

# A Procedure of Text Steganography Using Indian Regional Language

Indradip Banerjee

Department Computer Science & Engineering, University Institute of Technology,  
Burdwan University, Burdwan, India  
ibanerjee2001@yahoo.com

Souvik Bhattacharyya

Department Computer Science & Engineering, University Institute of Technology,  
Burdwan University, Burdwan, India  
souvikbha@gmail.com

Gautam Sanyal

Department of Computer Science and Engineering, National Institute of Technology,  
Durgapur, West Bengal, India.  
nitgsanyal@gmail.com

**Abstract** — In this paper we present a work of text steganography. Now a days, maintain the security of the secret information has been a great challenge. Sender can send messages habitually through a communication channel like Internet, draws the attention of third parties, hackers and crackers, perhaps causing attempts to break and expose the unusual messages. Steganography is a promising region which is used for secured data transmission over any public media. Substantial amount of research work has been accepted by different researchers on steganography. In this paper, a text steganography procedure has been planned with the help of an Indian regional language i.e. Oriya language. Text steganography together with quantum approach based on the use of two specific characters and two special characters like invited comas (opening and closing) in Oriya language and mapping technique of quantum gate truth table have been used.

**Index Terms** — Text Steganography, Quantum Steganography, Security, Cover Text, Stego Text

## I. INTRODUCTION

Information hiding is the ability to prevent or hidden certain aspects from being accessible to others excluding authentic user. It has many sub disciplines. One of the most important sub disciplines is steganography [2] which is derived from a work by Johannes Trithemus (1462-1516) entitled "Steganographia" and comes from the Greek language defined as "covered writing" [3]. It is an ancient art of hiding information in ways a message is hidden in an innocent-looking cover media so that will not arouse an eavesdropper's suspicion. Steganography diverges from cryptography in the sense that where cryptography focuses on keeping the contents of a

message secret by encryption technique, steganography focuses on keeping the presence of a message secret [20], [21].

Another form of information hiding is digital watermarking, which is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video or text only [22], [23]. A hidden channel could be defined as a communications channel that transfers some kind of information using a method originally not intended to transfer this kind of information. Observers are unaware that a covert message is being communicated. Only the sender and recipient of the message notice it. Steganography works have been carried out on different media like images, video clips, text, music and sound [24], [21].

In Image Steganography method the secret message is embedded into an image as noise to it, which is nearly impossible to differentiate by human eyes [25], [26], [7]. In video steganography, same method may be used to embed a message [6], [5]. Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range [7]. One major category, perhaps the most difficult kind of steganography is text teganography or linguistic steganography because due to the lack of redundant information in a text compared to an image or audio. The text steganography is a method of using written natural language to conceal a secret message as defined by Chapman et al. [4].

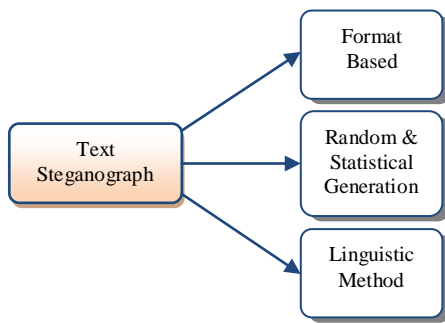


Figure 1: Types of Steganography

A. Quantum Steganography

Comparatively very little research work has been done in quantum steganography also. The idea of hiding secret messages as the error syndromes of a quantum error-correcting code (QECC) was introduced by Julio Gea-Banacloche in [28]. In his work Alice and Bob use the three-bit repetition code to transmit messages to each other using a shared secret key. All the noise in the channel that Eve perceives is because of these deliberate errors that Alice applies. In his model he assumes that Alice and Bob share a binary-symmetric channel. This work does not address the issue of whether the errors would resemble a plausible channel, nor does it consider the case where the channel contains intrinsic noise. Natori gives a simple treatment of quantum steganography which is a modification of super-dense coding [29]. Martin introduced a notion of quantum steganographic communication based on a variation of Bennett and Brassard's quantum-key distribution (QKD), hiding a steganographic channel in the QKD protocol [30]. Curty e.al. proposed three different quantum steganographic protocols [31].

