ISSN 2413-2632
Volume-4, No-4
January - June, 2019

Multidisciplinary Journal of European University of Bangladesh

Approved by UGC & Govt.

European University

(Centre of Excellence for European Standard Education in Bangladesh)

ISSN 2413-2632
Volume-4, No-4
January - June, 2019

Multidisciplinary Journal *of* European University of Bangladesh

European University of Bangladesh

Multidisciplinary Journal of European University of Bangladesh

Executive Editor
Obaidur Rahman

Disclaimer

Opinion expressed in the articles are those of the authors' and do not represent the point of view of the Editor or European University of Bangladesh

Price: Tk. 150.00 / US Dollar: 10

European University of Bangladesh
Permanent Campus: 2/4, Gabtoli, Mirpur, Dhaka-1216
Cell: 01713-006814, 01914-098494
Email: makhaneub@gmail.com

Published by:	**Publication Section** European University of Bangladesh, Dhaka.
Composed by:	**Md. Layeb Ali Molla**
Cover Designed by:	**Discovery Advertising.**
Printed by:	**M. M. Printers.**
Copyright:	**European University of Bangladesh, Dhaka, Bangladesh.**

Editorial Note

European University of Bangladesh is now in its permanent campus at the busiest gateway of Dhaka City --- Gabtali, Mirpur. We have successfully completed the construction of its 5.5 Lac sqft massive academic building. The University has by now more than 18,000 students, 450 Teachers – and around 350 support staff. We received more than 30 research-based articles for publication. After peer-reviewing we have selected seven articles for the current issue. So, it was a Herculean task to choose seven articles out of thirty.

This fourth Issue contains 7 (seven) articles covering multi-disciplinary issues. The first article deals with the concept of measuring effectiveness of teaching and the existing evaluation system of faculty members of EUB. The article also highlights the various aspects of the analysis of evaluation results and the recommended measures for further improvement. The authors of this article are Dr. Farzana Alam, Chairman, Department of Business Administration, Md. Mahmudul Hasan Chowdhury, Md. Azzajur Rahman and Abdullah Al Nafis. All of them are working with the faculty development activities of EUB and as such have expressed their views based on experience.

Five teachers, Mr. Biswas Kumar, Ahmedul Kabir, Md Abdullah al Forhad, Ahamad Ali and Mr. Obaidur Rahman wrote the article on design and implementation of steganographic application (one type of cryptography) for providing the confidentiality of information. This is a very interesting subject. The third article, Analysis of Chips on Hot Machine Method, has been authored by Nabili Sobha Islam. The fourth article, authored by Iftay Khairul Alam, Mushfeka Binte Kamal and Nadim Ibn Sayed, deals with the effect of corporate social responsibilities (CSR) on brand image. This article is written on the basis of a case study on ABA Group, Bangladesh. The fifth article is authored by Ahmedul Kabir, Biswas Kumar, Md Abdullah al Forhad, Ahamad Ali and Mr. Obaidur Rahman, Department of Computer Science and Engineering, European University of Bangladesh. It deals with an automated pest detection system utilizing histogram of oriented gradients with a mobile application. The sixth article, authored by Sheikh Salman, Md Arafat Hossain, Md. Maruf Hossain and Hasan Al Zaman, deals with an analysis of the plastic waste collection and wealth linkage in Bangladesh.

The seventh article, authored by Mr. Obaidur Rahman, Chairman, Department of Computer Science and Engineering, European University of Bangladesh, deals with the data encryption algorithms and comparison. This is a very critical area, needing special attention from the concerned academics and practitioners. It is hoped that all these articles will be of great interest to the esteemed readers of our journal.

European University of Bangladesh is a third-generation university with a clear vision to deal with a social problem --- higher education for poor students. With this end in view, we have kept our tuition fees very low, which is affordable for the economically backward section of our society. We are getting quick response from our target group of students. We hope our honourable readers would find the journal useful and benefit us with their valuable comments and suggestions.

Mr. Obaidur Rahman
Executive Editor

Contents

Measuring Effectiveness: Existing Evaluation Standard of Faculty Members at European University of Bangladesh

Dr. Farzana Alam*
Md. Mahmudul Hasan Chowdhury**
Md. Azzajur Rahman ***
Abdullah Al Nafis****

Abstrat: The Study investigated the usefulness of reflective assessments by students in combination with independent ratings of teaching performance of their faculty members at European University of Bangladesh. Student ratings conducted by the Faculty Development and Evaluation (FDE) Section are discussed in depth and final suggestions for further improvement are given. The FDE Section maintains confidentiality and neutrality in the every stage of the study to develop faculty performance. The Study found that faculty participants consistently expressed satisfaction with FDE development trainings and workshops. In addition, the research findings established that most faculty members voluntarily took necessary steps to improve their instructional effectiveness, though only a minority pursued these efforts in depth. A measure of effectiveness has remarkably improved their efforts; especially those who received consultative assistance therefore post evaluation training improved significantly.

Background

European University of Bangladesh's formal student evaluation system was introduced in 2015 and from that time onward department-wise performance evaluation critically discussed by an unbiased and independent Evolution Section called Faculty Development and Evaluation Section (FDE). The assessment of the effectiveness of faculty development programs is becoming increasingly important. This paper illustrated a brief summary of research findings, conducted on evaluation system and its modification system by Faculty Development and Evaluation Section (FDE) which aims to identify, measure and manage the quality parameters to evaluate teaching quality of faculty members in all the departments of European University of Bangladesh (EUB). The parameters have focused principally on what to evaluate and explain these indicators in detail. FDE is performing the role of Institutional Quality Assurance Cell (IQAC) within the

university and giving the right information in case of major decision making at university Syndicate Meeting, Academic Council Meeting and continuously reporting up-to-date status of the faculty development and evaluation activities to University Grant Commission (UGC). In each semester a detailed individual and department-wise reports prepared by FDE Section for open review meeting to disclose each faculty member's performance with the help of simple statistical tables, charts and graphs of the student feedbacks. From a research perspective Odden, Borman, and Fermanich (2004) argued that standard teacher's evaluation scores might be very useful in research on teaching effects on student learning. Assessment

on more than 250 (two hundred fifty) individual faculty members from each department had been collected, which was conducted on almost 20,000 (twenty thousand) students of EUB to

*** Chairperson and Associate Professor, Department of Business Administration.(EUB)**

**** Deputy Director, Faculty Development and Evaluation and faculty member Department of Business Administration. (EUB)**

***** Senior Lecturer, Department of Business Administration. (EUB)**

****** Senior Lecturer, Department of Business Administration. (EUB)**

collect data twice in each semester, once before commencement of Mid-Term Examination and the other before the Term Final Examination on last evaluation term. In addition, all respondents (students) were given the option to remain anonymous in the context of their participation .Each course evaluation had undergone through a well-structured process to appraise their current instructor's qualitative information about student learning experiences and perceptions of teaching techniques by FDE developed standardized survey questionnaire form.

Objectives

i. Quantitative and Qualitative assessment of the teachers' performance.

ii. Identification of the areas of strengths and weaknesses of Teachers' Performance.

iii. Future policy and strategy recommendations for improvement of teachers' perfor mance and transfer of learning.

Methodology and Data sources

i. Department wise trend analysis.

ii. In-depth analysis of student feedbacks.

iii. Mean Absolute Deviation (MAD) difference calculation of pre and post Transactional Analysis Training (TAT) scenario;

iv. Inter-departmental and cluster based statistical data analysis along with the trend study of evaluation on pre-mid to final exam.

Actual Evaluation Mechanism and Parameters

Teaching performance evaluation questionnaire is well-structured and developed by using **"Five point quality scale"** such as **Excellent** (100-80 > A+), **Very Good** (79-70 > A), **Good** (69-60 > B+), **Satisfactory** (59-50 > B) and Not **Satisfactory** (49-0 > C). Categorized by six parameters, where in each parameter there are selective qualitative questions as inside contents to find out the performance of respective faculty members.

Organization of the lesson

There are many equally effective ways to organize a course to accomplish a particular set of objectives. For example, a course could be arranged in any one of the following ways: chronologically, from concrete to abstract (or vice versa), from theory to application (or vice versa), around a set of questions, around a set of practical problems or case studies, according to disciplinary classifications and categories, etc. However it has been chosen to organize the course, the goal should be to create a structure that supports the learning objectives those have identified as follows:

✓ Were we (students) informed about the lesson before?

✓ Were materials well-organized and easy to understand?

✓ Was lecture started and ended on time?

✓ Did the modules help to understand, learn and apply the lesson?

✓ Were class tests taken regularly followed by the lesson?

Interpretation of teaching materials

Interpretation is a skill that a teacher can acquire consciously or unconsciously through an intensive process of learning, training, and experiencing in a formal classroom, in a set-up situation, or in a real-life situation. In teaching interpretations are designed intentionally to assist the students to be skillful prospective interpreters after graduation. The chosen parameters related to interpretation of teaching materials are as follows:

- ✓ Did the description of modules and teacher's explanation help to understand the lesson?
- ✓ Were the description and explanation of lecture relevant to subject matters?
- ✓ Would class-room discussion inspire creative thinking?

Presentation of teaching materials

Teaching materials are the tools used in the classroom. Teaching material is used by teachers to help learner improve reading and other skills, illustrate or reinforce a skill, fact, an idea and relieve anxiety, fears or boredom. Teaching materials are important because they create a visual and interactive experience for the students and assist students in learning. The tools are designed to involve the students, promote interaction, and promote faster learning and better comprehension. However the parameters related to presentation of teaching materials should support the learning objectives those have identified as follows

- ✓ Were pronunciation and presentation of the teacher clear?
- ✓ Were teaching modules brief but covered all the relevant issues?
- ✓ Were the teaching aids, such as, white board, chart, multimedia etc. helped to understand the lesson?

Interpersonal discussion inside the classroom

Teacher-student relationships play a crucial role in the quality of teaching and learning. Daily interpersonal interactions in classrooms are the building blocks of teacher-student relationships. From the perspective of the specific role and status of teachers and students in classrooms anticipated specific refinements from the general tendencies. The selective parameters are as follows:

- ✓ Did the teacher answer to the questions of the students directly and correctly?
- ✓ Did classroom discussion and group study help us (students) to understand the lesson?

Interpersonal discussion outside the classroom

Teachers always use group projects and collaborative activities to encourage teamwork in the classroom. This remains a positive way to foster interpersonal development. Teachers can also support interpersonal student relationships by identifying the things that deter friendship development and chosen parameters also support that views are as follows:

- ✓ Did the teacher spend time with the students outside the classroom and discussed the courses, topics and extra-curricular activities?
- ✓ Did the teacher spend extra time outside the classroom to improve their (students) study and make them resourceful?

Exam related discussion

For many students exams seem a necessary evil and time-consuming yet inevitable. Good assessment aim to provide a balanced, fair evaluation of each student. It can be achieved by using a variety of strategies and tasks. This gives students multiple opportunities, in varying contexts, to demonstrate what they know and can do. It also enables teachers to be confident in the accuracy of judgments about each student. The parameters adapted for exam related discussion are as follows:

- ✓ Did the teacher pick up the questions from the classroom teaching modules?
- ✓ Were the assignments helpful to self-study and creative thinking?

Statistical analysis and Results

Since its inception in Fall-2015, the FDE started the performance evaluation exercise of faculty members with the help of the students of all the departments. Big stride from yearly average of 60% in 2015 to 82% in 2019 crystallizes the university authorities' relentless effort to set the bar higher regarding pedagogy and knowledge transfer. Some of the crucial departments namely Textile Engineering, Civil Engineering, CSE and EEE experienced eye-staggering improvements during this time period. Even faculty members of newly established IPE department did remarkably well. In the beginning of the assessment procedure, a few departments struggled a bit to secure handy percentage but over the years they have been tremendously successful to solidify a strong position. Additionally, the pure science departments such as Chemistry, Physics, and Mathematics—which do not enroll students or offer programs by themselves—quite interestingly stood out among major departments since their initiations and occasionally bagged solid score of upper eighties on average which reasonably indicates these departments' proper management, sincerity and devotion towards students.

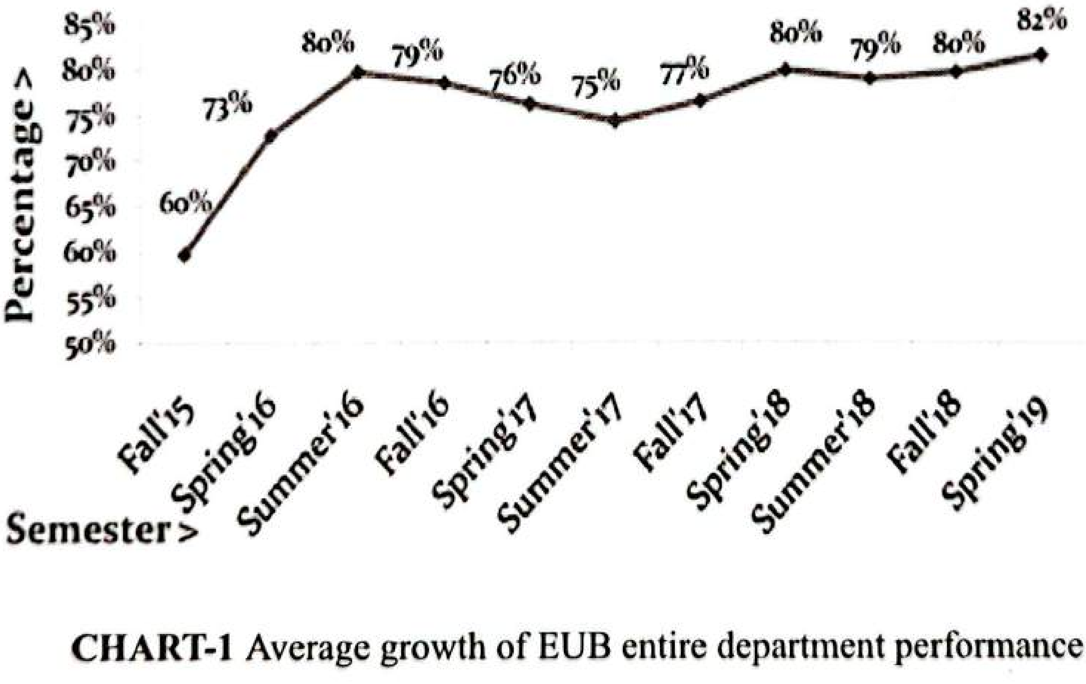
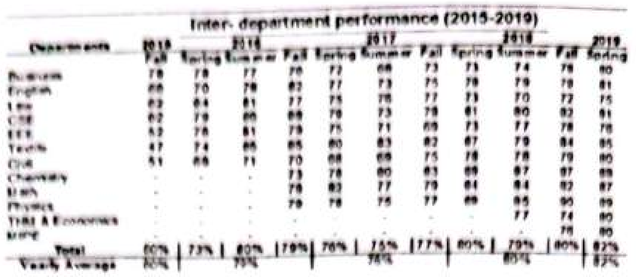


CHART-1 Average growth of EUB entire department performance



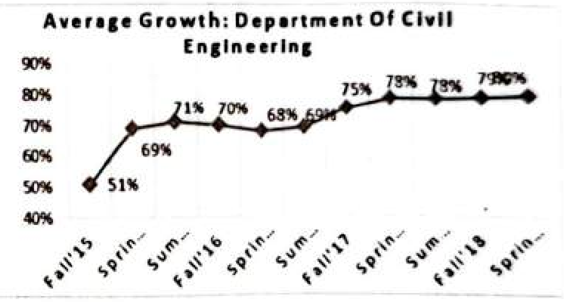
Inter- department performance (2015-2019)

Departments	2015	2016			2017			2018			2019
	Fall	Spring	Summer	Fall	Spring	Summer	Fall	Spring	Summer	Fall	Spring
Business	78	78	77	78	72	68	73	73	74	78	80
English	68	70	78	82	77	73	75	78	79	78	81
Law	82	84	81	77	75	78	77	73	70	72	75
CSE	62	79	80	88	78	73	78	81	80	82	81
EEE	52	76	81	79	75	71	69	73	77	78	76
Textile	47	74	80	85	80	83	82	87	79	84	85
Civil	51	69	71	70	68	69	75	78	78	79	80
Chemistry	-	-	-	73	78	80	83	88	87	87	88
Math	-	-	-	78	83	77	79	84	84	82	87
Physics	-	-	-	79	78	75	77	88	85	85	90
THM & Economics	-	-	-	-	-	-	-	-	77	74	85
[illegible]	-	-	-	-	-	-	-	-	-	75	85
Total	60%	73%	80%	79%	76%	75%	77%	80%	79%	80%	82%
Yearly Average	60%		75%			78%			80%		82%

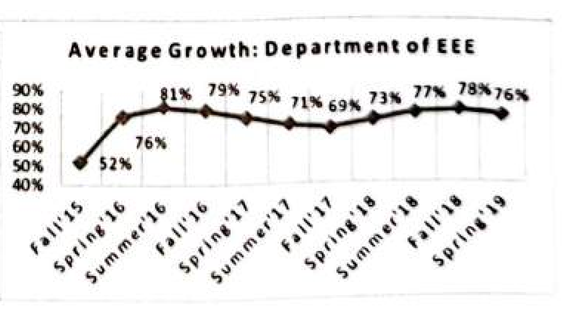
Department-wise Performance Evaluation: Fall 2015-Spring2019

On the other hand, Faculty members of social science leaning departments such as Business Administration, English, Law, THM and another newly established department Economics are solidly consistent in terms of their performance amid the fact that larger portion of regular students of the university belongs to these departments and historically been more rigorous in terms of providing lofty feedbacks. Aftermath of some radical initiatives such as launching modular-based system with intensive course loads, stern measure to reduce absenteeism, zero tolerance against unfair means in exam and strict marking in continuous assessment badly impacted performance evaluation of faculty members across departments at times. However, slowly but surely, students understood their wellbeing and at the same time faculty members adapted with the emerging developments quite successfully. Data on the Average Growth of EUB as appended in Chart-I, reveal that faculty members of Textile Engineering department, though bounced back in later semesters, scored the lowest percentage of forty seven in Fall-15 and Physics department holds the top percentage of ninety in Spring-19, and notably faculty members in Department of Chemistry and Mathematics alongside Physics are the most regular in their effort towards effective teaching and knowledge sharing.

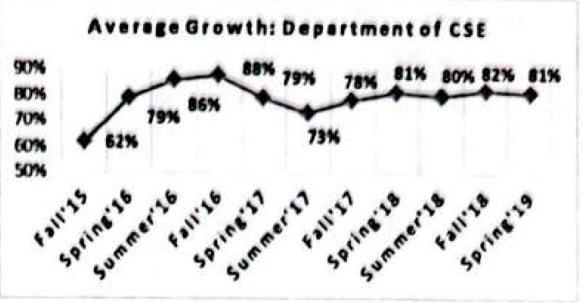
Department of Civil Engineering: Civil Engineering department, university's largest department in terms of faculty members and student volume, leapfrogged from 51% (Fall-15) to 80% (Spring-19) by hovering around 70% and so most of the times in last three and half years, which justifiably demonstrates the flagship department's continuous endeavor to push its benchmark higher.



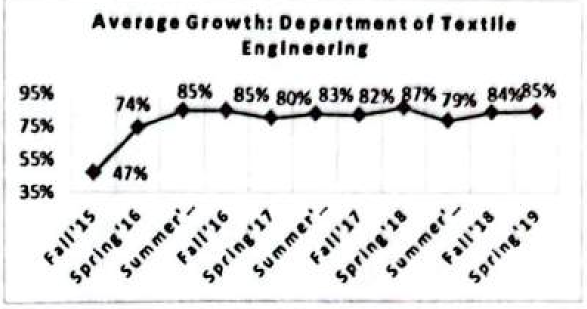
Department of Electrical and Electronic Engineering (EEE): Faculty members of the second largest department of the university EEE—though could not exceed the cutoff percentage of eighty except one in last eleven semesters—consistently performed around 75% on average and very much likely to reach the desired threshold very soon as recent steady performance indicates so.



