HIGH-CAPACITY MULTI-LAYER FRAMEWORK FOR HIGHLY ROBUST TEXTUAL STEGANOGRAPHY

[1]Ahmed khan, [2] Muhammad Sohaib, [3] Muhammad Faisal Amjad

[1 2 3] Department of Information Security, NUST, Pakistan.

[1] Department of Computer Science, COMSATS, Pakistan.

ahmed.khan@comsats.edu.pk , [3] faisal@nust.edu.pk

ABSTRACT- *A novel approach has been proposed to improve security and imperceptibility to achieve secure communication. Information hiding has been extensively functional on diverse fields due to enormous use of internet, with support of two major branches, digital watermarking and Steganography. The security issues become prime and necessary concern and energized requirement for better techniques for securing info. In this paper we have proposed a novel text steganography technique by using its technical properties. Proposed technique is storing of text files require less memory and it works faster and makes communication preferable to other mediums of steganography. Paper aim is to develop model to improve capacity, imperceptibility and robustness by multilayer textual steganography with combination of encryption, compression and embedding approach for data obscurity. Various functions are used to encrypt secret word for number of times in our proposed method. Compression is achieved through Lemple-ZIV compression method which as a result reduces size of secret word and embedding is achieved with help of permutation method. Experimental results show that proposed scheme has improved stego features as early research uses less embedding capacity approach which affects other two features.*

INTRODUCTION

In the field of data communication, security issues are the prime concern and therefore are given top priority. Classical cryptography is one of the methods to secure the data over the communication channel and furthermore, security is augmented by introducing the concept of steganography [1]. Steganography is the art of hiding secret information in cover message without getting attention of the third party as shown in Fig 1. Image, audio, video, text and network protocols can be the carrier of secret messages [2].

With the development of computer networks much information has been developed and exchanged on the internet [3]. Since dawn of written communication, people have been concerned to obscuring the content of communication by using cryptography; and obscuring the fact that communication takes place with the help of steganography [4].

Steganography hides the information in such a way that no one apart from the sender and intended receiver, suspects the existences of the message [5]. Stegnalysis is the analysis of the stego text in order to check its robustness and detect/ extract the secret messages [6]. A successful steganographic algorithm requires that steganographically hidden message cannot be detected by the malicious users [7].

Although, all digital file formats are used for steganography, but most suitable are the image and audio files, because of their high degree of redundancy [8-9]. However, text steganography is most difficult approach of information hiding because of low amount of redundancy in its nature [10-11]. Text steganography is broadly divided into two categories, one is technical text steganography and other is linguistic text steganography. Text Steganography: based on following parameters [12].

- **Robustness:** It is measure of strength of the hidden message so that it could not be revealed to an attacker [13-14].
- **Capacity:** It measures the amount of data that can be hidden in given cover like picture, sound, and database [15-16].
- **Perceptibility:** Advanced content steganography methods are considered recognizable when there is a possibility that hidden message can be perceived by an attacker [17].
- **Security:** When mystery data is imperceptible from the interloper during the transmission of data [18].
- **Integrity:** The legitimacy of a transmitted message [19], course of action that guarantee that the substance of message have not been modified. The content Steganography is craft of concealing the data by utilizing the regular dialect to cover a mystery message as characterized by Chapman at al [20]. Implanting calculations help to encode [21] the message and the resultant message is called stego-message which is transmitted over the correspondence channel [22].

During the transmission it is being observed by the unapproved viewers who will just perceive the transmission of guiltless message without finding the presence of the shrouded message in it [23-24]. Content Steganography is comprehensively characterized into four types [25-26], specialized Steganography, etymological Steganography, irregular & factual and different strategy Steganography [27-28].

Emoticon characters can also contain some information; however they have an inherent problem of increasing the size, when used for hiding information [29-30].

Technical steganography includes Word shifting technique, in which the secret message which is to be hidden is shifted horizontally i.e from left or right to represent bit 0 or 1 correspondingly.

Line shifting involves hiding the secret message vertically by shifting the lines of the text to some extent. Network steganography includes usage of protocols like TCP/IP [2-23]. Other methods of text steganography include hiding message in images, audio and video files.

Linguistic Steganography includes syntactic and semantic methods of data hiding. Syntactic technique involves using of punctuation marks like full stops, commas to hide the data and semantic method uses similar meaning word to hide text in that particular word without changing the context of the sentence. Random and statistical steganographic methods utilize random sequence of characters to conceal the information [7-9].

