A Generalized Model of Text Steganography by Summary Generation using Frequency Analysis

Anandaprova Majumder[1], Suvamoy Changder[2]

[1]Department of Computer Science & Engineering
Dr. B.C. Roy Engineering College, Durgapur, India
[2]Department of Computer Science & Engineering
National Institute of Technology, Durgapur, India
[1]anandaprova.majumder@bcrec.ac.in, [2]suvamoy.nitdgp@gmail.com

Abstract: **Hiding the existence of a message from any intermediary during data communication is the purpose of the method of steganography. Various media files like texts, images and audio e.t.c are used as the media for developing different text steganography algorithms. Media like text is considered to be a difficult target medium in this perspective as it lacks redundant information in it. This research work presents a generalized approach for text steganography, applicable on text samples of any language text, through a technique that uses an intelligent way of summary generation for data hiding. To hide data, we check for the existence of common letter pairs or double letter pairs in keywords of the paragraph, located in the set of normalized sentences of the paragraph. The proposed algorithm finds sentences to generate a possible summary of the text, known as cover text. Same way at the receiver end, we check for the existence of the keywords in the sentences of the summery, generated at the encryption end and gets the binary bits required to generate the secret message. The experimental result shows that the proposed algorithm gives satisfactory output with the cover text obtained from well available internet blogs.**

Keywords: **Information security, Text Steganography, Text Summary, Common letter pairs, Double letter pairs**

I. INTRODUCTION

The meaning of steganography is hidden writing. The principle of this hidden communication is hiding the existence of the secret infprmation from any outsider, whereas the concept of cryptography has a bit different point of view, which ensures that the message is not understandable instead of hiding the data transfer. The method of steganography aims to establish a communication in which is secured and absolutely unnoticed [1, 2, 11] in order to avoid suspicious interference to the data transfer method [3].

If a steganography method causes intervention of an unwanted receiver about the existence of hidden information in a carrier media file, that method is then considered to be a failure [3, 4]. The generalized model for Steganography, as shown in Fig.1, explains procedure of data transfer schematically. In a framework of steganography, the data embedding technique is unknown to outsider and known to the sender and the receiver only. As text files lack large scale redundant information, compared to other type of media files, text steganography methods can be considered toughest [5].

978-1-5386-4692-2/18/$31.00 ©2018 IEEE

This piece of research work presents a generalized model for text steganography using frequency analysis that generates the summary of a text file. The proposed embedding method takes as input an easily obtainable blog text in internet and the secret message to be sent to receiving end. The secret data to be sent is embedded in the summary by finding the keywords in the original text with the help of a parts of speech tagger and finding the presence of common or double letter pairs in those different keywords present in the text. As system output, a new summery is generated from the selected text sample which is the cover text, being send to the receiver. Following just the reverse procedure the receiver retrieves the secret bits from the cover text.

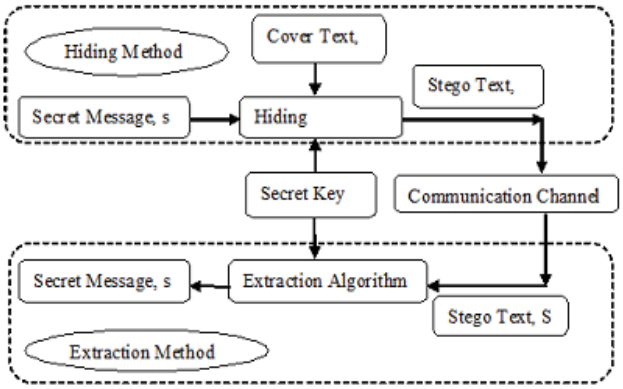

Fig. 1. Generalized Model for Text Steganography

II. PRELIMINARY OBSERVATIONS AND LITERATURE REVIEW

There are four basic kind of steganography methods where four different type of media files text file, image file, audio file and video file are used to embed the secret information. Text steganography involves the method of changing the features of some alphabets of the used language of the text sample, to changing words with their respective synonym within a text sample, to generating random character sequences for generating texts of readable format [8, 16]. Text steganography can be said to be the toughest of all steganography methods as it lacks enough redundant data in text files. Image, audio or

