International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-8 Issue-11, September 2019

OO Metric Analysis of Optimally Sparse LSB-Based Steganography in E-Learning Environment

Soumendu Banerjee, Sunil Karforma

***Abstract:** In an e-Learning environment, the communication between sender and receiver has been done via Internet. In general, while the sender sends their important documents to receiver through Internet, he/she encrypts the document which is decrypted by the receiver(s) at their end. In case of large images, decryption causes some sort of distortion, which may be overcome through our proposed model. The object oriented analysis of a system helps to make better understanding and cop up with the real world. The main characteristics of object oriented metric analysis are data hiding, data encapsulation, data abstraction, polymorphism etc. Here we calculate the values of different metrics like CK and MOOD metrics based on the class diagram of our proposed model regarding the transmission of documents from administrator to learner.*

***Keywords:** e-Learning, LSB based steganography, class hierarchy diagram, CK metric, MOOD metric*

I. INTRODUCTION

In general, in an e-Learning environment, the sender sends the documents after applying encryption. Whenever the receiver decodes the received encrypted documents, some sort of distortion is obvious. In our proposed model, we have overcome this problem with the help of Least Significant Bit steganographic approach. In this paper, we have analyzed the performance of our proposed model with the help of some metric analysis techniques, like Chidamber and Kemerer Metrics, Metrics for Object Oriented Design, Lorenz and Kidd[1,2] etc. These metric analyses can also be categorized based on size, cohesion, coupling, inheritance and so on. The performance analysis is important to make sure whether the system is compatible with the real world system or not. We have analyzed the metric values based on the transmission of payload image hiding into a cover image from the administrator to learner in an e-Learning environment, i.e., the learner will decrypt the document by applying decoding process and verify it for originality[3].
Section II covers the class hierarchy diagram[4] of the proposed optimal steganography approach. Section III includes the analysis of the metric values based on the class diagram of the proposed model and finally, we have concluded in section IV.

II. CLASS HIERARCHY DIAGRAM

Class diagram is a static UML diagram which helps the user in visualizing, describing and documenting different aspects of a system and also helps in implementing executable code of the software application. The class diagram of the proposed optimal LSB steganography model[5] is shown in figure1.

Revised Manuscript Received on September 07, 2019
Soumendu Banerjee, Assistant Professor, Department of Computer Science, St. Xavier's College, Burdwan.W.B. (India)
Sunil Karforma, Professor, Department of Computer Science, The University of Burdwan.W.B. (India)

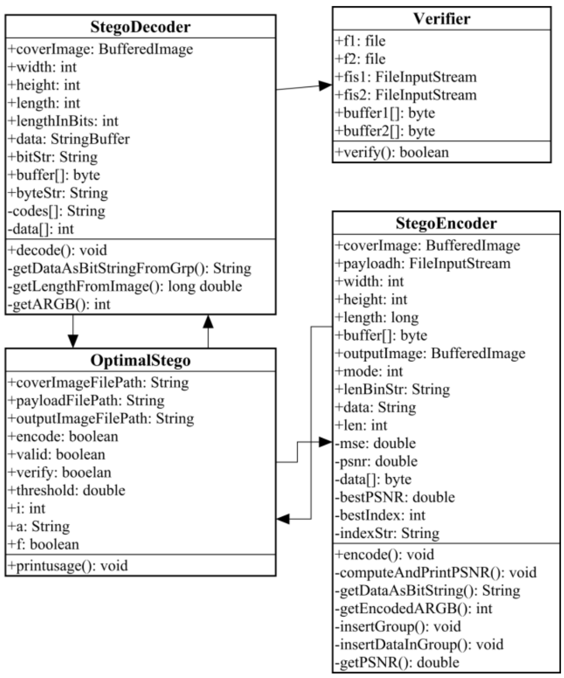

Figure1: Class diagram of proposed model

In the above class diagram, we have used four classes, namely, OptimalStego, StegoEncoder, StegoDecoder and Verifier.

Class OptimalStego
This class is the main class and it is inherited by the classes StegoEncoder and StegoDecoder. OptimalStego contains ten public data members and one public member function, which are used to help the user regarding the encoding and decoding process. This is used as the base class. The member function of this class is given below.
printusage(): This function is used to help the user to make the system run.
Class Verifier
It is used to check whether the file is attacked by noise or hacker while transmitting from administrator to learner. If any kind of attack occurs, then the position will be altered and affect the stego image. Class Verifier contains six public data members and one public member function. The member function of this class is given below.
verify(): This function is used to verify the image for originality.
Class StegoEncoder
This class contains the functions for embedding the secret image into the cover image which happens at the administrator's (i.e., sender) end. The following are the member functions of this class.
encode(): It is used to encode the secret image into cover image.

computeAndPrintPSNR(): It is used to search for best PSNR value of individual cases.
getDataAsBitString():This function converts an array of bytes to a binary string.
*getEncodedARGB():*This function stores the first 6 bits of the data into the color value.
insertGroup(): It is used for embedding the secret image into cover image.
insertDataInGroup(): It is used for inserting data into group.
getPSNR(): This function is used for calculating PSNR after embedding secret image into cover image for quality measurement of cover image after reconstruction.