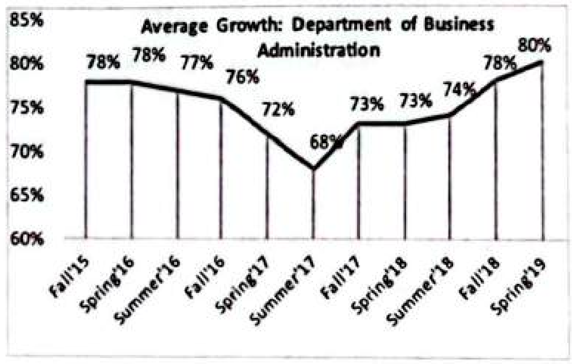
Department of Computer Science and Engineering (CSE): Faculty members of CSE department, the most prolific department of the university with regards to growth in recent times, scored 80% or above for six times in last eleven semesters and scored around upper seventies multiple times which warrants its consistency and robust performance over last couple of years.



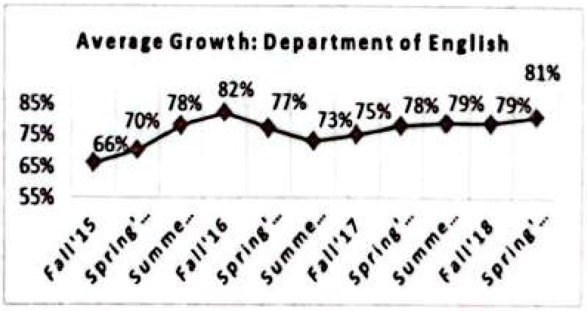
Department of Textile Engineering: On average faculty members of Textile Engineering department maintained their outstanding progress and grossly scored the desired cutoff percentage of eighty for eight times in last eleven semesters. Startling progress from 47% in Fall-15 to 85% in Spring-19, demonstrates its faculty members' girt for top-notch performance.



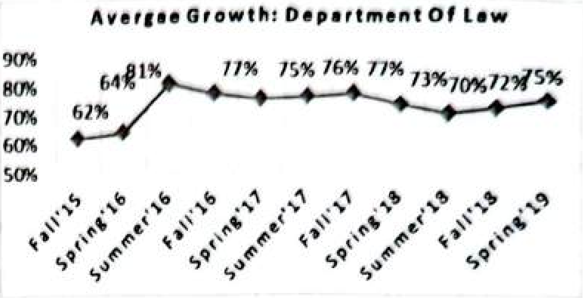
Department of Business Administration: Faculty members of Business Administration department, university's most trailblazing department with regard to introducing new rules and regulations to enhance student's capacity building, scored highest (78%) among all the departments during the introductory phase of the evaluation system in Fall-15, and with a rock solid consistency of around upper seventies on average. During the last couple of years this department finally hit the cutoff percentage of eighty in Spring-2019.



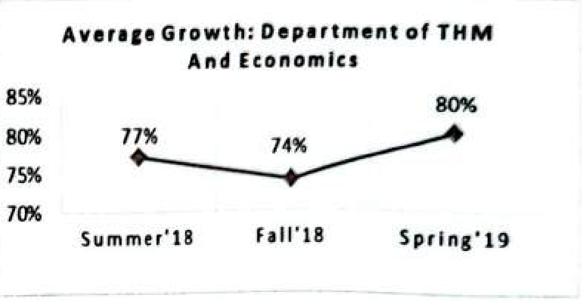
Department of English: In Department of English faculty members exceeded cutoff percentage of eighty twice in Fall-16 and Spring-19. Other than that most of the time teachers in this department performed around upper eighties on average with the exception of 66% in Fall-15, the very first semester when evaluation procedure officially kicked-off.



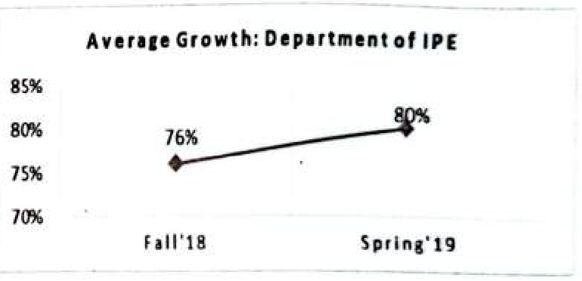
Department of Law: Faculty members in Department of Law scored around mid-seventies in last eight semesters with the exception of 81% in Summer-16. Though the performance was well below the cutoff percentage in the early days of performance evaluation, faculty members of this department are demonstrating steady progress in recent times.



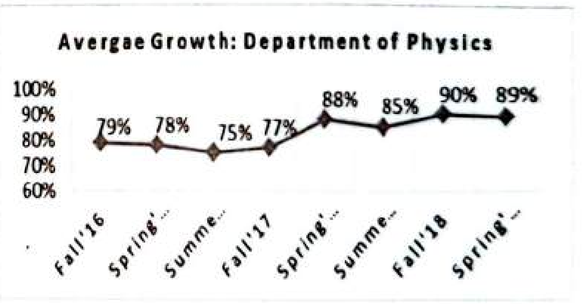
Department of THM and Economics: The combined archival data of recently merged THM (Tourism and Hospitality Management) and Economics department show that faculty members scored cutoff percentage of eighty in Spring-19 and balanced percentage of seventy seven in Summer-18, however experienced a slight dip at 74% in Fall-18.



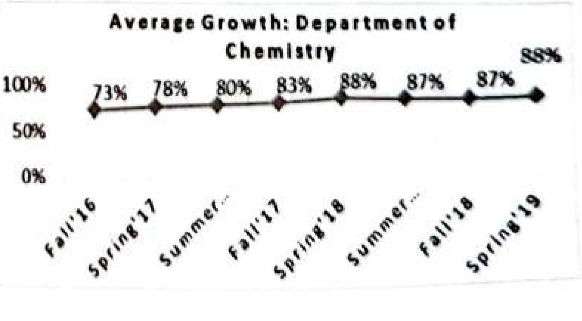
Department of Industrial Production Engineering (IPE): Faculty members of the newly opened, comparatively fledgling engineering department of the university IPE has demonstrated promising start as they scored 76% in Fall-18 and a desired cutoff percentage of eighty in Spring-19.



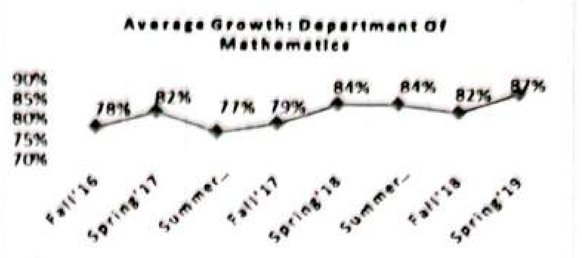
Department of Physics: From Fall-16 to Fall-17, faculty members of Physics department scored around upper seventies, and from that semester onwards they did tremendously good by achieving around upper eighties in last four consecutive semesters. Undoubtedly this great feat is exemplary for others.



Department of Chemistry: Some of the well-performed faculty members are from Department of Chemistry. Since their inclusion in FDE data bank they are the most consistent department among all others. From 73% in Fall-16 to 88% in Spring-19, faculty members of this department progressively attained some top-tier scores in between Spring-17 to Fall-18.



Department of Mathematics: Another consistent department which is regularly performing well in terms of top evaluation score is Mathematics. In last eight semesters, faculty members of this department exceeded cutoff percentage five times and scored upper seventies in rest of the three semesters.



Mean Absolute Deviation (MAD) Calculation: During the study of pre TAT and post TAT it has been observed that mean absolute deviation (MAD) of pre and post TAT has a remarkable positive impact on each of the department, where in study we calculated based on pre-determined mean standard 60 percent. Transactional Analysis Training (TAT) was conducted for the faculty members of different departments selected based on their previous semester assessment, those who have scored average below or equal to 60 percent in semester evaluation. Faculty Development and Evaluation Section conducted two Transactional Analysis Training (TAT) in two different year and from TAT we have taken sample **n = 46** for 2016 and **n = 26** for 2018 for MAD calculation.

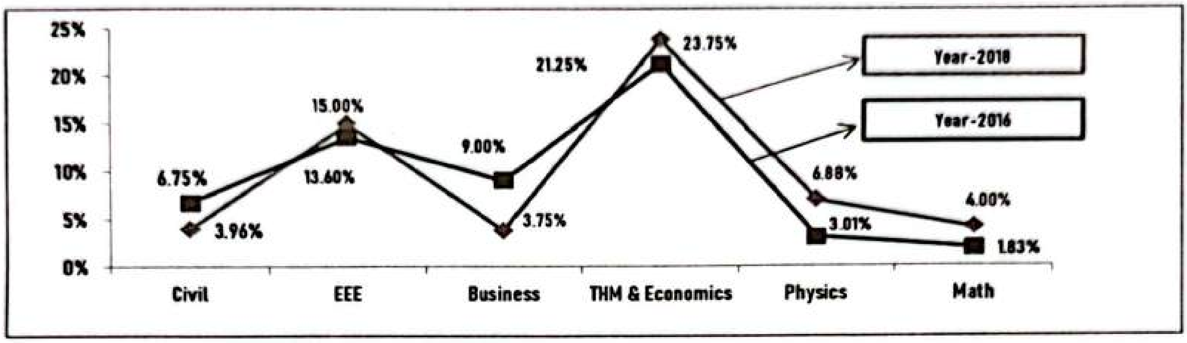


CHART: 2. Difference of pre and post Mean Absolute Deviation **(MAD)** in two different years.

As of the **(Chart -2)** above depicts the difference of mean absolute deviation (MAD) where we have shown the difference of the MAD from post TAT and pre TAT pattern of year 2016 and 2018 in separated ways. It has been found that Civil Engineering department of EUB, larger number of faculty members of civil department were participated in each period and trained based on the performance evaluation criteria, with a resulted mean difference (post-pre) positive 3.90% in 2016 and 6.75% in 2018 .Where Electrical Engineering department mean difference found 13.60% in 2016 and 15% in 2018. It has been perceived that thè both number of faculty members and students augmented in almost all departments of EUB from 2016 to 2018 in a considerable rate due to increased facilities, well qualified faculty members and the advanced, eco-friendly and attractive new campus enhanced the university spirit, created a healthy and positive environment for the students. Joint department like Tourism and Hospitality Management and Economics both shows a worthwhile trend of 23.75% in 2018 where it was 21.75% in 2016 which are comparatively higher than the mean absolute deviation of other departments. In case of basic science department like faculty member of Physics and Mathematics, the significant positive change in their performance after TAT training.

$$MAD = \frac{\sum_{i=1}^{n} | xi - \bar{x} |}{n}$$

xi : Performance Value for Period i

$\bar{x}$: Average Value

n : Number of Data

Equation: Mean Absolute Deviation (MAD)

In the teaching sessions during pre-midterm, it's essential for every faculty member to collect the modules and make it available in the classes and make it understandable to students. All the faculty members gone through this generalized process and make them flexible according to the academic demand of different departments allocated over two clusters. Pre-final assessments provide constructive feedbacks from students that help teachers of all departments to discover whether their performances have had positive effect on classroom or not and make them aware about improvement of their quality of teaching. Sharing these insights with new or struggling faculty members enable them to know how best to support, mentor and promote instructions when it comes to overall teaching effectiveness.

Challenges and Issues

This study identified the following conflicting aspects in existing evaluation mechanism which are hindering the efforts to discover the actual picture of faculty evaluation and development:

1. It has been observed that *new and adjunct faculty members* of various departments noticeably struggle to secure a handy evaluation percentage. This study by taking consideration the historical data from FDE achieves found that even in spite of their adequate experience and good academic credentials, they often face unfavorable welcome by the students across departments. Inadequate mutual understanding between teachers and students and often result into inadaptability of teachers to adjust with new academic environment inefficient transfer of knowledge, expectation mismatch of the relevant stakeholders. All these often lead to poor ratings of the new and adjunct faculty members' assessment score. In this case proper orientation with each faculty members and students could be a possible solution.
2. In case of *full-time faculty members,* though large portion of them are consistently doing good, but some are continuously scoring dismal figures. Complacency of the teachers, unwillingness to make teaching materials interesting, exploitation of work place loopholes and overall insufficient devotion make things challenging for poor performer in transferring knowledge effectively, hence gradually inclining towards uninspiring performance. At times, administrative affairs apart from regular teaching and consequentially disruptive attention to deliver knowledge effectively reduced evaluation performance which is not often clearly reflected in existing evaluation.
3. Some of the irregular students, especially of evening batches, who have very little participation in classroom activities due to job or other commitments, do not justifi ably qualify to assess a particular faculty member properly. However, they are doing so semester after semester unabatedly. Their evaluations irrespective of outcomes often blur the actual performance of a teacher. Furthermore, random marking of irregular students in evaluation forms which often create unusual zigzag, devoid of any significant statistical meaning time and again may eject a teacher in troubled water.

4. Some *insignificant* but categorically influential and statistically significant issues are personality clashes between students and young teachers, perceiving tenderness of female teachers as their vulnerability, being revengeful for pervious poor grade, and last but not the least syndicating to depreciate a particular teacher through deliberate ly assessing negatively. However, such issues are trivial and they are not significant enough to adversely affect the important findings of the evaluation exercise.

Policy Recommendation

European University of Bangladesh attach great importance to effective teaching and support faculty members in exploring ways and means to improve their teaching efforts. This evaluation strategy showed that the faculty development program improved the teaching competencies of the participants. Both the programs, the students, assessments of their teachers and the independent ratings of the trainees showed post-program improvements and were positively inter-correlated. The use of these multiple measures is a viable approach to evaluate the impact of a faculty development program. Its' high time for integration of ICT facilities in every step from collecting data to analytical reporting which will give more feasible, valid, and reliable data evaluation but outliers, errors and biasedness in big issue in data collection process.

Feldman (1979) also reports that ratings are somewhat higher when the instructor being evaluated is *present* in the room while the evaluation forms are being completed. Ryan et al. (1980) reported in a research paper that level of course, class size, subject area, workload of courses and extracurricular activities of teacher has a strong reflection on evaluation result. A study by Cranton and Smith (1986) shed further light on the effect of course characteristics, such as course level and class size on student ratings. The authors found that in case of lager class size that has strong negative impacts in effective classroom management regardless of course characteristics and teachers experience as a result in this case teachers ratings varied drastically. In some departments the course characteristics don't have any significant effect on student ratings, while in some cases the effect was in the opposite direction to that predicted. However, a new teaching method for improvement, refinement and experimentation with new ideas and learning contemporary technologies can be applied to ensure better understanding towards diverse group of students.

Whether it identifies the areas of weaknesses or possible strengths required to keep noticing and improving by the respective faculty member in class. To create professional development it is required to ensure mutual collaboration having sound understanding of learning strategies. The Module based teaching system, one of the basic strategies used by EUB and many European Universities in contemporary times, should be updated at certain interval basis based on the effective classroom management, future challenges andconsidering the upcoming changes. Modular curriculum is obligatory to follow the modern and experimented theories, concepts and ideas. Sense of priority in the class room should be selective that justifies acceptance of alternative constructive thoughts, diverse ideas and new perceptions. The extensive usage of Information and Communication Technology (ICT) can create a knowledge based practices among the faculty members which provide access to collective teaching contents for professional development. Learning resources through open sources can broaden the area of practices could lead towards an integrated social practices.

Acknowledgement

We want to express our sincere gratitude to Prof Dr. Mokbul Ahmed Khan, honorable Vice Chancellor of EUB for his most precious time, expert opinions and support, also grateful to all members of Faculty Development and Evaluation Section (FDE) for their continuous support throughout all the phases of this study.

References

1. *Calderon, (1996) T. G., Gabbin, A. L. and Green, B. P. (1998) Report of the committee on promoting and evaluating effective teaching (Harrisonburg, VA, James Madison University Press).*
2. *Cashin, W. E. (1988) Student ratings of teaching: a summary of the research (IDEA Paper No. 20) (Manhatten, KS, Kansas State University, Centre for Faculty Evaluation and Development).*
3. *Centra, J. A. and Creech, F. R. (1976) The relationship between student teachers and course characteristics and student ratings of teacher effectiveness. Project Report 76-1 (Princeton, NJ, Educational Testing Service).*
4. *Centra, J. A. (1993) Reflective faculty evaluation (San Francisco, Jossey-Bass).*
5. *Data from Faculty Development and Evaluation Section (FDE) from period Fall-2015-Spring 2019.*
6. *Feldman, K. A. (1993) College students' views of male and female college teachers: Part II—Evidence from students' evaluations of their classroom teachers, Research in Higher Education, 34, pp. 151- 211.*
7. *Kronk, A. K. and Shipka, T. A. (1980) Evaluation of Faculty in Higher Education (Washington, DC, National Education Association).*
8. *Odden, Allan; .Borman, Geoffrey; Fermanich, Mark Assessing Teacher, Classroom, and School Effects, Including Fiscal Effects, Peabody Journal of Education, v79 n4 p4-32 Oct 2004.*
9. *Tomasco, A. T. (1980) Student perceptions of instructional and personality characteristics of faculty: a canonical analysis, Teaching of Psychology, 7, 79_82.*
10. *Zoller, U. (1992) Faculty teaching performance evaluation in higher science education: Issues and implications (a 'cross-cultural' case study), Science Education, 76, pp. 673-684.*

Appendix

1. *Teaching Performance Evaluation Form*

EUROPEAN UNIVERSITY OF BANGLADESH

Teaching Performance Evaluation Form

Faculty Development and Evaluation Section

Teacher's Name:..

Course Code: ....Course Title: ....

Evaluating Date : ....Semester..................................Section:..........Total Students in the Section: ....

Performance Key	Excellent A^+ (100 - 80)	Very Good A (79 - 70)	Good B^+ (69 - 60)	Satisfactory B (59 - 50)	Not Satisfactory C (49 - 0)
❖ **Organization of the Lesson**					
1. We were informed about the lesson before.	□	□	□	□	□
2. Lecture materials were well-organized and easy to understand.	□	□	□	□	□
3. Lecture started and ended on time.	□	□	□	□	□
4. Module helps me understand, learn and application of the lesson.	□	□	□	□	□
5. Class tests were taken regularly (2Pre-mid tests and2 Pre-final tests) followed by the lesson.	□	□	□	□	□
❖ **Interpretation of teaching materials**					
6. Description of Lecture and teacher's explanation helps understand the lesson.	□	□	□	□	□
7. Description and explanation of Lecture were relevant to the subject matter and lesson materials.	□	□	□	□	□
8. Class-room discussion inspired my creative thinking.	□	□	□	□	□
❖ **Presentation of teaching materials**					
9. Pronunciation and presentation of the teacher were clear.	□	□	□	□	□
10.Teaching Modules were brief but covered all the relevant issues	□	□	□	□	□
11.Use of the teaching aids, such as, White Board, Chart, Multimedia etc. have helped understand the lesson	□	□	□	□	□
❖ **Interpersonal discussion inside the classroom**					
12. The teacher has answered to the questions of the students directly and correctly.	□	□	□	□	□
13. Classroom discussion and group study helped us to understand the lesson.	□	□	□	□	□
❖ **Interpersonal discussion outside the classroom**					
14.The teacher used to spend time with the students outside the classroom and discussed the courses, topic etc	□	□	□	□	□
15. Extra time spent by the teacher outside the class room helped us improving my study and knowledge.	□	□	□	□	□
❖ **Exam Related Discussion**					
16. The teacher picked up the questions from the classroom teaching Modules	□	□	□	□	□
17.Assignments were helpful to self-study & creative thinking.	□	□	□	□	□

❖ **Comments:**

Thanks for Your Honesty.

Design and Implementation of a Steganographic Application using Dictionary for Providing the Confidentiality of Information

Biswas Kumar*
Ahmedul Kabir*
Md Abdullah Al Forhad**
Ahamad Ali**
Md. Obaidur Rahman***

Keywords: Steganography, encryption, decryption, security, AES, DES

Abstract: *Information security is the way toward shielding information from unapproved access or interlopers. In present-day correspondence, the two senders and beneficiaries impart by informing in their day by day life. Correspondence might be in office, Banking, enterprises, Government reason, etc. It is a consuming inquiry that this kind of correspondence, we performed with one another either secure or not. These days, aside from the military and institutional information security, singular information security is critical. On the off chance that singular security is overlooked, touchy information can be harmed by unapproved clients or interlopers which are unambiguous. To ensure delicate information nobody can prevent the job from claiming information security. Among various kinds of security, procedure Steganography is essential to ensure individual information. It is the craft of concealing a message inside another medium so that keeps the identification of shrouded messages. Steganography shrouds information and it keeps outsiders out from realizing that the proposed message is even there. Just the planned beneficiaries realize it is there and coherent to them as it were. This framework is anything but difficult to design and give individual correspondence security by encoding and unscrambling information. It is troublesome and practically difficult for interlopers to discover unique messages. This proposal improves the information security of people, enterprises, banking framework, Government reason and so forth.*

Introduction

Information is an advantage that has esteem like some other resources. As an advantage, information should be verified from assaults. Because of the benefits of ICT, a large portion of information is kept electronically. The security of information has turned into principal issues. Nowadays correspondence happens PC to PC, PC to Server, Server to PC and so on. To give security and ensure delicate information, Steganography is an imperative security system. It is the specialty of concealing a message inside another medium so that keeps the recognition of shrouded messages. We plan and build up a steganography application so unapproved people or programmers can't hack the genuine messages. The blameless looking media in which a unique message is covered up is called spread, bearer or compartment. That is, the documents won't excite doubt to anybody not explicitly searching for them. Steganography is the investigation of implanting and concealing messages in a medium called a cover text.