video files are richer in possession of redundant information [6, 7]. Unidentifiable changes can easily be made to an image or an audio file, but it's not easy to put changes to text files as it will be easily distinguishable [9]. Text steganography method is still a popular one as to store a text file much less memory is required compared to other media files and it's also fast and easy to communicate, hence its preferable compared to other steganographic methods [10]. Text steganography can be superficially categorized into three basic types as follows: Format based, Random and Statistical generation based and Linguistic.

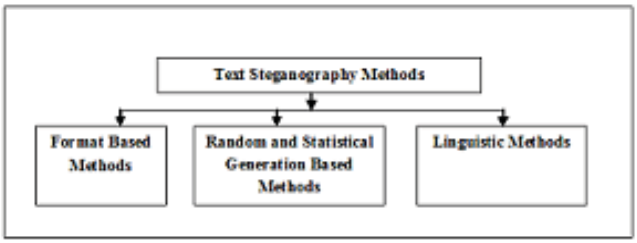

Fig. 2. Classification of Text Steganography Algorithms

III. EXISTING TEXT STEGANOGRAPHY METHODS

In this paragraph we are to discuss, some already existing text steganography methods.

A. Line Shift

Vertical shifting is applied to the lines of a sample text to some specific degree for hiding data in text [9, 10]. A line is shifted up for hiding bit '0' and a line is shifted down for hiding bit '1' [13]. Each marked line has two control lines on both sides for measuring direction of its movement, wheather a line has been shifted up or down. But it may draw suspicious attention.

B. Word Shift

Horizontal shifting of words is followed in this method of data hiding in text. If shifted left, a bit 0 is represented or if shifted right a bit 1 is represented [13]. This steganography method can be less identified, because different distance value between different words that fill a line is well accepted [10, 11]. But it can incur a retyping error.

C. Syntactic Method

Different punctuation marks are used in sentences like semi colon (;), colon (:), etc., which are used for hiding bit 0 or bit 1. But the disadvantage of the method is that the correct place for data insertion in the punctuation marks is of prime importance else it may generate erroneous output [12, 13].

D. White Steg

Extra blank space i.e. white spaces are added in this method for data embedding. Single space is added to hide bit 0 and more than one space are added to hide bit 1 at the end of terminating characters in case of Inter Sentence Spacing method [9]. A previously set number of spaces are inserted at the end of each line if End of Line Spacing method is followed.

E. Feature Coding Method

Secret data is embedded by changing some structural features of the alphabets of the sample text. A parser picks all the usable structural features for information hiding after going through the sample text document [15, 16].

F. Summary by Reflection Symmetry Method

To embed secret message following this method, reflection symmetry property is checked for the present characters in each sentence of the text sample both horizontally and vertically. Following the reflection symmetry property for different alphabets of the respective text sample, sentences are selected which generates a summary of the text, known as cover text [17].

IV. PROPOSED GENERALIZED MODEL FOR SUMMARY GENERATION

Our proposed method can be classified into 3 following subsections. The first section contains information about how text pre processing for summary generation is done. The next section is the section that contains details about text analysis for data hiding and the last i.e. the third section contains the data hiding and data extraction algorithms that work behind the process of data hiding through summary generation algorithm.

A. Text Preprocessing for summary generation

The first thing that is done in pre processing stage is basic stop word elimination and case folding. Followed to that, normalized length of a sentence is calculated by dividing the length of a sentence with the length of the largest sentence and the equation can be shown as follows.

$$\rho_i = {}^{n_i}/_{n_l} \quad \text{Eqn. 1}$$

Here, ρ_i denotes the normalized length of i^{th} sentence of a text n_i denotes the number of words in the respective sentence and n_l denotes the number of words in the longest sentence of the text. Considering a predefined threshold value ofρ_i, all the sentences having $\rho_i$value less than that, are penalized from the text.

