

A Survey of Hindi Text Steganography

Tatwadarshi P. Nagarhalli, Dr. J. W. Bakal, Neha Jain

Abstract— Steganography is an art of hiding secret message in an unsuspecting cover document. Over the many years many systems have been proposed for the same. With the advancement of technical know-how even the cover medium has under gone certain changes. Generally the cover mediums used include text, image, audio and video. Text steganography is one of the oldest techniques of steganography which still generates much interest for the researchers. Over the many decades text steganography has been adopted for many local languages, and popular language of Hindi is no different. This paper takes a look and analyses the different Hindi Text Steganography techniques that have been proposed.

Index Terms— Information Security, Text Steganography, Information Hiding, Hindi Text Steganography, Hindi Information Hiding, Devnagari Script Text Steganography, Devnagari Script Information Hiding.

1 INTRODUCTION

Steganography and Cryptography are very popular techniques that are used since ancient times for the purpose of sending secret and important messages. These techniques are used to ensure that the data is accessed only by the sender and intended receiver and not by any intruder. Steganography is the art of covered or hidden writing [23]. A Steganographic system embeds hidden content in unremarkable covered media so as to not arouse an eavesdropper's suspicion. Historical Steganographic methods made use of physical steganography i.e. the covers used were: human skin, scalp, etc. Whereas, the modern Steganographic methods make use of cover media such as image, audio, video, etc. Cryptography protects the information by converting the data into an unreadable format. This process is known as encryption [24].

Steganography hides the covert message but not the fact that two parties are communicating with each other. The steganography process generally involves placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme [25].

In summary:

steganography_medium = hidden_message + carrier + steganography_key.

Classification of Steganography:

- Author Tatwadarshi P. N. P.G. Student, Dept. of Comp. Engg., Shree L. R. Tiwari College of Engineering, Mumbai, India. E-mail: tatwadarshipn@gmail.com.
- Co-Author Dr. J. W. Bakal, Principal, Shivajirao S. Jondhale College of Engineering Mumbai, India. E-mail: bakaljw@gmail.com
- Co-Author Neha Jain, Asst. Prof., Dept. of Comp. Engg., Shree L.R. Tiwari College of Engineering, Mumbai, India. E-mail: nehajain206@yahoo.com.

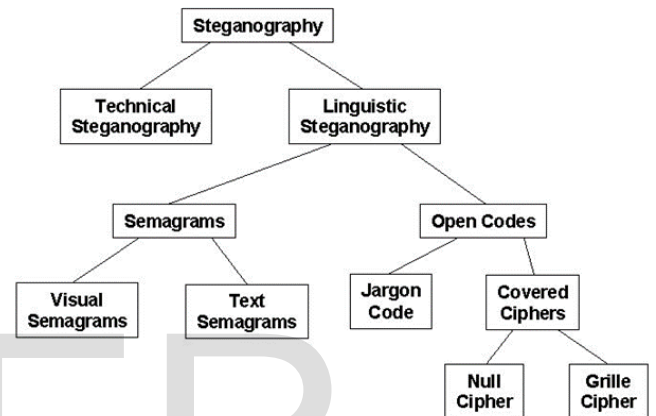


Fig. 1: Classification of Steganography Techniques [25]

Fig. 1 shows a common taxonomy of steganography techniques:

- i. Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods.
- ii. Linguistic steganography hides the message in the carrier in some nonobvious ways and is further categorized as semagrams or open codes.
- iii. Semagrams hide information by the use of symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or Website. A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters or handwritten text.
- iv. Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer. The carrier message is sometimes called the overt communication whereas the hidden message is the covert communication. This category is subdivided into jargon codes and covered ciphers.
- v. Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others. Jargon codes include warchalking (symbols used to indicate the presence and type of wireless network signal), underground terminology, or an innocent conversation that conveys special meaning be-

cause of facts known only to the speakers. A subset of jargon codes is cue codes, where certain prearranged phrases convey meaning.

