ISSN: 2454-1907
DOI: https://doi.org/10.29121/ijetmr.v4.i11.2017.125

IJETMR
International Journal of Engineering Technologies and Management Research
A Knowledge Repository

OBJECT ORIENTED METRIC BASED ANALYSIS OF TEXT TRANSMISSION IN E-LEARNING THROUGH NATURAL LANGUAGE STEGANOGRAPHY

Soumendu Banerjee [*1], Kh Amirul Islam [2], Sunil Karforma [3], Akash Nag [4]
[*1, 2, 4] Research Scholar, Department of Computer Science, The University of Burdwan, Burdwan, West Bengal, India
[3] Professor, Department of Computer Science, The University of Burdwan, Burdwan, West Bengal, India

Abstract:
E-learning is an application of information and communication technology in the field of learning. Through steganography the e-learning institution can provide security to other participants of e-learning like teacher and learner. Here we use text steganography with modified SNOW algorithm while passing secret texts from the administrator to the learner in an e-learning system. In this paper, we calculate the object oriented metric based analysis of CK and MOOD metrics of our proposed model, which ensures the advantages of code redundancy, code reusability, and cost effectiveness and so on.

Keywords: *Text Steganography; SNOW algorithm; Class hierarchy diagram; Object Oriented Metrics.*

Cite This Article: Soumendu Banerjee, Kh Amirul Islam, Sunil Karforma, and Akash Nag. (2017). "OBJECT ORIENTED METRIC BASED ANALYSIS OF TEXT TRANSMISSION IN E-LEARNING THROUGH NATURAL LANGUAGE STEGANOGRAPHY." *International Journal of Engineering Technologies and Management Research,* 4(11), 68-74. DOI: https://doi.org/10.29121/ijetmr.v4.i11.2017.125.

1. Introduction

Security plays a great role in any efficient e-learning system which should be provided by the administrator of the e-learning institution [1]. To make log in into any system, two essential requirements are log-in id and password and both of these are generally text based documents and very important to keep secret for security purpose. If these documents move to wrong hand then it will be very harmful for the e-learning institutions. Here we present our model regarding the transmission of texts securely from the administrator to the teacher in an e-learning system. Now, if an outsider knows about the log-in id and password to enter into an e-learning system, then he can easily upload wrong study material, can download all the related documents of study which was provided by that teacher, can upload wrong question papers and so on, which not only become a threat for the teacher but also make a bad reputation for the institution and also become harmful for the student. So the transmission of these texts should be kept secret. Text steganography is a technique through which the sender can hide the secret texts covered into

ISSN: 2454-1907
DOI: 10.5281/zenodo.1117165

another text file while sending to the receiver [2]. To provide security, here we have used a modified version of Steganographic Nature of Whitespace [3], where we apply Advanced Encryption Standard (AES) as a replacement of Information Concealment Engine (ICE) algorithm [4]. The whole process can be divided by three parts: compression, encryption and encoding scheme. Here we apply Huffman coding, which is a lossless data compression algorithm and the main two applications are to build Huffman Tree from input characters and traverse the Huffman Tree and assign codes to characters [5].

Then we apply AES algorithm for the encryption of 128 bit key which is sufficient to protect information at a secret level[6] and also easy to implement with a high speed and low RAM.

At the beginning of the message, immediately append after the text after the first line to separate the block of spaces, which is not possible unless the last 3 bits coded to zero spaces.

Metrics are units of measurement and according to E.V. Berard the five main characteristics of object oriented metric based analysis [7] are Localization, Encapsulation, Information hiding, Abstraction and Inheritance [8]. The advantages of object oriented metric based analysis over traditional system are reduction of maintenance cost, reuse of code, improvement of portability, compatible with real world system and so on. Here we calculate the values of object oriented metrics related to Chidamber and Kemerer (CK) Metrics and Metrics for Object Oriented Design (MOOD)[9], which are mostly used in metric analysis.

