Quantum Text Steganography Using Numeric Handwriting of Indian Regional Language

Dr. Indradip Banerjee^{#1}, Kaustav Bandyopadhyay^{*2}, Dr. Anand Mohan^{^3}, Prof.(Dr.) Ashok Kumar^{\$4}

[#] Department of CSE, University Institute of Technology, The University of Burdwan, Burdwan, India. ^{*} Department of CSE, MIET, Bandel, India.

[^] P.G Dept. of Physics C.M. Science College, L.N Mithila University, Darbhanga, Bihar, India. [§] M.L.S.M College, LN Mithila University, Darbhanga, Bihar, India.

Abstract — Secure & Hidden transmission over the public media is literally known as Steganography. Extensive capa city of work in this area of research has been recognized by different research group on steganography. In this contributions, a quantum based text steganography mechanism has been designed which can work in handwriting of Indian regional language Bengali. Here the quantum approach has been integrated before the embedding algorithm and mathematical function has been incorporate for encryption & decryption technique with this effort to enrich the security level. Text steganography together with mathematical function & quantum approach based on the use of handwriting characters in Bengali language with mapping truth table of quantum gate have been developed in this contribution.

Keywords — *Text Steganography, Numeric Handwriting and Security, Quantum Steganography.*

I. INTRODUCTION

Information smacking is the ability to prevent or hidden certain aspects from being accessible to others excluding authentic user. It has various sub castigations. Steganography is the term which is most catching sub disciplines in the universe of information hiding [1] which is imitative from a work by Johannes Trithemus (1462-1516) titled it "Steganographia" and the word comes from the language of Greek which literally means "covered writing". Steganography is the ancient art of hidden information through any cover and communication channel or an algorithm which is used for creating a stego without cover etc, so that will not possible to trace as well as suspect by an eavesdropper. Steganography is the concept has been emanates from cryptography in the sense that where cryptography is the concept to keep the content secret by encryption technique, whereas the steganography is the mechanism to secret the message within the channel by hiding technique [2].

Different researchers have been used diverse media like text, image, video, protocol, music and sound etc to develop the concept of steganography. Now the beautiful category is text, because this is the difficult kind of category in the terminology of steganography. Lack of redundant information is the challenge in the text steganography and thus this category is beautiful as well as difficult.

A. Quantum Steganography

Very little amount of research work has been done in quantum steganography. The idea of hiding secret messages as the error syndromes of a quantum errorcorrecting code (QECC) was introduced by Julio Gea-Banacloche [3]. In this development the three-bit repetition code has been used to transmit messages between Alice and Bob using the concept of shared secret key. Alice put the errors deliberately to create the noise and transmit it to the channel, and then Eve notices the errors which have been applied from sender zone and extract the messages by the receiver. He assumes that a binary-symmetric communication channel has been share in the established model by the help of Alice and Bob. This contribution does not report that the errors would resemble a believable channel or it considers the case of the existence of essential noise. Super-dense coding modification technique developed by Natori [4] gives a mechanism of quantum steganography in a simple behavior. Bennett and Brassard's developed protocol named as Quantum key distribution (QKD) which has been used by Martin to develop a notion of quantum steganography communication based on a variation of QKD to hide a communication channel [5]. There are three different types quantum steganography protocols have been developed by Curty [6].

B. Quantum gate:

Quantum circuit model of computation in quantum computing, a quantum gate or quantum logic gate is a basic quantum circuit which operates on qubits. Classical logic gates have been used by the conventional digital circuit's and here the qubits are termed as the building blocks of quantum circuits. These are uses the logic gates which are called Quantum logic gates (QLG), the QLG are reversible like other classical logic gates. However, the reversible gates have been used by the classical computing only. Quantum gates fundamentally can be symbolized as like matrices. A gate can be represented as $2^{kh} \times 2^{kh}$ unitary matrix where kh is the qubits. 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. The wellknown quantum gates used by various researchers are Phase shift gates, Hadamard gate, Fredkin gate, Pauli-Z gate, Pauli-Y gate, Pauli-X gate, Controlled gates, Swap gate, Toffoli gate, etc. Here we use Controlled gates to represent the qubits and control the operations.