Covered or concealment ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed. A grille cipher employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the hidden message. A null cipher hides the message according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word."

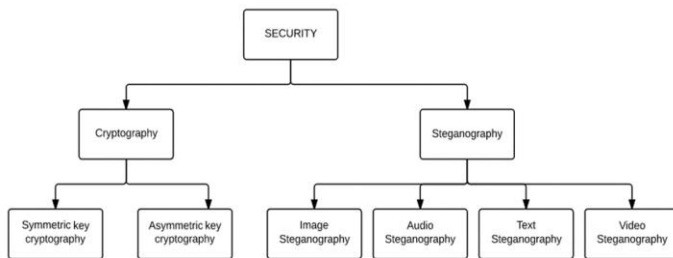


Fig. 2: Classification of security domain

Fig. 2 shows the classification of Security domains. Security domain can be classified as follows:

Steganography [23]: Steganography can be classified mainly into following categories:

- 1) Image Steganography: In image steganography, the data is hidden in a cover image. Images contain a lot of redundant information in which the data or the message can be embedded efficiently.
- 2) Video Steganography: Video steganography hides the data in a video. The pixel changes in the respective frames of videos are harder to detect than image steganography.
- 3) Audio Steganography: In audio steganography, data is hidden by modifying the audio signal so that the changes cannot be easily intercepted by unauthorized personnel.
- 4) Text Steganography: Text steganography hides data behind a cover text file.

Cryptography: Cryptographic algorithms can be classified further as symmetric key or asymmetric key cryptography algorithms. It depends on whether the algorithm that is to be used uses the same key or different key for encryption and decryption [26].

2 TEXT STEGANOGRAPHY

This paper pertains to text steganography and especially Hindi Text Steganography. Text steganography have been studied and new techniques have been invented and proposed over many decades. Initially the text steganography technique was limited to only English language and it started by inserting a

secret message into a paragraph, character by character, was introduced in the paper titled 'Steganography and Steganalysis' by Moreland [1]. Open spaces in the writings have also been used to encode hidden information. This is by using the inter sentence spacing, inter word spacing or end of line spacing [2, 3].

Techniques have also been proposed to exploit the differences in spelling of a same word in English. It is known that a same English word is spelled differently in US and UK styles. For example, the word 'Defence' is spelled in the US style as 'Defense' and in the UK style as 'Defence'. The paper titled 'Text Steganography by Changing Words Spelling' proposes that if in a sentence a US styled spelling is used then the hidden bit is '0' and if UK style is used then the hidden bit is '1' [4].

Another technique used is the shifting of the lines. The words are shifted vertically or horizontally to a certain degree. The degree of deviation hold the hidden message [5, 6, 7].

With the advent of Short messaging services (SMS), even those have been used to hide information. One techniques is by using the abbreviations that are generally used in the SMSs, if the abbreviations are used then the hidden bit is '1' and if the full for is used then the hidden bit is '0' [8]. Even the emoticons have been used to hide information. Here, a dictionary is created which maps a particular emoticon to an alphabet or a number [9]. For online chat these emoticons have been used to steganography purposes by dividing the emoticons into different set of emotions [10].

Inspiration has also been taken from ancient texts to provide new a technique of using a set or a combination of adjectives to hide secret information [11].

Even regional languages have been used to hide information. The large number of dots that are present in Arabic, Persian and Urdu languages provide ample opportunities for hiding secret data [12, 13, 14].

In the same way even the scope of stenographic approach in Hindi text is very vast. And considering the large amount of people using this medium as communication and the extent of leg room that is present for hiding secret information in a Hindi text it is important understand and explore the different techniques that have been proposed in the field of Hindi text steganography. Also, the language itself is so flexible that it provides ample opportunities for steganography.

Hindi text steganography can be classified into two types according to the usage of the Hindi letters and words. One type is usage of Hindi words and letters to store some other information in bit wise manner. The second type is where the Hindi text itself is encoded into some for or the other; that is, here the Hindi text itself is the secret message.