B. Quantum gate [19]

Quantum circuit model of computation in quantum computing [10] [1] [9], a quantum gate or quantum logic gate is a basic quantum circuit which operates on a small number of qubits. They are the building blocks of quantum circuits, like classical logic gates are basically for conventional digital circuits. Quantum logic gates are reversible like other classical logic gates. However, classical computing can be performed by the help of only reversible gates. Quantum gates are represented as matrices. A gate which acts on  $k$  qubits is represented by a  $2^k \times 2^k$  unitary matrix. The number of qubits in the input and output of the gate is equal. There are various types of quantum gates are represent the qubits. They are Hadamard gate, Pauli-X gate, Pauli-Y gate, Pauli-Z gate, Phase shift gates, Swap gate, Controlled gates, Toffoli gate, Fredkin gate, etc. Here we use Controlled gates to represent the qubits and control the operations.

NOT	<0>	<1>
<0>	0	1
<1>	1	0

Figure 2: NOT Gate Truth Table

C. Reversible Classical Logic [19]

The first concepts of the reversibility of computation were raised in the 1970s. There were two issues which are logical reversibility and physical reversibility, both were intimately connected. Logical reversibility reconstructs the input from the output of a computation or gate function. The NAND gate is explicitly irreversible, it has two inputs and one output, while the NOT gate is reversible (it's own inverse). In case of Physical reversibility the NAND gate has only one output, one of it's inputs has effectively been erased in the process, whose information has been irretrievably lost. The change in entropy that we would associate with the lost of one bit of information is  $\ln 2$ , which, thermodynamically, corresponds to an energy increase of  $kT \ln 2$ , where  $k$  is Boltzman's constant and  $T$  is the temperature. The heat dissipated during a process is usually taken to be a sign of physical irreversibility, that the microscopic physical state of the system cannot be restored exactly as it was before the process took place. Reversible logic gates are symmetric with respect to the number of inputs and outputs. The reversible NOT gate, whose truth table is given in Fig. 2. It can also write this in the form of a matrix, or as a graphic. The matrix form lists the lines in the truth table in the form  $\langle 0 \rangle, \langle 1 \rangle$ . The matrix field with 1's and 0's such that each horizontal or vertical line has exactly one 1, which is to be interpreted as a one-to-one mapping of the input to the output. A two-bit gate closely related to the NOT gate is the two-bit Controlled-NOT (or C-NOT) gate. Controlled-NOT gate shows in Fig. 3, performs a NOT on the second bit if the first bit is  $\langle 1 \rangle$ , but otherwise has no effect. The C-NOT is sometimes also called XOR, since it performs an exclusive OR operation on the two inputs bits and writes the output to the second bit.

C-NOT	<00>	<01>	<10>	<11>
<00>	1	0	0	0
<01>	0	1	0	0
<10>	0	0	0	1
<11>	0	0	1	0

Figure 3: NOT Gate Truth Table

The Controlled NOT gate (also C-NOT or CNOT) is a quantum gate that is an essential component in the construction of a quantum computer. The proof of operation [32] is given below:

Let  $\left\{ \begin{matrix} |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{matrix} \right\}$  be the orthonormal basis.

Let  $|\psi\rangle = x|0\rangle + y|1\rangle = \begin{bmatrix} x \\ y \end{bmatrix}$

and  $|\phi\rangle = y|0\rangle + x|1\rangle = \begin{bmatrix} y \\ x \end{bmatrix}$ .  $|\phi\rangle$  be the flip

qubit of  $|\psi\rangle$ .

Recall that  $|\alpha\rangle \otimes |\beta\rangle = |\alpha\rangle|\beta\rangle = |\alpha, \beta\rangle \dots(1)$

**i. When control qubit is 0**

First, we shall prove that:  $CNOT|0, \psi\rangle = |0, \psi\rangle$

Before we compute, however, note that our specific definition of  $CNOT$  assumes an eigen basis of

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Then, it's not difficult to verify

$$\text{that } |0, \psi\rangle = x|0\rangle|0\rangle + y|0\rangle|1\rangle = \begin{bmatrix} x \\ y \\ 0 \\ 0 \end{bmatrix} \dots(2)$$

Then

$$CNOT|0, \psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} x \\ y \\ 0 \\ 0 \end{bmatrix} = |0, \psi\rangle \dots(3)$$

Therefore  $CNOT$  doesn't change the  $|\psi\rangle$  qubit if the first qubit is 0.