***Senior Lecturer, Department of Computer Science and Engineering, European University of Bangladesh, Dhaka.**

****Lecturer, Department of Computer Science and Engineering, European University of Bangladesh, Dhaka.**

*****Associate Professor and Chairman, Department of Computer Science and Engineering, European University of Bangladesh, Dhaka.**

Steganography is identified with cryptography and is just about as old. It was utilized by the Ancient Greeks to conceal information about troop developments by linking the information on somebody's head and afterwards giving the individual a chance to develop out their hair. Basically, steganography is as old as dirt. When the message is covered up in the spread, the subsequent item is known as a stego-object. The Carrier turns into a "Stego" or stego medium after it conceals information into itself.

In this day and age, Information hacking is expanding step by step. It might bank information or any touchy information. With the quick advancement and broad utilization of the Internet, the security of information transmission turns out to be progressively vital. On the off chance that it's impractical to secure touchy information, it might hurt/harm different enterprises or a country hugely.

The mind can't help thinking that by what is meant by conceivable is to ensure our touchy information or Information. By examining a few cryptography and steganography calculation for information encryption and unscrambling, endeavor to structure and build up a security calculation for encryption and decoding of delicate information. Moreover, the shrouded message could be transmitted powerfully, to guarantee mystery information inserted, transmission, continuous extraction, so that the difficulty of visually impaired recognition by aggressor's increments enormously, can be improved by securing of the undercover correspondence. Information Super Highway has turned into a typical expression now. Presently, it is the necessity of a typical man. Individuals are continually discussing the sharing of information through different correspondence media. In this way, the need for use and doors are likewise expanding with the time. The trademark required in this application is to be quick, simple and verified. A typical man is utilizing this kind of utilization all around normally and continually. Be that as it may, to keep them verified is the most astounding test for designers and heads and it turns out to be progressively intricate and troublesome with the time too. The security issue is being raised constantly. Anecdotes about programmers with pernicious goals entering PC frameworks are inexhaustible. Different instances of misrepresentation, hacking and taking of information are in news constantly. A few cases are vital to the point that they are influencing the ordinary life too. A typical man is endeavoring to turn out to be increasingly mindful and alert while utilizing their ATMs, Bank represents exchanging cash, in paying a bill through charge cards and at different more events. There is dependably risk of taking off their information.

This Research expects to give a classification of information by structuring Steganographic Application Using Dictionary which will provide security for both Sender and Receiver. Keep up security with the goal that interlopers can't recover the delicate information of a client or associations.

Background

Steganography

Steganography is the craft of concealing a message inside another medium so that keeps the identification of shrouded messages [1][2][3][4]. Steganography shrouds information. It keeps outsiders out from realizing that the planned message is even there. Just the planned beneficiaries realize it is there and clear to them as it were. There are some fundamental Terminology Related to Steganography, for example, Carrier, Container, and Cover Media or Unobtrusive media, Message, Embedded Object, Stego or Stego Object.

General Idea Behind Steganography

In steganography, the message "set up the bomb" hidden by covering it with another sentence to pass on the first.

Fig. 1 describes the general idea of steganography. Fig. 2. Describes stego object creation method.

The available diverse sorts of steganographic systems are:

1. Pure steganography
2. Public key steganography
3. Secret key steganography

Pure steganography: Pure steganography is the way toward installing the information into the item without utilizing any private keys. This sort of steganography completely relies on the mystery. This kind of steganography utilizes a spread picture in which information is to be inserted, individual information to be transmitted, and encryption unscrambling calculations to install the message into a picture.

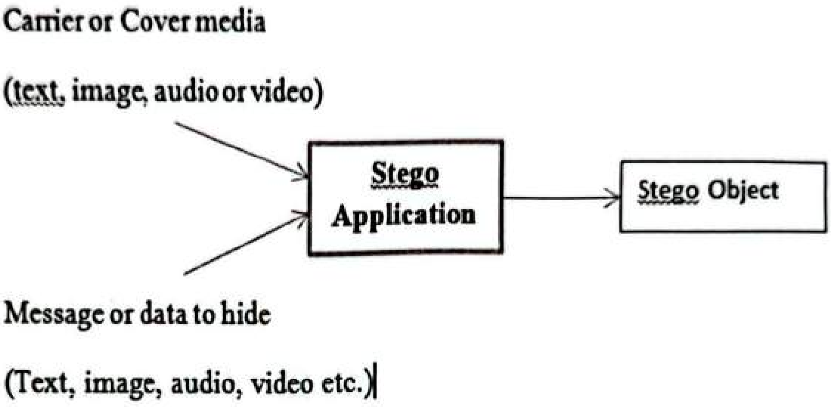


Fig. 1. The general idea of steganography.

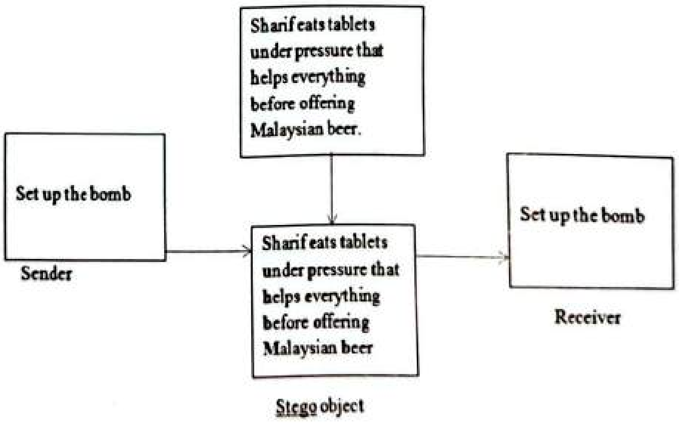

Sharif eats tablets under pressure that helps everything before offering Malaysian beer.
Set up the bomb
Sender
Sharif eats tablets under pressure that helps everything before offering Malaysian beer
Stego object
Set up the bomb
Receiver

Fig. 2. Stego object creation method.

This sort of steganography can't give better security since it is simple for separating the message if the unapproved individual knows the inserting technique. It has one favorable position that it diminishes the trouble in key sharing. Fig. 3. Describes Pure steganography process.

Secret key steganography: Secret key steganography is another procedure of steganography which utilizes a similar strategy other than utilizing secure keys. It utilizes the individual key for implanting the information into the item which is like the symmetric key. For decryption, it utilizes a similar key which is used for encryption.

This kind of steganography gives better security contrasted with unadulterated steganography. The primary issue of utilizing this sort of steganographic framework is sharing the secret key. In the event that the aggressor realizes the key, it will be simpler to decode and get to unique information. Fig. 4. Describes secret key steganography process.

Public key steganography: Public key steganography utilizes two sorts of keys: one for encryption and another for decryption. The key utilized for encryption is a private key and for decryption, it is an 'open key' and is put away in open databases. Fig. 5. Describes public key steganography process.

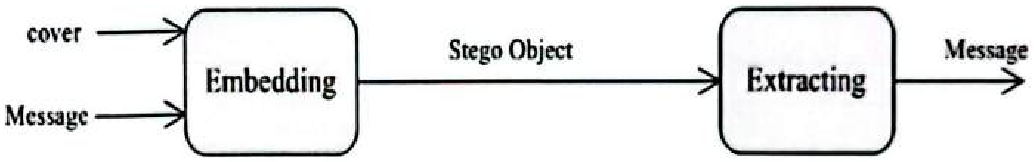


Fig. 3. Pure steganography process.

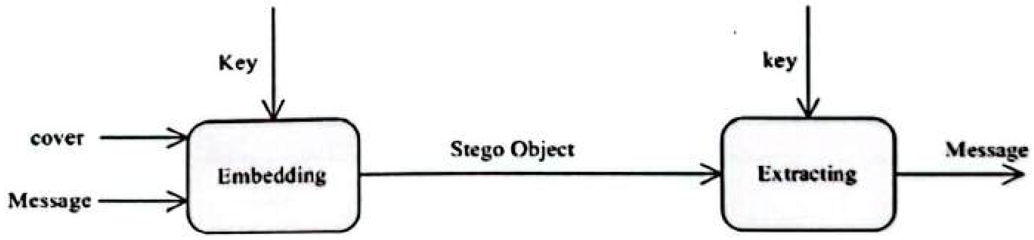


Fig. 4. Secret key steganography process.

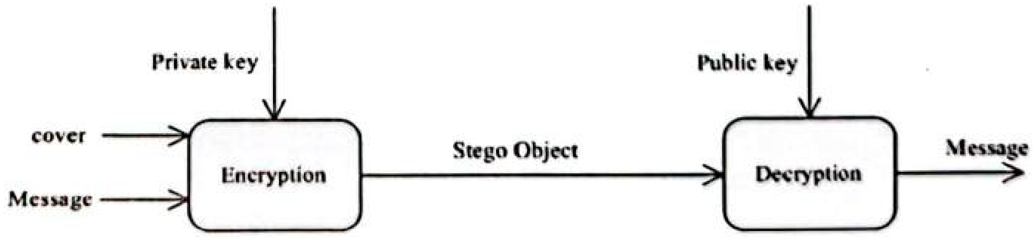


Fig. 5. Public key steganography process.

Implementation

There are a few steganographic precedents, for example, first Letter Steganography, second Letter Steganography, using diverse kinds of text styles, inserting parallel information utilizing open space Steganography, Open or additional room Steganography, Word moving Steganography, Ave Maria Steganography, Image Label Steganography, Audio Embedding Steganography, Image Embedding Steganography [5]. Among them, steganography utilizing word reference is a verified route for conveying the two senders and collectors. Along these lines, it is hard to discover the first messages for the gatecrashers. The word reference contains a few database tables for letter, thing, an action word, article and their comparing paired code [6]. The Dictionary should be accessible to senders and collectors and they consent to it. Fig. 6. Describes the proposed model.

Proposed Algorithm

a) Data Hiding:

Input: A message sequences {m1, m2, m3,.......,mn}

Output: Stego object sequences {s1, s2, s2,.....,sn}

1. Initialize the Dictionary with several database table.
2. Convert the message text into binary bit.
3. The binary bit can be divided into 16 bit chunks.
4. Follow the sentence pattern: article-noun-verb-article-noun
5. The first bit of Binary data can be represented by an article(for example 0 for a and 1 for the).
6. The next five bit can be represented by a noun.
7. The next four bit can be represented by a verb.
8. The bit can be represented by second article.
9. The last five bit can be represented by another noun.
10. Find a Stego object or a complete sentence.

Send the object/sentences to the receiver.

b) Data recovery:

Input: Stego object sequences {s1,s2,s2,.....,sn}

Output: A message sequences {m1, m2, m3,.......,mn}

1. Receive the stego object from sender.
2. Follow sentence pattern article-noun-verb-article-noun.
3. Convert this pattern into its corresponding binary bit.
4. Combine this bit into a single bit block.
5. Then divide the block into 8-bit order.
6. Select the letter of its corresponding bit which is stored in the dictionary.

Finally, we find the secret messages.

Table 1,2,3,4 describes the required table format in database. Fig. 6. Describes an example implementation of the proposed system. Where "hi" is the plain text and "a friend called the doctor" is encrypted text using proposed algorithm.

TABLE I. ARTICLE TABLE

Article Name	Binary code
a	0
an	0
the	1

TABLE II. NOUN TABLE

Noun Name	Binary code
friend	1001
doctor	1010
pen	1100
book	1101
computer	1110
....	....
phone	1111

TABLE III. VERB TABLE

Verb Name	Binary code
called	0001
eat	0010
sleep	0100
walk	1000
watch	1110
....	....
go	1010

TABLE IV. LETTER TABLE

Letter	ASCII code in binary value
H	01001000
I	01001001
A	01000001
B	01000010
....	....
R	01010010

Results and Discussion

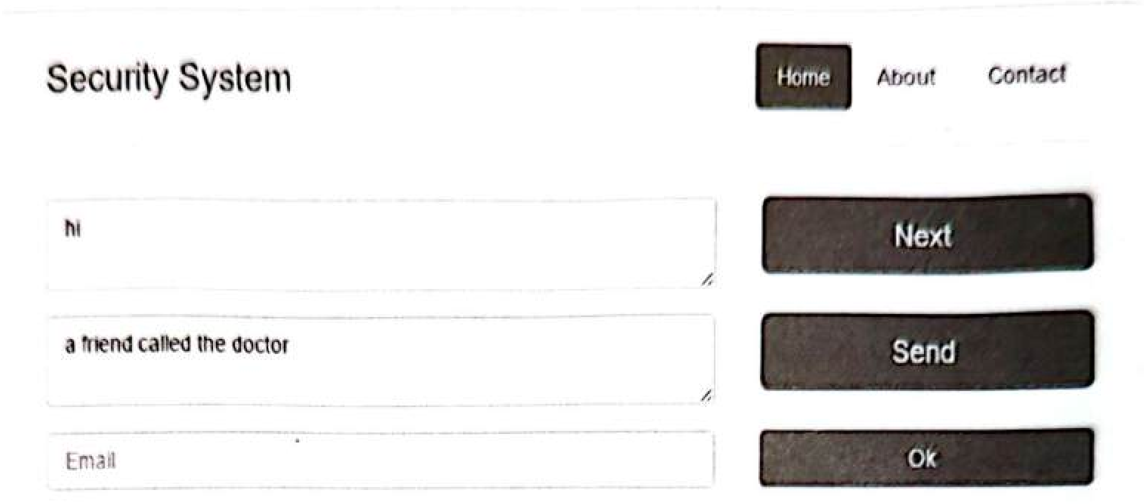
a) **Stego Object Creation:**

Original message: HI

Stego Object: a friend called a doctor

Sentences with the pattern: article-noun-verb-article-noun

- The first bit of binary data can be represented by an article (for example, 0 for 'a' and 1 for 'the').
- The next five bits can be represented by a noun (subject of the sentence).
- The next 4 bits can be represented by a verb.
- The next bit can be represented by the second article.
- The last five bits can be represented by another noun (object).



hi

a friend called the doctor

Email

Fig. 6. Proposed system example UI.

b) Comparative execution times (in seconds) of encryption algorithms:

Here various data encryption algorithm proposed algorithm, AES, DES, 3DES [7][8][9]. Fig. 7. Provides comparison of data load and execution time of various algorithms with proposed algorithm.

1st column contains Data input size in Byte and the next 4 column contains algorithms execution times. Table V shows that AES has minimum execution time and the second minimum execution time in proposed algorithm and relative increase [10].

Algorithm sequences based on their execution times:
AES< Proposed Algorithm < DES< 3DES

Algorithm Execution time: The following graph shows the Execution time of different types Encryption algorithm by loading data.

TABLE V. COMPARISON OF EXECUTION TIME

Input size Byte	Proposed Algorithm	AES	DES	3DES
0	0	0	0	0
10	0.008389	0.005381	0.008878	0.009541
20	0.016778	0.010624	0.017756	0.025482
30	0.025167	0.018143	0.026734	0.029223
40	0.033556	0.022524	0.035512	0.038964

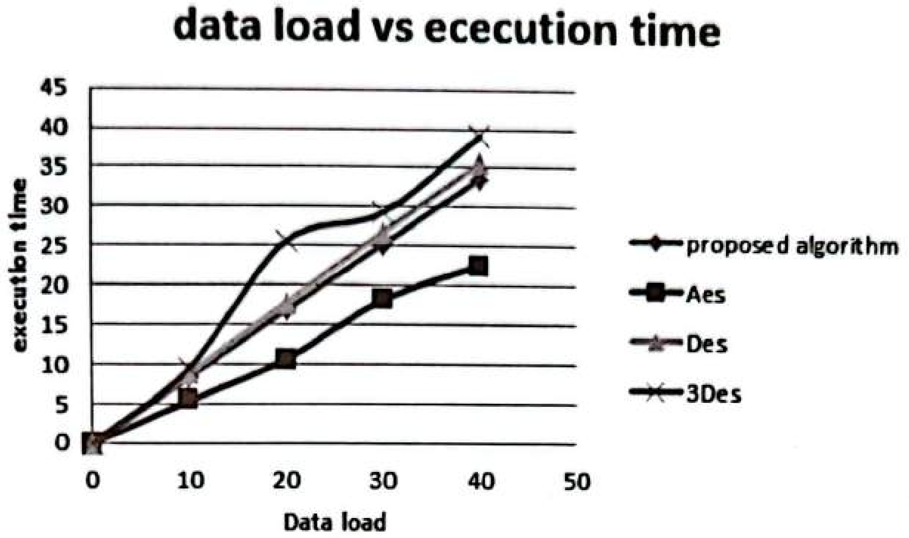


Fig. 7. Data load vs. execution time.

Conclusion and Future Works

Remote correspondences security is a region of significance to the media communications industry, where verification and information encryption are the real concerns. With the interest, remote interchanges likewise become a noteworthy wellspring of new vulnerabilities. Related security arrangements are being created to address new vulnerabilities. Remote correspondence shortcomings are on the expansion because of the development of cutting edge administrations, due to the need for legitimate confirmation, and the substantial sending of portable advances. This has created testing issues in the security of remote frameworks and applications working in remote situations. This proposition issue is to look for the improvement of new procedures, models and speculations that assist for a superior assurance of the portable and remote correspondence frameworks; evaluate and upgrade the dimension of security of the present remote correspondence frameworks, administrations and systems.

Our proposed algorithm is still slower compared to AES. So in near future we will try to improve our algorithm in respect to AES and also implement real time system with more accuracy.

References

1. M Baykara, R Das, "A steganography application for secure data communication", Electronics, Computer and Computation (2013) - ieeexplore.ieee.org.
2. Made SumarsanaAdi Putra, GelarBudiman, LedyaNovamizanti. Implementation of Steganography using LSB with Encrypted and Compressed Text using TEA-LZW on Android, 2014.
3. Abdinasir Hassan Ali, Maslin Masrom , Analysis and Implementation of Security Algorithms for Wireless Communications.
4. Johnson, N. F., Duric Z. veJajodia S., 2001. Information Hiding: Steganography and Watermarking - Attacks and Countermeasures, Boston.
5. Reddy, H.S.M.; Sathisha, N.; Kumari, A.; Raja, K.B., "Secure steganography using hybrid domain technique," Computing Communication and Networking Technologies (ICCCNT), 2012 Third International Conference on , vol., no., pp.1,11, 26-28 July 2012.
6. Kumar, R.P.; Hemanth, V.; Shareef, M., "Securing Information Using Sterganoraphy," Circuits, Power and Computing Technologies (ICCPCT), International Conference on, vol., no., pp.1197,1200, 20-21 March 2013.
7. Mandal, Akash Kumar, Chandra Parakash, and ArchanaTiwari. "Performance evaluation of cryptographic algorithms: DES and AES." Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on.IEEE, 2012.
8. Sui, Xin-guang, HuiLuo, and Zhong-liang Zhu. "A steganalysis method based on the distribution of first letters of words." 2006 International Conference on Intelligent Information Hiding and Multimedia.IEEE, 2006.
9. Xin-guang, Sui, LuoHui, and Zhu Zhong-liang. "A Steganalysis Method Based on the Distribution of Characters." 2006 8th international Conference on Signal Processing.Vol. 4.IEEE, 2006.
10. Gaba, Jyoti, and Mukesh Kumar. "Implementation of steganography using CES technique." Image Information Processing (ICIIP), 2013 IEEE Second International Conference on. IEEE, 2013.