Table 1.Types of text Steganography

Types Text Steganography	Techniques
Technical (TS)	Word shifting, Line shifting, Feature coding, HTML tag, Image, Audio, Video and Network Steganography
Linguistic (TS)	Syntactic, Semantic, Abbreviations and Change of spelling
Random & Statistical	Probabilistic context-free grammar, Character Sequence, Words Sequence and Sequences-text mimicking

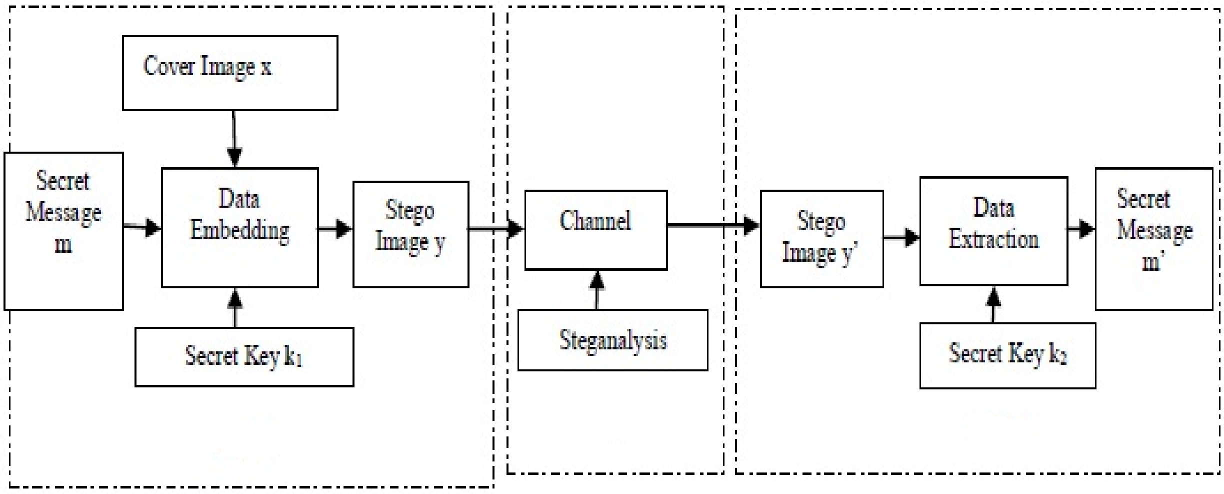

Fig.1 Steganography Process

In another technique, statistical properties such as letter frequencies and word length are widely utilized to generate a resultant word which as a result will point to the same statistical properties as depicted by the actual word which is present in the cover source. The existing schemes [1-2,9-13,23,30] are mostly using single security layer for data transmission, which trim down robustness of the hidden information due to the absence of encryption and permutation. Data hiding using LSB technique is not a recommended option as the hidden data can be extracted by the analysis of LSB. The techniques used in [3-4,21] of text Steganography has drastic effects on imperceptibility, which is quite low than the acceptable level. As a result the pattern of alphabets are changed and statistical detection of the text dig out imperceptibility differences of natural and stego-text. In the schemes [1-2,4-5,9,11,13,16,19,22], the cover message provides small storage capacity. Usage of small scale dictionary and incomplete vocabulary restrict their hidden capacity.

The paper is organized as follows: The related work and proposed methodology along with algorithms is elaborated in section 2 and section 3 respectively. Section 4 presents the experimental results and the paper is concluded in section 6.

RELATED WORK

Less work has been done in textual steganography as compared with other mediums as shown in Table 1 like Image, audio and video [5,7,14].

In [1] Singh et al. have shown a brand new approach on textual content steganography throughout null space inside cover information regarding camouflaging. The secret information is camouflaged via introducing extra bright and null spaces, inside plain textual content of the cover data file. The white and null spaces are adjusted according to the binary of the secret message. It is pertinent to mention that for each 1 and 0 a different white/ null space is used in LSB. Downside of suggested process: hidden text has been hidden in LSB which is more vulnerable to attacks by malicious users. Thamaraiselvan et al. [2,10] have proposed a new process, utilizing the inter-word and also inter sentence spacing with an aim to increase capacity feature of text steganography. Any change in the inter word or inter sentence by the attacker will ruin the hidden text at the decoder end.

In [3] Qi et al. have suggested a technique which; uses synonyms of the secret text to be hidden in the cover text. However, an attacker can replace the chosen synonym with another synonym and therefore the hidden text will become meaningless at receiver end. Wang et al. [4] suggested new linguistic steganography scheme that based upon the fact that the hidden word indicates the same meaning as the cover word. Downside is that the hidden information can be tracked through few Natural Language processing NLP-based schemes.

Mirielle. Hassan [5] Shirali-Shahreza et al.; suggested a brand new approach, which is based on hiding the data in to the words which are frequently used in the cover image. Proposed process wherever provide the safety measures of technique information, can be used throughout circumstances wherever we've got to spend less the tiny amount data. Downside; a malicious user can detect the frequently used words in the stego text and replace them with another word, resultantly the hidden text will become insignificant for the receiver.

