Communication in Veil: Enhanced Paradigm for ASCII Text Files

Khan Farhan Rafat
Dept. of Computer Science
International Islamic University
Islamabad, Pakistan

Muhammad Sher
Dept. of Computer Science
International Islamic University
Islamabad, Pakistan

***Abstract*—Digitization has a persuasive impact on information and communication technology (ICT) field which can be realized from the fact that today one seldom think to stand in long awaiting queue just to deposit utility bills, buy movie ticket, or dispatch private letters via post office etc. as these and other such similar activities are now preferably being done electronically over internet which has shattered the geographical boundaries and has tied the people across the world into a single logical unit called global village. The efficacy and precision with which electronic transactions are made is commendable and is one of the reasons why more and more people are switching over to e-commerce for their official and personal usage. Via social networking sites one can interact with family and friends at any time of his/her choice. The darker side of this comforting aspect, however, is that the contents sent on/off-line may be monitored for active or passive intervention by the antagonistic forces for their illicit motives ranging from but not only limited to password, ID and social security number theft to impersonation, compromising personal information, blackmailing etc. This necessitated the need to hide data or information of some significance in an oblivious manner in order to detract the enemy as regards its detection.**

This paper aims at evolving an avant-garde information hiding scheme for ASCII text files - a research area regarded as the most difficult in contrast to audio, video or image file formats for the said purpose.

Keywords— Embedded Secrets; Hide and Seek; Eccentric way of writing; ASCII Text Steganography; Communication in Veil; Stealth Communication

I. INTRODUCTION

The ease with which digital contents can be allegedly copied and distributed over the internet is the driving force behind exploration of new information hiding techniques for content's protection, verification, and its legitimate distribution. However, research that was primarily focused on protecting digital rights has inadvertently given way to steganography having Greek origin [1] which with the introduction of computers, has evolved into a science for in veil communication.

The name steganography first appeared in a manuscript entitled Steganographia written by Trithemus (1462-1516) and is a composition of two Greek words στεγανό-ς (Steganos) and γραφ-ειν (Graphos) which in English means covered writing [2]. The difference between cryptography and steganography is that the later hides the existence of secret data [3] whereas former concerns itself in making that data unintelligible [4].

A. Techniques for Steganography

Steganography can be realized through any of the following three ways [5]:

- **Insertion:** It involves direct embedding of secret information inside the body of Cover which results in an increased stego object file size. *One such old technique involves writing of data past end-of-file (EOF) mark that remains in veil to naive computer user.*
- **Substitution:** Information is hidden inside the cover by substituting secret information with cover's contents. The Stego Object may or may not retain actual Cover file size. *For example if 01001011 be the pixel elementthen a secret message bit 0 inserted at Least Significant Bit (LSB) position results in Stego byte as 01001010, where the change is so inconsequential that it easily deceives human eye.*
- **Cover Generation:** In this technique a Cover is generated based on the secret information that need covertly communication. *Spam Mimic is a freely available program that hides secret text message by generating random but meaningful text phrases.*

B. How Steganography Works

Steganography exploits limitations in Human's Auditory-Visual System (HAVS) that are briefly summarized as follows:

- **Inadequacy of Vision:** "Highest Resolution Perceivable Pixels: 28 Seconds Of Arc" as reported in [6] where subsequent discussion explicates on variety of physical factors as major hindrance for premier spatial frequencies being misconstrued by the human eye while eye's edifice and biological tests confer on an all-out professed frequency of around one cycle per arc minute (half arc-minute pixels) thereby failing to differentiate colors (where RGB Color ranges from 0(zero) to 2^24-1 in numbers).
- **Inexactitude of Auditory System:** The way head is contoured together with external ear (Pinna) enacts ethereal variations on entrant sounds according to its angle of inception in ear and can be apprehended as a filtering process. Human beings can hear voices having

frequency bounds 20 Hz to 20 KHz; both inclusive, however, age plays a significant role on the hearing threshold [7]. Further loud sounds tend to dominate modest ones and hence data may be superimposed on extremely low pitched noise that remain oblivious to human in presence of loud sounds.

C. Paper Plan

Rest of the paper is intended as follows: Section II briefly deliberates on ASCII text file format and the challenge it offers to researchers in devising text cover based steganographic schemes followed by related research in that area. Evaluation parameters for our proposed scheme are discussed in Section III while our choice of steganographic model is given in Section IV. Section V actually deliberates on our proposal. Quantified Test results and allied illustrations are given in Section VI. Section VII explains conjectural aspect of our proposed scheme while Section VIII explains its advantages and limitations. Future work follows in Section IX whereas Section X concludes the discussion.

