкомпьютерам традиционного кластерного типа. Это направление не считается как основное, определяющее будущее области суперкомпьютерных вычислений Японии. Работы ведутся в Токийском технологическом институте.

К-компьютер – самый мощный и статусный суперкомпьютер Японии, разработанный по программе создания перспективных стратегических суперкомпьютеров. Головная организация этого проекта - Институт физических и химических исследований (RIKEN). Этот институт наиболее приближен к Министерству образования, культуры, спорта, науки и технологии (MEXT), отвечающего за суперкомпьютерную тематику, является его исследовательским центром. Этот проект можно считать японским ответом на американский проект DARPA HPCS.

В общей сложности, этот проект создания К-компьютера обошелся в 1 млрд. евро (около 1.5 млрд. долларов). Пиковая производительность К-компьютера ~ 10 PFLOPS, производительность на тесте Linpack – 8-9 PFLOPS, но самая важная характеристика – возможность достижения на реальных приложениях производительности около 1 PFLOPS. В качестве таких приложений разработчики ориентировались на 8 прикладных областей, при этом в качестве главных областей были выделены нанотехнологии и область живых систем.

Имеются также партнерские проекты государственного и частного сектора, ориентированные на разработку программного обеспечения систем экзауровня. Один из таких проектов – EADI (Exascale Application and Data Initiative), возглавляемый фирмой Fujitsu и представляющий собой заключительный этап разработки 10 PFLOPS-ой системы (RITKEN NGS, К-компьютер) для японского правительства. EADI – это комплексный проект, который включает все направления работ Fujitsu по линии экзафлопсных вычислений.

Особняком стоит проект создания военного суперкомпьютера экзамасштабного уровня «Стрела времени», который рассматривается далее в этом разделе. Ведутся работы по био- и квантовым компьютерам, но информации о создании суперкомпьютеров на этих технологиях пока нет.

До недавнего времени в Западной Европе большая часть работ в области суперкомпьютеров и суперкомпьютерных вычислений была связана с разработкой того или иного программного обеспечения, множества приложений, а также новыми направлениями в области элементно-конструкторских технологий. Значительная часть специалистов работала и работает в филиалах американских фирм, причем их привлечение к такой работе со стороны американцев – сознательная и широко проводимая политика использования зарубежных высококвалифицированных ресурсов в интересах США.

Оригинальных инновационных суперкомпьютерных проектов, тем более связанных с разработкой собственной элементной базы, не было, хотя возможности для таких работ явно были и есть, но проводилась политика полностью ориентироваться в этих вопросах на американские разработки. Исключением была только разработка коммуникационной сети EXTOLL.

В последние два года ситуация стала меняться, появилась политическая воля иметь в Европе большую самостоятельность в такой важнейшей отрасли, как суперкомпьютерные технологии и их приложения. В связи с этим, появились инновационные проекты создания аппаратных средств мультипетафлопсных и экзафлопсных систем, например DEEP (с применением Xeon Phi, сети EXTOLL, правда при значительном участии Intel), Mont Blanc (ядра ARM и графические ускорители Nvidia). Запущен крупнейший проект разработки программного обеспечения экзамасштабных систем CREST.

При этом ряд проектов был запущен с сильным участием российской компании Т-платформы, которая кроме кластерных суперкомпьютеров при этом выходила и на инновационные возможности создания собственной элементно-компонентной базы. Есть мнение, что именно это и было главной причиной занесения компании Т-платформы в марте 2013 года в США в черный список.

Знаковых успехов по линии создания мультипетафлопсных суперкомпьютеров и продвижения к экзафлопсным системам пока нет, хотя несколько крупных кластеров собственной разработки уже попали в верхнюю часть списка Top500 и организовано несколько вычислительных центров, ориентированных в будущем на вычисления экзафлопсного уровня.