An Analysis of Chips on Hot Machining Method

Nabili Sobha Islam*

Keywords- Hot machining, Surface roughness, Hardness, Chip analysis, Machinability

Abstract: *Hot machining method consists, basically, in the heating of the work piece hundreds of degrees Celsius above room temperature with the aid of an external source of heat. Thus, the reduction of the shear stress of the material of the piece is gotten and, hence, is possible to obtain better surface finish in relation to the conventional machining. This review paper presents a survey on chip analysis of hot machining method.*

Introduction

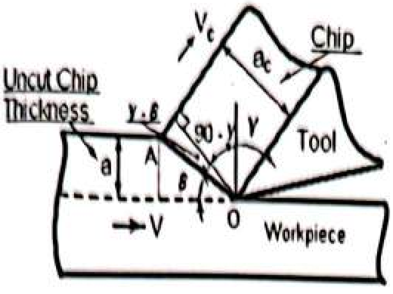
In machining process, instead of increasing the quality of the cutter materials, softening of the work piece is one of an alternate. In hot machining, a part or whole of the work piece is heated [5]. Heating is performed before or during machining [1]. Hot machining prevents cold working hardening by heating the piece below the recrystallization temperature and this reduces the resistance to cutting and consequently favors their composition and properties. From the past experiments it was found the power consumed during turning operations is primarily due to shearing of the material and plastic deformation of the metal removed. Since both the shear strength and hardness values of engineering materials decrease with temperature, it was thus postulated that an increase in work piece temperature would reduce chip reduction co efficient and increase machinability.

When force is applied by cutting tool against the work piece, the uncut layer deforms first elastically followed by plastic deformation due to the shearing action near the cutting edge of the tool. Shearing takes place along a shear zone and shear is of maximum at the shear plane [2]. After passing out of the shear plane, the deformed material slides along the tool face as chip as cutting progresses [Fig. 1]

Different types of chips of various shape, size, color etc. are produced by machining depending upon:

- type of cut., continuous (turning, boring etc.) or intermittent cut (milling)
- work material (brittle or ductile etc.)
- cutting tool geometry (rake, cutting angles etc.)
- Levels of the cutting velocity and feed (low, medium or high)
- cutting fluid (type of fluid and method of application)

***Lecturer, Department of Mechanical and Industrial Production Engineering, European University of Bangladesh, Dhaka.**



Notations:
a - thickness of the uncut chip
a_c - thickness of the chip
OA - the shear plane
β - shear angle
γ - rake angle
V - Cutting velocity
V_c - Velocity of chip movement

Fig 1: chip formation

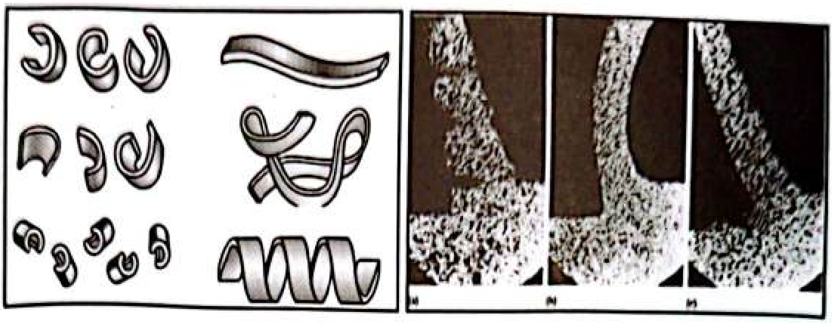


Fig. 2: various shapes of chips

The chip is enormously variable in shape and size in industrial machining operations. The formation of all types of chips involves a shearing of the work material in the region of a plane extending from the tool edge to the position where the upper surface of the chip leaves the work surface. A very large amount of strain takes place in this region in a very short interval of time, and not all metals and alloys can withstand this strain without fracture. Gray cast iron chips, for example, are always fragmented, and the chips of more ductile materials may be produced as segments, particularly at very low cutting speed [3]. This discontinuous chip is one of the principal classes of chip form, and has the practical advantage that it is easily cleared from the cutting area. Under a majority of cutting conditions, however, ductile metals and alloys do not fracture on the shear plane and a continuous chip is produced. Continuous chips may adopt many shapes - straight, tangled or with different types of helix. Often they have considerable strength, and control of chip shape is one of the problems confronting machinists and tool designers. Cutting parameters include tool materials, tool angles, edge geometries (which change due to wear, cutting speed, feed, and depth of cut), and the cutting environment (machine tool deflections, cutting fluids, and so on) [4]. Further complications result from the formation of the built-up edge on the cutting tool.

The chip formation and morphology are definitely affected by tool geometry and cutting parameters such as cutting speed (v), feed rate (s), and depth of cutting (a). An experiment investigation has been presented to study the influence of chip deformation in orthogonal cutting. Chip has been analysis by observing the color, shape and thickness of the chips. Generally, for thickness measurement following equation has been used [Fig 3].

Chip reduction co-efficient, K =t2 /t1 > 1
From the figure t2 =chip thickness

t1 = uncut chip thickness

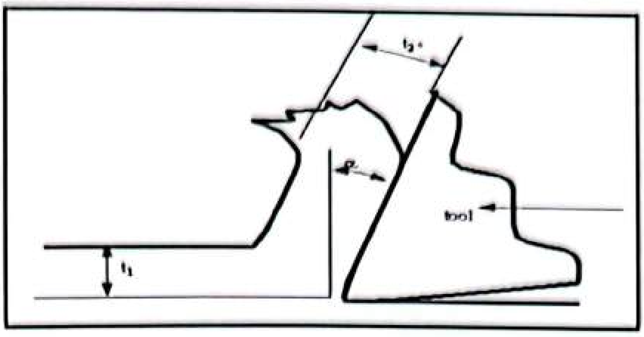


Fig. 3: chip formation

Experimental Condition

The experiment has been done at room temperature and with preheating the work piece of stainless steel in turning operation using the following parameters cutting speed, depth of cut, feed for the experimental work as follows:

Cutting speed, Vc= 75-115 m/min Feed rate, f = 0.1-0.14 mm/rev Depth of cut, dp= 1.5 mm Preheating temperature, ϴ= 3500C

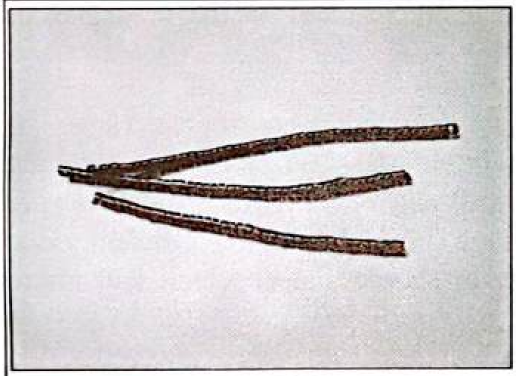
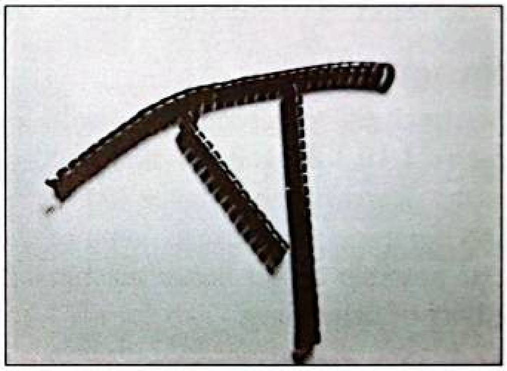
Room temperature condition	Preheated temperature condition
	
Cutting speed – 75 m/min Feed rate – 0.10 mm/rev Chip shape – Long tubular Chip color - Golden Chip reduction co-efficient – 1.67	Cutting speed – 75 m/min Feed rate – 0.10 mm/rev Chip shape – Long tubular Chip color – Burn blue Chip reduction co-efficient – 1.34

Fig 4: Chips reduction co- efficient in two different temperature

Result and Discussion

Using the following parameters, chip reduction co-efficient vs cutting speedgraph was plotted for different feed in two conditions [Fig 4]. Here it can be shown in the graph that chip reduction co-efficient is reduced in the pre-heating temperature than the normal temperature in different feed rate and cutting speed in Fig. 5 and Fig. 6.

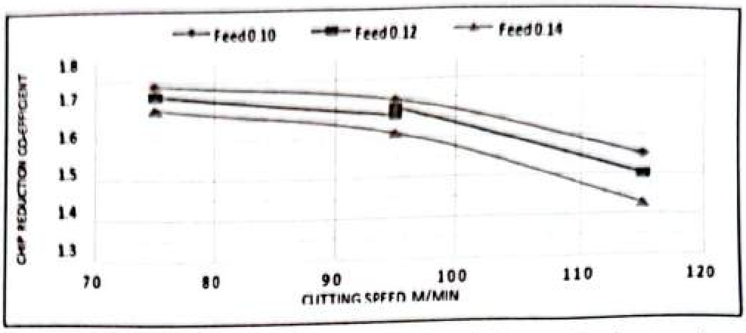


Fig 5: Chip reduction co-efficient vs cuttling speed for different feed rate (room temperature)

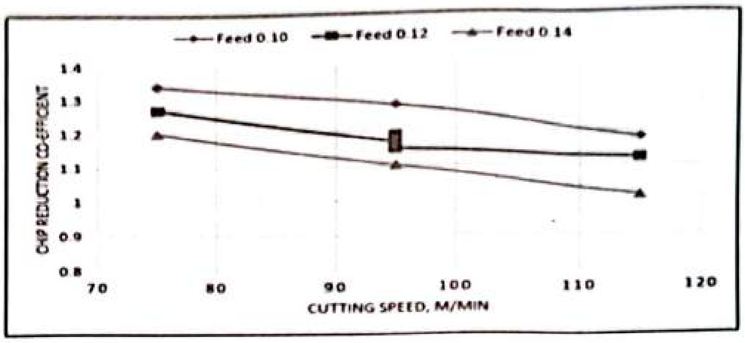


Fig. 6: Chip reduction co-efficient vs cutting speed for different feed rate (pre heating temperature)

Conclusion

The chip analysis represents the results of chip reduction co-efficient range for room temperature 1.10-1.67 and for preheated condition 1.01-1.34. With this reducing value denotes the decreasing of chatter (up to 58.18%) and better surface finish for preheated condition. So using the hot machining method the chip reduction co- efficient reduced and it will be possible to get better machinability of stainless steel which will improve the productivity of machining.

References

1. *M.Davami, M. Z. (2008). Investigation of Tool Temperature and Surface Quality in Hot Machining of Hard-to-Cut Materials. World Academy of Science, Engineering and Technology, 2(10), 672–676.*
2. *Mohamad, U. A. K. B., Nurul Amin, A. K. M., Arif, M. D., and Bin Abdul Muthalif, A. G. (2013). Influence of Magnetic Field on Chip Serration Frequency for Turning Stainless Steel AISI 304. Applied Mechanics and Materials, 394, 217–221.*
3. *Mohammad Ishtiyaq Hossain, A. K. M Nurul Amin. Comparison of Uncoated and Coated Carbide Inserts in End milling of Ti-6Al-4V in Terms of Surface Roughness.*
4. *Mia, M., Khan, M. A., and Dhar, N. R. (2017). Study of surface roughness and cutting forces using ANN, RSM, and ANOVA in turning of Ti-6Al-4V under cryogenic jets applied at flank and rake faces of coated WC tool. International Journal of Advanced Manufacturing Technology, pp. 1–17.*
5. *M.A. Lajis, A.K.M. Nurul Amin, A.N.M. Karim (2012). Surface Integrity in Hot Machining of AISI D2 Hardened Steel." Advanced Materials Research, Trans Tech Publications, 50, 40-50.*
6. *Madhavulu, G., and Ahmed, B. (1994). Hot Machining Process for improved metal removal rates in turning operations. Journal of Materials Processing Technology, 44(3–4), 199–206.*

Effect of Corporate Social Responsibilities (CSR) on Brand Image: A case study on ABA Group, Bangladesh

Iftay Khairul Alam*
Mushfeka Binte Kamal**
Nadim Ibn Sayed***

Keywords: CSR activities, Brand image, RMG, Philanthropic responsibilities, Ethical responsibilities.

Abstract: *Now-a-days, corporate social responsibility has become an important tool ofmarketing and plays an important role in establishing superior brand image in the competitive market. This article is focusing on analyzing the effect of corporate social responsibility activities on the brand image of ABA Group, Bangladesh which is leading company in the RMG sector of the country. Quantitative research strategy and survey research method have been followed here to complete the research. The researcher has used both the primary and secondary data to get an accurate research result. CSR activities (philanthropic responsibilities, ethical responsibilities, legal responsibilities and economic responsibilities) are the independent variables and brand image is counted as the dependent variable in this paper. CSR activities such as sponsorship, charity works, maintaining green environment, safer workplace without gender discrimination, employee facilities and etc. are performed by ABA Group which has brought a good brand image for the company in the international marketplace which leads to increase foreign buyers, helps the company to get many recognized awards and certificates In future, to make the brand image more superior, ABA Group can run educational institute, training center and hospitals in the local community to do the welfare of the local community.*

Introduction

CSR or Corporate Social Responsibility is currently an important issue in the new trend of business world. Corporate Social Responsibility implies acting, designing and performing business activities which will help the society, consumers and environmental issue of the country (Balmer, 2007). On the other hand, a brand image can be addressed as the perception of consumers for a brand which they hold in their mind (Keller, Apéria and Georgson, 2012). In RMG sector, corporate social responsibility performing companies create a soft corner in the mind of customers and buyers as those companies are doing well being to the customers as well to the societies. Corporate social responsibility activities create a good image of the companies in the market and thus perform the emotional branding on the consumers' minds. CSR is a strong marketing strategy which can be adopted by the companies to increase the brand image and value in the market (Gupta, 2013). For the above reason, the researcher is going to investigate the impact of CSR (corporate social responsibility) activities on the brand image of ABA Group, Bangladesh. ABA group is a readymade garments producer which was established in 1992 (Abagroupbd.com, 2019). Since then, it has been working to manufacture with responsibility

* **Lecturer, Department of Textile Engineering, European University of Bangladesh**
** **Senior Lecturer, Department of Business Administration, European University of.Bangladesh**

by ensuring the most dynamic interaction among human, machine and method and to leave the world a better place for the generation to come (Abagroupbd.com, 2019).

a) Research Objectives

The objectives of the research are given below:

- To analyse the corporate social responsibilities (CSR) practices of ABA Group, Bangladesh
- To discover the issues related to brand image of ABA Group, Bangladesh
- To scrutinize the effect of activities related to corporate social responsibilities (CSR) on brand image of ABA Group, Bangladesh
- To recommend some strategies regarding CSR practices for ABA Group, Bangla desh which will improve the company's brand image to the buyers of different countries.

Theoretical Framework

Independent Variables	Corporate social responsibility	Conducting different activities for the well-being of the society as well as developing the image of the organization towards the customers and society (Balmer, 2007).
	Philanthropic responsibilities	Subsidizing resources to the public as well as improving the standard of living of the society (Crane and Matten, 2007).
	Ethical responsibilities	Doing the right and fair things in the organization.
	Legal responsibilities	Doing business by maintaining the government's law.
	Economic responsibilities	Developing the country's economic condition through the business activities (Arvidsson, 2008).
Dependent Variable	Brand Image	The perception of consumers for a brand which they hold in their mind (Seo and Yang, 2015).

Figure: Theoretical Framework of the Research (Source: Own)

2. Literature Review

Company is a legal entity and that is why they have some responsibility towards the society. According to Crane and Matten, (2007) being responsible a business organization needs to conduct some wellbeing activities for the society and environment. It helps business organizations to develop a strong brand image among the customers. As per the research of Arvidsson and Peitersen (2008), by engaging in corporate social responsibilities this type of organizations try to conduct some ethical activities as well as social responsibilities to develop the society economy and environment around the business area and to the country. Conducting corporate social responsibilities, organizations also try to get acceptance among the customers by gaining their trust. Society as a whole is being served by different organizations as a part of their corporate social responsibility.

Different authors and researchers developed different types of Corporate Social Responsibility models and concepts but two corporate social responsibility ideas will be described below: Pyramid of Corporate Social Responsibility is developed by Carroll (2004) and it is one of the most renowned models for corporate social responsibility. It is one of the youngest models based on corporate social responsibility and it can help organizations to deal with different situations.

In his model Carroll partitioned corporate social responsibilities in the following parts:

- Economic region
- Legal region
- Ethical region
- Philanthropic region.

The first entity is the economic entity where it means to earn profit for the stakeholders and according to Carroll (1991, business organization itself is a profit earning entity for the society. The second one is the legal entity where Carroll (2004) said that business organization need to adhere with the laws and regulations set by the government for the sake of the society and environment as well as the people related with the business. Ethical entity is the third one of the pyramid and Carroll (2004) said that it is closely related with the legal entity, as business organization need to be ethical in its operations and a righteous practice is expected from them. Philanthropic entity referred by Carroll (2004) as a contribution to the society and the environment and serving them for their betterment.

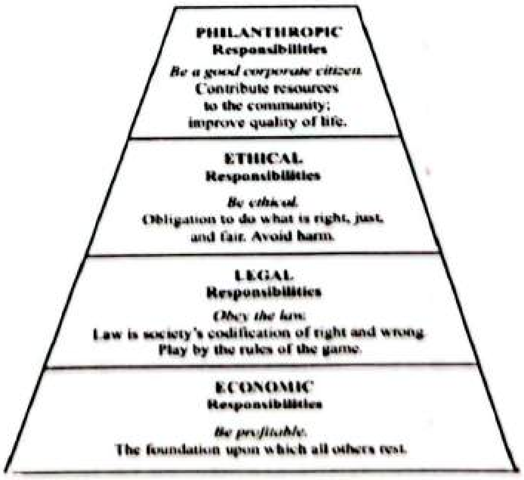


Figure: Carroll's Pyramid of Corporate Social Responsibilities (Carroll, 2004)

Claydon (2011) developed a new theory that connects customer's viewpoint and what they need from business organizations as their corporate social responsibilities. The model is called "Customer Driven Corporate Responsibilities" or CDCR.

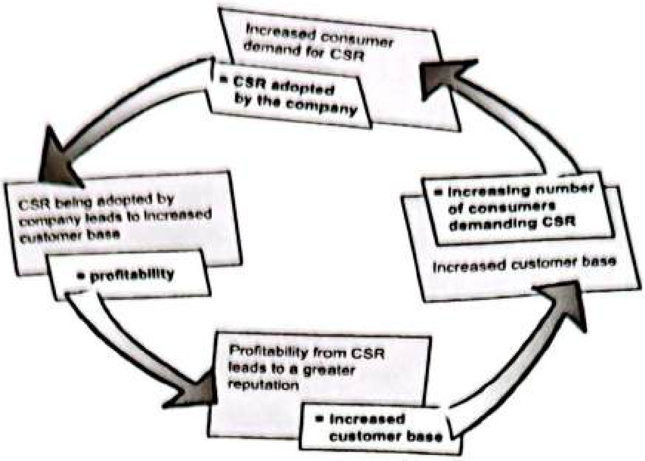

Increased consumer demand for CSR
■ CSR adopted by the company
CSR being adopted by company leads to increased customer base
■ profitability
Profitability from CSR leads to a greater reputation
■ Increased customer base
■ Increasing number of consumers demanding CSR
Increased customer base

Figure: Claydon's New Model of Consumer-Driven Corporate Responsibility (Carroll, 2004)

The figure below describes the connection between the two models described above and how they connect with CSR:

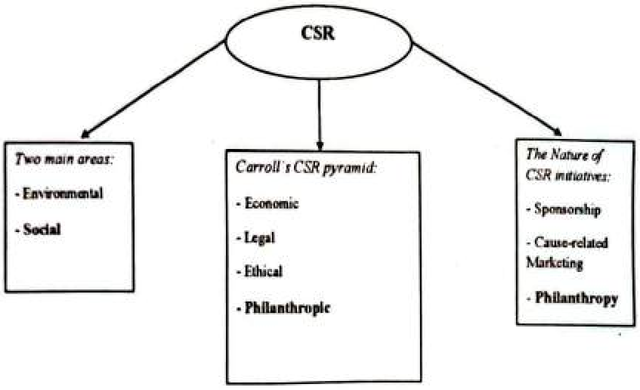


Figure: Area of Relevance concerning Corporate Social Responsibilities (Frederick, 2006)

The center point of these two models is the philanthropic activities and how business can use them to conduct CSR. Philanthropic activities also know as magnanimity and the motivation behind philanthropic activities is that a business organization is also social entity and it has to deliver its responsibilities to the society and its people. Craneand Matten (2007) said that the philanthropic activities are mainly responsible to increase a positive viewpoint among the customers.