In this paper, we have analyzed the values of the object oriented metrics based on the class hierarchy diagram of the proposed model regarding the transmission of texts securely from the developer to the teacher. Section II includes the class hierarchy diagram of the proposed model regarding the transmission of texts secretly from the developer to the teacher in an e-learning system. Section III covers the metric based analysis of the proposed model based on the class diagram and finally, we conclude in section IV by showing some future scope.

2. Class Diagram of Proposed Model

Class diagram is a part of the static structural Unified Modeling Language (UML) diagram, which is used to represent the structure of a system by showing the classes of the system and their attributes, operations (or methods) and the relationship among objects [10]. The class diagram of our proposed model is shown in Figure1 [11] regarding the secure transmission of text from developer to learner. In this class diagram we have used five classes: HuffmanTree, HuffmanEncoder, AESencryption, Node and StegoMain.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1117165

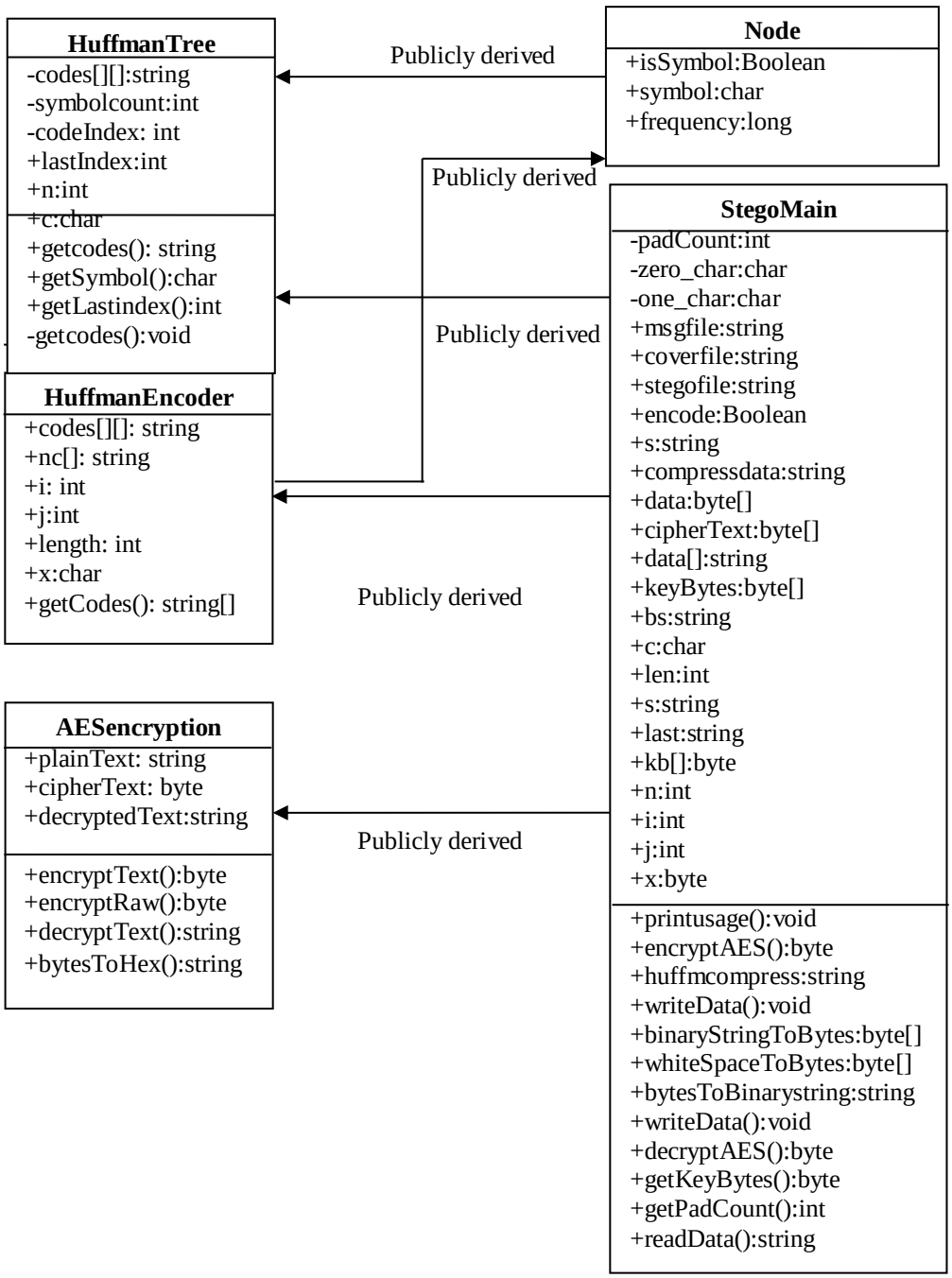

Figure 1: Class diagram of the proposed model

3. Metric Based Analysis of Proposed Model

In this paper, we calculate the values of the Chidamber and Kemerer (CK) metrics and Metric for Object Oriented Design (MOOD) metrics [12]. Some metrics of the CK metrics are discussed below:

ISSN: 2454-1907
DOI: 10.5281/zenodo.1117165

- **NOA** (Number of Attributes): It represents the total number of attributes of the classes.