II. Related Research

A. ASCII Text File Format

American Standard Code for Information Interchange abbreviated as ASCII, is a 7-bit code that facilitates text communication between different devices. One of the salient attributes distinguishing ASCII file format from other file formats like image, audio and video is that the former lacks auxiliary space that later exploits in projecting bounded contents. Another trait of Text files is that these are saved and presented for view in the manner the human beings are familiar with. The draw back with ASCII character codes is that changing its single bit results in code that may render a character or word as erroneous/misspelled thereby drawing immediate attention of the viewer. This, however, is also what makes ASCII text centric steganography a challenging task for researchers and hence is the prima facie of this research.

B. Literature Review

Steganography by virtue of being seamless in idiosyncrasy has emerged as a preferred choice for information hiding. Following discussion categorically expand on how text steganography is being used for covert communication.

1) English Language Specific Steganography: Following is the discussion on Steganographic schemes that exploits syntax and semantics of English language:

a) Acronym: Acronyms are contractions for comparatively long or frequently used words/phrases like As soon as possible which is abbreviated as ASAP. Author [8] suggested using acronyms together with corresponding words / phrases of English language to hide bits of secret information. The methodology works by arranging words/phrases in one of the two column table, the other column of which is populated with corresponding acronyms. The column containing words/phrases are labeled as "0" while acronyms are headed by label "1". Table 1 indicates one such arrangement.

TABLE I. Acronyms and Words/Phrases Arranged in a Two Column Table

ACRONYMS	WORDS
2L8	Too Late
ASAP	As Soon As Possible
C	See
CM	Call Me
F2F	Face to Face

Next, text cover composed of words/phrases and acronym is prepared. Secret information to be hidden inside the body of text cover is translated into bits. Text cover is then iterated to search for words/phrase or acronym matching those in the table till end of the message. Each time a word/phrase or acronym run into secret message bit (in sequence), it is examined with reference to column head (label) of the table. If secret message bit is 0 and the corresponding matching text in cover is word/phrase i.e., column labeled as 0, the cover text remains unchanged. However, if the secret message bit is 1 and the corresponding matching text in cover is word/phrase, the word/phrase in cover text is replaced by its corresponding acronym. In short, binary message bit 0 corresponds to having word/phrase in the Stego Object while binary message bit 1 corresponds to having acronym in place of words/phrases.

*b) Synonym:*Authorin [9]applied the aforesaid methodology on English language words that share same meaning/sense for the purpose of information hiding. Table 2 shows an arrangement of words having same sense/meaning and arranged in a two column table.

TABLE II. Different Words Sharing Same Meaning

WORDS	SYNONYMS
Big	Large
Chilly	Cool
Small	Little
Smart	Clever
Spaced	Stretched

c) Steganography through words that are spelled differently in British and American language: In [10] authorsextended aforementioned methodology on words that are spelled differently in British and American English - for information hiding purpose. Table 3 shows list of some of the words that are spelled differently in British and American language.

TABLE III. List of Word(s) Spelled Differently in British and American English

AMERICAN ENGLISH	BRITISH ENGLISH
Center	Centre
Criticize	Critise
Favorite	Favourite
Fulfill	Fulfil

*2) Miscellaneous Schemes for Text Steganography:*Following is a brief discussion on miscellaneous text-based steganographic schemes:

*a) Manipulation of Text Contents:*Authors in [11] suggested a number of eccentric proposals for data hiding in English Language text through modifications like making syntax errors, replacing words/phrases with their acronyms, artifact word format etc. as shown below:

- Inducing typographical errors – writing "there" in place of "there"
- Opting for "yr" in place of "your" and "TC" rather than "Take Care"
- Inserting extra carriage returns or segregating text into uneven paragraphs, or altering line or word space.
- Using annotating text e.g., :) that denotes 'pun'
- Use of bilingual text – "we always commit the same mistakes again, and 'je ne regrette rien'!".

*3) Use of Blank/Space Character:*In [12]authors proposed scheme that represents secret binary bit 1 with a single space while secret binary bit 0 depicts a double space. Following example illustrates the concept:

Example: Let 11010001 be the bits of our secret message bits and let "*A quick brown fox jumps over the lazy dog.*" be the cover text. Going in parallel with said scheme binary bit 0 will represent double spaces while no additional space is inserted for binary message bit 1. Resulting stego object after bit embedding will take the form*"A quick brownfoxjumpsoverthelazydog.", where black spaces denote a double space.*

*4) Steganography via Word Mapping Method:*In their attempt to increase capacity of data embedding by inserting 'spaces' based on word length of the cover authors [13] employed additional file form keeping locations of words targeted in hiding secret message bits. Table 4 shows substitution criteria for their proposed scheme.

5) Both Stego Object and index file are needed to retrieve hidden information at receiver's end. As comprehended from the said table, even and odd word lengths are compared with secret message bit pairs for inserting single or double space after identifying the word and location file updated accordingly.