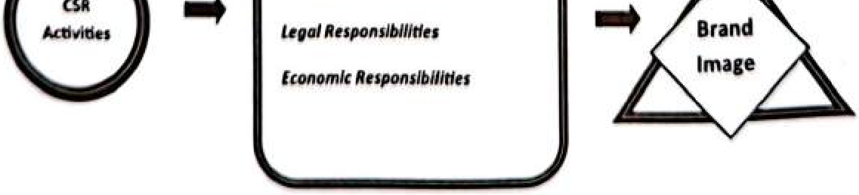


Figure: Conceptual Framework (Source: Own)

3. Research Methodology

The research has followed the quantitative research strategy because the researcher has collected numerical data through the questionnaire and analyzed the data statistically to generate the accurate result. Survey research method has been used here. Both primary data and secondary data have been collected to complete the research; primary data has been collected through a structured questionnaire of 5-point likert scale and secondary data has been collected from different published journals, newspaper article, company websites and etc. Probability sampling method has been used here; the samples are the employees of the ABA Group and the sample size is 100. The collected data has been analyzed by using SPSS and the results have been presented statistically through different table, graph andchart.

4. Result Analysis and Discussion

4.1 Correlation Analysis

The correlation analysis has been done here to determine the strong point of the relationship between the independent and dependent variables. In this research, philanthropic responsibilities, ethical responsibilities, legal responsibilities and economic responsibilities are the independent variables and brand image is the dependent variable. The table shows that a positive correlation exists among all the independent and dependent variables and the rate of this correlation between PR and ER is 0.94 wherever it is 0.0 between LR and 0.57 along with ECORES. Correlation between ER and LR is 0.0, with BI it is .90.The research result shows that all the independent and dependent variables are interrelated and positive correlation has been proved among them. As per the law of correlation matrix, some rate of correlations among the variables are moderate to strong because the rate is .5 to 1 and some rate of correlations among the variables are not strong because they stand below .5.

Correlations Matrix

	PR	ER	LR	ECORES	BI
PR	1.00				
ER	0.94	1.00			
LR	0.00	0.00	1.00		
ECORES	0.57	0.00	0.19	1.00	
BI	0.61	0.90	0.82	0.67	1.00

**. Correlation is significant at the 0.01 level (2-tailed).

Table: Correlation Analysis

4.2 Regression Analysis

In this research, Brand Image (BI) is measured as the dependent variable, the table shows the regression value is 0.846 then it indicates that those independent variables have an effect on the dependent variable by 84.6%. So the independent variables philanthropic, ethical, legal and economical- responsibilities have an effect on dependent variable brand image by 84.6%. It proves that independent variables have a strong influence over the dependent variable brand image of ABA Group.

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.910	0.858	0.846	0.737
a. Predictors: (Constant),PR,ER,LR,ECORES				

Table: Model Summary of Regression Analysis

The coefficient table shows the different effect above the dependent variable brand image (BI). Now the PR have beta of 0.92, ER 0.87, LR 0.30 also ECORES adapts a beta of 0.56. The research result shows that the most effect is put by philanthropic responsibilities and the lowest effect is put by economical responsibilities on the dependent variable brand image.

Coefficients						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
			Std. Error			
1	(Constant)	7.12	1.22		5.83	0.00
	PR	0.99	0.14	0.92	0.57	0.57
	ER	0.95	0.12	0.87	-1.23	0.22
	LR	0.44	0.10	0.30	-1.61	0.11
	ECORES	0.67	0.10	0.56	-1.80	0.07
a. Dependent Variable: BI						

Table: Coefficients of Regression Analysis

4.3 Discussion

CSR activities by ABA group actually facilitate the organization to a great extent in making altruism within the market among the competitors. The company sponsors local community programs and in the time of natural calamities helps the local community around the factory. ABA group donates a handsome amount of money for the educational expenditure of its employees' children. It additionally provides backing to the individuals relating to religious purpose like Hajj. Moreover, the company keeps up international standard for running its business and for supporting the environment. Environmental safety issues are the principle priority of ABA group. All the obligatory measures have been taken by the company to accomplish environmental safety. Energy savings has been ensured by ABA group up to 45% by optimizing power consumption and using renewable energy. Reduction of carbon footprint up to 45% is one of their notable achievements. Waste water management in industries of our country is still an issue to be settled but ABA group has taken some exemplary steps regarding this. They have ensured 100% reuse of waste water and their waste disposal to landfill is 0%. Projects pursuing LEED certification earn points across several categories: Location and Transportation, Sustainable Sites, Water Efficiency, Energy and Atmosphere, Materials and Resources, Indoor Environmental Quality, Innovation and more (GBIG, 2019). Based on the number of points achieved, a project then earns one of four LEED rating levels: Certified, Silver, Gold or Platinum. For ensuring safety and sustainable workplace most of their factories have achieved LEED certification notably they have achieved LEED platinum certification for the very first time in Bangladesh.

A total of 13 best green building factories of Bangladesh were honored with "LEED Green Factory Award" to recognize their efforts in sustainability by achieving LEED Platinum certification and ABA Group is the pioneer of them (Kalerkantho, 2019). These CSR activities or philanthropic responsibilities of CSR have created a positive brand image for the company in the international market of RMG and thus many international buyers get attracted towards the company as well as remain loyal to the ABA Group for next purchases.

ABA group maintain high standard of work environment ensuring worker's rights and benefits according to the local and international legislations. The company pays the employees regularly and accurately. They ensure 100% compliance which assures all the related benefits of all employees here and maintain legal responsibilities of CSR. Ethical responsibilities of CSR activities performed by ABA Group quite perfectly. ABA group maintain high ethical stand regarding work standard. Employees are ensured with high standard of work environment and safety. Management offers training to unskilled employees and arranges training related to their work safety. Dedicated team from compliance and HRM department promotes issues for the welfare of the employees (Abagroupbd.com, 2019). The activities regarding employees' welfare include safe workplace without gender discrimination, emergency leave on health issues, counseling for employees, maintaining standard work hour and handsome remuneration for overtime duties. They have arrangement of Medicare center, day care center for the children of employees, subsidized lunch benefits and so on (Abagroupbd.com, 2019). These practices of ABA group have increased the company's brand value and brand image among the competitors in the market and this work as a great marketing tool for the ABA Group. The company provides a green environment around the factory which helps the climate a lot. All the CSR activities maintained by ABA group have bring positive brand image in the market and spread the company name as a well maintained RMG manufacturer among the global market. So, the result and the discussion part have proved that corporate social responsibilities (CSR) have a positive effect on brand image of ABA Group, Bangladesh.

5. Conclusion

The aim of the research is to analyze the effect of activities related to corporate social responsibilities (CSR) on brand image of ABA Group, Bangladesh. Quantitative research strategy and survey research method have been followed here to complete the research. The researcher has used both the primary data and secondary data to get an accurate research result. Structured questionnaire was used here to collect data. In this research, philanthropic responsibilities, ethical responsibilities, legal responsibilities and economic responsibilities are the independent variables and brand image is the dependent variable. ABA Group perform different kinds of CSR activities such as sponsorship, charity works, maintaining green environment, safer workplace without gender discrimination, employee facilities and etc. These activities have bring a good brand image for the company in the international marketplace which leads to increase foreign buyers, helps the company to get many recognized awards and certificates and spreads a strong fame about the company among the RMG industry of Bangladesh. To make the brand image more superior, ABA Group can run educational institute, training center and hospitals in the local community to do the welfare of the local community.

6. Recommendation

Though ABA group performs a ton of CSR activities, however following recommendations can be given to perk up the CSR strategy which will bring more brand value and a strong brand image for the company. The recommendations are:

- ABA Group have many sister concerns. The company may take the initiatives to turn all the concerns into green factory in order to help the global climate.
- The company can open hospitals and clinics in the different local community to help its employees and their family.
- Educational institutes can be run by the ABA Group for the offspring of the workers'
- The company can open training institute concerning RMG for the youth generation which will be run by the top management of the company.
- ABA Group can sponsor country's national sports programs so that the company will be recognized both in national and international market.

References

1. *Abagroupbd.com. (2019). ABA Group – Manufacturing with Responsibility. [online] Available at: http://abagroupbd.com/ [Accessed 25 Apr. 2019].*
2. *Arvidsson, A., Bauwens, M., and Peitersen, N. (2008). The crisis of value and the ethical economy. Journal of Futures Studies, 12(4), 9–20.*
3. *Balmer, J., Fukukawa, K. and Gray, E. (2007). The Nature and Management of Ethical Corporate Identity: A Commentary on Corporate Identity, Corporate Social Responsibility and Ethics. Journal of Business Ethics, 76(1), pp.7-15.*
4. *Crane, A. and Matten, D. (2007). Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization. Oxford: Oxford University Press.*
5. *Carroll, A.B. (2004). Managing ethically with global stakeholders: A present and future challenge. Academy of Management Executive, 18(2), 114–120.*
6. *Carroll, D. (1991). The pyramid of corporate social responsibility: Toward the moral management of organisational stakeholders. Business Horizons, 34(4), 39–48.*
7. *Claydon, J. (2011). A new direction for CSR: the shortcomings of previous CSR models and the rationale for a new model. Social Responsibility Journal, 7(3), 405–420.*
8. *Database.dife.gov.bd. (2019). [online] Available at: http://database.dife.gov.bd/index.php/factories/details/4/3643 [Accessed 25 Apr. 2019].*
9. *GBIG. (2019). VINTAGE DENIM STUDIO LTD Dashboard :: Green Building Information Gateway. [online] Available at: http://www.gbig.org/activities/leed-*
10. *1000006026/dashboard?fbclid=IwAR3_y1Yevj78GINlcdrq0yj0qq4fvx1-JbYm1P9KkGbBF1RI3jeyvPw7wACM [Accessed 25 Apr. 2019].*
11. *Gupta, G. and Kaur, S. (2013). Sustainable Development - Through Corporate Social Responsibility (CSR) in Times of Economic Slowdown. Sidd. - A Jrnl. Deci. Mak., 13(3), p.203.*
12. *Frederick, W. C. (2006). Corporation, be good! Indianapolis: Dog Ear Publishing.*
13. *Kalerkantho. (2019).* বিশ্বসেরা২পোশাককারখানা।কালেরকণ্ঠ *[online] Available at: 1RqG8Kxc6TuMhNR37xN89Z1wFO6p4k1abwwq-C0SIAZjpzL-ztM#sthash.mkxaE0BN.dpuf [Accessed 25 Apr. 2019].*
14. *Keller, K., Apéria, T. and Georgson, M. (2012). Strategic brand management. Harlow, England: New York*
15. *Seo, H. and Yang, J. (2015). Influences of the Fit between the Corporate Brand Image and Corporate Social Responsibility(CSR) on Brand Attitudes: Focuses on Consumers' Donation Tendencies and CSR Massage Framing. The Korean Journal of Advertising, 26(7), pp.99-121.*

An Automated Pest Detection System utilizing Histogram of Oriented Gradients with a Mobile Application.

Ahmedul Kabir*
Biswas Kumar*
Md Abdullah Al Forhad**
Ahamad Ali**
Md. Obaidur Rahman***

Keywords—image processing, pest detection, HOG

Abstract: *Rice is the world's most imperative sustenance and an essential nourishment source for in excess of 33% of the total populace. This harvest is staple nourishment for Bangladeshis and served in each supper of the day so it is essential to sustenance security. Rice may lose its amount and quality when rice is assaulted by a various pest. Thusly, it is a top need to discover viable techniques to decrease the dimension of their invasion in the paddy fields. In agribusiness, pest control has dependably been considered as the most difficult errand for ranchers. The expanding request of these yields pulled in the consideration of various researchers and specialists to discover successful techniques and improve crop assurance procedures. We break down and order the pest control component in innovative and coordinated arrangements. At that point, we think about the pest control systems are dependent on their adequacy and other execution parameters. The mechanized pest distinguishing proof framework will begin with photographs utilizing android versatile applications. Catch photographs will be sent to the server utilizing pesticide applications. For Pest database, we utilized 10 pests from Bangladesh Agricultural University and irritation site. At that point, we build up a model. This model will distinguish the bug by applying different image processing methods. At image-processing segment histogram of oriented gradients (HOG) feature extraction technique is utilized. Accuracy is calculated for HOG feature extraction. Lastly, useful pesticide information will be sent to the user mobile.*

Introduction

Paddy stands out as the most used nourishment plants and is broadly grown in ASIA. Paddy is an imperative harvest worldwide and over a portion of the total populace depends on it for nourishment. With the developing populace everywhere throughout the world, the interest in nourishment thing like rice is expanding like never before. The ecological impacts (for example soil, climate) on the development of paddy have a noteworthy commitment to the creation rate of rice everywhere throughout the world. In any case, the following real impact on expanding creation is the compelling administration of paddy illnesses and pests. Ranchers lose an expected normal of 37% of their rice harvest to pests and illnesses consistently [1]. It is vital that the ranchers get the opportunity to recognize the state of their paddy well early before it is past the point of no return, so as to keep away from any benevolent debacle that can be brought about by the sicknesses. Exact finding and auspicious explaining of paddy illness is along these lines an indispensable part of rice generation the executives going for improved profitability

***Senior Lecturer, Department of Computer Science and Engineering, European University of Bangladesh, Dhaka, Bangladesh.**

****Lecturer, Department of Computer Science and Engineering, European University of Bangladesh, Dhaka, Bangladesh.**

*****Associate Professor and Chairman, Department of Computer Science and Engineering, European University of Bangladesh, Dhaka, Bangladesh.**

prompting expanded benefits. The majority of the ranchers utilized the customary pest the board strategies which is the ordinary shower program dependent on calendars as opposed to the nearness of insect pests on the paddy fields. These synthetic concoctions murder valuable creepy crawlies which destroy pests in harvests.

To adapt to these issues, a mechanized pest distinguishing proof framework is basic as it demonstrated helpful in observing substantial fields of yields, and along these lines consequently recognizes the nearness of pests when they show up in paddy fields. Therefore, looking for a fast, automatic and accurate method to identify insect pests in the paddy field is of great realistic significance. Early discovery will assist ranchers with avoiding tremendous misfortune. Innovation backing would help them in this viewpoint by cutting on the expense of pesticides. A strong demand now exists in many countries for non -chemical control methods for pests or diseases. However, no automatic methods are available which precisely and periodically detect the pests on plants. Truth be told, underway conditions, nursery staff intermittently watches plants and look for pests. This manual strategy is tedious. With the ongoing progression in picture handling design acknowledgement methods, it is conceivable to build up a self-governing framework for illness order of harvests. In this paper, we focus on early pest detection.

Background

Paddy Overview

Paddy also known as rice is the starchy seeds of an annual southeast Asian cereal grass (Oryza sativa) that cooked and used for food. This cereal grass that is widely cultivated in warm climates for its seeds and by-products. Rice is one of the most utilized food plants and widely grown originated in ASIA. Rice is an important crop worldwide and over half of the world population relies on it for food.

Paddy Pest, Symptoms and Management

Generally, it is not recommended to spray in the early stages of crop growth (0–40 DAP) because the plant can recover from much of the damage without any loss to yield.

In the early stages of the rice crop, several common insects such as the leaf-folder, whorl maggot, and armyworms can cause highly visible damage symptoms; however, the damage is rarely enough to reduce yield because the crop can compensate for early damage over the rest of the growing season.

In most cases, insecticides applied in rice fields during the early crop stages to control pest are unlikely to benefit farmers economically. Instead, they can cause an imbalance in the natural insect population that may lead to pest outbreaks.

Related Study

[1] The authors developed an innovative classification system that automatically detects harmful insects in greenhouse based on image analysis and scene interpretation. [2], the authors developed a software prototype for early pest detection on the infected crops in the greenhouse. Support Vector Machine algorithm was used to classify the extracted insect pests from the image to estimate their density inside the greenhouse. [3], the authors present an automated video surveillance technology for pest detection on the infected images of rose

leaves in the greenhouse. The proposed cognitive vision system is combined with image processing, learning and knowledge-based techniques which can automatically identify and count mature whiteflies captured in the images. [4], the authors setup a network of cameras to continuously survey a greenhouse. The interpretation of the extracted insect pests from the image is done using neural learning and knowledge-based techniques. [5], the authors captured images were then processed through the system where different image processing algorithm and techniques were used to identify the regions of interest and represent those regions as scale-invariant feature transform (SIFT) or speeded-up robust features (SURF) descriptors. [6], the authors study on automatic identification of whiteflies, aphids and trips' in the greenhouse was based on image analysis. They presented an innovative decision support system using different image processing techniques. [7], the authors proposed a new method of pest detection by binocular stereo to get the location information about pest affected in crops, which was used for guiding the robot to spray the pesticides automatically. They proposed a Back propagation neural network for recognition of leaves, diseases, pests. [8], they have implemented SVM (support vector machine) method to reduce the usage of herbicides by sprinkling them only in the areas where weed is present. In this paper, they implemented digital image processing using the MATLAB software to detect the weed areas in an image. A distinct algorithm name as the relative difference in the pixel in densities (RDI) was proposed for detecting pest named as white fly affecting various leaves. The algorithm can only be used in greenhouse-based crops, but also agriculturally based crops as well.

Implementation

System Overview

The system consists of a mobile application, which will enable the farmers to take images of paddy using their mobile phones and send it to a central server where the central system in the server will analyze the pictures based on visual symptoms using image processing algorithms in order to measure the disease type. An expert group will be available to check the status of the image analysis data and provide suggestions based on the report and their knowledge, which will be sent to the farmer as a notification in the application. Fig. 1 contains the general system architecture.

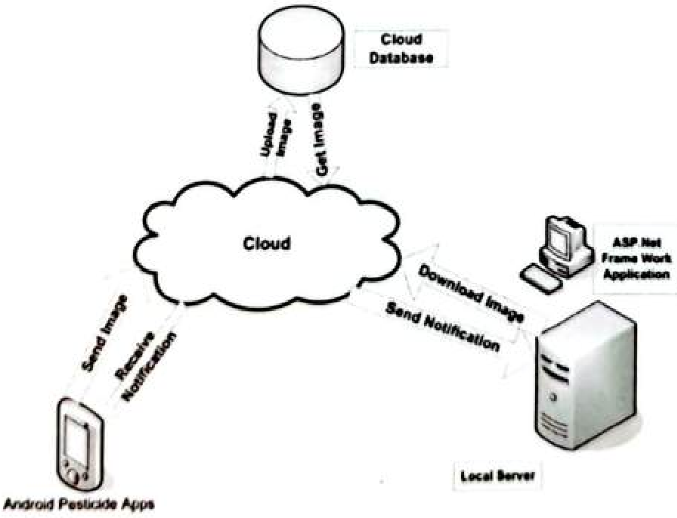


Fig. 1: General system architecture.

Hog Feature

HOG is a dense feature extraction method for images. Dense means that it extracts features for all locations in the image (or a region of interest in the image) as opposed to only the local neighborhood of key points like SIFT.

Intuitively it tries to capture the shape of structures in the region by capturing information about gradients. It does so by dividing the image into small (usually 8x8 pixels) cells and blocks of 4x4 cells. Each cell has a fixed number of gradient orientation bins. Each pixel in the cell votes for a gradient orientation bin with a vote proportional to the gradient magnitude at that pixel.

To reduce aliasing, the pixels votes are bilinearly interpolated. This interpolation happens in both the orientation as position. This statement is important - it means that a pixel will not only vote for its orientation bin, but also for the to neighboring orientation bins (e.g. it the gradient orientation at a pixel is 45 degrees, it will vote with a weight of 0.5 for the 35 to 45 degree bin and a weight of 0.5 for the 45 to 55 degree bin). Similarly, it will vote for these two orientation bins not only in its cell, but also in the 4 neighboring cells of its cell. The weights here are decided by the distance of the pixel from the cell centers.

Histograms are also normalized based on their energy (regularized L2 norm) across blocks. Since the blocks have a step size of 1 cell, a cell will be part of 4 blocks. This defines four differently normalized versions of the cell's histogram. These 4 histograms are catenated to get the descriptor for the cell. Typically, the elements of histograms are also capped at some value.