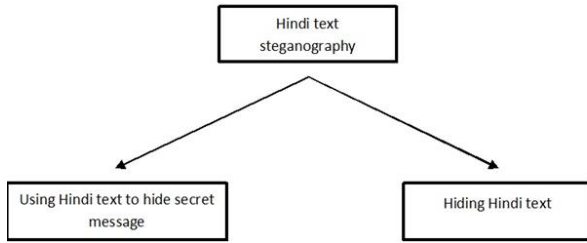


Fig. 3 Classification of Hindi Text Steganography

The Fig. 3 shows the classification of Hindi text steganography. Extensive research has been carried out for hiding bit level information into the Hindi word whereas unfortunately no credible techniques for hiding Hindi text has been proposed.

3 TECHNIQUES FOR USING HINDI TEXT TO HIDE OTHER INFORMATION

Following Techniques have been proposed in the field of Hindi Text Steganography.

3.1 Hindi Text Steganography using Diacritics and its Compound words [15, 16]

This paper proposes two techniques for the purpose of data hiding.

a. Text Steganography using Hindi letters and its Diacritics

Generally in any language the formation of the sentence is possible by the use of consonants and vowels. And complex sentences contain compound letters and sentences. The proposed technique uses these consonants, vowels and compound letters. Here, the secret message is converted into ASCII code; the ASCII code is in binary form. Now, Hindi consonants and vowels are used in the sentence to denote '0' and compound letters are used to hide '1'. These Hindi letters are then used to form a meaningful Hindi sentence. For example

```

01 01 0011 011 1 010 001100 1
इसे यहाँ जबर्दस्त पढ़ाना तो बहुत अरण्यरोदन हैं।

01 01 100 11 1
अभी उसे लाकर दादा से

011 0000 1 01 1011 1 0011 011
अखाड़ा रखकर मैं उसे पाठशाला में इलतिजा करूँगी।
    
```

Fig. 4 Hindi Text Steganography using Hindi Letters and its Diacritics [15, 16]

The Fig. 4 provides the example of hiding binary bits in Hindi letters (sentences).

Major drawback of the system is that the encoding and decoding is a majority manual work and a very tedious task. It requires, especially for the decoding part, people who have full command on Hindi language and its structure, this re-

stricts the use of the technique.

b. Text Steganography using Hindi Numerical code

In the proposed technique all the consonants and vowels are given specific numerical code. These consonants and vowels in total forms 15 different categories. The coding scheme has been given as follows

Hindi Vowels						
4	4	3	4	2	2	0
अ	आ	इ	ई	उ	ऊ	ऋ
1	1	4	4	4	4	
ए	ऐ	ओ	औ	अं	अः	

Fig. 5 Vowel Encoding Scheme [15, 16]

Fig. 5 shows the coding scheme for the Hindi Vowels proposed in the paper

Hindi Consonants					
5	6	7	8	9	
क	ख	ग	घ	ङ	
10	11	12	13		
च	छ	ज	झ	ञ	
10	11	12	13		
ट	ठ	ड	ढ	ण	
5	6	7	8	9	
त	थ	द	ध	न	
5	6	7	8	9	
प	फ	ब	भ	म	
5	6	7	8	9	
य	र	ल	व	श	
10	11	12	14		15
ष	स	ह	क्ष	त्र	ज्ञ

Fig. 6 Consonant Encoding Scheme

The Fig. 6 shows the coding schemes for Hindi consonants. Even in this technique the decoding part will require proficiency in Hindi language and structure of sentence.

3.2 Hindi Text Steganography by Shifting of Matra [17]

It has been seen that any Hindi word when used in a sentence has a specific structure; that is, it is always seen that the consonant is followed by a vowel at the end, without exception. The proposed techniques make use of this characteristics for stenographical purpose. When a vowel 'e', which is pronounced as 'a', is added to any consonant a 'matra' is added to the top of the consonant.