Table 2. Techniques Comparison Table

Techniques	**LSB Based [1]**	**Replacing Bits in Words [2-3]**	**Replacing same bits in spaces [4, 10-11]**	**Replacing secret word in 'Specific WORDS' [5-9,12, 14-15]**	**Expected Result of Proposed Method**
Domain	**Text**	**Text**	**Text**	**Text**	**Text**
Capacity	**Low**	**High**	**High**	**Low**	**High**
Robustness	**Low**	**Low**	**Low**	**High**	**High**
Imperceptibly	**High**	**Low**	**High**	**High**	**High**

In [6] Patel et al., with proposed a great process by utilizing BLOWFISH encryption. Benefits with this paper according to hybrid strategy employing bright spaces concerning terms and also sentence together with RJ (right justification). However, the downside is the time required for encryption and also the fact of using LSB technique for data hiding, which is definitely not safe. The entire strength of the proposed scheme is the BLOWFISH algorithm.

In [7-8] Zhi-li et al. suggested a powerful linguistics steganography using NICETEXT, TEXTO and also Markov chain dependent methods to secure data. A mix of both strategies using bright spaces concerning terms and also sentence throughout RJ (right justification) using LSB technique [6]. Desai et al., [9] suggested way of data hiding using encryption and random LSB method for encoding and decoding. Though, the present scheme gives higher capacity feature and dual layer security but using LSB method isn't safe [7].

In [11] Yilai et al. mentioned a method which uses binary chunks to hide data and in this paper they have used three LSBs to hide data. Imperceptibility of the proposed scheme is much better successfully, although low in robustness because tag removal could potentially identify change made in text.

In [12] POR et al. mentioned a new textual content camouflaging system which is similar to the techniques used in [11] but it increased capacity in spaces that remain render with respect to DASH TOOL if information is hidden in inter-word, inter sentence, start and end of the line assumed to be camouflaging undetected. This process provides the low robustness contrary to opponents to be able to disclosing information which lessens imperceptibility indirectly.

In [13-14] Rehmani et al. suggested a way of hiding data using LSB approach but utilizing images as a cover rather than text. These layers comprise on LSB and also facts randomization throughout bits of pixels

of electronic digital photos methods which make robust mechanism. Imperceptible and also hides maximum capacity enhanced and also makes obstacles regarding opponents, although with similar time LSB definitely not safe and also facts is usually removed or altered following using monarchy decryption, had robustness definitely not ensured on account of LSB throughout spatial sector.

In [15] Gupta et al.; Reviewed the benefit of simple strategy throughout image steganography in semantic, abbreviation, phrase punctuation and also phrase spacing methods. This kind of process is actually cumbersome to the enemy which enables it to obtain much better benefits together with all the three notable features of steganography.

In [16-17] Hafeez et al; mentioned a way of facts camouflaging throughout textual content steganography employing disarray unclear thresh having character frequency (CF) in this particular papers facts is actually camouflaging in numerous detail layers top zero to be able to seven chunks using some protection. The real key decision through hit-or-miss process result, display robust facts camouflaging next to textual content steganography process. Down sides with this textual content camouflaging strategy, camouflaging data available as one covering using the image steganography acquiring one aspect of steganography just about all facet should be insured totally or comparatively then suggested strategy.

In [18] Altigani et al; suggested a new protocol by utilizing hybrid way of help make the knowledge camouflaging through using AES and also phrase moving process. Substantial part data important applied such as 128 chunks employing encryption process definitely avoided rather than by hand second important encryption. This process definitely not solves capacity problem and also using AES enhanced encryption time.

PROPOSED FRAMEWORK

In this section, each phase of the proposed model is further explained below. Table 2 contains the notations and their details used in the proposed algorithm.

Encryption Phase: As shown in Fig.2First step is to generate a secret message. Select word of maximum length from secret message. Apply +1 increment on selected word. Then apply random generation character method on output of step 3. Generate even and odd bases generation on output of step 4. Replace secret message character by applying permutation method to complete embedding process. Calculate the character frequency of secret message. Select a cover message with following condition: Cover message COF (Character Frequency) >= Secret massage COF. Apply compression on output of step 5. Generate stego message. Now proceed to the decryption process.

Decryption Phase: Receive the stego message. Extract the secret message from cover message. Decompress the message. Secret message is successfully decrypted after reversing the encryption phase steps. Following algorithm is used to encrypt, decrypt and compress the message according to our proposed model using multi layer approach:

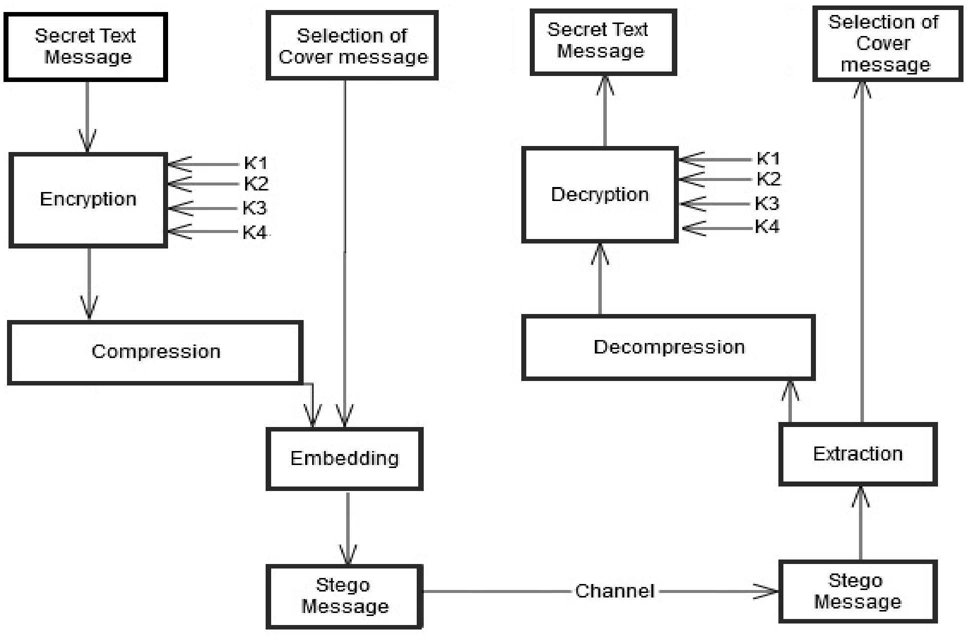

Fig.2 Encryption and Decryption Process

Table 2.Symbol description table

Symbol	Description
Ψ_i	Token Array
Ψ	Secret text
$l_{\Psi k}$	Length of secret key (bits)
$\mathfrak{K}$	Cover text
$\varepsilon_{\mathfrak{K}}$	Permutation order
$\wp_{\mathfrak{K}}$	Permutated text array
$\vartheta_{\mathfrak{K}}$	Dictionary Words
λ	Table for corresponding words
t_i	Temporary Text
$\mathfrak{R}$	Recovered Text
$D(\Psi,\mathfrak{R})$	Decryption Ψ via R
$E(\Psi,\mathfrak{R})$	Encryption Ψ via R
$\mathfrak{H}$	Maximum length word
$\underline{d}$	Array increamenting factor
r_i	Word Position

The proposed encryption algorithm produces imperceptible stego text. Firstly, secret text and cover text are taken as inputs. With the purpose of maximum information embedding, we choose the maximum length word for embedding in cover text after tokenizing the whole secret text via space delimiter. As shown in Fig 1. K1 is the first step taken to enhance the robustness of our scheme. It increments the selected word by +1. K2 is to layer the K1 by implanting the concept of randomly generated characters via incrementing the set of distinct numbers. K3 is called Layer3 which increments the text via set of even/odd numbers. Furthermore, for achieving high imperceptibility by maintaining the context of the cover text, we select the innocent words from the dictionary after permuting the output of K3. These words are then replaced with words of cover text. Lempel-Ziv compression algorithm [18] will be used to reduce the size of stego text. Embedding process will be performed after comparing the frequency of alphabets which hold the relation, cover text character frequency >= secret text character frequency. This algorithm refines the hiding process in the domain of text steganography which is fruitful to achieve the better robustness and imperceptibility factor.

The proposed decryption algorithm produces secret text same as the time of embedding the secret information in cover text. Firstly, extract the words places and match each word of the stego text from the secret table and take the word opposite to it.

Algorithm 1 ENCRYPTION ALGORITHM

```
procedure ENCRYPTION ($\Psi$,$\mathfrak{K}$)
   alpha_array ← {a,A,b,B,...,z,Z}
   $\Psi$ ← lowercase($\Psi_i$)|uppercase($\Psi$)
   $\Psi_i$ ← tokenize($\Psi$, ‘ ’)
   $\mathfrak{H}$ ← ‘ ’
    Foreach word w in $\Psi_i$
          IF (length(w)> length($\mathfrak{H}$))
              $\mathfrak{H}$ ← w
    End For
    Foreach char c in $\mathfrak{H}$
          $\mathfrak{H}$(i) ← c+1
    End For
    đ ← {1,2,3,…}
    Foreach char c in $\mathfrak{H}$
          $\mathfrak{H}$(i) ← $c_i$+ đ (i)|$c_{i+1}$ + đ (i+1) |$c_{i+2}$ + đ (i+2)....
    End For
    đ ← {1,2,1,…}
    Foreach char c in $\mathfrak{H}$
          $\mathfrak{H}$(i) ← $c_i$+ đ (i)|$c_{i+1}$ + đ (i+1) |$c_{i+2}$ + đ (i+2)....
    End For
    $\wp_{\mathfrak{K}}$ ← permutate($\mathfrak{H}$)
    Foreach word w in $\vartheta_{\mathfrak{K}}$
          IF equalize_meaning(x, $\mathfrak{H}$) && CharFrequencyEquilizer($\mathfrak{K}$, $\wp_{\mathfrak{K}}$)
                 $r_i$ ← index($\mathfrak{K}$, $\mathfrak{H}$)
                 $\mathfrak{K}$ ($r_i$) ← w
                 return LempleZivCompression($\mathfrak{K}$)
          End IF
    End For
end procedure
```