Самый мощный суперкомпьютер петафлопсного уровня был недавно разработан в ФГУП РФЯЦ-ВНИИЭФ (г.Саров). Эта организация является реальным лидером в сегменте суперкомпьютеров высшего диапазона производительности. Очевидно, что именно на эту организацию сделана ставка Правительством в вопросе создания суперкомпьютеров уровня 10, 100 и 1000 Пфлопс. Это предприятие ядерного оружейного комплекса и атомной

промышленности, что все объясняет. ГК «Росатом» подготовила в мае 2011 года Концепцию по экзафлопсным технологиям, в ее подготовке участвовали несколько организаций (Департамент развития научно-производственного блока ядкрного оружейного комплекса, ФГУП «РФЯЦ-ВНИИЭФ», ФГУП РФЯЦ-ВНИИТФ, Департамент развития Минобрнауки России, ФГУП «НИИ «Квант», ИПМ им. М.В.Келдыша РАН, ИПС им. А.К. Айламазяна РАН, НИИСИ РАН, МСЦ РАН, НИИММ им. Н.Г. Чеботарева при КГУ, ННГУ им.Н.И.Лобачевского, МГУ им. М.В.Ломоносова, МАИ, МГТУ им. Н.Э. Баумана), а ФГУП РФЯЦ-ВНИИЭФ была головной.

Т-платформы и МГУ им, М.В.Ломоносова – это другая группа разработчиков, они недавно подписали Меморандум о намерениях по сотрудничеству в области создания суперкомпьютеров нового поколения экзафлопсного уровня. Это конкуренты группы, возглавляемой ФГУП «РФЯЦ-ВНИИЭФ».

Основу еще одной группы составляют ИПМ им. М.В.Келдыша РАН и ФГУП НИИ «Квант» – две организации с большой историей в несколько десятилетий совместных работ. Кроме сотрудничества с ФГУП"РФЯЦ-ВНИИЭФ они ведут ряд проектов самостоятельно, поскольку работают главным образом в других прикладных областях. В последнее время к этой группе присоединились ЗАО «ВТ-Консалтинг», ООО «Е-троник», СПбГПУ, ФГУП ВО «Внештехника», Центр инженерных разработок физического факультета МГУ. Всегда было сотрудничество с ИПС им. А.К. Айламазяна РАН и ОАО «НИЦЭВТ», МСЦ.

По инновационной линии пока созданы три центра соразработки специальных экзафлопсных суперкомпьютеров для следующих областей: материаловедение (LANL – головнной исполнитель), перспективные реакторы (ANL – головной исполнитель) и процессы горения (SNL – головной исполнитель). Это направление можно охарактеризовать как оптимизацию применения КМОП-технологий. Ведется множество небольших проектов фундаментальных исследований, причем одно из основных направлений – новые модели организации параллельных программ для экзафлопсных суперкомпьютеров, новые run-time системы и операционные системы, новые средства параллельного программирования.

Крупная инновационная программа разработки в DoE инновационного экзафлопсного суперкомпьютера ожидается после 2013 года. В настоящее время для поддержки основных промышленных вендоров запущена предапрительная программа FastForward по разработке процессоров и модулей памяти, а также системы хранения данных. По мнению авторов, наибольший интерес представляет проект фирм Cray/NVIDIA Echelon.

Китай традиционно виртуозно воспринимает, копирует и развивает чужие проекты, применяя при этом новейшие технологии, которые также часто имеют иностранное происхождение, часто из Японии, Сингапура и Тайваня. Ведутся эволюционные и инновационные направления. Главный разработчик – Министерство обороны Китая в виде NUDT, университета оборонных технологий Китая.

По эволюционной линии авторы оценивают отставание китая от США не более 2-3 лет. В настоящее время собран суперкомпьютер Tianhe-2 (проект «Полет дракона») с производительностью 30 Пфлопс. Эта разработка пока не афишируется, применяется американская и собственная элементная база, как микропроцессоры, так и сетевые СБИС. В 2016 годудолжен быть построен 100 Пфлопсный суперкомпьютер (проект «Тайваньский ястреб»).

По инновационной линии пока известно лишь о проекте СТ-2 создания военного суперкомпьютера (проект «Удар грома») экзафлопсного уровня производительности для ршения информационных задач, на базе которого посредством изменения баланса в используемых микропроцессорах разного типа можно построить экзафлопсный суперкомпьютер и для научно-технических расчетов. По имеющимся сведениям, в основу этого проекта были положены российский проект СКСН Ангара и американский ParalleX.