**ii. When control qubit is 1**

Now, we shall prove that  $CNOT|1, \psi\rangle = |1, \phi\rangle$ , which means that the  $CNOT$  gate flips the  $|\psi\rangle$  qubit. Similarly to the first demonstration, we

have  $|1, \psi\rangle = \begin{bmatrix} 0 \\ 0 \\ x \\ y \end{bmatrix}$ .

$$\text{Then } CNOT|1, \psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ x \\ y \end{bmatrix} = x \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} + y \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \dots (4)$$

As we can see that  $|1,1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$  and  $|1,0\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$ ,

using these on the equation above gives

$$CNOT|1, \psi\rangle = x|1,1\rangle + y|1,0\rangle = |1, \phi\rangle \dots (5)$$

Therefore the  $CNOT$  gate flips the  $|\psi\rangle$  qubit into  $|\phi\rangle$  if the control qubit is set to 1. A simple way to observe this is to multiply the  $CNOT$  matrix by a column vector, noticing that the operation on the first bit is identity, and a NOT gate on the second bit.

**D. Text Steganography**

The affluence of electronic documented information available in the world as well as the exertion of serious linguistic analysis makes this an interesting medium for steganographic information hiding. Moreover the Text is one of the ancient media used in steganography. Letters, books and telegrams hide secret messages within their texts in earlier time i.e. before the electronic age comes. Text steganography refers to the hiding of information within text i.e. character-based messages. There are three basic categories of text steganography (Fig. 1) maintained here: format-based methods, random and statistical generation and linguistic methods. [8]

**i. Format-based methods [8]:** This methods use the physical formatting of text as a space in which to hide information. Format-based methods usually modify existing text for hiding the steganographic text. Insertion of spaces or non-displayed

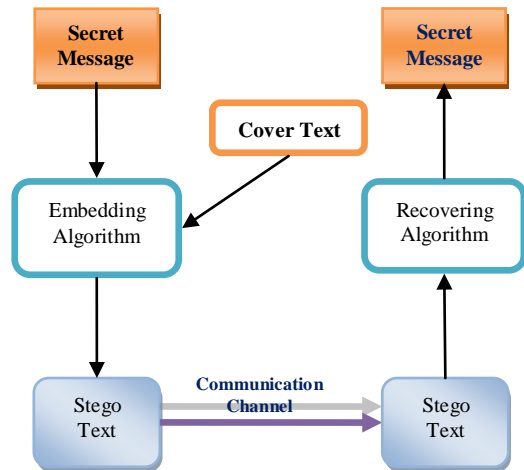


Figure 4: Mechanism of Text Steganography

characters, careful errors tinny throughout the text and resizing of fonts are some of the many format-based methods used in text steganography.

**ii. Random and statistical generation method [8]:**

This avoid comparison with a known plaintext, steganographers often resort to generating their own cover texts. Character sequences method hide the information within character sequences.

**iii. Linguistic methods [8]:**

The affluence of electronic documented information available in the world as well as the exertion of serious linguistic analysis makes this an interesting medium for steganographic information hiding.

Fig. 4 shows the mechanism of text steganography. Firstly, a secret message will be covered up in a cover-text by applying an embedding algorithm to produce a stego-text. The stego-text will then be transmitted by a communication channel to a receiver.

In this paper, an approach of quantum text

steganography using Oriya character mapping method has been proposed based on the use of some special character. Here the quantum truth table also mapped to increase the security level and complexity. In this method the length of the stego and the cover are same so prediction of existence of message is difficult in view of that characteristics, so this one is the unique method which has been developed in this steganography approach.

ASCII	Character	ASCII	Character		
107	୩	34	'	0	0
107	୩	39	'	0	1
109	୩	34	'	1	0
109	୩	39	'	1	1

Figure 5: Mapping Technique

The proposed scheme has been enthused by the author's previous work [11], [12], [13], [14], [15], [16], [17], [18] on various approaches of steganography methods. The quantum truth table approach has been incorporated from previous work [18].

This paper is organized into the following sections. Section II describes the proposed model. Algorithms of various processes like embedding, extracting and GUI are discussed in Section III. Analyses of the results are in section VI. The last section describes the concluded part of the work.

II. THE PROPOSED MODEL

Text steganography, whatever this paper exactly deals with, uses regional language, specifically the Oriya text as the medium where to hide information. Here the explanation of text steganography remains wide in order to differentiate it from the more specific "linguistic steganography". Text steganography can involve anything from changing the ASCII character from the specific position of an existing text.