Algorithm 2 DECRYPTION ALGORITHM

```
procedure DECRYPTION ($\Psi$,$\lambda$,$\varepsilon_{\mathfrak{K}}$,$\wp_{\mathfrak{K}}$)
    $\Psi$ ← LempleZivDecompression($\Psi$)
      $\mathfrak{R}$ ← ‘ ’
      $t_i$ ← ‘ ’
   Foreach integer i in length($\Psi$)
      $t_i$ ← index($\Psi$,$\varepsilon_{\mathfrak{K}}$)
      IF (equalize_meaning($t_i$, $\vartheta_{\mathfrak{K}}$))
             $\mathfrak{R}$ ← $t_i$
      End IF
   End For
      $\wp_{\mathfrak{K}}$ ← permutate(recovered_text.tokanize($\mathfrak{R}$, ‘ ‘),$\varepsilon_{\mathfrak{K}}$)
   Foreach word w in $\wp_{\mathfrak{K}}$
      đ ← {1,2,1,…}
      $\Psi$ (i) ← $c_i$- đ (i)|$c_{i+1}$ - đ (i+1) |$c_{i+2}$ - đ (i+2)....
      đ ← {1,2,3,…}
      $\Psi$ (i) ← $c_i$- đ (i)|$c_{i+1}$ - đ (i+1) |$c_{i+2}$ - đ (i+2)....
      $\Psi$(i) ← $c_i$- 1|$c_{i+1}$ - 1 |$c_{i+2}$ - 1....
   End For
   Return $\Psi$
end procedure
```

Permute the words according the secret permutation order which was implanted to maintain the context of the cover text. Lempel-Ziv decompression algorithm [18] will be used to get the file with its original size and maximum information. Layers will be vanished one by one after applying the decrementing factor dec to even/odd, random generation vector and -1 to get back to secret text respectively. Integrity of the hidden information is only kept in secret key. Permutation is used to reordering alphabets to create more diffusion. For example, a word taken from paragraph to change secretly and make it innocent but length of changed word would be different from the original.

Original secret word: attack

After 1+ each character: buubdl

After incrementing the each character via random generation vector {123,…}: cwxcfo

After incrementing the each character via even/odd vector {1212…}: dyyegn (length n=6)

After permuting the word dyyegn (26^n times), a suitable word “dynamic” from dictionary has been selected whose length is dynamic(7) > dyyegn(6). This word of incremented length would be effective to preserve the security of secret text if attacker tries to decode or extract the word of different length.

EVALUATION

The first problem which we encountered was the security aspect of the text steganography. Majority of the schemes were hiding data by making use of single layer data transmission and also utilizing LSB technique for data hiding, which had drastic effects on the robustness of the hidden data. The current technique improves the security of the hidden data by encrypting the hidden text a number of times so that it becomes meaningless to malicious user.

The proposed scheme is not based on LSB technique of data hiding, therefore the inherent weakness of the LSB method is also encountered in the proposed scheme. As shown in Fig 3, a graphical representation of the inverse of key length and secret image size (percentage of cover image). This behavior shows that the secret image length increases according to the cover image length and require more keys, probability of getting secret key is impossible. As shown in Fig 4-5, Attackers success and failure is only depends upon length of secret key.

Statistics will be completely hidden because high imperceptible and robustness feature. The second hitch which came across during the course of our research was that proposed schemes had drastic consequence on imperceptibility aspect of steganography, which was quite low than the satisfactory level and also the pattern of alphabets was altered, which as a result leads to high chances of being detected by the malicious user. The proposed scheme improves imperceptibility to a greater extent by catering for both the issues as the data to be hidden is first matched with the words in the dictionary.

The proposed scheme improves imperceptibility to a greater extent by catering for both the issues as the data to be hidden is first matched with the words in the dictionary.

The chosen word is then matched with the text in the cover text and if the word gives similar meaning as being used in the cover text and do not change the context of the sentence, only then it is chosen and cover text is replaced with the stego text as shown in Fig 6. Above figure shows that distortion in the cover text increases as the secret image embedding percentage increases.

Comparison between the proposed scheme and LSB bit embedding clearly shows that imperceptibility feature improved as replacing cover word by secret word in a way that context of the stego text become innocent as shown in Fig 7.This aspect is observed by calculating the feature of PSNR decibel quantity. It shows that the bits embedding in cover text is same as the bit value in secret text. The third drawback which we identified was the storage capacity of the image being used to hide text.