There are some more bells and whistles, and I refer the interested reader to the paper (Page on lear.inrialpes.fr) which also has a lot of evaluations for the parameters (eg. normalization strategy, cell and block sizes, cell and block geometry etc.) and also describes how to use these features with a linear SVM for detecting objects.

Machine learning, support vector machines (SVMs, also support vector networks [1]) are supervised learning models with associated learning algorithms that analyze data used for classification and regression analysis. Given a set of training examples, each marked as belonging to one or the other of two categories, an SVM training algorithm builds a model that assigns new examples to one category or the other, making it a non-probabilistic binary linear classifier. An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall on.

In addition to performing linear classification, SVMs can efficiently perform a non-linear classification using what is called the kernel trick, implicitly mapping their inputs into high-dimensional feature spaces.

When data are not labeled, supervised learning is not possible, and an unsupervised learning approach is required, which attempts to find natural clustering of the data to groups, and then map new data to these formed groups. The clustering algorithm which provides an improvement to the support vector machines is called support vector clustering[2] and is often used in industrial applications either when data is not labeled or when only some data is labeled as a preprocessing for a classification pass. Fig. 2 contains HOG visualization, Fig. 3 contains SVM classification, Fig. 4 contains Input image. And Fig. 5 contains Pest Detection.

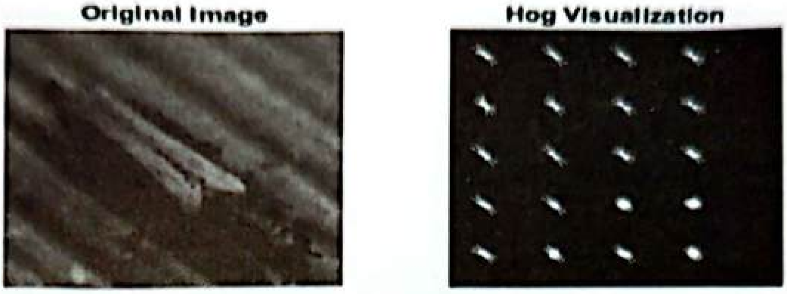


Fig. 2: Fog Visualization.

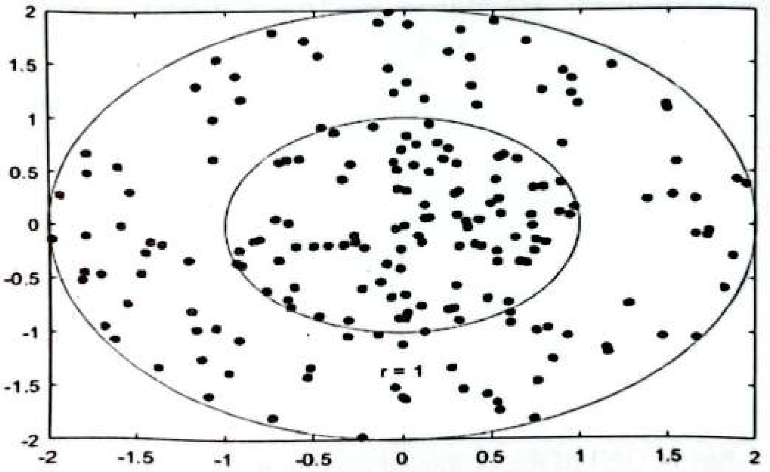


Fig. 3: SVM classification.

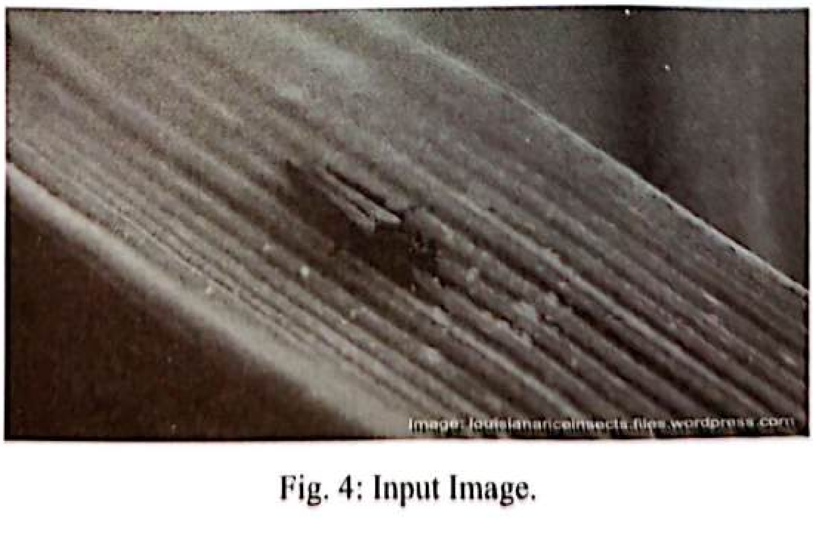


Image: louisianancelnsects.files.wordpress.com

Fig. 4: Input Image.

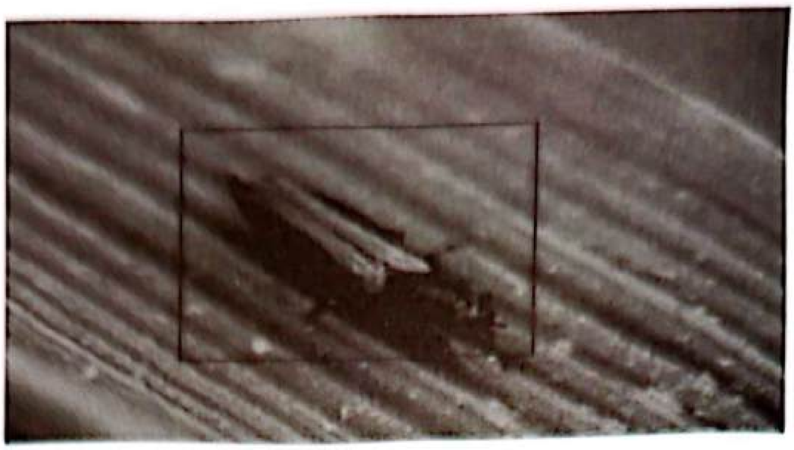


Fig 5. Pest Detected.

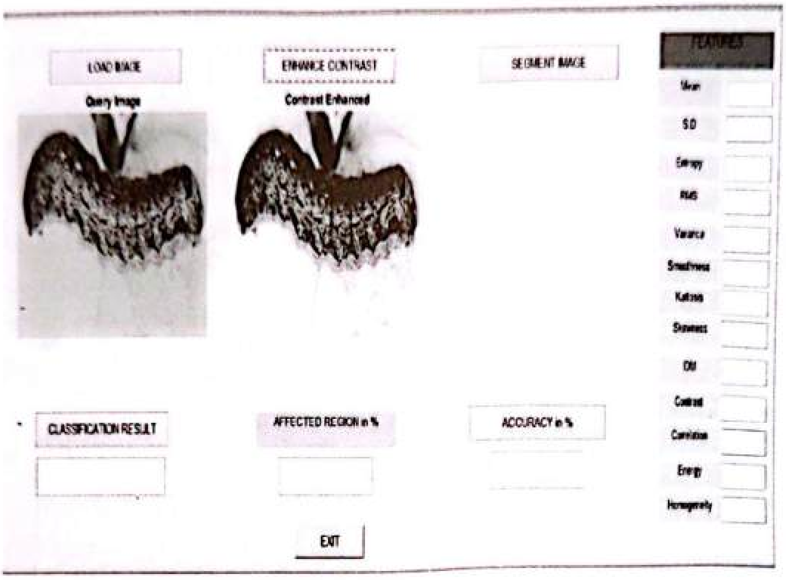
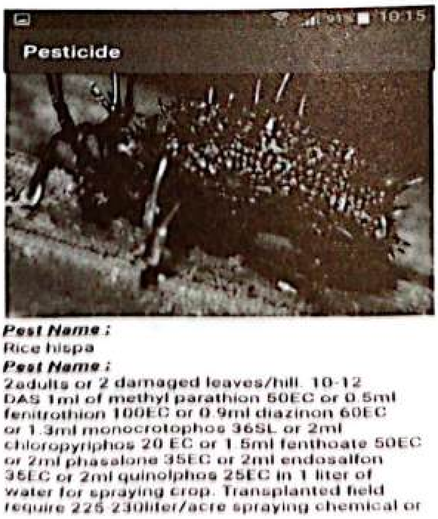


Fig. 6: GUI of the proposed system with input image.

User Notification

Finally, user will be notified with useful information about the pest. Fig. 7 contains the used notification example.



Pest Name :
Rice hispa
Pest Name :
2adults or 2 damaged leaves/hill. 10-12 DAS 1ml of methyl parathion 50EC or 0.5ml fenitrothion 100EC or 0.9ml diazinon 60EC or 1.3ml monocrotophos 36SL or 2ml chloropyriphos 20 EC or 1.5ml fenthoate 50EC or 2ml phasalone 35EC or 2ml endosalfon 35EC or 2ml quinolphos 25EC in 1 liter of water for spraying crop. Transplanted field require 225 230liter/acre spraying chemical or

Fig. 7: Notification to user mobile.

Experimental Results and Discussion

TABLE VI. CORRECT RATE AND MISS RATE OF EACH PEST IN PEST RECOGNITION PROCEDURE

SL no	Pest Name	Correct Rate (CR)	Miss rate (MR)	Accuracy
1	Rice Hispa	5	0	100%
2	Black Bugs	7	1	87.5%
3	Root Weevil	7	1	87.5%
4	Rice Thrips	5	0	100%
5	Rice whorl maggot	7	1	87.5%
6	Mealy Bug	8	2	80%
7	Stem Borer	8	1	88.89%
8	Mole cricket	7	1	87.5%
9	Cutworm	9	2	81.8%
10	Rice Skipper	7	1	87.5%

Fig. 8 contains the Performance Accuracy (%) Measurement for HOG.

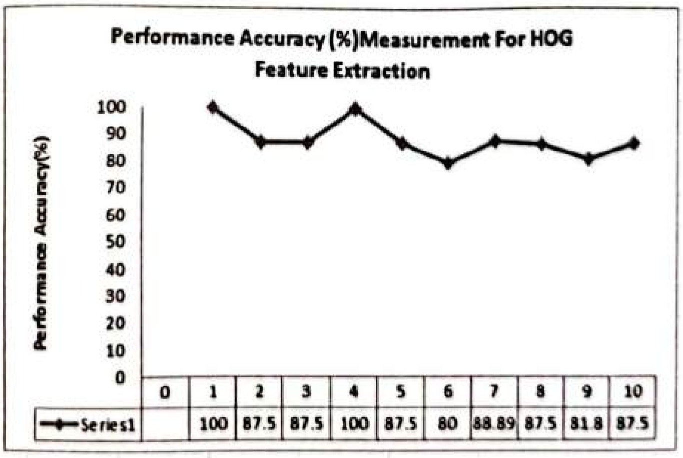


Fig. 8: Performance Accuracy (%) Measurement for HOG.

Conclusion and Future Works

We have considered few limitations to the system. One of the drawbacks is regarding time for image analysis of paddy pests. When we send an image to server, we cannot find our result in short time. Because experts are recognizing pest using image processing techniques. So, it requires few minutes. If we use a cloud computing system this problem can be solved. In addition, the system is developed in English which might be challenging for the rural farmers to use. In order to actually spread this system for mass usage, it is essential that mobile application contains the instructions in Bangla.

References

1. *R. Kumar, V. Martin and S. Moisan, "Robust Insect Classification Applied to Real Time Greenhouse Infestation Monitoring".*
2. *R.G. Mundadal, V.V. Gohokar, "Detection and Classification of Pests in Greenhouse Using Image Processing," Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735. Volume 5, Issue 6 (Mar. - Apr. 2013), PP 57-63.*
3. *S.R. Pokharkar and V.R. Thool, "Early Pest Identification in Greenhouse Crops using Image Processing Techniques," International Journal of Computer Science and Network (IJCSN).*
4. *V. Martin, S. Moisan, B. Paris and O. Nicolas, "Towards a video camera network for early pest detection in greenhouses," ENDURE International Conference 2008 Diversifying crop protection, October 2008.*
5. *K. Venugoban and A. Ramanan, "Image Classification of Paddy Field Insect Pests Using Gradient-Based Features," International Journal of Machine Learning and Computing, Vol. 4, No. 1, February 2014.*
6. *J. Cho, J. Choi, M. Qiao, C. Ji, H. Kim, K. Uhm and T. Chon, "Automatic identification of whiteflies, aphids and thrips in greenhouse based on image analysis," International Journal Of Mathematics And Computers In Simulation.*
7. *Maria Petrou and Panagiota Bosdogianni (2003). Image Processing: The Fundamentals. 3rd Edition, John Wiley and Martin, V., Moisan, S., Paris, B., Nicolas, O. " O.50 - Towards a video camera network for early pest detection in greenhouses", ENDURE International Conference, 2008.*
8. *International Journal of Electrical and Electronics Research ISSN 2348-6988 (online) Vol. 2, Issue 4, pp: (187-194), Month: October - December 2014.*

Analysis of the Plastic Waste Collection and Wealth Linkage in Bangladesh

Sheikh Salman*
Md. Arafat Hossain**
Md. Maruf Hossain***
Hasan Al Zaman****

Keywords: PET. Pyrolysis, Hydrolysis, Flexural strength.

Abstract: *Disposal of plastic waste in environment is considered to be a big problem due to its very low biodegradability and presence in large quantities. Therefore, finding alternative methods of disposing waste by using friendly methods are becoming a major research issue. This research focuses on the efficient reuse of waste plastic in the production of concrete. Polyethylene terephthalate (PET) waste plastic was used as a partial replacement for sand by 0%, 5% and 12%, with aggregate concrete mixtures. Nine cubes were molded for compressive strength test and nine beams were cast for flexural strength tests. Curing ages of 5, 14, and 20 days for the concrete mixtures were applied in this work. These tests include compressive strength and flexural strength test. The results show that there is a possibility to produce plastic mix concrete beam and column. This study ensures the reuse/recycle of waste plastic as a sand- substitution aggregate in concrete gives a good approach to reduce the cost of materials and solve some of the solid waste problems posed by plastics.*

Introduction

Today plastics play a dominant role for industrial and domestic applications because of their excellent properties and merits. These are very popular because of their high strength and stiffness as a result of low relative density, corrosion resistance, and good electrical and thermal insulating properties and inexpensive compared to other metals on volume basis. Plastic may be defined as organic materials that can be easily molded or shaped by mechanical or chemical action to give non-crystalline substances that are solid at ordinary temperatures. Plastic may be defined as materials made up of long chain molecules based on carbon and hydrogen [2]. Economic growth and changing consumption and production patterns are resulting into rapid increase in generation of plastic waste in the world [4].The world's annual consumption of plastic materials has increased from around 5 million tons in the 1950s to nearly 100 million tons; thus, 20 times more plastic is produced today than 50 years ago (UNEP 2009).

Importantly, resources are being used to meet the increased demand for plastic, and on the other hand, more plastic waste is being generated. The rapid growth of plastic waste in cities of developing countries, including Bangladesh presents a dilemma. Cities historically have been centers of industry and commerce and magnets for millions of people, however, the sheer size of cities and the rapid, continuing influx of rural migrants cast doubt on their ability to continue providing improved standards of living including plastic waste management for their inhabitants [3]. Plastic consumption has grown at a tremendous rate over the past two decades

***Lecturer, Dept. of Mechanical and Industrial Production Engineering, European University of Bangladesh, Dhaka.**

****Industrial Engineer, Intersoff Apparels Ltd.**

*****Officer-Operation, Planning and Research, Viyellatex Group Ltd.**

******Management Trainee Officer, UTC Group Ltd.**

as plastics now play an important role in all aspects of modern lifestyle. Collection and disposal of plastic waste has emerged as an important environmental challenge and its recycling is facing roadblocks due to their non-degradable nature.

More importantly, a very promising method of recycling plastics is the chemical modification or the de- polymerization of the waste to recover its basic chemicals. However, there are two ways to achieve de-polymerization; (1) hydrolysis and (2) pyrolysis. This study ensures the reuse of waste plastic materials and solves some of the solid waste problems.

Materials and Methods

Materials: There are various materials used in this study such as Cement, Fine Aggregate, Coarse Aggregate, Water and Plastics. The mixing ratio of the materials is given in table 1.

Table 1:Mixing proportion for various materials

Specimen, (p)	Cement (kg/m^3)	Aggregate (Kg/m^3)	Sand (Kg/m^3)	Waste (Kg/m^3)	Percentage of waste from sand	Weight Ratio
P1	355	850	540	0	0%	1:1.5:2
P2	355	850	513.7	27.3	5%	
P3	355	850	475.2	64.8	10%	

Method of Fabrication: The Fabrication method is demonstrated by the following figure 1.

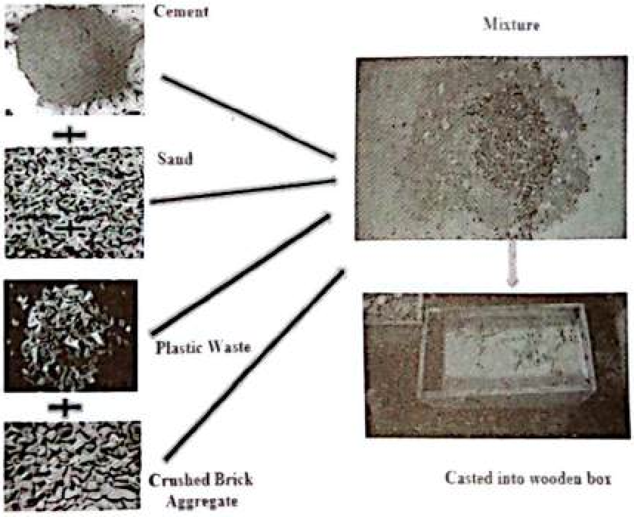


Figure 1. Fabrication method

Result and Discussion

The results of the compressive strength tests for the waste plastic concrete mixtures are shown in the figure-2. By increasing the waste plastic ratio, the results show a tendency for compressive strength values of waste plastic concrete mixtures to decrease below the plain mixtures at each curing age. This trend can be attributed to the decrease in adhesive strength between the surface of the waste plastic and the cement paste, as well as the particles' size on the increase of waste plastic increase.

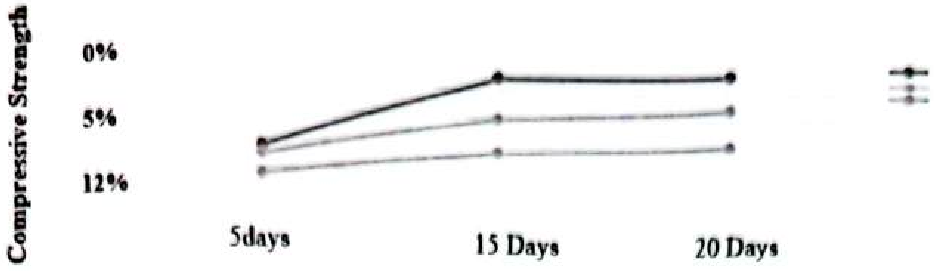


Fig. 2: Compressive strength data

The results of the flexural strength tests for the plastic concrete mixtures are illustrated in Figure 4.4.2. These results show that the flexural strength of waste plastic concrete mixtures at each curing age is prone to decrease with the increase of the waste plastic ratio in these mixtures. This trend can be attributed to the decrease in adhesive strength between the surface of waste plastic particles and the cement paste, as well as the hydrophobic nature of plastic material which may limit the hydration of cement. Therefore, the hydration is developed slightly with time. Among 5% and 12% mixture of plastic waste mixed concrete beams the maximum flexural strength shows that 5% plastic waste eat the curing stage of 20 days which is 4.9 MPa and the minimum value of flexural strength 3.5 MPa is obtained from the 12% plastic waste mixed concrete beams at the curing stage of 5 days.

Concrete mixture made of 5% plastic waste contains an average strength for both compressive and flexural test. So this ratio can be used to solve some solid waste problems posed by plastics. This experiment evaluates that if the amount of plastic waste can be decreased then the strength will be increased. But it is not the aim of experiment to remove the plastic waste from the building element of concrete beams and columns. If a little amount of plastic waste can be added to each beam and column then a large amount of plastic waste can be reduced from the world. The environmental issues and the negative effects of waste plastic will be reduced with the proper use of plastic waste into building construction. There are so many ways and scopes to recycle plastic waste but it is not possible to recycle all of the waste plastic. So as a filler material of building material plastic waste can be the best solution.