- **WMC** (Number of Methods): It represents the total number of methods present in the classes.
- **CBO** (Coupling between Objects): It counts the number of other classes to which the particular class is coupled.
- **RFC** (Response for a class): It calculates the number of methods that can be invoked in response to a message in that class.

Table 1: Metric values according to the proposed model

Object Oriented Metrics	Classes of proposed model				
	HuffmanTree	**HuffmanEncoder**	**AESencryption**	**Node**	**StegoMain**
NOA	6	6	3	3	23
NOM	4	1	4	0	12
CBO	2	2	1	2	3
RFC	16	13	16	5	21

Now, we will graphically represent the above values and discuss on these:

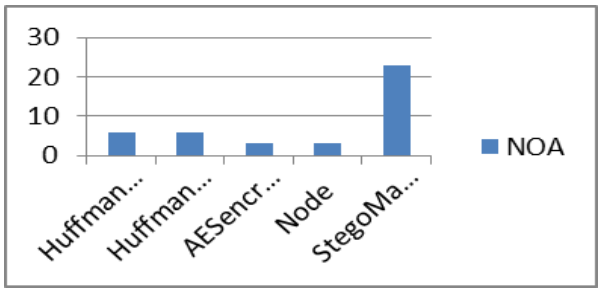

Figure 2: values of NOA metrics

Fig2 shows the metric values of NOA of all the classes used in our proposed model. NOA is used for making an estimate about the required time and effort to maintain a class. Here we can see the maximum value is 23, which is okay.

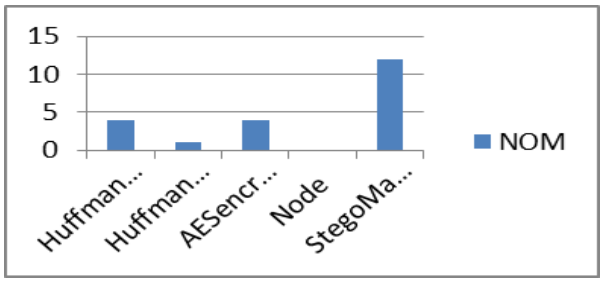

Figure 3: values of NOM metrics

Figure 3 shows the values of the metric NOM of all the classes used in our proposed model. NOM is also used in making estimation about the required time and effort to maintain a class. Here we can see the maximum value is 12, which indicates that the system is easy to maintain.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1117165

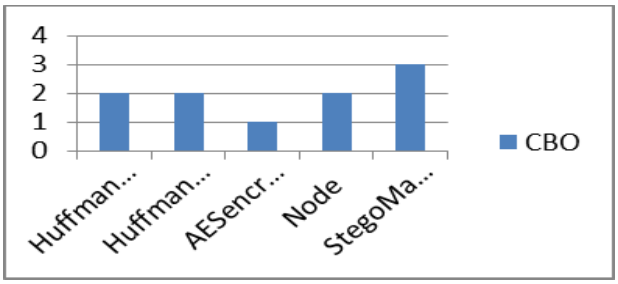

Figure 4: values of CBO metrics

Fig4 shows the values of CBO metrics of all the classes. The value of 0 means the class is not a part of the system. The value ranged between 1 to 4 is good [13], which indicate that the system is loosely coupled.