In the proposed schemes, the cover message provides small storage capacity which as a result restricts the options of hiding the data. Fig 7 shows that proposed scheme is improving the capacity feature and this feature improves more as the secret image size increases. The schemes also utilize a limited dictionary for the exact word matching. The proposed scheme caters for the aspect of storage

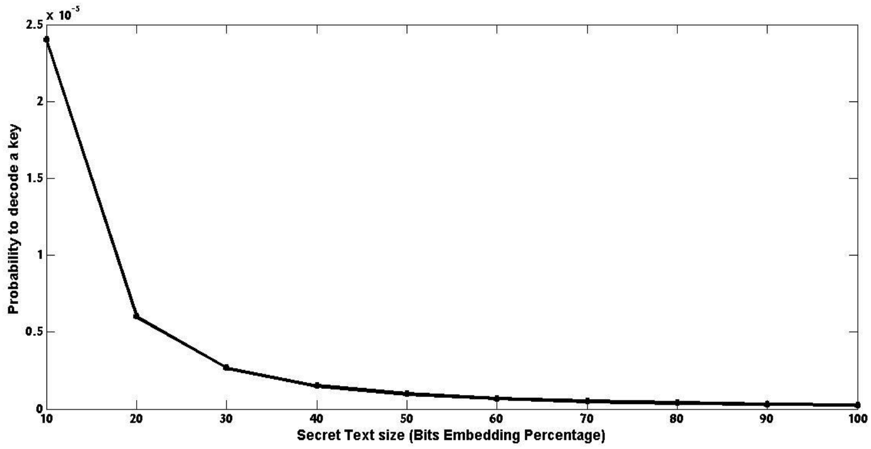

Fig.3 A Robustness test (Probability of attackers guess to decode the secret key)

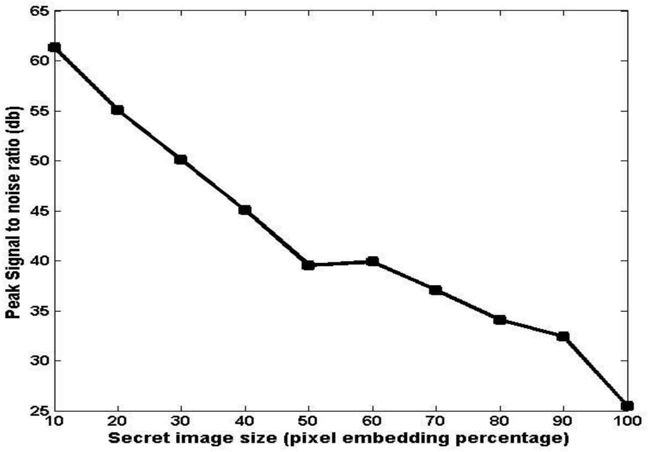

Fig.4 An Imperceptibility Feature Test (Peak Signal to noise ratio after embedding the secret text)