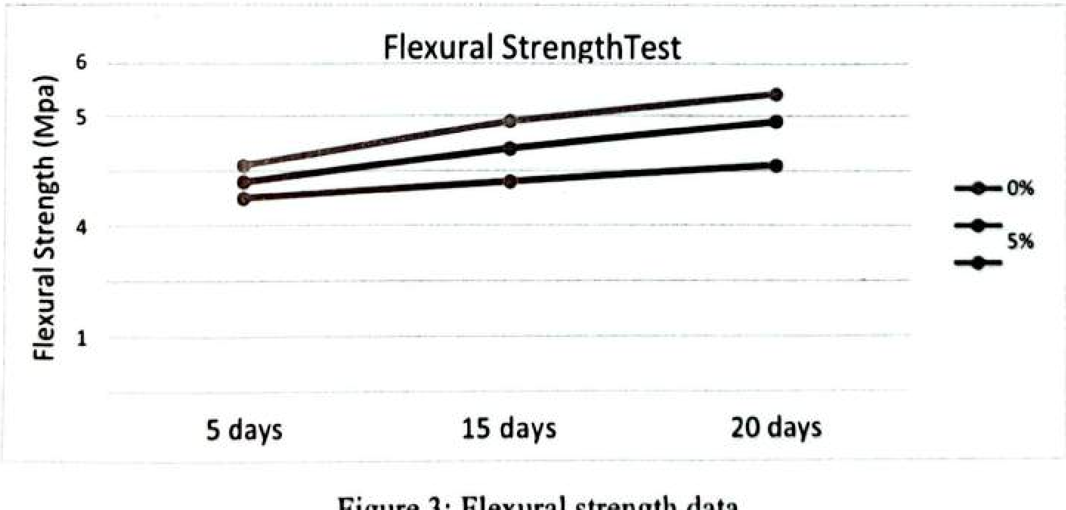


Figure 3: Flexural strength data

Conclusion

At the end of the thesis it can be said that the objectives of this thesis are achieved. We have got the compressive strength and flexural strength value above the minimum required strength for constructing a building. So it can be easily said that plastic waste is a great option as a building material and it also reduces the pressure on the basic building materials. This thesis has shown that plastic recycling activities have become economically profitable venture and thus play an important role as livelihood for many residents in the metropolis.

References

1. *Agamuthu, P., Khidzir, K. M., and Hamid, F. S. (2009). Drivers of sustainable waste management in Asia. Waste Management and Research, 27(7), 625–633.*
2. *Alamgir, M., and Ahsan, A. (2007). Municipal solid waste and recovery potential : Bangladesh perspective. Iran. J. Environ. Health. Sci. Eng., 4(2), 67–76.*
3. *Briassoulis, D., Hiskakis, M., and Babou, E. (2013). Technical specifications for mechanical recycling of agricultural plastic waste. Waste Management, 33(6), 1516–1530.*
4. *Concern, W. (2015). Environmental Challenges of Plastics Waste in Bangladesh.*
5. *Contreras, F., Ishii, S., Aramaki, T., Hanaki, K., and Connors, S. (2010). Drivers in current and future municipal solid waste management systems: cases in Yokohama and Boston. Waste Management andResearch, 28(1), 76–93.*
6. *Dahlén, L., and Lagerkvist, A. (2010). Evaluation of recycling programs in household waste collection systems. Waste Management and Research, 28(7),577–586.*
7. *Hopewell, J., Dvorak, R., and Kosior, E. (2009). Plastics recycling: challenges and opportunities. Philosophical Transactions of the Royal Society B: Biological Sciences, 364(1526), 2115–2126. https://doi.org/10.1098/rstb.2008.0311*
8. *Hotta, Y., and Aoki-Suzuki, C. (2014). Waste reduction and recycling initiatives in Japanese cities: Lessons from Yokohama and Kamakura. Waste Management and Research, 32(9), 857–866. https://doi.org/10.1177/0734242X14539721*
9. *Islam, F. A. S. (2016). Solid Waste Management System in Dhaka City of Bangladesh, 4(1), 192–209.*
10. *JICA. (2005). the study on the solid waste management in Dhaka city-clean Dhaka master plan, (March 2005), 1–98.*
11. *Kabir, M. R. (2016). Municipal Solid Waste Management System : A Study on Dhaka North and South City Corporations. Journal of Bangladesh Institute of Planners, 8(December), 35–48.*
12. *Laadila, M. A., Hegde, K., Rouissi, T., Brar, S. K., Galvez, R., Sorelli, L., Abokitse, K. (2017). Green synthesis of novel bio composites from treated cellulosic fibers and recycled bio-plastic polylactic acid. Journal of Cleaner Production, 164, 575–586.*

Data Encryption Algorithms and Comparison

Md. Obaidur Rahman*

Keywords: Encryption Algorithm, Performance, Analysis, AES, DES, Blowfish, TripleDES, Cryptography

Abstract: *In the modern world information security is the process of protecting information. It protects its availability, confidentiality and integrity. Access to stored information in computer databases has greatly expanded. More and more companies store business and personal information on their computer than ever before. Most of the stored information is strictly confidential and not intended for public viewing. There are two main characteristics that define and distinguish one encryption algorithm from another are ability to protect protected data from attacks, as well as its speed and efficiency. This paper compares performance between the four most common encryption algorithms: DES, 3DES, Blowfish, and AES. The comparison has been carried out by running several encryption settings for processing data blocks of different sizes to estimate the encryption / decryption rate of the algorithm. Simulation has conducted using C++ programming language.*

Introduction

The value of exchanging data over the Internet or other types of media is increasing. Finding the best solution that provides the necessary protection against data hijackers and providing these services in a timely manner is one of the most active items in security related communities.

This paper tries to provide a fair comparison between the most common and used algorithms in data encryption. Since our main task is to find out the performance of these algorithms with different settings, the presented comparison takes the behavior and performance of the algorithm into account when using different data loads.

Encryption is one of the primary means of ensuring the security of confidential information. The encryption algorithm performs various substitutions and plaintext conversions (the original message before encryption) to convert it into encrypted text (the encrypted message after encryption). Many encryption algorithms are widely available and are used in information security. Encryption algorithms are divided into two groups: Symmetric key (also called a secret key) and Asymmetric-key (called public key) encryption [2].

Secure Wi-Fi system for wireless networks: experimental evaluation is a network security system for an application using the proposed algorithm. As for some cryptographic system, it is usually being used to protect communication channels using public key exchange based on algorithms such as DES, AES, Triple DES and Blowfish. From key exchange, it depends on the key used to encrypt data transmitted over an unsecured Internet channel. In addition, the existing cryptographic algorithm is based on the data separation model developed by IBM Horst Feistel [27].

***Associate Professor and Chairman, Department of Computer Science and Engineering, European University of Bangladesh, Dhaka, Bangladesh.**

In this paper, we propose an intensive study of the idea of sending an encrypted file through the cloud, despite the original file is using the DES cryptography algorithm [4].

The goal is to provide evidence of which encryption method is more powerful and efficient while transferring an encrypted file, so the original file is not available even on the network.

Thus, even if the intermediate user sees the data, he will not be able to understand them. This is why confidentiality and integrity are maintained. Consequently, the security of cloud data will be enhanced. This work can be improved using a hybrid approach by integrating several cryptography algorithms [28].

Cryptography

The main goals of using cryptography will be discussed in this section along with the common terms used in this field.

Cryptography is commonly referred to as learning secrets, while it is currently most attached to the definition of encryption. Encryption is the process of transforming plain text, "unhidden" into mysterious, "hidden" in order to protect it from data thieves. This process has another part, where the cipher text must be decrypted at the other end to be understood. Figure.1 shows a simple stream of commonly used encryption algorithms.

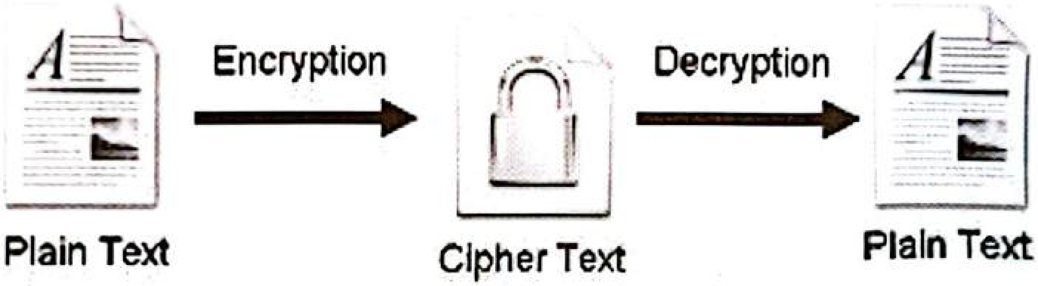


Fig.1 Encryption-Decryption Flow

Cryptographic System is define as "a set of cryptographic algorithms along with key management processes that support the use of algorithms in some application context." This definition defines the entire mechanism that provides the necessary level of security, consisting of network protocols and data encryption algorithms.

Cryptography

This section explains the five main goals behind the usage of Cryptography. Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories:

Authentication

The sender and receiver can confirm each other's identity and the origin/destination of the information.

Access Control

The prevention of unauthorized use of resources is termed as access control. Access control mechanism allows only authenticated users to use information or resources.

Secrecy *or* Confidentiality

The protection of data from unauthorized disclosure is called data confidentiality. There are four levels of data confidentiality as:

Connection Confidentiality

The protection of all user data in one connection is called connection confidentiality. All communications are confident in the confidentiality of communication. Data must be sent through this confident connection to ensure confidentiality.

Confidentiality of Safety

In this case, protection is performed in all user data in a single data block, and then it can be transmitted over any connection.

Confidentiality of Selective Field

With selective privacy of the fields, protection is provided only in selected areas of information.

Confidentiality of the Flow of Movement

The information cannot be understood by anyone for whom it was unintended.

Integrity

Data integrity is the belief that the data received should be exactly the same as those sent by sender. The integrity of the data can be of different types:

- Integrity of the connection with the recovery, which detects any unauthorized modification of the entire data sequence with attempts of recovery.
- Integrity of connection without restoration, only detects unauthorized change of all information without attempts of recovery.
- The integrity of the connection with the selective field ensures the integrity of the selected field within the user data with attempts of recovery and without attempts to restore it as needed.

Non Repudiation

The protection against denial by an entity or group of entities involved in a communication or having participated in all or part of communication, is provided by non-repudiation. Non repudiation can be provided on both, origin and destination end. It proofs that the message was sent by the specific entity as well as the message was received by the specific party.

All the above discussed services are provided by both public key cryptography and private key cryptography. Here we are designing a new private key cryptographic algorithm, hence now we'll discuss about private key cryptography.

Block Ciphers and Stream Ciphers

Secure file transfer protocols like SFTP, FTPS, HTTPS, and WebDAVS encrypt data through symmetric key ciphers. One of the main categorization methods commonly used for encryption techniques is based on the form of input data they operate on. These ciphers can be classified into two groups: stream ciphers and block ciphers. This section discusses the main features of the two types, operation mode, and compares them in terms of security and performance.

Block Cipher

The most important symmetric (meaning the same key is used for both encryption and decryption) algorithms are block ciphers. The general operation of all block ciphers is same - a given number of bits of plaintext (a block) are encrypted into a block of ciphertext of the same size.

Encryption:

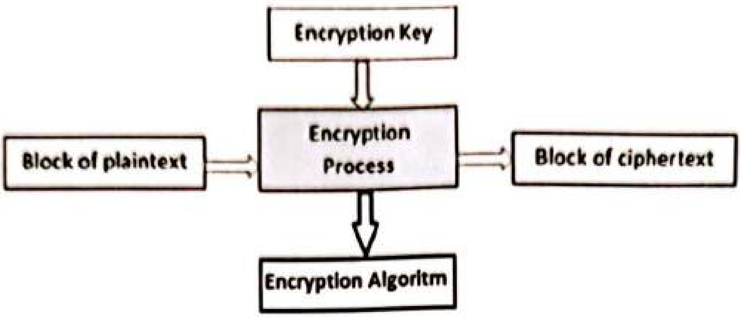


Fig.2. Encryption process with Block Cipher

Decryption:

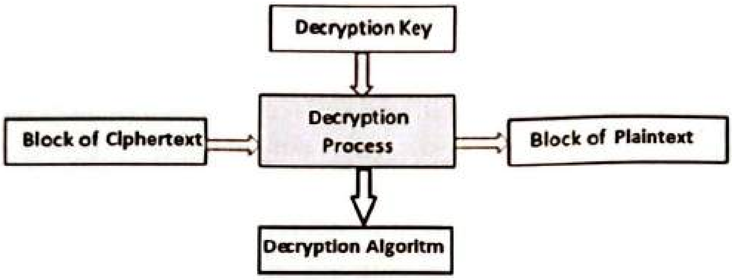


Fig.3. Decryption process with Block Cipher

ECB (Electronic Codebook Mode) is the simplest mode of operation for a block cipher. The input data is padded out to a multiple of the block size, broken into integer number of blocks, each of which is encrypted independently using the key. In addition to simplicity, ECB has the advantage of allowing any block to be decrypted independent of others. Thus, lost data blocks can not affect the decryption of other blocks. The disadvantage of ECB is that it aids known-plaintext attacks. If the same block of plaintext is encrypted twice with ECB, the two resulting blocks of ciphertext will be the same.

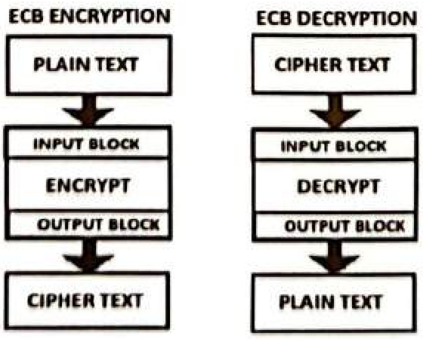


Fig.4 Block Cipher ECB Mode

Stream Ciphers

A stream cipher is an encryption algorithm that encrypts 1 bit or byte of plaintext at a time1. It uses an infinite stream of pseudorandom bits as the key. Stream cipher consists of two major components: a key stream generator and a mixing function. Mixing function is usually just an XOR function, while key stream generator is the main unit in stream cipher encryption technique. For example, if the key stream generator produces a series of zeros, the outputted ciphered stream will be identical to the original plain text. Figure 5 shows the operation of the simple mode in stream cipher.Stream ciphers are designed to implement an idealized cipher, known as the One-Time Pad.

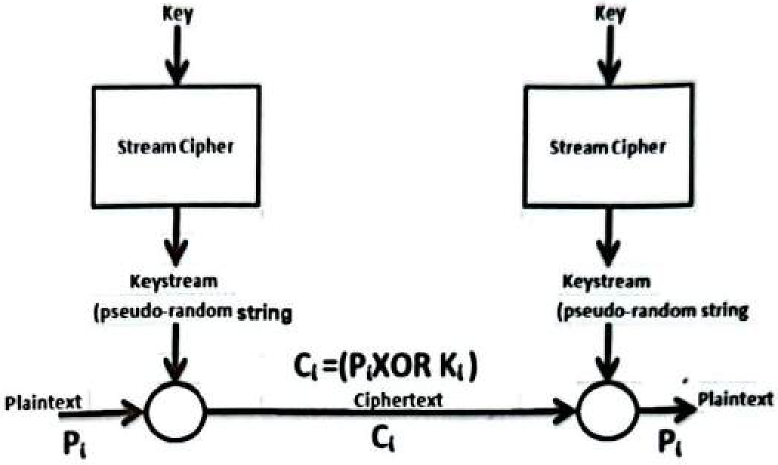


Fig. 5 Stream Cipher (Simple Mode)

Block Cipher Encryption – Operations:

The general operation of all block ciphers is the same - a given number of bits of plaintext (a block) are encrypted into a block of cipher text of same size. Thus, all block ciphers have a natural block size - the number of bits they encrypt in a single operation. Block ciphers can be operated in several modes as:

1) CBC (Cipher Block Chaining)
2) ECB (Electronic Code Book)
3) CFB (Cipher Feedback)
4) OFB(Output Feedback).

CBC (Cipher Block Chaining): CBC is the most commonly used mode of operation for a block cipher. Prior to encryption, each block of plaintext is XOR-ed with the prior block of ciphertext. After decryption, the output of the cipher must then be XOR-ed with the previous ciphertext to recover the original plaintext. The first block of plaintext is XOR-ed with an initialization vector (IV), which is usually a block of random bits transmitted. CBC is more secure than ECB because it effectively scrambles the plaintext prior to each encryption step. Since the ciphertext is constantly changing, two identical blocks of plaintext will encrypt to two different blocks of ciphertext. CBC can be used to convert a block cipher into a hash algorithm. To do this, CBC is run repeatedly on the input data, and all the ciphertext is discarded except for the last block, which will depend on all the data blocks in the message. This last block becomes the output of the hash function.

ECB is the simplest mode of operation for a block cipher. The input data is padded out to a multiple of the block size, broken into a integer number of blocks, each of which is encrypted independently using the key. In addition to simplicity, ECB has the advantage of allowing any block to be decrypted independently. Thus, lost data blocks can not affect the decryption of other blocks. The disadvantage of ECB is that it aids known-plaintext attacks. If the same block of plaintext is encrypted twice with ECB, the two resulting blocks of ciphertext will be the same.

CFB (Cipher Feedback): The CFB mode is similar to the previously described CBC mode. The main difference is that one should encrypt ciphertext data collected from the previous round (so not the plaintext block) and then add the output to the plaintext bits. It does not affect the cipher security but it results in the fact that the same encryption algorithm (as used for encrypting plaintext data) should be used during the decryption process.

OFB (Output Feedback): Output Feedback Mode (OFB) converts a block cipher into pseudo-random number generator. The output ciphertext is feed back into the input of the block cipher, and this process will be repeated to produce a stream of pseudo-random bits. The bit stream is completely determined by the algorithm, the key, an initialization vector and the number of bits (k) feed back into the cipher during each step. The stream of bits can then be XOR-ed with the plaintext to produce ciphertext, effectively converting the block cipher into a stream cipher.

Stream Cipher Encryption – Operations:

For the stream cipher, the bit stream is encrypted using an encryption key. In general, streaming cipher works bit by bit of plain text and creates cipher-text. In the stream cipher, the encryption key is constantly changing according to the plaintext bits and therefore, each time it processes different cipher texts for the same plain text but the block cipher produces the same cipher each time for the same plain text.

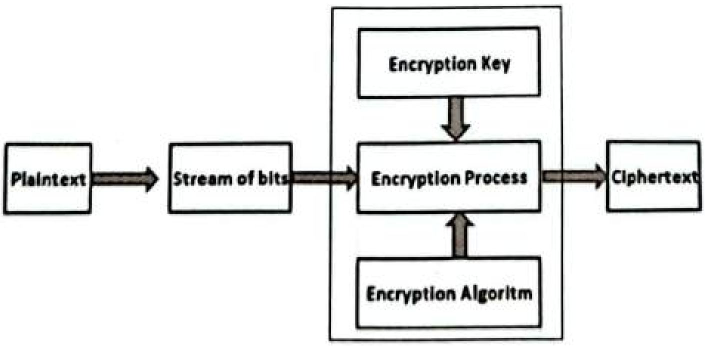


Fig.6. Encryption process with Stream Cipher

Symmetric and Asymmetric Encryptions Process:

The procedure of Data Encryptions can be generally divided into two categories depending on the type of security keys used to encrypt / decrypt the inputted data. Both of the categories are: asymmetric and symmetric encryption methods, figuring out in fig 7.