Followed to that, a well existing parts of speech tagger is used for tagging different parts of speech of a sentence and provided with different weighing factor w_i^k for k^{th} word in i^{th} sentence. The parts of speech like determinant, pronoun, conjunction, preposition and interjections are removed from the sentences for calculation. The terms are found in sentences which are having weighing factor same as w_n i.e. the weight factor for noun; their frequency is calculated in paragraph, known as term frequency, tf. Terms with high tf value, are considered as keywords. For calculating the term frequency, we need to

count the no of times the term t occurred in text document d. Hence,

$$tf(t,d) = f_{t,d} / \sum wordcountind$$

Eqn. 2

For searching of keywords in the text, we have calculated a new weight factor α_k^i for each i^{th} word in the k^{th} sentence of the text document d. Hence,

$$\alpha_k^i = tf(t_k^i, d) / \sum wordcountind$$

Eqn. 3

Now, a threshold value is fixed for finding keywords. The words with α_k^i values greater than the predefined threshold value are considered as keywords. The sentences which don't contain any keywords are further penalized to reduce the size of the original text towards getting a summery which is moving forward to generate the corresponding stego text.

B. Text Analysis for Data Hiding

The data hiding algorithms we have studied so far were applicable to the text and applied any one out of the existing 3 possible types of text steganography methods, named format based, random and statistical generation based or linguistic based methods. There are 3 factors capacity, security and robustness for any text steganographic algorithm and in our case the result obtained is going to be the best one in this respect.

We can consider our method, to show us a novel method of text steganography, in which the cover text is no way formatted or it is generated following some specific grammar or following any statistical or random generation. If the cover-file changes its structure for hiding secret data then the method may incur a chance of loss of data which may happen due to retyping error. To avoid this in the proposed method, we hide our message by generating summary of the text sample obtained in internet blogs or any easily available media file following frequency analysis of existing common letter pairs or double letter pairs in different literature. Our method is much secured compared to the methods that hide the secret bits by structure change of the text file. In our paper for simplicity of description, we have considered samples from English language text as example. This procedure obviously claims for more security.

Frequency analysis can be justified with the fact that, in any given text sample of any language, certain letters or certain letter combinations occur with different frequency values. If large amount of text of said language is statistically analyzed an accurate average letter frequency can be calculated. Such calculations can be easily made now with availability of efficient computing facility and large collection of text documents. Variety of text samples can be obtained from different sources and can be treated as examples (internet blogs, press reporting, general fiction or may be some write ups of different background).

As studied from different sources, we can say that the most common letter pairs used in English language texts as "TH", "HE", "AN", "RE", "ER", "IN", "ON", "AT", "ND", "ST", "ES", "EN", "OF", "TE", "ED", "OR", "TI", "HI", "AS" and "TO". The mostly used double letter pairs used in English language texts can be said as "LL", "EE", "SS", "OO", "TT", "FF", "RR", "NN", "PP" and "CC".

The set of common letter pairs, mentioned above, we have named as L_{CP} and the set of double letter pairs, mentioned above, we have named as L_{DP}. Our method searches for the common letter pairs or the double letter pairs in the keywords mentioned in the sentences independent of their location of obtain ability, they maps some bit representations of the secret bit stream. More over our method checks for the features of the letters of the corresponding language and classifies the alphabet depending on those obtained features. For simplicity of description, we have considered English alphabet as example and classified that alphabet set into 3 following sets L_S, L_C and L_{SS}. Out of the 3 sets L_S, L_C and L_{SS}, L_S denotes the set of letters having slanting lines, L_C denotes the set of letters having curve lines and L_{SS} denotes the set of letters having either or both sleeping and standing lines.

Considering the features of the 3 mentioned sets, we have further classified the set L_{CP} into L_{CPS} and L_{CPD} respectively, where L_{CPS} contains the members in which both the sub-member alphabets belong to same feature set and L_{CPD} contains the members in which both the sub-member alphabets belong to different feature sets.