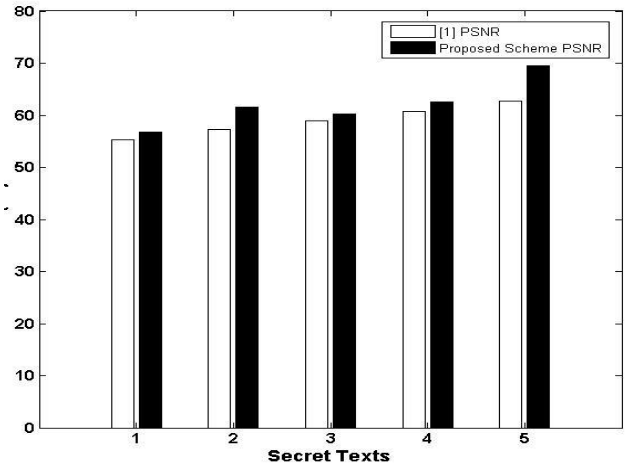

Fig.5 An imperceptibility feature comparison of the

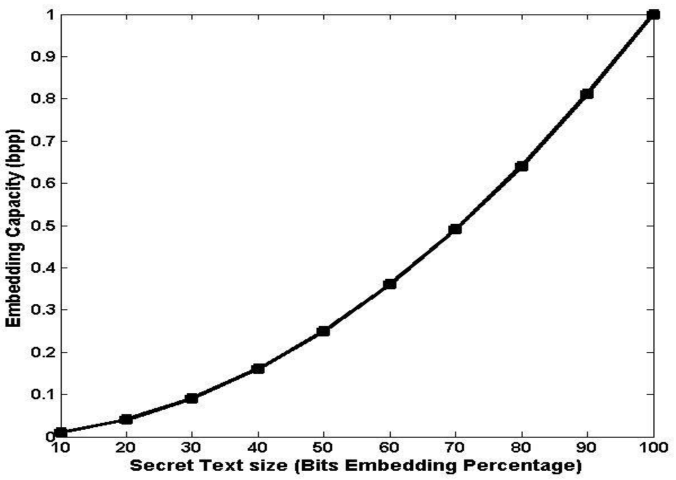

Fig.6 Capacity Feature Test

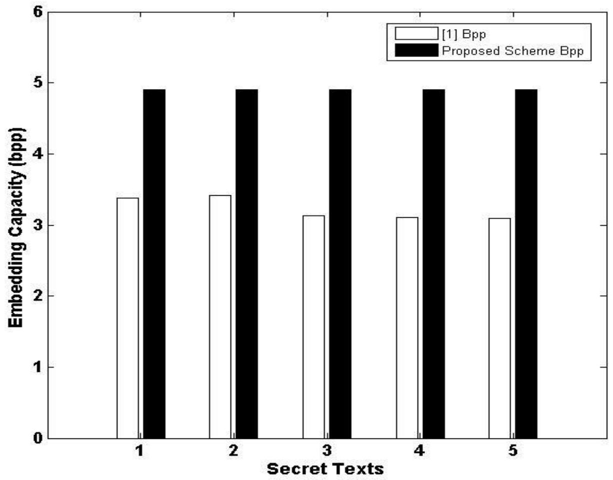

Fig.7 Capacity feature comparison of proposed scheme and LSB embedding scheme [1]

capacity as shown in Fig 8. In our proposed scheme the capacity of the cover text is first checked and if the capacity of the cover is less than the stego text then the cover text is discarded and a new cover text is selected. The cover text is only selected if it satisfies a condition that the storage capacity of the cover text should be equal or larger than the stego text.

Comparison between the proposed scheme and LSB bit embedding clearly shows that capacity feature improved as replacing cover word by secret word in a way that context of the stego text become innocent as shown in Fig 9. Bit per pixel embedding factor is observed the proposed scheme has effect on all bits of each letter of cover text.

DISCUSSION

Security of data during transmission is achieved through cryptography which is further augmented by using steganography which hides the existence of secret data. Combination of both cryptography and steganography can provide a better and more accurate solution of securing the transmitted data.

Text Steganography is termed more difficult due to lower redundancy in its nature. The parameters like capacity, perceptibility, robustness, integrity and capacity forms the basis of text steganography.

It is pertinent to mention that mediums like images, audio and videos are widely used for hiding the existence of data due to the ease of the entire steganographic process.

However, text steganography gives more security. Various techniques of hiding data in text of cover image have been discussed like hiding information in null spaces, utilizing the inter-word and inter sentence spacing, using synonyms of the secret text to be hidden in the cover text, hiding the data in to the words which are frequently used in the cover.

The proposed scheme hides the text by using multi time encryption, compression on secret message and embeds the data into cover message with an aim to get better robustness, imperceptibility, integrity and capacity. The proposed scheme caters for security, imperceptibility and capacity aspects of text steganography by using multilayer encryption, using words with similar meaning as in cover text and using cover text having capacity larger than stego text.

CONCLUSION

Information hiding has been useful with backing of two noteworthy branches, advanced watermarking and Steganography. The security issues and classification of the delicate data has turned into prime and essential concern, as different occasions of worldwide security issues invigorated the prerequisite for better strategies for securing the machines and the information they store, change and transmit.

The proposed system is based on text steganography by utilizing their specific properties, since the its requires less memory and its work quicker, and makes correspondence desirable over different mediums of steganography like picture, sound and feature for information covering up. The point of this paper is to build up a model which can enhance limit, indistinctness and strength by utilization of multi layer content into content stenography with the blend of encryption and inserting methodology for haziness of information.

REFERENCES

[1] Singh, P., Chaudhary, R., & Agarwal, A. (2012). A Novel Approach of Text Steganography based on null spaces. *IOSR Journal of Computer Engineering*, *3*(4), 11-17.

[2] Thamaraiselvan, R., & Saradha, A. (2012). A Novel approach of Hybrid Method of Hiding the Text Information Using Stegnography. *IJCER*, *1*(1).

[3] Qi, C., Xingming, S., & Lingyun, X. (2013, January). A secure text steganography based on synonym substitution. In *Conference Anthology, IEEE* (pp. 1-3). IEEE.

[4] Wang, F., Huang, L., Chen, Z., Yang, W., & Miao, H. (2013, August). A novel text steganography by context-based equivalent substitution. In *Signal Processing, Communication and Computing (ICSPCC), 2013 IEEE International Conference on* (pp. 1-6). IEEE.

[5] Shirali-Shahreza, M. H., & Shirali-Shahreza, M. (2008, August). A new synonym text steganography. In *International conference on intelligent information hiding and multimedia signal processing* (pp. 1524-1526). IEEE

[6] Patel, K., Utareja, S., & Gupta, H. (2013). A Survey of Information Hiding Techniques. *International Journal of Emerging Technology & Advanced Engineering*, *3*(1), 347-350.