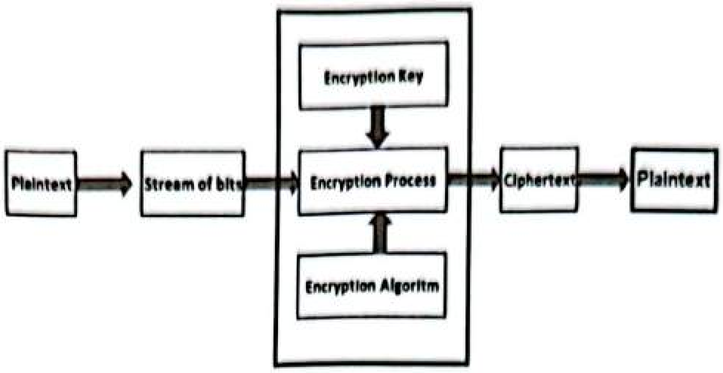


Fig.7. Symmetric and Asymmetric Encryptions Process

Symmetric Encryption

In this type of encryption, the sender and the receiver agree on a secret (shared) key. Then they use this secret key to encrypt and decrypt their sent messages. Fig 8 shows the process of symmetric cryptography. Node A and B first agree on the encryption technique to be used in encryption and decryption of communicated data. Then they agree on the secret key that both of them will use in this connection. After the encryption setup finishes, node A starts sending its data encrypted with the shared key, on the other side node B uses the same key to decrypt the encrypted messages.

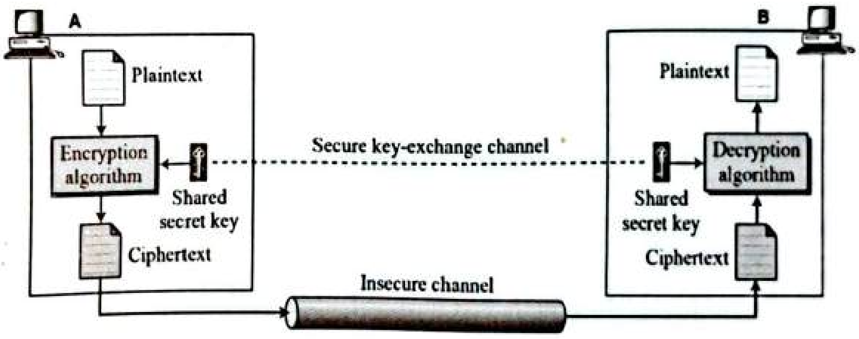


Fig.8. Symmetric Encryption

Concerning Problems behind symmetric encryption is how to share the secret key safely between two nodes. If the key becomes known for any reason, the whole system will be compromised. Key management for this type of encryption is problematic, especially if a unique secret key is used for each peer connection, then the total number of secret keys that will be stored and managed for n-nodes will be n (n-1) / 2. Some terms of symmetric encryptions are:

1) A and B agree on a cryptosystem.

2) A and B agree on the key to be used.

3) A encrypts messages using the shared key.

4) B decrypts the ciphered messages using the share key.

Asymmetric Encryption

Asymmetric Encryption is another type of encryption that uses two keys. More details, what Key1 can encrypt, only Key2 can decrypt, and vice versa. It is also known aspublic key cryptography (PKC). Typically users use two keys: the public key, which is known to the public, and the private key, which is known only to the user. Figure 9 below shows the use of two keys between node A and node B. After agreeing on the type of encryption to be used in a connection, node B sends its public key to node A. Node A uses the resulting public key to encrypt its message. Then, when the encrypted messages arrive, node B uses its private key to decrypt them. Some terms of symmetric encryptions are:

1) A and B agree on a cryptosystem.

2) B sends its public key to A.

3) A encrypts messages using the negotiated cipher and B's public key.

4) B decrypts the ciphered messages using its private key and the negotiated cipher.

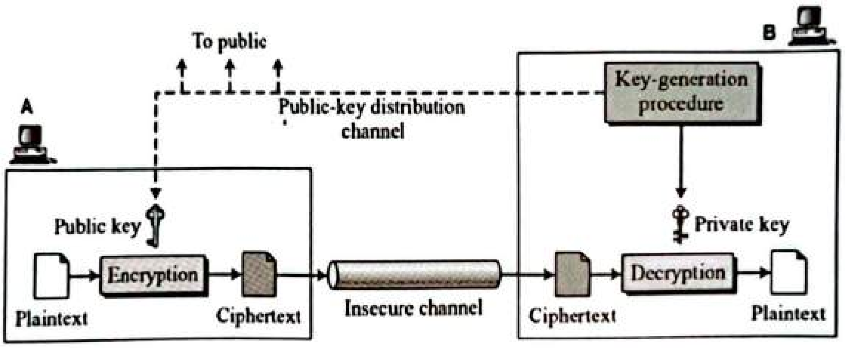


Fig.9. Asymmetric Encryption

This system doesn't face the problem of symmetric encryption when managing private keys. But on the other hand, this unique public key encryption feature makes it mathematically more susceptible to attacks. Moreover, Asymmetric Encryption methods are almost 1000 times slower than symmetric ones, because they require more processing power.

Hybrid technology is commonly used to take advantage of both methods. In this method, asymmetric encryption is used to exchange the secret key, and then symmetric encryption is used to transfer data between the sender and receiver.

Comparison Algorithms (DES, 3DES, AES and Blowfish)

This section is intended to give readers the necessary information to understand the key differences among the compared algorithms.

DES: (Data Encryption Standard) is one of the most common and widely available cryptographic systems. It was developed by IBM in the 1970s, but was later adopted by the National Institute of Standards and Technology (NIST). The algorithm is submitted to the National Bureau of Standards (NBS) to propose a candidate to protect confidential unclassified e-government data. It is now taken as an unsecured reason for its small size, and a brute force attack is possible in this. The key length is 56 bits, and the block size is 64 bits. It is vulnerable to key attacks when a weak key is used. It began with a 64-bit key, and then the NSA imposed a restriction on the use of DES with a key length of 56 bits, therefore, DES discards 8 bits of a 64-bit key, and then uses a compressed 56-bit key derived from a 64-bit key for Data encryption in block size 64 bits. DES can work in different modes - CBC, ECB, CFB and OFB, which makes it flexible. In January 1999, the distributed network and the Electronic Frontier Foundation (EFF) merged to publicly crack the DES key in 22 hours and 15 minutes. It is believed that the algorithm is practically safe in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been replaced by Advanced Encryption Standard (AES) [14-16].

3DES: As an enhancement of DES, the3DES (Triple DES) encryption standard was proposed. Stronger version of DES called TrippleDES, uses three 56-bit key to encrypt each block. The first key encrypts the data block, the second key decrypts the data block and the third key encrypts the same data block again. The 3DES version requires a 168-bit key that makes the process quite secure and much safer than the plain DES. But it is a known fact that 3DES is slower than other block cipher methods.

AES: The Advance Encryption Standard (AES) algorithm was developed in 1998 by Joan Damen and Vincent Rayman, which is a block cipher with a symmetric key [7]. The AES algorithm can support any combination of data (128 bits) and a key length of 128, 192 and 256 bits. The algorithm is called AES-128, AES-192 or AES-256, depending on the key length. In the process of decrypting encryption, the AES system runs 10 rounds for I28 keys, 12 rounds for I92 keys and 14 rounds for 256-bit keys to get the final ciphertext or get the original AES text. These blocks are treated as an array of bytes and organized as a 4×4 matrix, which is called a state. For both encryption and decryption, the cipher begins with the addition of the Round Key step [30]. However, before reaching the last round, this exit goes through nine main rounds, during each of which four transformations are performed; 1- Subbytes, 2- Line shift, 3- Mixed columns, 4- Add round key. Decryption is the reverse process of encryption using inverse functions: reverse bytes of replacement, rows of reverse shears and columns of reverse mixing. Each round of AES is governed by the following conversions [12]: Conversion of the replacement byte AES contains a 128-bit data block, which means that each of the data blocks has 16 bytes. With a subbyte transformation, each byte (8-bit) of a data block is converted to another block using an 8-bit substitution block, which is known as the Rijndael Sbox [13].

Blowfish: Blowfish was first published in 1993 [6]. This is a block cipher with a symmetric key with a key length from 32 to 448 bits and a block size of 64 bits. According to its structure, this is a feistel network. Blowfish is a symmetric block cipher that can be used as an unofficial replacement for DES or IDEA. It accepts a variable-length key, from 32 to 448 bits, which makes it ideal for both home and commercial use [8]. Blowfish was designed by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Since then, it has been significantly analyzed and is gradually gaining popularity as a reliable encryption algorithm. It suffers from a weak key problem; it is known that no attack was successful. Blowfish is not patented, has a free license and is available for any use [24].

Comparison of Results for DES, 3DES, AES and Blowfish

This section discusses the results obtained from other resources to represent complete picture of the performance of the compared algorithms.Figure10is figuring out that the Blowfish algorithm provides theencryption time. Based on encryption time, we select Blowfish technique for further evaluation.

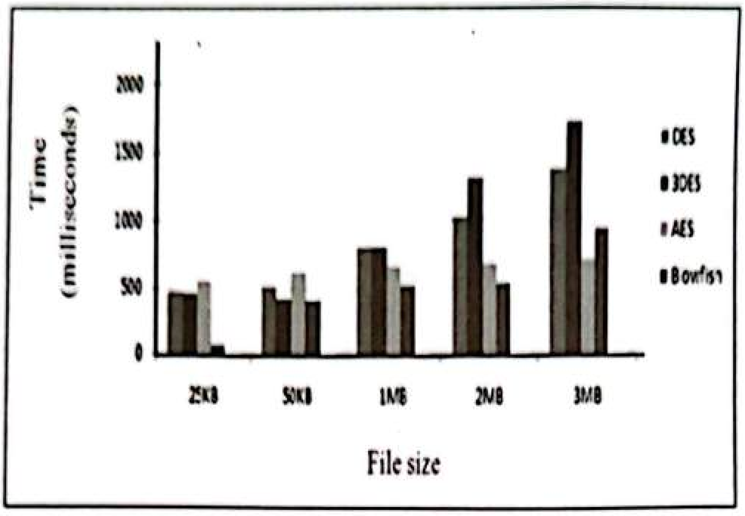


Figure.10. Encryption time vs. File size for DES, 3DES, AES and Blowfish.

Figure.11is figuring out that the decryption time for all algorithms is faster than encryption time. In addition, the blowfish algorithm provides the fastest decryption time. Based on decryption time the feature we choose the blowfish technique to consider at the next level of assessment.

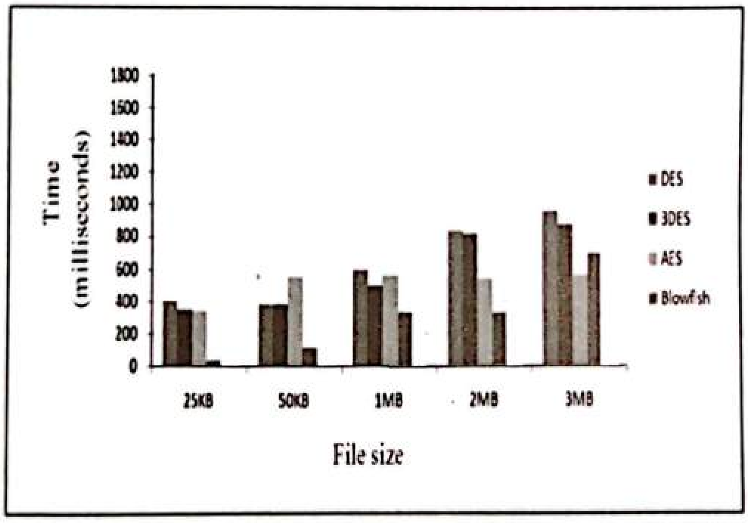


Figure.11. Decryption time vs. File size for DES, 3DES, AES and Blowfish

Table.1 shows the amount of memory required for block operations of all cryptographic methods that we studied. Blowfish consumes less memory than other types of algorithms.

Algorithms	Memory Used (KB)
DES	18.2
3DES	20.7
AES	14.7
BlowFish	9.38

Table 1: Comparison of memory used

Figure.12 is figuring out that AES exhibits the highest avalanche effect, while Blowfish exhibits the lowest avalanche effect. This again draws attention to AES for further analysis and improvement as an entropy test and final experiment. Table 2 shows that Blowfish writes the highest average entropy per encryption byte. This should highlight the achievements of the blowfish algorithm to be considered as a new security aspect.

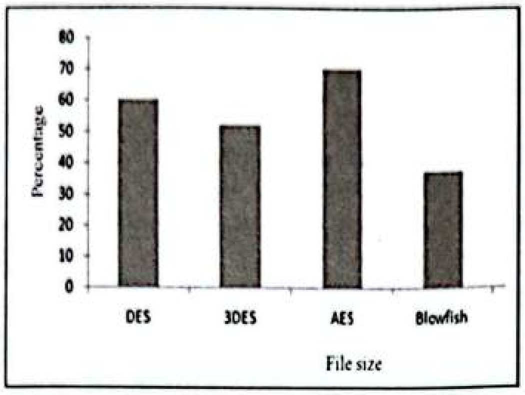


Figure.12. Avalanche effect for DES, 3DES, AES and Blowfish

Algorithms	Average entropy per byte of encryption
DES	2.9477
3DES	2.9477
AES	3.84024
BlowFish	3.93891

Table 2: Average entropy values

This table3 presents the AES requires that the largest number of bits for optimal encryption, while DES requires the minimum number of bits for optimal encryption.

Algorithms	Average number of bits required for optimally encode a byte of encrypted data
DES	27
3DES	40
AES	256
BlowFish	128

Table 3: Average entropy values

In this article, we examined various algorithms and encryption methods to improve security of data transmission, protect the information using cryptography, to provide a detailed description of information protection using cryptography and various algorithms. In addition, we have developed a new cryptographic algorithm, which is based on the concept of a block cipher, such as XOR and shift operation.

The experiments are the speed metrics for some of the most commonly used cryptographic algorithms. All of them were written in C ++, compiled with Microsoft Visual C ++ 2005-2018 SP1 (optimization of the whole program, optimized for speed) and worked on the Intel Core - 2

1.83 GHz processor with 2 GB of RAM under Windows 7 32-bit mode. X86 / MMX / SSE2 assembly language procedures were used for integer arithmetic, AES, VMAC, Sosemanuk, Panama, Salsa20, SHA-256, SHA-512, Tiger, and Whirlpool. (OpenMP support has been disabled, so only one CPU core was used for this test.). The experiments were performed couple of times to assure that the results are consistent and are valid to compare the different algorithms.

Since the security features of each algorithm as their strength against cryptographic attacks have already known and discussed. The chosen factor here to determine the performance is the algorithm's speed to encrypt/decrypt data blocks of various sizes.

Conclusion

Each of the cryptographic algorithms has strengths and weaknesses. We select a cryptographic algorithm based on the requirements of the application. Based on the results of the experiment and comparison, the Blowfish Algorithm is an ideal choice in the case of time and memory in accordance with the criteria for guessing attacks and the required functions, since it records the shortest time among all the algorithms. It also consumes less amount of memory. If confidentiality and integrity are key factors, you can choose an AES algorithm. If the demand of the application is network bandwidth, DES is the best option. We can assume that the Blowfish and AES algorithms are used to prevent the application from guessing attacks, and it can be applied on top of all Internet protocols based on IPv4 and IPv6. This article shows that different algorithms need different amount of time and memory consumption for the process of encryption.

References

1. *Priyadarshini P, Prashant N, Narayan DG, Meena SM. A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Computer Science. 2016;78:617- 624.*
2. *Yogesh K, Rajiv M, Harsh S. Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures. International Journal of Computer Science and Management Studies. 2011;11(3):60-63.*
3. *Jeeva AL, Palanisamy V, Kanagaram K. Comparative analysis of performance efficiency and security measures of some encryption algorithms. International Journal of Engineering Research and Applications. 2012;2(3): 3033-3037.*
4. *Alanazi HO, Zaidan BB, Zaidan AA, Jalab HA, Shabbir M, Al-Nabhani Y. New Comparative Study Between DES, 3DES and AES within Nine Factors. Journal of Computing. 2010;2(3):152-157.*
5. *Ritu T, Sanjay A. Comparative Study of Symmetric and Asymmetric Cryptography Techniques. International Journal of Advance Foundation and Research in Computer. 2014;1(6):68-76.*
6. *Mahindrakar MS. Evaluation of Blowfish Algorithm based on Avalanche Effect. International Journal of Innovations in Engineering and Technology. 2014;4(1):99-103.*
7. *Ritu P, Vikas k. Efficient Implementation of AES. International Journal of Advanced Research in Computer Science and Software Engineering. 2013;3(7):290-295.*
8. *Pratap CM. Superiority of blowfish Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering. 2012;2(9):196-201.*
9. *Preetha M, Nithya M. A study and performance analysis of RSA algorithm. International Journal of Computer Science and Mobile Computing. 2013;2(6):126-139.*
10. *Karthik S, Muruganandam A. Data encryption and decryption by using triple DES and performance analysis of crypto system. International Journal of Scientific Engineering and Research. 2014;2(11):24-31.*

11. Elminaam DSA, Kader HMA, Hadhoud MM. Performance Evaluation of Symmetric Encryption Algorithms. International Journal of Computer Science and Network Security. 2008;8(12):280-286.

12. Akash KM, Chandra P, Archana T. Performance Evaluation of Cryptographic Algorithms: DES and AES. IEEE Students' Conference on Electrical, Electronics and Computer Science. 2012:1-5.

13. Ritu P, Vikas k. Efficient Implementation of AES. International Journal of Advanced Research in Computer Science and Software Engineering. 2013;3(7):290-295.

14. Karthik S, Muruganandam A. Data encryption and decryption by using triple DES and performance analysis of crypto system. International Journal of Scientific Engineering and Research. 2014;2(11):24-31.

15. Stallings W. Cryptography and network Security: Principles and Practice. 5th Edition Pearson Education/Prentice Hall; 2011.

16. DES. Available from: http://www.tropsoft.com/strongenc/des.htm

17. 3DES. Available from: http://www.cryptosys.net/3des.html

18. Preetha M, Nithya M. A study and performance analysis of RSA algorithm. International Journal of Computer Science and Mobile Computing. 2013;2(6):126-139.

19. 3DES. Available from: http://en.wikipedia.org/wiki/Triple_DES

20. Aman K, Sudesh J, Sunil M. Comparative Analysis between DES and RSA Algorithm's. International Journal of Advanced Research in Computer Science and Software Engineering. 2012;2(7):386-391.

21. Xin Z, Xiaofei T. Research and Implementation of RSA Algorithm for Encryption and Decryption. 6th International Forum on Strategic Technology. 2011:1118-1121.

22. Preetha M, Nithya M. A study and performance analysis of RSA algorithm. International Journal of Computer Science and Mobile Computing. 2013;2(6):126-139.

23. Stallings W. Cryptography and network Security: Principles and Practice. 5th Edition Pearson Education/Prentice Hall; 2011.

24. Pratap CM. Superiority of blowfish Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering. 2012;2(9):196-201.

25. Bono SC, Green M, Stubblefield A, Juels A, Rubin AD, Szydlo M. Security analysis of a cryptographically- enabled RFID device. In: SSYM'05: Proceedings of the 14thconference on USENIX Security Symposium. 2005.

26. Schneier B, Kelsey J. Unbalanced Feistel networks and block cipher design. In: Proceedings of the Third International Workshop on Fast 12 Software Encryption. 1996:121-144.

27. Polimon J, Hernandez-Castro JC, Estevez-Tapiador JM, Ribagorda A. Automated design of a lightweight block cipher with genetic programming. Int J Know-Based Intell Eng Syst. 2008;12(1):3-14.

28. Pooja B. Optimization of Cryptography Algorithms in Cloud Computing. International Journal of Computer Trends and Technology. 2017;46(2):67-72.

29. Sonal S, Prashant S, Ravi Shankar D. RSA algorithm using modified subset sum cryptosystem. 2nd International Conference on Computer and Communication Technology. 2011:457-461.

30. Shraddha D. Performance Analysis of AES and DES Cryptographic Algorithms on Windows and Ubuntu using Java. International Journal of Computer Trends and Technology. 2016;35(4):179-183.

31. RFC2828],"Internet Security Glossary", http://www.faqs.org/rfcs/rfc2828.html

32. [Nadeem2005]Aamer Nadeem et al, "A Performance Comparison of Data Encryption Algorithms", IEEE 2005

33. [Earle2005] "Wireless Security Handbook,". Auerbach Publications 2005

Journal of European University of Bangladesh Volume : 4, No: 4, 2019

European University of Bangladesh

eUb

education for liberty

Approved by UGC & Govt.

January-June, 2019

Permanent Campus : 2/4, Gabtali, Mirpur, Dhaka-1216.