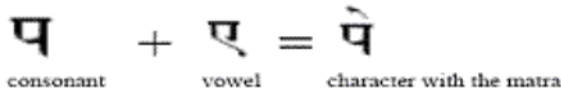


Fig. 7 Consonant with medial vowel (matra) [17]

The Fig. 7 shows the changes in the consonant when the matra 'e' is added. A stroke of tilted line is added above the consonant.

By shifting the matra slightly to the right information can be hidden. If the binary value to be hidden is '0' then the character remains unchanged, and if the binary value to be hidden is '1' then the matra is shifted slightly towards the right. For example:

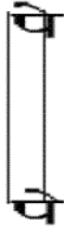


Fig. 8 Horizontal shifting (towards right) of the 'matra' (ligature) of the Hindi character [17]

The Fig. 8 shows the slight horizontal movement of the matra towards the right. This horizontal movement indicates the hidden binary bit is '1' and if the character is kept unchanged then the hidden bit is '0'.

The main advantage of this method is the scope that it provides to hide information, very large number of bits can be hidden. The disadvantage of this technique is the over reliance on Optical Character Recognition; also a fixed font has to be used to get the desired results.

3.3 Hindi Text Steganography Using Matraye, Core Classification And HHK Scheme [18]

This paper proposes three techniques for hiding binary bits into the Hindi sentences.

- a. Hindi Text Steganography by using Character Modifiers (Matra)

When a vowel is added to the consonant a matra is added to the consonant in Hindi. Here, the matra can be added on the top of the consonant or at the bottom or to the side of the consonant. The proposed techniques uses the matra's added on top of the consonant and at the bottom of the consonant. If the bit to be hidden is '0' then the matra is added at the bottom of the consonant and if it is '1' then the matra is added at the top of the consonant.

- b. Hindi Text Steganography by using Open header, bar, no bar and special characters

In this technique the header, the full stop and the special characters of the Hindi language is used to hide two bit data. The full stop in Hindi is denoted by a bar '|'. The use and non-usage of these characters ensures the hidden meaning. The encoding and decoding is performed with the help of the given table.

TABLE 1
CHARACTER ENCODING SCHEMES

Type	Encoding
Open header	00
Bar	10
No Bar	01
Special Characters	11

The table 1 gives the encoding scheme of the proposed technique.

- c. Using HHK Encoding (Hindi Hexadecimal modified Katapayadi Encoding) Scheme

Here a text to be hidden is first converted into its ASCII value. The ASCII value obtained here is in the binary form. This binary ASCII value is converted to Hexadecimal code. A sequence of Hindi characters and words are found for the equivalent hexadecimal code.

One of the major merit of the proposed techniques is that, techniques have been proposed for not only hiding one bit binary bit even two bit binary bit are considered and for the first time rather than hiding bits characters and words are hidden in the third technique.

3.4 A Novel Approach to Hindi Text Steganography [19]

This paper proposes three techniques for hiding binary bits with the help of Hindi language.

- a. Punctuation mark based

Here a table of punctuations that are available in the Hindi language are used to store hide bit sequence. The encoding and the de coding is performed with the help of the table given.

TABLE 2
ENCODING TABLE FOR PUNCTUATION MARKS

0	.	" "	"
1			' '	()
2	;	-	:-	o
3	-	?	!	^

The table 2 provides the encoding scheme for the punctuation marks proposed in the paper.

The bits to be encoded are mapped with the appropriate punctuation marks and used in a Hindi sentence. For example to hide 'se', which can be represented in binary as 01 11 00 11 01 10 01 01. The corresponding Hindi sentence can be given as

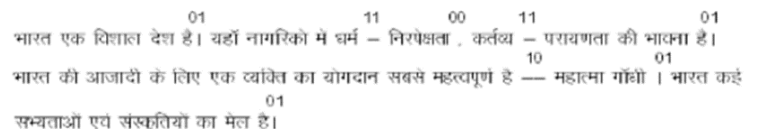


Fig. 9 Punctuation mark Encoding

The Fig. 9 shows the successful integration of the bits in the Hindi sentence, proposed in the paper.