Япония более самостоятельна и креативна в своих проектах, отличается сильной закрытостью. Имеются эволюционное и инновационное направление. По эволюционному направлению был разработан суперкомпьютер Tsubame и K-компьютер (10 петафлопс), причем если в Tsubame используется американская элементная база, то в К-компьютере – собственная. Намечено создание Tsubame-3 производительностью 30 петафлопс.

По инновационной линии известен пока лишь проект военного суперкомпьютера «Стрела времени», который разрабатывается Силами самообороны Японии, но за счет изменения состава микропроцессоров в вычислительных узлах может быть переориентирован на решение научно-технических задач.

По линии работ по элементной базе пост-Муровской эры достигнуты заметные результаты в области сверхпроводниковой электроники, которые можно расценивать как не хуже американских, по квантовым клеточным автоматам и квантовым компьютерам. Традиционно сильны позиции по коммуникационным сетям, где их можно считать мировым лидером.

Западная Европа ведет проекты экзафлопсных суперкомпьютеров эволюционного типа DEEP и Mont Blanc, это новое явление, раньше разработкой собственных аппаратных средств так активно не занимались, использовалась американская техника. Есть потенциал организации и самостоятельных инновационных проектов, но слишком много специалистов работают на США и Китай. Обсуждается вопрос создания европейского микроэлектронного гиганта типа фирмы Intel. Организовано несколько

центров выполнения экзафлопсных вычислений, много работ ведется по программному обеспечению для экзафлопсных систем.

В России пока только сформулирована Концепция экзафлопсных технологий, крупное целевое финансирование пока не открыто, но финансирование отдельных небольших исследовательских проектов уже началось.

Количество публикаций по этой тематике в России невелико. Судя по открытым данным, отставание России от США в классе задач с хорошей пространственно-временной локализацией обращений к памяти составляет около 10 раз (тест Linpack, рейтинг Top500), а в классе задач с плохой пространственно-временной локализацией – не менее 100 раз (тест BFS, рейтинг Graph500, тест RandomAccess, рейтинг HPCChallenge).

II. Supercomputers of Post Moore's Era

Считается, что предел развития кремниевых технологий – около 5 нм. Имеются оценки, что этот предел будет достигнут в 2020-2024 году, а проблемы начнутся уже после 2014 года, когда будет достигнут уровень 14-15 нм. Это пессимистические прогнозы.

Оптимистичные прогнозы по развитию КМОП-технологий обычно исходят от фирмы Intel. В настоящее время Intel и еще три фирмы в мире (TSMC, STMicroelectronics и Samsung) промышленно освоили технологию 22 нм, это произошло в 2012 году, в то время, как по прогнозам это должно было произойти в 2016 году.

Важны также планы по усовершенствованию модулей памяти, поскольку от них сильно зависит сейчас быстродействие и энергопотребление систем. Фирма Intel ведет работы совместно с фирмой Micron Technologies над созданием гибридного куба памяти (HMC, Hybrid Memory Cube).

Оптимистические прогнозы развития кремниевых технологий в настоящее время несколько успокаивают, но уже не позволяют снять напряженность в исследованиях и разработках по новым вариантам элементной базы для логических схем и памяти, вариантов соединения компонентов кристаллов и собственно кристаллов. Срок достижения предела развития кремниевых технологий (окончания действия закона Мура) близок и темпы приближения к нему опережают предсказания, что видно на примере технологий 22 нм. Работы по созданию новых технологий элементной базы ведутся уже несколько десятилетий, но в настоящее время ни одна из них не готова для практического использования вместо кремниевых технологий и пока речь может идти о выборе тех, которые можно было бы использовать хотя бы через 10 лет.

Вместе с тем, для отдельных вычислительных устройств и даже блоков готовые решения есть, есть и явно приоритетные направления исследований по элементной базе будущих суперкомпьютеров с уровнем производительности зетта (10^{21}) и более уровня.