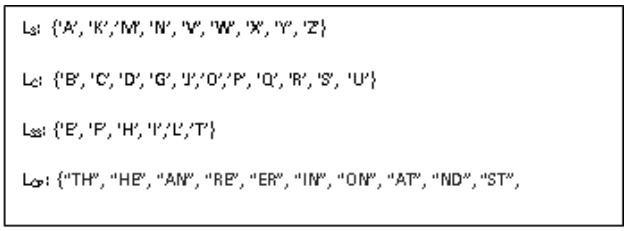

Fig. 3. Different considered alphabet sets

The mapping of the bit representation of the secret bit stream is done according to the presence of the member of the sets L_{DP}, L_{CPS} or L_{CPD}, in the keywords of the text, obtained in different sentences, can be shown in the following table.

Existence of member of set L_{DP}, L_{CPS}, L_{CPD}	Corresponding Bit representation
No or both members of L_{CPS} and L_{CPD} present	00
Only members of L_{DP} present	01
Only member of L_{CPS} present	10
Only member of L_{CPD} present	11

Fig. 4. Mapping of bit representation

C. Data Hiding through Summary Generation Algorithm

For hiding the secret message through the proposed process, first the secret message is converted from the alphanumeric form to the binary bit pattern and all the required pre processing is done on the text chosen for summery generation. Followed to that the data hiding method is applied on that text for hiding the bit pattern which is done by finding the presence of some letter pairs in the keywords of the selected text sample. The hiding method finally generates summary of the original text sample.

Hiding Algorithm:

Input: 1. Secret data to be hidden

2. A sample text written in any language (may be a Newspaper article), e.g. text sample in English, taken from a blog

Steps:

1. The secret data is first converted to its ASCII form and followed by that to respective binary bit pattern.
2. The total length of bit pattern is checked to be either even or odd. If an odd pattern is found, a '0' bit is added as the most significant bit and then total bit pattern is divided into a set of group of bits, each of size two.
3. The case text file is also set to upper case.
4. The insignificant still mostly used words of more frequency are eliminated, like determinants, which generally don't have contribution to the meaning of the text.
5. By finding the length of sentences and length of the largest sentence, the average length is calculated, which is known as the normalized length. The sentences of length less than the threshold value of normalized length are removed.
6. The mostly used words are found; specifically nouns and they are considered to be the keywords.
7. The sentences containing the keywords are collected.
8. If a sentence contains more than one keyword, for the simplicity of application only the first keyword is considered.
9. Now the common letter pairs or the double letter pairs are searched out of the set available in English literature in the sets L_{CPS} {"TH", "HE", "AN", "TE", "TI", "HI", "OR"}, L_{CPD} {"RE", "ER", "IN", "ON", "AT", "ND", "ST", "ES", "EN", "OF", "ED", "AS", "TO"} and L_{DP} {"LL", "EE", "SS", "OO", "TT", "FF", "RR", "NN", "PP", "CC"} in the keywords of the sentences of the text.
10. For each group of secret bits, if a match is found as per the mapping mentioned in the figure 3, the respective sentence is added in the summery file, else to be moved to the next sentence.
11. The steps 8 and 9 are performed until the generated bit pattern is fully used up.
12. The generated summary is the cover text sent through communication channel to the receiver.
13. The title of the generated summery is kept same as it was in case of the original text chosen for example.

Output: 1. The generated summary of the text sample, sent as cover text.

2. The set of keywords

Reversely, for extraction of the secret message, the keywords are scanned from each sentence and the corresponding pair of binary values represented by them, are appended in a file, that stores secret bits, shown in fig 3.The generated binary bit pattern, is transformed to the alphanumeric form, which is the secret data that the sender sent.