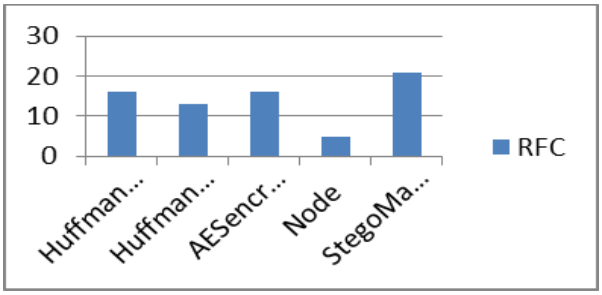

Figure 5: Values of RFC metrics

Fig.5 shows the value of the metric RFC. It is calculated using the formula {M}U{Ri}, for all i, {Ri}=Set of methods called by i and {M}=Set of all methods in the class. If the value increases then it becomes difficult to understand the complexity of the class and if it keeps low, then the polymorphism becomes greater. Here the optimal value of RFC is found.

Now, we calculate the values of the MOOD metrics in the following section:

Equation for **AHF**=$\sum_{i=1}^{TC} A_h(C_i) / \sum_{i=1}^{TC} A_d(C_i)$

$A_d(C_i)= A_v(C_i)+ A_h(C_i)$, where $A_d(C_i)$= total attributes defined in class C, $A_v(C_i)$= Attributes visible in class C and $A_h(C_i)$= attributes hidden in class C.

Table 2: Value of AHF of proposed model

	Classes of proposed system					
	HuffmanTree	**HuffmanEncoder**	**AESencryption**	**Node**	**StegoMain**	**Summation (∑)**
$A_h(C_i)$	3	0	0	0	3	6
$A_v(C_i)$	3	6	3	3	20	35
$A_d(C_i)$	6	6	3	3	23	41
AHF	6/41=0.146					

The AHF value of our proposed model is 0.146, shown in Table2 that lies in between 0 and 1, which is acceptable.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1117165

Equation for **MHF**=$\sum_{i=1}^{TC} M_h(C_i) / \sum_{i=1}^{TC} M_d(C_i)$ //TC means total number of class

Where $M_d(C_i)= M_v(C_i)+ M_{h`}(C_i)$ where $M_d(C_i)$= methods defined in class C, $M_v(C_i)$= methods visible in class C and $M_{h`}(C_i)$= methods hidden in class C

Table 3: Value of MHF of proposed model

	Classes of proposed system					
	HuffmanTree	**HuffmanEncoder**	**AESencryption**	**Node**	**StegoMain**	**Summation(∑)**
$M_h(C_i)$	1	0	0	0	0	1
$M_v(C_i)$	3	1	4	0	12	20
$M_d(C_i)$	4	1	4	0	12	21
MHF	1/21=0.048					

The value of MHF of our proposed model is calculated by using Table3, which is 0.048. Low value of MHF means insufficiently abstracted implementation and high MHF indicates the less functionality. So, this value is okay [14].

Equation for **AIF**=$\sum_{i=1}^{TC} A_i(C_i) / \sum_{i=1}^{TC} A_a(C_i)$

Where $A_a(C_i)= A_d(C_i)+ A_i(C_i)$, $A_a(C_i)$=number of attributes available, $A_d(C_i)$= number of attributes defined and $A_i(C_i)$= number of attributes inherited

Table 4: Value of AIF of proposed model

	Classes of proposed system					
	HuffmanTree	**HuffmanEncoder**	**AESencryption**	**Node**	**StegoMain**	**Summation(∑)**
$A_d(C_i)$	6	6	3	0	23	38
$A_i(C_i)$	26	23	23	6	0	78
$A_a(C_i)$	32	29	26	6	23	116
AIF	78/116=0.672					

The value of AIF is 0.672, that is shown using Table4. If the value of AIF is 0, then it means lack of inheritance but here the value is greater than 0 and less than 1, which is acceptable.