Тем не менее, круг занятых в этих работах российских специалистов стал обозначаться, началась работа с ними как с экспертами данной области. В дальнейшем это поможет дать более точные и объективные оценки, но уже первый опыт изучения этих направлений показал, что эту работу уже пора вести непрерывно, содействовать координации.

Достижение физических ограничений КМОП-технологий и проводимые работы по новым технологиям, которые напрямую связаны с наномиром и квантовыми эффектами, сделали вновь актуальными несколько забытые в разработчиками суперкомпьютеров в период успешного действия закона Мура вопросы по физическим ограничениям производительности вычислительных систем. При оценке и систематизации работ по разным вариантам перспективной элементной базы и оценке пределов повышения производительности суперкомпьютеров (это было одной из задач данного прогноза) оказалось удобным использовать базовые положения этих работ, а именно: оценку минимальных энергетических затрат (ограничение Лэндауэра); утверждение о зависимости вычислений и выделяемого тепла, т.е. связи между информацией и термодинамикой (принцип Неймана-Лэндауэра).

По представленному в разделе материалу можно акцентировать внимание на следующих аспектах:

1. В настоящее время промышленно освоена кремниевая (КМОП) технология 22 нм, но всего четырьмя фирмами в мире – Intel, TSMC, Samsung и STMicroelectronics. По прогнозу Intel, уровень 5 нм будет достигнут уже в 2020 году. Считается, что дальнейшая миниатюризация невозможна, а закон Мура перестанет работать не позже 2024 года.
2. Эффективное использование КМОП-технологий в ближайшее время и вплоть до окончания действия закона Мура связано с различными приемами оптимизации: архитектуры (специализированные процессоры и ускорители), микроархитектуры; соединений на кристалле и между кристаллами; конструктивов в виде 3D сборки модулей и 3D СБИС. Работы такого типа ведутся и рассматриваются как основные при создании экзафлопсных суперкомпьютеров, но они связаны с преодолением слишком многих проблем.
3. Новые решения в области элементно-конструкторской базы (технологий пост-Муровской эры) могут облегчить создание экзафлопсных суперкомпьютеров и стать основой для создания суперкомпьютеров следующих уровней производительности. Основные задачи при разработке новых вариантов элементной базы: повысить частоту работы, снизить

энергопотребление, добиться высокого уровня интеграции.

4. Современные микропроцессоры работают на частоте 3-6 GHz. Устройства на базе сверхпроводниковых технологий (RSFQ) могут работать на частоте нескольких сотен GHz, по публикациям известны образцы, работавшие на частотах 20GHz и 80 GHz. Устройства на базе квантовых клеточных автоматов (QCA) могут работать на частоте порядка THz.
5. Теоретический предел затрат на обработку одного бита информации в обычных компьютерах нереверсивного типа составляет kT ln2 (ограничение Лэндауэра, далее для простоты kT). Для устройств на современных КМОП-технологиях характерна оценка затрат на бит обрабатываемой информации около 1000000 kT. Из публикаций известно о получении на экспериментальном сумматоре на базе RQL-технологии (оптимизированного варианта RSFQ-технологий) затрат на один бит в 1000 kT. Было также опубликовано, что при использовании nSQUID технологии (еще один оптимизированный вариант RSFQ) было получено, что на устройстве типа сдвиговый регистр затраты на один бит составляют несколько kT. Это обнадеживающие результаты, но следует признать, что такие технологии пока пригодны для создания реконфигурируемых решающих полей арифметических устройств для реализации потоковых вычислений.

   Работ по продвижению этих технологий еще много, эти технологии будут наверняка применяться в сочетании с КМОП-технологиями.
6. Ограничение Лэндауэра и требование обеспечения работы без сбоев на протяжении длительных отрезков времени для обычных суперкомпьютеров нереверсивного типа (без специальных мер по сохранению энергии при обработке информации) обуславливают верхнюю границу физически достижимой производительности суперкомпьютеров в несколько десятков экзафлопс, это ограничение получило название «точка Стерлинга».
7. Дальнейший рост производительности возможен после принципиального пересмотра суперкомпьютеров и перехода к их реверсивной организации, а также применении хотя бы в виде ускорительных блоков квантовых компьютеров и аналоговых компьютеров, возможно также построенных на квантовых принципах.
8. Важнейшим первым в истории вычислительных систем примером компьютера последнего типа является 128-кубитовый квантовый компьютер канадской фирмы D-Wave. Процессор этого компьютера быстрее двух процессоров Xeon (2.6 GHz) на переборном алгоритме глобальной минимизации на четыре порядка, но требует для работы температуры, близкой к абсолютному нулю.
9. Работы по вариантам перспективной элементной базы пост-Муровской эры отлично организованы на федеральном уровне в США, активно ведутся в Японии. Эти две страны – явные мировые лидеры в этом плане.