The input messages can be in any digital form and are often treated as a bit stream. Pick two pair of this bit stream of message one by one. Then select the proper Oriya Text as cover and change it to it's equivalent binary code. Then a matrix formed with the help of message length and map the C-NOT truth table (how to map it, shown in Fig. 6) from left most corner in a sequence (vertically or horizontally), after that start embedding one by one if the mapped value showing not '1' value. After that secret message has been embed to the cover text by replacing the next ASCII of "୩" and "୩" by ASCII 34 i.e. [ ' ] and 39 i.e. [ ' ] in Oriya language based on the mapping information given in Fig. 5 to generate the stego text. By the help of replacing technique the stego length are being same as cover. At the

receiver side with the help of same mapping algorithm and other different reverse operation has been carried out to get back the original information.

Figure 6: Quantum Truth Table Mapping

A. Solution Methodology

The proposed system involves two windows i.e. SENDER SIDE and RECEIVER SIDE. The user will be someone who is aware with the process of information hiding and will have adequate knowledge of steganography systems. The user have a duty to select a plain text message from a file, another Oriya text to be used as the carrier (cover text) and then use the proposed embedding method which will hide the message in the selected cover text and will procedure the stego text. The user at the receiver side should be able to extract the message from the stego text with the help of different reverse process in chronological manner to un-hide the message from the stego text. The GUI of the proposed solution has been shown in Fig. 7.

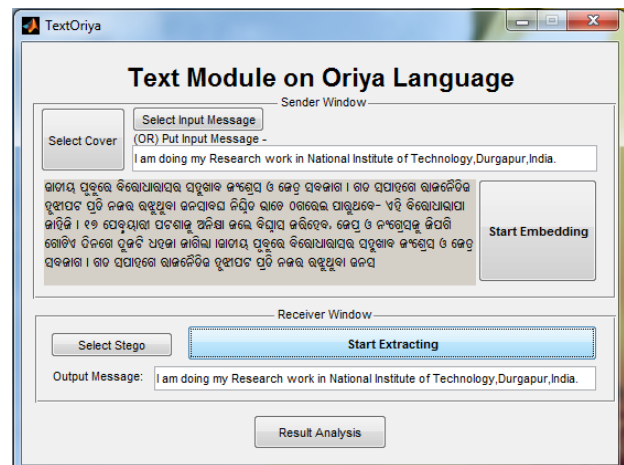


Figure 7: GUI Representation



III. ALGORITHMS

In this section, algorithms for different processes used both in the sender side and receiver sides are described which are furnished below:

A. Algorithm for Message Embedding

- Select the message & Oriya cover. Check whether the selected text is capable of embedding. If not possible repeat this step otherwise continue.
- Map the quantum C-NOT gate to the matrix MATMSG (N x N) vertically or horizontally & Put the message value by replacing '0' in the matrix MATMSG.
- Check the message sequence and pick first two bit sequence (MSG). Start from the first character of the cover text (TX).
- Start checking & embedding.
  - If MSG='11' & character "ଲ" from the TX then change from ASCII (109,254) to (109,39)
  - Else If MSG='10' & character "ୠ" from the TX then change from ASCII (109,254) to (109,34)
  - Else If MSG='01' & character "ୡ" from the TX then change from ASCII (107,254) to (107,39)
  - Else If MSG='00' & character "ୢ" from the TX then change from ASCII (107,254) to (107,34)
- Repeat the above step for the remaining bit sequence of the message and prepare the stego text.

B. Algorithm for Message Extracting

- Select the stego text put in MATMSG (N x N) matrix and map the quantum C-NOT gate to the matrix vertically or horizontally.
- Extract the message value from '0' Th position of C-NOT. Pick values one by one from MATMSG and create MSG.
- Select the stego text TX.
  - If "ଲ" and next ASCII is 39, MSG='11'.
  - Else If "ୠ" and next ASCII is 34, MSG='10'.
  - Else If "ୡ" and next ASCII is 39, MSG='01'.
  - Else If "ୢ" and next ASCII is 34, MSG='00'.

C. Algorithm of GUI in Sender side

- Select the Cover Text from the set of Text files.
- Check whether the selected text is capable to do the embedding or not. If not possible then error.
- Select the message in text form.
- Embed the encrypted message in the cover text to form the stego text.

D. Algorithm of GUI in Receiver side

- Receive the text with embedded message along with positions.

Extract the encrypt form of message from the Stego Text.