b. Synonym Based

In this technique a four level mapping table is created where the advantage of having multiple synonyms in the Hindi language is used to hide two bit binary at a time. At the encoding side when a secret message is to be hidden it is first converted to binary and then with help of the mapping table appropriate words can be chosen. The mapping table can be created as

0	1	2	3
सफल	समृद्ध	धन्य	सौभाग्यशाली
संघ	मातृभूमि	राष्ट्र	देश
आजादी	स्वतंत्र	स्वाधीन	मुक्त
अरादान	भागदान	सहयोग	योगदान
असह्यार	महत्त्वपूर्ण	आवश्यक	प्रभाक्शाली
बहुत	बहुतेरे	अनेक	कई
अध्यापन	शिक्षा	सीख	उपदेश
प्रबन्ध	संगठन	संघटन	व्यवस्थापन

Fig. 10 Table of Synonyms

The Fig. 10 shows table where the Hindi word and its corresponding three synonyms used for the mapping purpose.

And, to hide 'se', which can be represented in binary as 01 11 00 11 01 10 01 01. The corresponding Hindi sentence can be given as

01 11 00 11 01 10 01 01
 भारत एक समृद्ध देश है। भारत की आजादी के लिए एक व्यक्ति का योगदान सबसे महत्त्वपूर्ण है —
 महात्मा गाँधी । भारत में अनेक , शिक्षा प्रदान करने वाले संगठन हैं।

Fig. 11 Synonyms based Encoding

The Fig. 11 shows the successful integration of the bits in the Hindi sentence, proposed in the paper.

c. Sanskrit classification based

Here a two level mapping table has been proposed which will contain Tatbhav and Tatsama words. Tatbhav hides '0' and Tatsama hides '1'. Tatbhav is the actual word or the synonym of a word whereas Tatsama is not an exact synonym but still a very closely related word to the main word, here a Sanskrit word is used for the same purpose. The table given is

0	1
सावन	श्रावण
छाता	छत्र
मार	मयूर
नाच	नृत्य
रात	रात्रि
साँप	सर्प
आग	अग्नि
सूरज	सूर्य

Fig. 12 Table of Tatbhav and Tatsama

The Fig. 12 shows table where the encoding scheme has been given. Tatbhav is encoding scheme for '0' whereas tatsama serves the purpose for '1'.

To hide 's' whose binary value is 01 11 00 11, the corresponding Hindi sentence can be given as

0 1
 सावन में समान्यतः अच्छी वर्षा होती है। लोग छत्र लेकर घरो से निकलते हैं।
 1 1 0 0
 मयूर नृत्य करने लगते हैं। रात में साँप इत्यादि निकल आते हैं। अग्नि की भाँति
 1
 सूर्य लुप्त हो जाता है।

Fig. 13 Sanskrit classification based Encoding

The Fig. 13 shows the successful implementation of the proposed technique.

The major advantage of these techniques is that it is easy to implement because of the dictionary's that have been used in all the techniques. But the drawback of these systems is that to hide even a small information a very large paragraph or essay of Hindi sentences needs to be created.

3.5 Ancient Kalapayidi System Sanskrit Encryption Technique Unified [20]

This paper proposes converting of English words into an appropriate Hindi words having the similar meaning with the help of an English-Hindi dictionary. Then, these Hindi alphabets are converted to numerical values with the help of Kalapayidi System mapping. Now at the odd positions 1 is added to the numerical set that has been found. This new set of numerical values are again checked with the Kalapayidi System to get a possible meaningful Hindi words. Once a meaningful Hindi words have been found then using Hindi English dictionary appropriate English words are found. This is the encrypted cypher text.

For example 'Love is God', this is converted using the Hindi-English dictionary

‘प्रेम हि ईश्वर’

Fig. 14 'Love is God' in Hindi

Fig. 14 shows the example of how the English sentence in Hindi using the Hindi-English dictionary.