Equation for **MIF**=$\sum_{i=1}^{TC} M_i(C_i) / \sum_{i=1}^{TC} M_a(C_i)$

Where $M_a(C_i)= M_d(C_i)+ M_i(C_i)$, $M_a(C_i)$=number of methods available, $M_d(C_i)$= number of methods defined and $M_i(C_i)$= number of methods inherited

Table 5: Value of MIF of proposed model

	Classes of proposed system					
	HuffmanTree	**HuffmanEncoder**	**AESencryption**	**Node**	**StegoMain**	**Summation(∑)**
$M_d(C_i)$	4	1	4	0	12	21
$M_i(C_i)$	12	12	12	1	0	37
$M_a(C_i)$	16	13	16	1	12	58
MIF	37/58=0.638					

ISSN: 2454-1907
DOI: 10.5281/zenodo.1117165

The value of MIF is 0.638, that is shown using Table5. If the value of MIF, like the value of AIF, is 0, then it means lack of inheritance but for our proposed model, the value is greater than 0 and less than 1, which is acceptable.

4. Conclusion

The object oriented metric based analysis of our proposed model ensures the improvement of authenticity and secrecy. In any kind of e-learning systems, other than e-learning, like e-commerce, e-governance everywhere text documents are very essential and should keep secure from the outside world. This analysis has done based on some of the metrics under Ck metric and MOOD metric to achieve the facilities of object oriented design over traditional design. Here other encryption algorithms other than AES can be implemented, but AES is easy to implement in both hardware and software and also more secure than some other encryption techniques.

References

[1] Weippl, R.E (2005), Security in E-Learning, Springer
[2] N.Rani and J.Chaudhury, "Text steganography techniques: A review", International Journal of Engineering Trends and Technology (IJETT), July-2013, vol-4(7), ISSN: 2231-5381, PP: 3013-3015
[3] M.Kwan, "SNOW", Darkside Technologies Pty Ltd CAN 082 444 246 Australia, 1998
[4] S.Mansor, R.Din and A.Samsudin, "Analysis of natural language steganography", International journal of computer science and security (IJCSS), vol:3(2), pp:113-125
[5] http://www.geeksforgeeks.org/greedy-algorithms-set-3-huffman-coding
[6] Edward V. Berard, Metrics for Object-Oriented Software Engineering, The Object Agency, Inc.
[7] Balagurusami E., Object oriented programming with C++ (Tata McGraw Hill, New Delhi, 2006)
[8] http://ce.sharif.ir/courses/85-86/1/ce924/resources/root/4.%20Kamandi_OOMetrics.pdf
[9] https://en.wikipedia.org/wiki/Class_diagram
[10] Kh A.Islam, S.Banerjee, S.Karforma and A.Nag, "Securing Text Transmission in E-learning through Natural Language Steganography: An Object Oriented Approach", October 17 Volume 3(10) , International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRSCE), ISSN: 2454-4248, pp:234-237
[11] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[12] S.Banerjee and S.Karforma, "Object oriented metric based analysis of space efficient LSB based steganography including compression for securing transmission of e-learning documents", International journal of mechanical and production engineering research and development (IJMPERD), ISSN:2249-6890, June- 2017, vol-7(3), pp-11-18
[13] http://support.objecteering.com/objecteering6.1/help/us/metrics/metrics_in_detail/coupling_between_object_classes.htm
[14] http://www.aivosto.com/project/help/pm-oo-mood.html

*Corresponding author.
E-mail address: bansoumendu @ gmail.com