Extraction Algorithm

Input: 1. Cover Text received by receiver
2. The set of keywords, generated at the hiding end

Steps:

1. The cover text and the keywords sent by the sender are found, which are basically the nouns obtained from different sentences.
2. If a sentence contains more than one keyword, only the first keyword is to be collected in the list.
3. The obtained keyword of a sentence is checked, and the information is found that it represents which set following fig. 3. The bit pairs, represented by respective common letter pair or double letter pair, are appended.
4. The generated secret bit pattern is then transferred to alphanumeric form by considering 7 bits together from the least significant bit side.
5. The step 3 and 4 are continued until the total generated bit stream is converted to required alphanumeric form.
6. The generated message is the secret data, sent by the sender via text summary generation.

Output:

1. The hidden Secret Message

V. EXPERIMENTAL RESULTS AND ANALYSIS

The text sample chosen for implementation of proposed algorithm i.e. the input text to our system is basically a text obtained from an easily available internet blog as shown in Fig. 5. A pre processing is done on the chosen text for better summery generation and after normalizing the sentences of the text following Eqn. 1, the too small ones are penalized. Followed to that after analyzing the text the keywords of that text are generated following Eqn. 3as shown in figure 7.For

hiding, the alphanumeric secret message that is to be embedded in the cover text, is taken as "1st", as depicted in Fig. 6. First message is converted to ASCII code representation and followed to that binary pattern "11000111100111110100" is generated. The length of the generated bit pattern being even, it's divided into groups of bit pairs. Thus obtained first group is "00" if from least significant bit position, the consideration is done. We have used the approach based on searching the presence of common letter pairs or double letter pairs in the keywords of the sentences present in chosen text for implementation of our novel method of text steganography based on summary generation and we have referred the Fig 3 and Fig 4for that. Our method then scans sentences of the chosen text sample, as depicted in Fig. 5 and the sentence that is picked first, is "Having one's own house is a blessing of God." The scanned sentence is containing the keyword "house" which is belonging to the group '00' as the keyword obtained in this sentence is not containing any common letter pair or double letter pair. As the keyword "house" can hide '00', so the sentence containing that keyword is picked and stored in the file containing summary of the text, the cover text file. The same procedure is followed and the following sentence is checked and the keyword obtained is "good", which belongs to group "01" since it contains the double letter pair "OO". The next pair of bits for hiding is "11" and the next sentence is not having any such keywords that can represent "11", so this sentence would not be selected to be added in the summary and system will find the next sentence. Same method is repeatedly followed to get the output of our system which is the expected text summary as shown in Fig. 7.

Reversely the cover text is taken as input in the receiver end, as shown in Fig. 7 and scans for the presence of common letter pair or double letter pair in the keywords of it. The first sentence that is scanned is "Having one's own house is a blessing of God." The sentence contains the keyword "house" that belongs to group "00"so the bit pair value '00' is stored in a file. The system will again start to scan the next sentence and will obtain the next keyword "good" representing the bit pair "01" and the bit value '01' is appended with the previous file. The same approach is followed accordingly to get the total bit pattern "11000111100111110100". The generated bit pattern is then transformed to its alphanumeric equivalent form. Followed to that the characters of the secret message are generated that was sent by the sender. In this example the secret message sent by sender is, "1st" that was embedded in the text summary by the sender, is regenerated by receiver as shown in Fig. 8.

Having one's own house is a great blessing of God. One feels good, safe and secure at his home. A house, you know is an important necessity. The quality of life improves when you have a comfortable house of your own. It gives you an opportunity to turn some of your dreams into reality. You decorate your room as per your taste. You look after your garden with trees of fruits and flowers with loving care.

I live in a small house not far from my school. It is little way back from the road. A path leads from the gate to the porch. Small garden of my house has lovely blooms throughout the year. Downstairs there is a lounge, which is general living room with television. This room is used as

Fig. 5. Selected Text obtained from an essay in a blog

1st

Fig. 6. Secret Text, to be hidden

House, Garden, Room, Window, Good, Children, Home, Tree, Flower, Comfort

Fig. 7. Keywords generated after text pre processing

Having one's own house is a great blessing of God. One feels good, safe and secure at his home. You look after your garden with trees of fruits and flowers with loving care. Small garden of my house has lovely blooms throughout the year. Downstairs, there is a lounge, which is general living room with television. Most comfort is there in the front lawn facing drawing room with a large window. Children's room is there in the upstairs. The largest

Fig. 8. Cover Text, obtained after embedding the secret text

1st

Fig. 9 Extracted Text

You look after your garden with trees of fruits and flowers with loving care.