Now using the Kalapayidi scheme it is converted to 1258428. Now here the odd positions are added with 1. So the new numerical set is 2268529. Now again using the Kalapayidi system a meaningful hindi words are found. And this meaningful Hindi words are converted to meaningful English

words using the dictionary again.

The problem with this method is that it is very confusing and difficult to implement. Also, the decryption part of the algorithm has not been mentioned and it seems extremely difficult to get back the original text from the cipher text.

3.6 Cross Language Cipher Technique [21]

This paper proposes a technique where English plain text is converted to a cipher text, in Hindi. The conversion is not according to dictionary. Here using the simple substitution cipher, the English sentences or words are first considered in an alphabetical format. Then, these alphabets are converted into their ASCII value. A mapping table is maintained where each ASCII code of English alphabets is mapped to a corresponding ASCII value of a Hindi alphabet.

After the mapping is complete a set of Hindi alphabets are obtained, this is the cypher text. At the receiver side the reverse process is carried out to get the hidden English word.

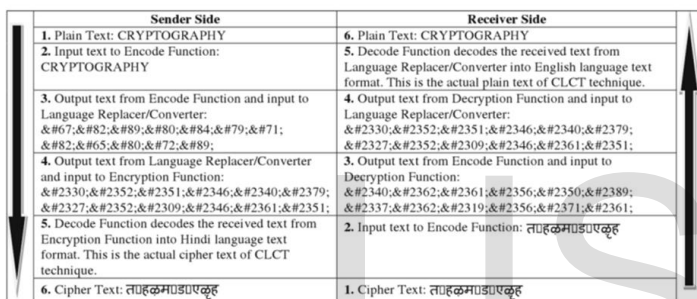


Fig. 15 Encryption and Decryption algorithm for Cross Language Cipher Technique

Fig. 15 shows the algorithm of encryption and decryption algorithm with an example of the proposed technique.

One major drawback of the system is that the Hindi cipher text is not a meaningful Hindi word that is, it is a non-logical set of Hindi alphabets which might indicate to the ev's dropper that this is a coded message and is carries some hidden message.

4 CONCLUSION

The paper has analysed six papers which have proposed techniques to hide bit-level information or used Hindi or Devnagari script in some way or the other to hide information. The working, advantages and the problems of the proposed systems have been analysed in detail in this paper. Extensive research have been carried out in the field of Hindi text steganography. And all the techniques proposed have, in their unique way, proven to be very useful.

The main hindrance and problem that remains though, it is to hide very small amount of data a very large number of Hindi words are used. Further research needs to be undertaken to tackle this drawback. Also, it has been seen that all the techniques that have been proposed pertains to hiding binary bits into Hindi words. So, further research is also necessary in the field of Hindi text steganography where Hindi words can be hidden in some

other form or medium.