IV. RESULTS ANALYSIS

There are mainly three phases that should be reserved into account when discussing the results of the proposed method of text steganography with the help of Oriya Language. The authors simulated the proposed system and the results are shown in the Fig. 8, 9 and 10. This method satisfies both security aspects and hiding capacity requirements. It generates the stego text with minimum degradation which is not very revealing to people about the existence of any hidden data, maintaining its security to the eavesdroppers. Besides the security level has amplified through the encoding of the secret message

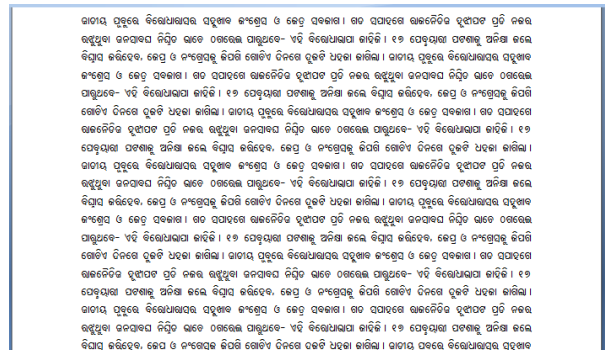


Figure 8: Cover Text

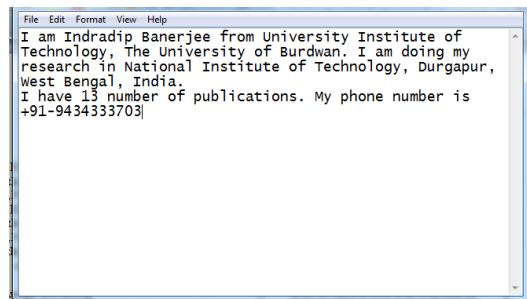


Figure 9: Secret Message

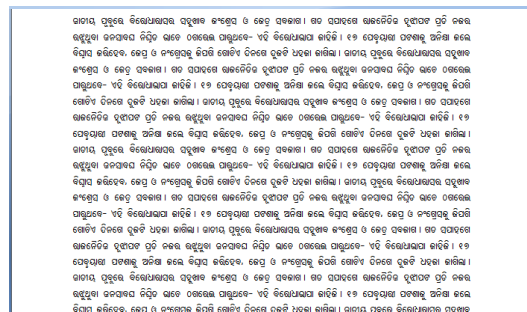


Figure 10: Stego Text

MESSAGE LENGTH (In Character)	CORRELATION VALUE
10	0.99978
50	0.99888
100	0.99776
150	0.99665
200	0.99553
250	0.99442
300	0.99330
350	0.99218
400	0.99107

500	0.98884
1000	0.97772
2000	0.95561

Figure 11: Correlation values of cover and stego text in different length of message

before embedding operation. This method hides two bit per word in the cover text which reflects the high embedding capacity of the system. Although the embedding capacity of the proposed method depends upon the embedding sequence, pattern of the cover text. This method hides two bit per word in the cover text which reflects the high embedding capacity of the system. Although the embedding capacity of the proposed method is depends upon the Oriya characters. In this method the length of the stego and cover are same and unchanged. So due to the said reason the steganalysis part can also handle.

A. Similarity Measure

For comparing the similarity between cover text and the stego text, the Correlation method for measuring similarity between two strings has been computed. The Correlation [27] is a measure of similarity between two strings.

*Correlation:* The most familiar measure of dependence between two quantities is the Pearson product-moment correlation coefficient [27], or “Pearson’s correlation”. It is obtained by dividing the covariance of the two variables by the product of their standard deviations. Karl Pearson developed the coefficient from a similar but slightly different idea by Francis Galton. The Pearson correlation is +1 in the case of a perfect positive (increasing) linear relationship (correlation), -1 in the case of a perfect decreasing (negative) linear relationship (anticorrelation)[27] and some value between -1 and 1 in all other cases, indicating the degree of linear dependence between the variables. As it approaches zero there is less of a relationship (closer to uncorrelated). The closer the coefficient is to either -1 or 1, the stronger the correlation between the variables. If the variables are independent, Pearson’s correlation coefficient is 0, but the converse is not true because the correlation coefficient detects only linear dependencies between two variables.