Class StegoDecoder

This class is used for extracting the secret image from the stego image and it happens at the learner's end. It contains nine public and two private data members, one public and three private member functions. We mention below the member functions of this class.
decode(): This function is used for decoding the encoded image.
getDataAsBitStringfromGroup(): This function deals with images in RGB format.
getLengthFromImage(): It is used to find the length of the image at the time of decoding.
getARGB(): This function is used to convert the image into RGB format.

III. PERFORMANCE ANALYSIS

Based on the above class diagram(figure1), we have calculated the metric values[6,7], which have shown using the following tables[8,9].

NOA denotes the number of attributes

NOM denotes the number of methods

CBO denotes the number of other classes to which the class is coupled

DIT denotes the maximum path from the node to the root in the inheritance tree

NOC denotes the number of subclasses inherits the methods of the parent class

RFC= {M} U all i {Ri}, where where{ Ri} is the set of methods called by method i and { M } = set of all methods in the class.

Table1: CK metric values for Optimal LSBS model

Object-Oriented Metrics	Classes of proposed model			
	Stego Encoder (SE)	StegoDecoder (SD)	Verifier (VF)	OptimalStego (OS)
NOA	17	11	6	10
NOM	7	4	1	1
DIT	1	1	2	0
CBO	1	2	1	2
NOC	0	1	0	2
RFC	7	6	2	3

Designs of the above classes are represented in the following column charts.

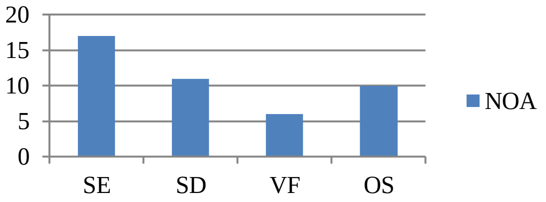

Figure2. NOA of Optimal LSBS model

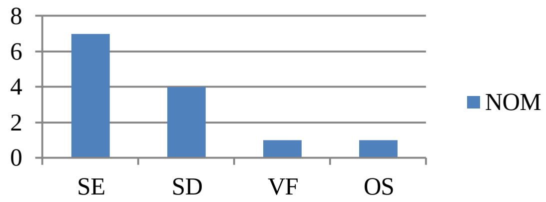

Figure3. NOM of Optimal LSBS model

Figure2 and Figure3 shows the metric values of NOA and NOM of all the classes used in our proposed model, which should be kept down. So these values of our proposed model are satisfactory.

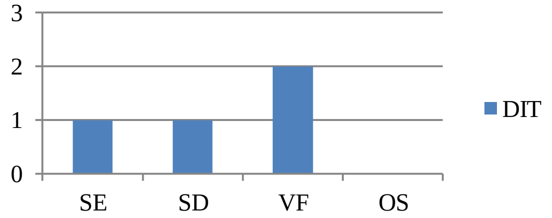

Figure4. DIT of Optimal LSBS model

Figure4 shows the values of DIT metrics which ranges between 1 and 2 and this indicates that the system is easy to maintain.

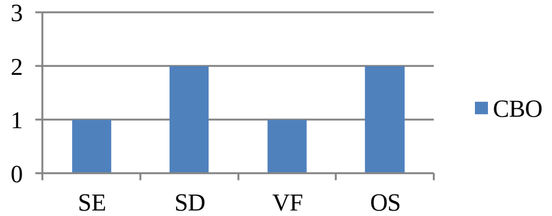

Figure5. CBO of Optimal LSBS model

Figure5 shows the values of CBO metrics of proposed model. The value ranges between 1 and 2 and this indicates that the system is loosely coupled which is a property of good design.
system is easy to maintain.

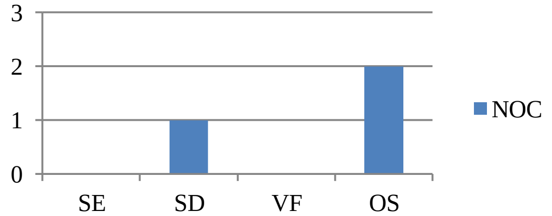

Figure6. NOC of Optimal LSBS model

Figure6 shows the values of NOC metrics of proposed model. The maximum value is 2.

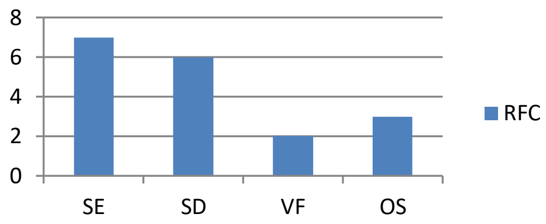

Figure7. RFC of Optimal LSBS model

Figure7 shows the values of the metric RFC. Here the maximum value is 7 and minimum is 2, which is acceptable.

MOOD metric analysis of proposed model

In the following section, we will calculate the values of the MOOD metrics.