REFERENCES

- [1] T. Moreland, "Steganography and steganalysis", Leiden Institute Of Advanced Computing Science, www.liacs.nl/home/tmoerl/privtech.pdf
- [2] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding", IBM Systems Journal, Vol. 35, Issues 3&4, 1996, pp. 313-336.
- [3] R. Popa, "An Analysis of Steganographic Techniques", The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of computer science and Software Engineering, 1998.
- [4] Shirali-Shahreza, "Text Steganography by Changing Words Spelling", Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference 17-20 Feb. 2008
- [5] S. H. Low, N. F. Maxemchuk, J. T. Brassil, and L. O'Gorman, "Document Marking and Identification Using Both Line and Word Shifting", in 14th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '95), vol.2, 1995, pp. 853-860.
- [6] A. M. Alattar and O. M. Alattar, "Watermarking electronic Text Documents Containing Justified Paragraphs and Irregular Line Spacing", in SPIE, Security, Steganography, and Watermarking of Multimedia Contents VI, vol. 5306, pp. 685-695.
- [7] Y. Kim, K. Moon and I. Oh, "A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics", in 7th International Conference on Document Analysis and Recognition (ICDAR03), 2003, pp. 775-779.
- [8] M. Shirali-Shahreza, M. H. Shirali-Shahreza, "Text Steganography in SMS", International Conference on Convergence Information Technology, 2007, 2260 – 2265
- [9] T. P. Nagarhalli, "A New Approach to SMS Text Steganography using Emoticons", International Journal of Computer Applications (0975 – 8887) National Conference on Role of Engineers in Nation Building (NCRENB-14), 2014.
- [10] Z. Wang, "Emoticon-based Text Steganography in Chat", Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications, pp. 457-460, 2009.
- [11] T. P. Nagarhalli, "A New Approach to Text Steganography Using Adjec-tives", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 5, May 2015, pp. 3147-3152
- [12] M. H. Shirali-Shahreza, M. Shirali-Shahreza, "A New Approach to Persian/Arabic Text Steganography", In Computer and Information Science, ICIS-COMSAR 2006. 5th IEEE/ACIS International Conference, pp 310-315, 10-12 July 2006.
- [13] M. H. Shirali-Shahreza and S. Shirali-Shahreza, "A Robust Page Segmentation Method for Persian/Arabic Document", WSEAS Transactions on Computers, vol. 4, Issue 11, Nov. 2005, pp. 1692 – 1698.
- [14] J. A. Memon, K. Khowaja and H. Kazi, "Evaluation of steganography for Urdu /Arabic text", Journal of Theoretical and Applied Information Technology, pp. 232 – 237.
- [15] K. Alla, and R. Siva Rama Prasad, "A Novel Hindi Text Steganography using Diacritics and its Compound words", IJCSN International journal of Computer Science and Network Security, Vol. 8 No. 12, 2008, pp. 404 – 409.
- [16] K. Alla, and R. Siva Rama Prasad, "An Evolution of Hindi Text Steganography", Sixth International Conference on Information Technology: New Generations, IEEE, 2009, pp. 1577 – 1578.
- [17] S. Changder, N. C. Debnath and D. Ghosh, "Hindi Text Steganography by Shifting of Matra", International Conference on Advances in Recent Technologies in Communication and Computing, IEEE, 2009, pp. 199 – 202.
- [18] K. Alla, and R. Siva Rama Prasad, "A New Approach to Hindi Text Steganography Using Matraye", Core Classification And HHK Scheme, Seventh International Conference on Information Technology, IEEE, 2010, pp. 1223 – 1224.
- [19] M. Srivastava, M. Q. Rafiq and R. K. Tiwari, "A Novel Approach to Hindi Text Steganography", Second International Conference on Advances in Communication, Network, and Computing, CNC, Springer, 2011, pp. 295 – 298.
- [20] A. K. Agarwal and D. K. Srivastava, "Ancient Kalapayidi System Sanskrit Encryption Technique Unified", International Conference on Signal Propagation and Computer Technology (ICSPCT), IEEE, 12-13 July 2014.
- [21] L. Singh and R. Johari, "Cross Language Cipher Technique", Security in Computing and Communications: Third International Symposium, SSCC

- 2015, Kochi, India. Springer International Publishing Switzerland, August 10-13 2015.
- [22] S. Changder, D. Ghosh and N. C. Debnath, "Linguistic approach for text steganography through Indian text", 2010 2nd Int. Conf. on Computer Technology and Development, 2010, pp. 318-322.
- [23] V. Sharma and S. Kumar, "A new approach to hide text in image using Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 4, April 2013.
- [24] M. Pavan, S. Naganjaneyulu and C. Nagaraju, "A Survey on LSB Based Steganography Methods", International Journal of Engineering and Computer Science, Vol.2, Issue 8, August 2013.
- [25] G. C. Kessler "An Overview of Steganography for the Computer Forensics Examiner", February 2004 (updated February 2015), http://www.garykessler.net/library/fsc_stego.html.
- [26] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard, last accessed on: 12/9/2015.

IJSER