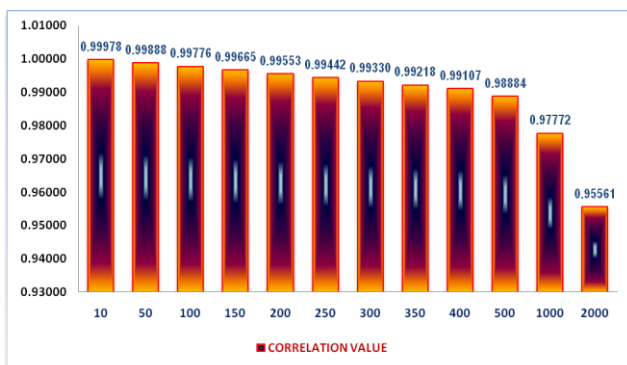


Figure 12: Representation Correlation values of Cover and Stego

If we have a series of  $n$  measurements of  $X$  and  $Y$  written as  $x_i$  and  $y_i$  where  $i = 1, 2, \dots, n$  then the sample correlation coefficient can be used in Pearson correlation

$r$  between  $X$  and  $Y$ . The sample correlation coefficient is

$$r_{xy} = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{(n-1)S_x S_y} \dots\dots\dots (6)$$

where  $\bar{x}$  and  $\bar{y}$  are the sample means of  $X$  and  $Y$ ,  $S_x$  and  $S_y$  are the sample standard deviations of  $X$  and  $Y$ . The number of matching (but different sequence order) characters divided by two defines the number of transpositions. The Correlation score of comparing cover text and stego text is shown in Fig. 11 and the chart in Fig. 12 represent the Correlation of different stego of various length of message.

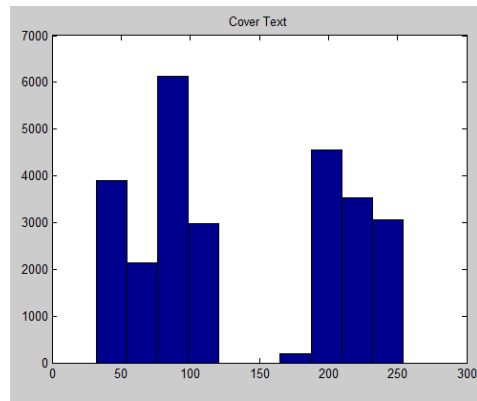


Figure 13: Graph of Cover Text

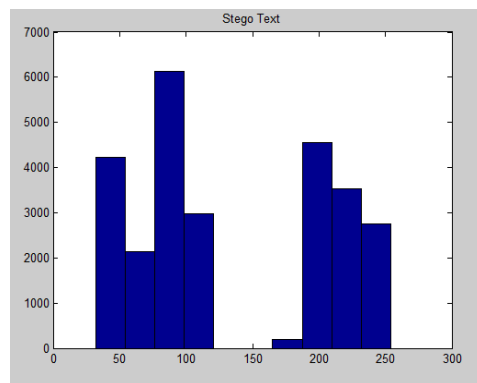


Figure 14: Graph of Stego Text

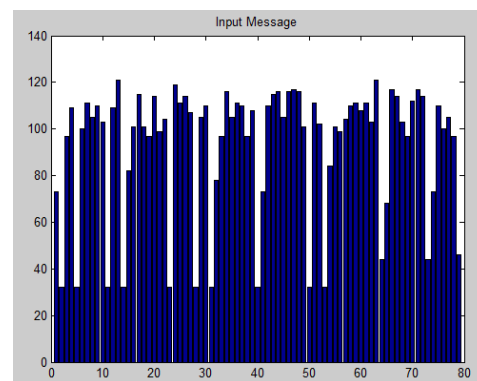


Figure 15: Graph of Input Message

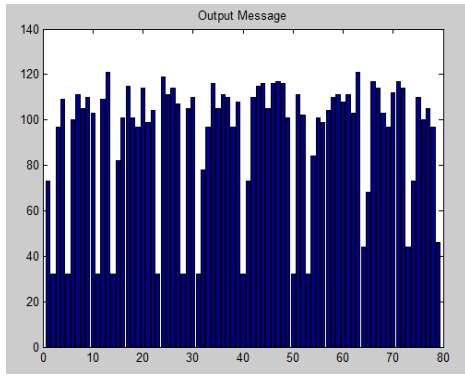


Figure 16: Graph of Output Message

In Fig. 13 and Fig. 14 it has been observed that the cover and stego graphs both are remain same. The Fig. 15 and Fig. 16 shows that the Input and Output messages graphs are same; from this view also we can proof our technique. In Fig. 17 shows the computation time of Stego and Message generation, the graph shows in Fig. 18. To observe the computation time it is proved that the receiver side message generation system is faster than sender side stego generation system.