[7] Wang, Z. H., Chang, C. C., Kieu, T. D., & Li, M. C. (2009, November). Emoticon-based text steganography in chat. In *Computational Intelligence and Industrial Applications. PACIIA 2009. Asia-Pacific Conference on* (Vol. 2, pp. 457-460). IEEE.

[8] Inoue, S., Makino, K., Murase, I., Takizawa, O., Matsumoto, T., & Nakagawa, H. (2001, November). A proposal on information hiding methods using XML. In *The 1st Workshop on NLP and XML* (pp. 707-710).

[9] Desai, S., Amreliwala, S., & Kumar, V. (2014). Enhancing Security in Mobile Communication using a Unique Approach in Steganography.

[10] Por, L. Y., & Delina, B. (2008, April). Information hiding: A new approach in text steganography. In Q. Li, S. Y. Chen, & A. Xu (Eds.), *WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering* (No. 7). World Scientific and Engineering Academy and Society.

[11] Yong, X., Juan, L., & Yilai, Z. (2012, July). A high capacity information hiding method for webpage based on tag. In *Digital Manufacturing and Automation (ICDMA), 2012 Third International Conference on* (pp. 62-65). IEEE.

[12] Por, L. Y., Wong, K., & Chee, K. O. (2012). UniSpaCh: A text-based data hiding method using Unicode space characters. *Journal of Systems and Software*, *85*(5), 1075-1082.

[13] Agarwal, M. (2013). Text steganographic approaches: a comparison. *arXiv preprint arXiv:1302.2718*.

[14] Rahmani, M. K. I., & Kamiya Arora, N. P. (2014). A Crypto-Steganography: A Survey. *International Journal of Advanced Computer Science and Application*, *5*, 149-154

[15] Gupta, S., & Gupta, D. (2011). Text-Steganography: Review Study & Comparative Analysis

[16] Bhattacharyya, D., Das, P., Bandyopadhyay, S. K., & Kim, T. H. (2009). Text steganography: a novel approach. *International Journal of Advanced Science and Technology*, *3*, 79-86.

[17] Tayel, M., Shawky, H., & Hafez, A. E. S. (2013, January). A hybrid chaos-fuzzy-threshold steganography algorithm for hiding secure data. In *Advanced Communication Technology, 2013 15th International Conference on* (pp. 156-161). IEEE.

[18] Altigani, A., & Barry, B. (2013, August). A hybrid approach to secure transmitted messages using advanced encryption standard (AES) and Word Shift Coding Protocol. In *Computing, Electrical and Electronics Engineering (ICCEEE), 2013 International Conference on* (pp. 134-139). IEEE.

[19] Wang, F., Huang, L., Chen, Z., Yang, W., & Miao, H. (2013). A novel text steganography by context-based equivalent substitution. In *Signal Processing, Communication and Computing, 2013 IEEE International Conference on* (pp.1-6).

[20] Shu, Y., Liu, L., Tian, W., & Miao, X. (2011). Algorithm for information hiding in optional multi-text. *Procedia Engineering*, *15*, 3936-3941.

[21] Karadogan, I., & Das, R. An Examination on Information Hiding Tools for Steganography.

[22] Khairullah, M. (2009, December). A novel text steganography system using font color of the invisible characters in Microsoft Word documents. In *ComputerElectrical Engineering, 2009. Second Int.l Conference on* (Vol. 1, pp. 482-484). IEEE.

[23] Wang, Z. H., Chang, C. C., Kieu, T. D., & Li, M. C. Emoticon-based text steganography in chat. In *Computational Intelligence and Industrial Applications, 2009. PACIIA 2009. Asia-Pacific Conference on* (Vol. 2, pp. 457-460). IEEE.

[24] Kumar, A., & Pooja, K. (2010). Steganography-A data hiding technique. *International Journal of Computer Applications*, *9*(7), 19-23.

[25] Meng, P., Hang, L., Yang, W., Chen, Z., & Zheng, H. (2009, July). Linguistic steganography detection algorithm using statistical language model. In *Information Technology and Computer Science, 2009. ITCS 2009. International Conference on* (Vol. 2, pp. 540-543). IEEE.

[26] Shukla, C. P., & Chadha, M. R. S. (2014). A Survey of Steganography Technique, Attacks and Applications. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(2).

[27] Singleton, N. Computerized Image Processing for Forgery Prevention.

[28] Nag, A., Ghosh, S., Biswas, S., Sarkar, D., & Sarkar, P. P.. An image steganography technique using X-box mapping. In *Advances in Engineering, Science and Management, 2012 International Conference on* (pp. 709-713). IEEE..

[29] Dagar, S. Highly randomized image steganography using secret keys. In *Recent Advances and Innovations in Engineering (ICRAIE), 2014* (pp. 1-5). IEEE.

[30] OSMAN, B., DIN, R., MUDA, T. Z. T., & OMAR, M. N. A Performance of Embedding Process for Text Steganography Method.