I live in a small house not far from my school. Small garden of my house has lovely blooms throughout the year. This room is used as reception room for guests. Most comfortable is the drawing room with a large window facing the front lawn.

Fig. 10 Summery of the selected text as generated by the Auto summarize Tool of MS Word

As our approach follows a summary generation algorithm for the purpose of data hiding, we also need to check how good the generated summary is, by following the standard summary evaluation process along with the maintained similarity between the sent text and the received text. The key factors for

this evaluation process are finding the compression ratio and retention ratio. If we denote length of summary and information in it with the terms L_s and I_s and if we denote length of full text and information in it with the terms L_T and I_T, then the compression ratio(R_C) and retention ratio(R_R) are denoted as follows.

$$R_C = L_S / L_T$$

Eqn. 4

$$R_R = I_S / I_T$$

Eqn. 5

On the basis of the above mentioned factors a comparison is done between the proposed method and the other 2 existing methods and the following table shows the details of it.

Evaluation Process	Auto Summarize method	Summary by Reflection Symmetry method	Proposed method
R_C	0.35	0.38	0.37
R_T	0.58	0.62	0.81

Fig. 11. Comparative analysis of proposed method with existing methods

VI. ADVANTAGES AND DISADVANTAGES

Our proposed method does not change the structure of the file to embed secret information and creates a text summary of an easily available text media like newspaper article or blog posts. As the structure is kept unchanged, it won't draw any suspicious attention. Our method also provides a semantically better output, if a comparison is done with the output generated by the Auto Summarize Tool, provided by Microsoft Words. More over data hidden using the proposed algorithm can be of huge volume as no restriction is applied on the text size. This method can be applied on text samples of user's choice which may be of any language by analyzing more and more text samples of the same language.

But as the method may take some more amount of time in pre processing section of the text, it may be considered as disadvantage of the system from the point of view of time complexity. Though the pre processing section helps to generate a more accurate and meaningful summary from the perspective of better compression and retention ratio.

VII.CONCLUSION AND FUTURE SCOPE

A generalized model for text steganography has been proposed in this paper by text summary generation using frequency analysis. This approach is a generalized one as it is applicable on text samples of any language text, through a technique that uses an intelligent way of summary generation for data hiding. The proposed method checks for the existence of common letter pairs or double letter pairs in keywords of the paragraph, located in the set of normalized sentences of the paragraph for hiding secret message. Reverse method is followed at the receiver side, the existence of the keywords in the sentences of the summary generated at the encryption end are checked and the relevant bit pairs are placed to get the actual message sent by the sender back at the receiver side. Future research can be done to reduce time of pre processing the proposed system incurs in perspective of getting a much compressed summary with more information.

REFERENCES

[1] C .Cachin, "An Information-Theoretic Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306318, 1998

[2] R Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE pp. 1019-1022, 2001.

[3] G. Simmons, "The prisoners problem and the subliminal channel, " CRYPTO, pp.51–67, 1983.

[4] J. Chen, T. S. Chen, M. W. Cheng, "A New Data Hiding Scheme in Binary Image, " in Proc. Fifth Int. Symp.on Multimedia Software Engineering. Proceedings, pp. 88-93 (2003).

[5] G. Doërr and J.L. Dugelay, "A Guide Tour of Video Watermarking", Signal Processing: Image Communication, vol. 18, Issue 4, 2003, pp. 263-282.

[6] G. Doërr and J.L. Dugelay, "Security Pitfalls of Frameby- Frame Approaches to Video Watermarking", IEEE Transactions on Signal Processing, Supplement on Secure Media, vol. 52, Issue 10, 2004, pp. 2955-2964.