III. Summary

1. Есть значительные проблемы при создании экзафлопсных суперкомпьютеров по производительности и энергопотреблению (сеть, память и процессор), отказоустойчивости и продуктивности программирования.
2. Элементно-конструкторская база позволяет использовать мультиядерность (1000-кратно), повышенную пропускную способность кристаллов по вводу-выводу (3D-компоновка, TSV), оптические соединения между платами («Holley», WDM-технологии) и внутри кристаллов (нанотрубки), новая технология памяти (HMC, NVRAM).
3. Есть архитектурно-программные решения – массовая мультитредовость и модель разделения вычислений/доступа к данным (MT и DAE), потоковость (MD/DF), локализация данных и вычислений (RPC), гибридность/функциональная специализация (10x10), глобально-адресуемая память (PGAS/APGAS/HPGAS), интеллектуальная отказоустойчивость (Resilience).
4. Подходы к решению – эволюционный (DoE NNSA/ASCR), умеренно-инновационный (DoE ASCR), агрессивно инновационный (DARPA), инновационно-эволюционный&эмуляционный (DoE ASCR, NSF).
5. Сложность проблем и неочевидность решений за рубежом потребовала привлечения ресурсов не только на федеральном уровне, но и на региональном и мировом. Цели работ по экзамасштабной тематике (DARPA) и экзафлопсной (DoE) имеют отличия, но методы их достижения во многом совпадают. Зарубежный опыт показывает, что в организационном плане важным является централизованная формулировка целей работ и управления ими (формирование и поддержка «силового поля»). Работы по экзафлопсным суперкомпьютерам находятся на переходном этапе от применения только кремниевых технологий к переходу на применение пост-Муровских перспективных технологий.

References Références Referencias

1. Моляков, А.С. Тихоокеанско–азиатские петафлопсы / А.С. Моляков, В.С. Горбунов, П.В. Забеднов // Открытые системы. СУБД. – 2011. – №7. – С. 26 – 29.

2. Олифер, В.Г.. Компьютерные сети / В.Г. Олифер. – СПб.: Изд – во Питер, 2004. – 199 с.
3. Моляков, А.С. Исследование скрытых механизмов управления ОС на различных платформах /А.С. Моляков // Известия Южного Федерального Университета..Технические науки. – Таганрог: Изд – во ТТИ ЮФУ, 2007. – №1. – С. 137 – 138.

Global Journals Inc. (US) Guidelines Handbook 2017

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

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

- 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.

FARSC accrediting is an honor. It authenticates your research activities. After recognition as FARSC, you can add 'FARSC' 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:

FARSC 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 FARSC 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 FARSC 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 FARSC, 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 FARSC 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 FARSC 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 FARSC, 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 FARSC 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 FARSC 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 FARSC is eligible to earn from sales proceeds of his/her researches/reference/review Books or literature, while publishing with Global Journals. The FARSC 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 FARSC member can decide its price and we can help in making the right decision.

The FARSC 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 COMPUTING (MARSC)

The ' MARSC ' title is accorded to a selected professional after the approval of the Editor-in-Chief / Editorial Board Members/Dean.
The “MARSC” is a dignified ornament which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., MARSC or William Walldroff, M.S., MARSC.

MARSC accrediting is an honor. It authenticates your research activities. After becoming MARSC, you can add 'MARSC' 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.

MARSC 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 MARSC, 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 MARSC 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 MARSC, 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 convenient, 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.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

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.

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

save our planet

Global Journal of Computer Science and Technology

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

ISSN 9754350