Message Length (In Character)	Computation Time (in Second)		
	Stego Generate (A)	Message Generate (B)	Difference (B-A)
10	0.2184	0.1872	-0.0312
50	0.858	0.7956	-0.0624
100	1.8876	1.5132	-0.3744
150	2.3556	1.7472	-0.6084
200	3.2136	2.4024	-0.8112
250	3.8688	2.6364	-1.2324
300	4.2276	3.8376	-0.39
350	5.2572	3.7128	-1.5444
400	6.162	4.4304	-1.7316
500	7.2852	5.2572	-2.028
1000	13.6501	9.8437	-3.8064
2000	26.6294	19.7809	-6.8485

Figure 17: Computation Time of Stego & Message generation

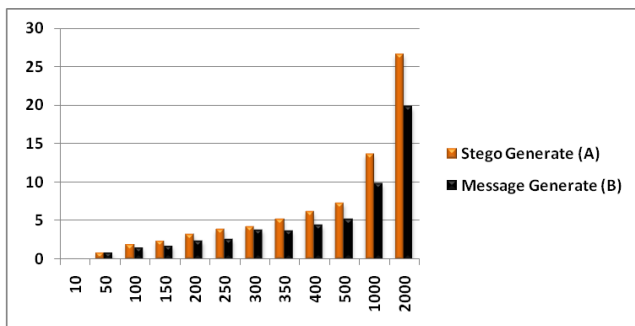


Figure 18: Representation Computation Time values of Stego & Message

V. CONCLUSIONS

In this paper the authors presented an approach of text steganography method using Oriya language by the help of quantum truth table mapping technique. This property

generates the stego text with minimum degradation. In this method the length of stego and cover remain same and this property enables the method to avoid the steganalysis also. The result shows that the performance of the technique is satisfactorily. This work can be extended by using other Indian regional language.

REFERENCES

- [1] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. Proc. Roy. Soc. Lond. A, 400 (1985), 97-117.
- [2] Fabien A.P. Petitcolas, Ross J. Anderson, Markus G. Kuhn: Information Hiding—A Survey, Proceedings of the IEEE, Vol. 87, No. 7, July 1999, pp. 1062-1078, ISSN 0018-9219.
- [3] K. Bennett. Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text. Purdue University, CERIAS Tech. Report, 2004.
- [4] Kran Bailey Kevin Curran. An evaluation of image based steganography methods. 1999.
- [5] G. Doerr and J.L. Dugelay. Security pitfalls of framebyframe approaches to video watermarking. IEEE Transactions on Signal Processing, Supplement on Secure Media., 52:2955–2964, 2004.
- [6] G. Doerr and J.L. Dugelay. A guide tour of video watermarking. Signal Processing: Image Communication., 18:263–282, 2003.
- [7] S. Low N.F. Maxemchuk J.T. Brassil and L. O.Gorman. Electronic marking and identification techniques to discourage document copying. IEEE Journal on Selected Areas in Communications, 13:1495–1504, 1995.
- [8] Krista Bennett (2004). "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text". CERIAS TR 2004-13.
- [9] D. Deutsch. Quantum computational networks. Proc. Roy. Soc. Lond. A, 425 (1989), 73-90.
- [10] R. P. Feynman. Quantum mechanical computers. Found. Phys. 16(1986), 507.
- [11] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal. "Novel text steganography through special code generation." In Proceedings of International Conference on Systemics, Cybernetics and Informatics (ICSCI-2011), Hyderabad, India., Jan 5-8, 2011.
- [12] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal. "The text steganography using article mapping technique (AMT) and SSCE". Journal of Global Research in Computer Science, 2, April 2011.
- [13] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal. Design and implementation of a secure text based steganography model. In 9th annual Conference on Security and Management (SAM) under The 2010 World Congress in Computer