C. Reversible Classical Logic:

Theories of reversibility of computation were introduced in the year 1970. Logical and physical reversibility, these two issues are the main part and both the topics were intimately connected. Logical reversibility technologies are taken the input from the output of that gate function or by same computation technique. The NAND gate is explicitly irreversible, it has two inputs and one output, while the NOT gate is reversible (it's own inverse). In Physical reversibility issues the NAND gate has been used and that has only one output, in the design of the process it has been observed that one of the inputs of the gate has effectively been erased, whose evidence has been permanently vanished. The modification in the value of entropy that can be associated with the loss of one bit of information is ln 2, which, thermodynamically, corresponds to an energy increase of $kh^{Tm} \ln 2$, where kh denoted as Boltzman's constant and Tm stands for temperature. The heat degenerate at the time of running the process is usually taken to be a sign of physical irreversibility, that the microscopic physical state of the system cannot be restored correctly as it was earlier the course took place. By the support of inputs and outputs it can be understood that the Reversible logic gates are symmetric. The reversible NOT gate, whose truth table is given in Fig. 1. It can also write this in the form of a matrix, or as a graphic. The matrix arrangement gradients the shapes of truth table and the gradients are shown in the form of $\langle 0 \rangle$, $\langle 1 \rangle$. The matrix fields are written in the form of 1's and 0's such that each vertical line or in horizontal line has exactly a single 1, which has been understood as a one-to-one plotting 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. 2, performs a NOT on the second bit if the first bit is $\langle 1 \rangle$, but

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

Figure 1: NOT Gate Truth Table

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 2: NOT Gate Truth Table

otherwise has no effect. The C-NOT gate is wellknown as XOR gate, since the exclusive OR operation has been performed by the help of the two input bits and composes the output to the second bit.

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 [7] is given below:

Let
$$\left\{ \left| 0 \right\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \left| 1 \right\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$$
 be

the orthonormal basis.

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

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

qubit of $|\psi\rangle$.

Recall

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

i. In case of 0 control qubit

First, it can be prove that: $CNOT | 0, \psi \rangle = | 0, \psi \rangle$

Before the phase of computation, it has been noted that the specific definition of *CNOT* assumes an eigen basis of

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

Then, it's not difficult to verify

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

Then

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

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

ii. In case of 1 control qubit

Now, it 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
$$|1, \psi\rangle = \begin{bmatrix} 0 \\ 0 \\ x \\ y \end{bmatrix}$$
.
Then $_{CNOT} |1, \psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$... (4)
As we can see that $|1,1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$ and $|1,0\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$.

using these on the equation above gives

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





Text is the prehistoric and difficult media used in the literature. Letters and telegrams in the earlier time used to hide the secret messages within their texts i.e. before the electronic era comes. Text steganography mechanism used for hiding any type of information inside the text i.e. character-based messages. There are three basic categories of text steganography have been proposed by different researchers illustrated in Fig. 3. Three categories are termed as format-based, random as well as statistical generation and linguistic technique. [8]

i. Format-based methods [8]: In this method the physical formatting of text has been used to hide the secret information. Format-based methods generally adjust existing text for hiding the steganography text.

ii. Random and statistical generation method [8]: This method can avoid the plaintext where as in

this method the researchers generate their own cover texts by their algorithm. Character sequences method can hide the information within the character sequences.

iii. Linguistic methods [8]: The prosperity of electronic documented information was available in the world as well as the application of serious linguistic analysis makes this interesting medium for information hiding.

Fig. 4 shows the mechanism of text steganography. At the beginning of the system, a secret message can embed to a cover-text through an embedding algorithm and after that form a stego-text. Next step is entitled transmission, transferred the stego-text to the receiver via a communication channel.



Figure 4: Mechanism of Text Steganography

In this paper, an approach of Quantum Text Steganography has been projected based on the use of Numeric Handwriting of Indian Regional Language. Indian regional language Bengali has been used in this study. Here the quantum truth table also mapped to increase the security level and complexity. A new code representation mathematical function has been anticipated here to achieve high level of security. Before the embedding operation each character of the secret message has been encoded using this mathematical function by means of passkey and then embeds into cover text by the proposed text steganography method to form the stego text. In this method the length of the stego and the cover are identical, so prediction of existence of message is complicated in view of that distinctiveness. This is the Bengali language method which can work in different languages and has been developed in this steganography approach.



Figure 5: GUI Representation

The proposed development has been designed and implemented from a previous work [9] which has been developed and published on English language methods. The novel quantum approach has been incorporated in this research and The Revised SSCE Value has been used to increase the security level.

Organization of the paper is as follows: At first the proposed model has been furnished in Section II. Section III shown some of the algorithms of developed processes. Mathematical Analysis has been designated in section IV. Section V is for the analysis part of the results and the last section deals with the conclusion of the work.