Attribute Hiding Factor (AHF) of proposed model

Table2: Value of AHF of Optimal LSBS model

	Classes of proposed system				
	Stego Encoder	**StegoDecoder**	**Verifier**	**OptimalStego**	**Summation(∑)**
$A_h(C_i)$	6	2	0	0	8
$A_v(C_i)$	11	9	6	10	36
$A_d(C_i)$	17	11	6	10	44
AHF	8/44=0.181				

The AHF value of our proposed model, as shown in Table2, is 0.181 which lies between 0 and 1 and so is acceptable.

Method Hiding Factor (MHF) of proposed model

Table3: Value of MHF of proposed model

	Classes of proposed system				
	Stego Encoder	**StegoDecoder**	**Verifier**	**OptimalStego**	**Summation(∑)**
$M_h(C_i)$	6	3	0	0	9
$M_v(C_i)$	1	1	1	1	4
$M_d(C_i)$	7	4	1	1	13
MHF	9/13=0.692				

The value of MHF of our proposed model, as shown Table3, is 0.692 and this is reasonable.

Attribute Inheritance Factor (AIF) of proposed model

Table4: Value of AIF of Optimal LSBS model

	Classes of proposed system				
	Stego Encoder	**StegoDecoder**	**Verifier**	**OptimalStego**	**Summation(∑)**
$A_d(C_i)$	17	11	6	10	44
$A_i(C_i)$	10	16	9	20	55
$A_a(C_i)$	27	27	15	30	99
AIF	558/99=0.55				

The value of AIF, as shown using Table4, is 0.55 and this is acceptable.

Method Inheritance Factor (MIF) of Optimal LSBS model

Table5: Value of MIF of Optimal LSBS model

	Classes of proposed system				
	Stego Encoder	**StegoDecoder**	**Verifier**	**OptimalStego**	**Summation(∑)**
$M_d(C_i)$	6	4	1	1	12
$M_i(C_i)$	1	2	1	1	5
$M_a(C_i)$	7	6	2	2	17
MIF	5/17=0.294				

The value of MIF is 0.294, as shown in Table5, which lies between 0 and 1 and thus, it is acceptable.

IV. CONCLUSION

We have analyzed the value of the object oriented metrics to achieve flexibility regarding the transmission of encrypted documents from the sender to receiver in an e-learning system. The same model can also be applied in other online transactions like e-Commerce or e-Governance, where the receiver needs the original data without any kind of distortion.

REFERENCES:

1. K.K.Aggarwal, Y. Singh, A. Kaur, R. Malhotra, "Empirical study of object oriented metrics", Journal of Object Technology, ETH Zurich, Chair of Software Engineering, Vol. 5(8), November-December 2006, pp: 149-173
2. A.Kamandi, "Object Oriented Metrics", Sharig University of technology, spring 2007
3. S.Banerjee, "Object Oriented Modeling of Optimal LSB-based Steganography for Secure Transmission of E-learning Documents", International Journal of Computer Sciences and Engineering, Vol-7(1), January-2019, pp: 208-214
4. Rajib Mall, Fundamentals of Software Engineering (Prentice Hall of India, New Delhi, 2006)
5. S.Banerjee, A.Nag, Kh.A.Islam, S.Karforma, "Optimally Sparse LSB-based Steganography for Secure Transmission of E-learning related Documents", IJRECE, Vol-7(1), January-March-2019, pp: 2458-2467
6. S. Karforma and S. Banerjee, "Object oriented metric based analysis of ElGamal digital signature algorithm for study material authentication", IJSTM, vol-4(1), sept-15, pp: 522-530
7. S.Banerjee, S.Karforma, "Object Oriented Metrics Based Analysis of DES algorithm for secure transmission of Mark sheet in E-learning", IJCSE, Vol-4(1), February-2016, pp: 093-098
8. http://ce.sharif.edu/courses/8586/1/ce924/resources/root/4.%20Kamandi_OOMetrics.pdf
9. S.Muktamyee, "An overview of Object Oriented Design Metrics", (Master Thesis) Department of Computer Science, Umeå University, Sweden June 23, 2005.

AUTHORS PROFILE

Dr. Soumendu Banerjee has completed his B.Sc(H) in Mathematics, MCA and PhD in the field of authentication issues in e-Learning from The University of Burdwan. Now, he is acting as a contractual lecturer at St. Xavier's College, Burdwan. He has published more than fifteen National/International journal papers and conference proceedings. His fields of research interest include cryptography, digital watermarking, digital certificate, digital watermarking and steganography.

Dr. Sunil Karforma has completed B.E. (Computer Science and Engineering) and M. E. (Computer Science and Engineering) from Jadavpur University. He has completed Ph. D. in the field of Cryptography. He is presently holding the post of Professor and the Head of the Department in the Department of Computer Science, The University of Burdwan. Network security, e-commerce, e-learning and e-governance are his field of interest in research area. He has published approximately 90 research papers in reputed National and International journals and proceedings.