[7] Subhranil Som (2015) "Encryption Technique Using Elliptic Curve Cryptography through Compression and Artificial Intelligence", International Conference on CSI-2015, Theme: Digital Life, Springer Proceedings and Scopus Indexed, 2 – 5 December 2015, New Delhi, India.

[8] K. Gopalan, "Audio steganography using bit modification", Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03), vol. 2, 6-10 April 2003, pp. 421-424.

[9] PengMeng, Liusheng Huang, Zhili Chen, Wei Yang, Dong Li, " Linguistic Steganography Detection Based on Perplexity", International Conference on MultiMedia and Information Technology, pp 217-220, 2008.

[10] Abhishek Bhardwaj, Subhranil Som, S. K. Muttoo, (2018) "HS1-RIV: Improved Efficiency for Authenticated Encryption", International Journal of Engineering and Technology (UAE), Scopus Indexed, DOI: 10.14419/ijet.v7i2.7.10871, Vol. 7, Issue 2.7, Page 502-506.

[11] S.H. Low, N.F. Maxemchuk, J.T. Brassil, and L.O'Gorman, "Document marking and identification using both line and word shifting", Proceedings of the Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '95), 2-6 April

[12] Y. Kim, K. Moon, and I. Oh, "A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics", Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03), 2003, pp. 775–779

[13] K. Rabah, "Steganography-The Art of Hiding Data", Information Technology Journal, vol. 3, Issue 3, pp. 245-269, 2004.

[14] Shirali-Shahreza, M.H.; Shirali-Shahreza, M., "A New Approach to Persian/Arabic Text Steganography ", Computer and Information Science, 2006. ICIS-COMSAR 2006. 5th IEEE/ACIS International Conference on 10-12 July 2006 Page(s):310 – 315.

[15] S. Changder, N.C. Debnath, "An Approach to Bengali Text Steganography", Proceedings of the International Conference on

Software Engineering and Data Engineering (SEDE-08), ISBN: 978-1-880843-67-3, pp. 74-78, July, 2008, Los Angeles, California, USA.

[16] Som S., Banerjee M., (2013) "Cryptographic Technique by Square Matrix and Single Point Crossover on Binary Field", 1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA'13), IEEE Explorer, Print ISBN: 978-1-4673-2820-3, February 12 – 14, 2013, Sharjah, UAE.

[17] S. Changder, N.C. Debnath, D. Ghosh, "LCS based Text Steganography through Indian Languages" Proceedings of 2010 3rd IEEE International Conference on Computer Science and Information Technology(ICCSIT 2010), ISBN: 978-1-4244-5539-3, pp. 53-58(vol 8) July, 2010, Chengdu, China

[18] S. Changder, S.Das, D.Ghosh, "Text Steganography through Indian Languages using Feature Coding Method", Proceedings of the 2nd International Conference on Computer Technology and Development (ICCTD), 2010, 10.1109/ICCTD.2010.5645849, Page(s): 501 – 505, November 2010, Cairo.

[19] Seema Nath, Subhranil Som (2017), "Security and Privacy Challenges: Internet of Things", Indian Journal of Science and Technology, Scopus Indexed, included in 'Web of Science' and included in the list of journal recommended by UGC, Vol 10(3), DOI: 10.17485/ijst/2017/v10i3/110642, ISSN (Print) : 0974-6846 ISSN (Online) : 0974-5645, January 2017.

[20] S. Changder, N.C. Debnath, D. Ghosh, "A Greedy approach to Text Steganography using Properties of Sentences" Proceedings of the Eighth International Conference on Information Technology: New Generations (ITNG), 2011, ISBN: 978-1-61284-427-5 Pages(s): 30-35, April, 2011, Las Vegas, NV.

[21] A. Majumder, S. Changder, "A Novel Approach for Text Steganography: Generating Text Summary using Reflection Symmetry" published in Procedia Technology (ISSN: 2212-0173), Elsivier, Volume 10, Pages 1-998 (2013), First International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013, Pages(s): 112-120, September 25-27, 2013, University of Kalyani, Department of Computer Science & Engineering.