II. THE PROPOSED MODEL

This paper exactly deals with text steganography, uses Indian regional language Bengali handwritten 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. The input message encrypted using mathematical function & passkey and it is treated as a bit stream. Pick two pair of this bit stream of message and transfer to its math function equivalent value with the help of passkey. Then select the handwritten Bengali Indian Regional Language Text as cover and map it accordingly. Then a matrix formed with the help of message length and map the C-NOT truth table 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. Subsequently the embedding process continues with the secret message and the cover text in Bengali Regional language to generate the stego text based on the algorithm. By the help of replacing technique the stego length are being same as cover. The receiver side runs the reverse algorithm and do the reverse operations to get back the information send by the sender zone.

A. Solution Methodology

The proposed system involves two windows i.e. SENDER and RECEIVER. The user will be someone who will have adequate knowledge of steganography systems. The user first select the Bengali language handwritten characters and plain text message from a file or enter text in specified area of software, another text to be used as the carrier (cover text) which is in Bengali language and put a Revised key as password. Then with the help of proposed embedding technique the message has been hidden in the handwritten Bengali numeric character. At the receiver zone the receiver receives the mapping technology as well as the mapped Bengali handwritten numeric characters which are required to extract the message. Then the mathematical function used for decrypt the information. Fig. 5 displays one of the GUI Exemplification of the mechanism.

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 Encryption / Decryption

- Select Passkey (Password), message and pick one by one character then convert to its ASCII equivalent.
- Change ASCII code to our generated code from *Mathematical Function* and add Passkey to produce a Function value which is depending on Passkey. Convert to its character equivalent.

B. Algorithm for Message Embedding

• Select the message and encrypt the message with *Mathematical Function*. Then select the Indian Regional Language Bengali handwritten numeric character as 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.
- Repeat the above step for the remaining bit sequence of the message and prepare the stego text.

C. 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 and extract using Bengali handwritten character

IV. MATHEMATICAL ANALYSIS

Encryption and Decryption: The entry that lies in the mi^{th} row and the mj^{th} column of a matrix is typically referred to as $(mi, nj)^{th}$ entry of a matrix **MA** is most commonly written as MA[mi,nj] or $ma_{mi,nj}$. $MA = [ma_{mi,nj}]_{mi=1,2,...,mi}$ and nj=1,2,...,nj

Row and Column operations are ways to change matrices. In this function three types of Row and three types of column operations have been occurred, which are furnished below –

Row Operations

- 1. Interchange row *mi* and *mj* ($R_{mi} < --> R_{nj}$)
- 2. Multiply row *mi* by *s*, where $s \neq 0$ ($_{s}R_{mi} \rightarrow R_{mi}$)
- 3. Add *s* times row *mi* to row *nj* ($_{s}R_{mj} \rightarrow R_{nj}$) Column Operations
- 1. Interchange column *mi* and *nj* ($C_{mi} < --> C_{nj}$)
- 2. Multiply column *mi* by *s*, where $s \neq 0$ (${}_{s}C_{mi}$ $\rightarrow C_{ni}$)
- 3. Add s times column *mi* to column *nj* (${}_{s}C_{mj} \longrightarrow C_{nj}$)

Now for SSCE value we perform a column operation on matrix MA. After performing a column operation on MA[mi, nj] it produce MA'. $MA[mi, nj] \rightarrow MA'$ [mi, nj]

After that transpose the MA' [*mi*, *nj*] matrix and formed MA'^{T} [*mi*, *nj*].

Now it is transformed to an array i.e. place in an orderly arrangement in a linear order.

Then add Passkey (known as password) Pi with MA'^{T} [mi, nj] transformed matrix and produced Pi. MA''^{T} [mi, nj].

V. 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 Bengali Handwritten Languages. The authors simulated the proposed system and the results are shown in the Fig. 6, 7 and 8. This method hides two bit per word in the cover text which reflects the high



Figure 9: Graph of Input and Output Message



Figure 10: Granh of Cover Text and Stego Text

embedding capacity of the system. Although the embedding capacity of the proposed method is depends upon the characters of Bengali Handwritten Languages. 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.

চিটেড মায়ের কালিয়া। উপজলে কা চিটেড মায়ে ৫০০ প্রাথ, আলু বড় এটো লয়া টুকরো করে ঘটনাচাটি ১৫ কাপ পৌরাজাৰাটা বর চায়চের ২ চায়চ, আলাবাটা ১ চা চায়চ, জনুম্বেট্ডো ১ চা চায়চ, লারাজটো ১ চা চায়চ, গরমানলা পরিমান মতের। কেচাপারা ১ টা নৃন্ মিটি মান অনুমাটি টোমাটো ১ টা মাজারি মাপের তেল ১৫০ প্রায়। প্রশালী চিটেড মাত বেতে বুয়ে নুন ও অনুদ মানিয়ে ভাজনে। চিটেড মাতের কালিয়া। উপজনা বর চিটেড মাতে ৫০০ প্রায়, আলু বড় মটো লাম টুকরো করে, মটারচাটি ১৫ কালে পৌরোজাটা বর চায়চের ২ চামচ, আলাবাটা ১ চা চায়চ, বনুলাইডো