- Science, Computer Engineering and Applied Computing (WorldComp 2010), Las Vegas, USA, July 12-15, 2010.
- [14] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal. Implementation of a novel text based steganography model. In National Conference on Computing and Systems (NACCS), Dept. of Computer Science, The University of Burdwan, Burdwan, India., Jan 29, 2010.
- [15] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal. A novel approach of secure text based steganography model using word mapping method (WMM). International Journal of Computer and Information Engineering 4:2 2010 - World Academy of Science, Engineering and Technology (WASET), 4:96103, Spring 2010.
- [16] Souvik Bhattacharyya, Indradip Banerjee, Arka Prokash Mazumdar and Gautam Sanyal. Text steganography using formatting character spacing. IJCS, 13, Decembar, 2010.
- [17] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal. A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier. Journal of Global Research in Computer Science, 2, April 2011.
- [18] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal. An Approach of Quantum Steganography through Special SSCE Code. International Journal of Computer and Information Engineering - World Academy of Science, Engineering and Technology (WASET), Issue 0080:2011, Article 175, Page: 939-946.
- [19] Ashok Muthukrishnan. Classical and quantum logic gates: An introduction to quantum computing. Quantum Information Seminar (Friday, Sep.3, 1999), Rochester Center for Quantum Information (RCQI).
- [20] Ross J. Anderson. and Fabien A.P. Petitcolas. On the limits of steganography. IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright and Privacy Protection, 16:474-481, 1998.
- [21] JHP Eloff T Mrkel and MS Olivier. An overview of image steganography. In Proceedings of the fifth annual Information Security South Africa Conference, South Africa, 2005.
- [22] S.P. Mohanty. Digital watermarking: A tutorial review. International Journal of Digital Evidence, Fall 2003, 2003.
- [23] N.F. Johnson. and S. Jajodia. Steganography: seeing the unseen. IEEE Computer, 16:26-34, 1998.
- [24] Kran Bailey Kevin Curran. An evaluation of image based steganography methods. International Journal of Digital Evidence, Fall 2003, 2003.
- [25] D. Kahn. The codebreakers - the comprehensive history of secret communication from ancient times to the internet. Scribner, 1996.
- [26] Z. Duric N. F. Johnson and S. Jajodia. Information hiding: Steganography and digital watermarking attacks and countermeasures. Kluwer Academic, 2001.
- [27] S. Dowdy and S. Wearden. Statistics for research. Wiley. ISBN-0471086029, page 230, 1983.
- [28] J. Gea-Banacloche. Journal of Mathematical Physics, pages 43, 4531, 2002.
- [29] S. Natori. Quantum computation and information. Topics in Applied Physics (Springer, Berlin/Heidelberg), 102:235-240, 2006.
- [30] K. Martin. Lecture Notes in Computer Science, pages 4567, 32, 2008.
- [31] M. Curty and D. J. Santos. 2nd Bielefeld Workshop on Quantum Information and Complexity, 2000.
- [32] Nielsen, Michael A. & Chuang, Isaac L. (2000). Quantum Computation and Quantum Information. Cambridge University Press. ISBN 0-521-63235-8.



**Indradip Banerjee** received his MCA degree from IGNOU in 2009, PGDCA from IGNOU in 2008, MMM from Annamalai University in 2005 and BCA (Hons.) from The University of Burdwan in 2003. Currently he is working as a Technical Assistant in Computer

Science and Engineering Department at University Institute of Technology, The University of Burdwan. His areas of interest are Steganography, Cryptography and Quantum Computing. He has published 13 papers in International and National Journals / Conferences.



**Souvik Bhattacharyya** received his B.E. degree in Computer Science and Technology from B.E. College, Shibpur, India, presently known as Bengal Engineering and Science University (BESU) and M.Tech degree in Computer Science and

Engineering from National Institute of Technology, Durgapur, India. Currently he is working as an Assistant Professor in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. He has a good no of research publication in his credit. His areas of interest are Natural Language Processing, Network Security and Image Processing. He has published nearly 20 papers in International and National Journals / Conferences.





**Gautam Sanyal** has received his B.E and M.Tech degree National Institute of Technology (NIT), Durgapur, India. He has received Ph.D (Engg.) from Jadavpur University, Kolkata, India, in the area of Robot Vision. He possesses an experience of more than 25 years in the field of teaching and research. He has published nearly 60 papers in International and National Journals / Conferences. Two Ph.Ds (Engg) have already been awarded under his guidance. At present he is guiding six Ph.Ds scholars in the field of Steganography, Cellular Network, High Performance Computing and Computer Vision. He has guided over 10 PG and 100 UG thesis. His research interests include Natural Language Processing, Stochastic modeling of network traffic, High Performance Computing, Computer Vision. He is presently working as a Professor in the department of Computer Science and Engineering and also holding the post of Dean (Students' Welfare) at National Institute of Technology, Durgapur, India.