Figure 6: Cover Text in Proposed Text Steganography Technique

B Annuel Meters The Car Pave New Inte Book Name: Big Data Security Berles: Frontiers in Computational Intelligence

Figure 7: Message in Proposed Text Steganography Technique

চিট্টে মাহেৰ কালিয়া। উপকলৰ বৰ চিট্টি মাহে ৫০০ প্ৰাম, আৰু বড় বটো লয়া টুকরো করে মটনচটি ৯.৫ কাপ, পৌয়াজনাটা বর চামচের ২ চামচ, আনাবাটা ১ চা চামচ, অনুমর্ভয়ে ১ চা চামচ, লয়ার্ছয়ে ১ চা চামচ, অবমানলা বানোন মতে। | কেজালারা ১ টা নুন, মিটি মাহ বেয়ে মুন্যাটি টোমাটো ১ টা মাজারি মতেল, কেল ১৫০ প্রমা। রালালী - চিট্টি মাহ বেয়ে মুনা ও অনুদ মাজিয়ে জাজুন। চিট্টি মাহের কালিয়া। উপকলা বর চিট্টি মাহ ৫০০ প্রাম, আৰু বড় বটো লয় টুকরো করে, মটরচটি ৯.৫ কাল, পৌয়াজনটো বর চামচের ব চামচ, আনাবাটা ১ চা চামচ, অনুসর্ভয়ো

Figure 8: Stego Text in Proposed Text Steganography Technique

A. Similarity Measure:

Similarity comparison is the most important in this type of research because if the stego and cover are

likely to similar then no one can understand the activity. So the Correlation method has been used for measuring similarity between original and transmitting message.

 TABLE I:

 CORRELATION VALUES OF COVER AND STEGO

 TEXT IN DIFFERENT LENGTH OF MESSAGE

MESSAGE LENGTH (In Character)	CORRELATION VALUE
10	0.99976
50	0.998787621
100	0.997577235
200	0.995159513
300	0.992745838
400	0.990336183
500	0.987930524
600	0.985528835
700	0.983131092
800	0.98073727
900	0.978347344

If we have a series of *n* measurements of *X* and *Y* written as cx_i and cy_i where i = 1, 2, ..., n. After that the sample correlation coefficient used in Pearson correlation *cr* between two variables i.e. *X* and *Y*. The sample correlation coefficient is written

where cx and cy are the sample means of X and Y, CS_{cx} and CS_{cy} are the sample standard deviations of X and Y. The number of different sequence order matching characters divided by two defines the number of transpositions. The Correlation score of comparing cover text and stego text is shown in Table 1 and the chart in Table 2 represent the Correlation of different stego of various length of message.



Figure 11: Representation Correlation values of Cover and Stego

Message Length (In Character)	Computation Time (
	Stego Generate (A)	Message Generate (B)	Difference (B-A)
10	0.1404009	0.1872012	0.0468003
50	0.6552042	0.6864044	0.0312002
100	1.2168078	1.3572087	0.1404009
200	1.9344124	3.0576196	1.1232072
300	2.7144174	3.3228213	0.6084039
400	3.5724229	4.3836281	0.8112052
500	4.5396291	5.616036	1.0764069
600	5.6940365	7.0512452	1.3572087
700	7.4256476	8.4864544	1.0608068
800	10.4208668	10.8576696	0.4368028
900	9.5784614	10.8888698	1.3104084
1000	9.3288598	11.4192732	2.0904134

 TABLE II:

 COMPUTATION TIME OF STEGO & MESSAGE GENERATION



Figure 12: Representation Computation Time values of Stego & Message

COMPARISON WITH OTHER TEXT STEGANOGRAPHY METHODS				
Method	Text Steganography	Text Steganography by	Text Steganography	Proposed Text
Name	by Changing Words	Inter-word Spacing and	by Using Letter	Steganography
	Spelling. [10]	Inter paragraph Spacing	Points and	
		Approach. [11]	Extensions [12]	
Details of	In this method the	In this method, the lines or	In this method the	In this method the Bengali
the	author proposed a	paragraph of the text are	Arabic language is	language is used to embed
Method:	method for	vertically shifted to some	used to embed any	any secret message by
	embedding the secret	degree (for example, each	secret message by	making some changes in
	message by placing	line shifts1/300 inch up or	using the pointed	some of the English letters to
	the US words for	down) or the words of any	letter to hold 1 and	hold 00,01,10,11. A quantum
	hiding the bit 0 and	line are shifted	un pointed letters to	approach has been used to
	UK words for hiding	horizontally and	hold 0	increase the level of security.
	the bit 1.	information is hidden by		
		creating a unique shape of		
		the text.		
No of	single(0 and 1)	single(0 and 1)	single(0 and 1)	double(00,01,10,11)
Embedding				
Bits:				
Changes	In Word(US for 0,UK	In Lines, Word or	In Letter(pointed	In Letter(changing the letter
Occurred:	for 1)	Paragraph.(one space for	letter for 0,unpointed	pattern)
		0,two space for 1)	letter for 1)	
Embedding	The embedding	Greater than Method 1	Greater than Method	Greater than the previous
Capacity:	capacity of this	but lesser than Method	1 and Method 2 but	three method because one
	method is the lowest	3,Method 5 because here	lesser than Method 4	change of letter embed two
	compared to other 4	increasing the white	and Method 5	bits simultaneously.
	methods because it	spaces embedding	because it changes a	
	used a whole word to	capacity can be increased	single letter to	
	embed bit 0 or bit 1.	but this increasing can	embedding a bit 0 or	
		also be done at some	DIT I.	
		extent. Otherwise it will		
		be easy to trace the		
St	NI-4 A	changes made in the text.	Net Anniheshie	0.00
Similarity	Not Applicable	Not Applicable	Not Applicable	0.99
Measure:				

TABLE III:

In Fig. 10 it has been observed that the cover and stego graphs both are remain same. The Fig. 9 shows that the Input and Output messages graphs are same;

from this view also we can proof our technique. In Table 2 shows the computation time of Stego and Message generation and graph shows in Fig. 12. To

observe the computation time it is proved that the receiver side message generation system is faster than sender side stego generation system.

Table 3 describes the comparison of Bengali Text Steganography with other Text Steganography Methods in tabular form.

VI. CONCLUSIONS

The above contribution totally based on text steganography. Here the authors have used the approach by handwritten numeric character of Bengali Indian Regional Language. The quantum truth table mapping technique also used to increase the security. This property generates the stego text with minimum degradation. Here with the help of Mathematical function and user's entered Passkey the author extend the security level in view of cryptography also along with Steganography technique. The lengths of both the cover as well as stego are same and this can established that the method can avoid steganalysis. The result shows that the performance of the technique is satisfactorily. In future the author can be extended this work in different Indian regional languages.

REFERENCES

- 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.
- [2] 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.
- [3] J. Gea-Banacloche. Journal of Mathematical Physics, pages 43, 4531, 2002.
- [4] S. Natori. "Quantum computation and information". Topics in Applied Physics(Springer, Berlin/Heidelberg), 102:235– 240, 2006.
- [5] K. Martin. Lecture Notes in Computer Science, pages 4567, 32, 2008.
- [6] M. Curty and D. J. Santos. 2nd Bielefeld Workshop on Quantum Information and Complexity, 2000.
- [7] Nielsen, Michael A. & Chuang, Isaac L. (2000). "Quantum Computation and Quantum Information." Cambridge University Press. ISBN 0-521-63235-8.
- [8] Krista Bennett (2004). " Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text". CERIAS TR 2004-13.
- [9] Indradip Banerjee, Kaustav Bandyopadhyay, Anand Mohan. (2020) "Text Steganography Using Numeric Handwriting" "International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 04, Pages: 7802-7816, March 2020" ISSN: 1475-7192, Scopus Index.
- [10] M. Shirali-Shahreza, "Text Steganography by Changing Words Spelling". 10th International Conference on Advanced Communication Technology, 2008. ICACT 2008. (Volume:3). Page(s): 1912 – 1913, ISSN : 1738-9445, Conference Location : Gangwon-Do, Date of Conference: 17-20 Feb. 2008, Publisher: IEEE.
- [11] Lip Yee Por, Kok Onn Chee, Tan Fong Ang and Delina Beh. "An enhanced embedding method using inter-sentence, interword, end-of-line and inter-paragraph spacing", International Journal of the Physical Sciences. Vol. 6(36), pp. 8130 - 8142, 30 December, 2011. ISSN 1992 - 1950 ©2011 Academic Journals.
- [12] S. Khan, B. Abhijitha, R. Sankineni, B. Sunil. "Polish text steganography method using letter points and extension", IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015. Date of Conference: 5-7 March 2015, Page(s): 1 – 5, Print ISBN: 978-1-4799-6084-2, Conference Location : Coimbatore, Publisher: IEEE.