TABLE IV. EVEN AND ODD WORD LENGTH

SECRET BIT PAIR	WORD SIZE	NUMBER OF BLANK SPACES AFTER
00	EVEN	TWO
01	EVEN	ONE
10	ODD	TWO
11	ODD	ONE

III. EVALUATION PARAMETERS

Perceptibility is the foremost requirement of any steganography system that does not involve sound. However, as regards its security nothing can precisely be said except to harden Wendy's efforts towards cracking or breaking a system by opting for information theoretically secure solutions consequent from the following deliberation:

Using Cachin [14] formal definition of security of steganographic system as:

$$D(P_c||P_s) \leq \varepsilon \qquad (1)$$

, one may infer that *perfect security* may be achieved whenever $\varepsilon = 0$, where P_c is the probability distribution of cover, P_s is that of stego object respectively over set of alphabets **A**,and $D(P_c||P_s)$ is computed using following:

$$D(P_c||P_s) = \sum_{a\epsilon A} P_c\,(a) log_2(\frac{Pc(a)}{Ps(a)}) \qquad (2)$$

Authors [15], however, differed on the aforesaid notion of perfect security by highlighting bound constraint concomitant with equation (2), and have elucidated with example that security is neither a measurable commodity nor can it be quantified.

IV. PREFERRED MODEL

Simmons [16] was first to propose a model based scenario for stealth communication where for Alice and Bob having agreed on a secret mode of communication before being sent to jail were kept in separate cells under supervision of Warden Wendy, must decide on their escape plan without raising suspicion. The two types of errors Warden Wendy may commit in such a scenario include:

- Type – I error:A hidden message gets detected by Wendy where in fact no message was sent.
- Type-II error:A secret message gets through Wendy as unnoticed.

Obviously we want our proposed scheme to maximize probability of occurrence of Type – II error.

Through literature review on model based steganography we found the one presented by [17] as close to what we have anticipated concerning evolution and implementation of our proposed solution. The same is illustrated in Figure 1 followed by its brief explanation.

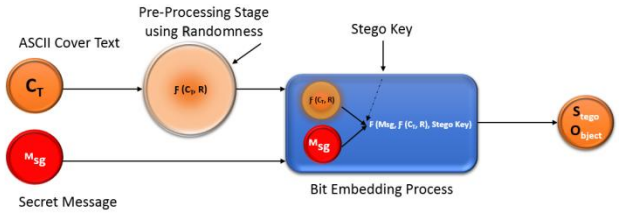

Fig. 1. Information Theoretically Secure Model for Steganography.

As apparent from Figure 1, the idea is to induce some sort of uncertainty in cover text (via some random process) and thereafter performing bit embedding over it, the theoretical substance of which is explicated in Section VII.

V. Proposed Steganographic Scheme

A. Objective

Of the three techniques used in steganography discussed earlier, our proposed scheme uses insertion for hiding secret message bits inside ASCII cover text file. However, to alleviate the overall effect of insertion on size of stego object we concentrated on increasing bit embedding capacity per byte in the cover text but without needing support of some additional file that must also be transferred along with stego object.

B. Preludes

To achieve aforesaid objective we extended our research on existing ASCII codes using Visual Basic 6 as our experimenting tool, and found eight such codes that can safely be inserted inside ASCII cover text file without raising perceptibility concern when the file gets opened with Microsoft Windows default application called 'Notepad'. For ease we shall refer to these ASCII codes as '**S.code**' in subsequent discussion. Further to retain insertion of additional bytes confined to reasonable range we considered total spaces in ASCII Text file as our threshold for byte insertion beyond which the scheme ceases to work. Another aspect of this selection was that change of words may not hamper the hidden bits where extra spaces not prefixed by any of the S.code(s), on account of malevolent activity, can easily be ignored at the time of bit extraction at receiving end.

Since $x = log_2^y \rightarrow y = 2^x$, hence $x = log_2^8 \rightarrow 8 = 2^x \; for \; x = 3$meaning thereby that each extra byte inserted in ASCII cover text using any of the S.code(s) can serve as a place holder for three bits of secret information.

The eight S.code(s) were first randomly shuffled and then assigned a tri-bit group (Range: 000 to 111) in sequence as shown in Table 5.

TABLE V. Default Allotment of Tri-bits to S.code(s)

Index	S.code	Tri-Bits	Re-Arranged
0	28	000	
1	29	001	
2	30	010	
3	129	011	
4	141	100	
5	143	101	
6	144	110	
7	157	111	

The tri-bits are later re-arranged on the basis of stego_key value where the starting point for tri-bit re-arrangement is obtained using following formula:

$$S_p \leftarrow (\sum_{i=0}^{31} Stego\_Key[i] * (i+1)) MOD \; 8 \qquad (3)$$

i.e. S_p holds the index value of the tri-bit groups starting from which the rest of the groups will be written in top down order against index 0 to 7 in 4th column of Table 5 for subsequent use. For example, let the starting point S_p be 6 then Table 5 will take the form shown in Table 6. As apparent S_p will vary from message to message.

TABLE VI. Key Dependent Allotment of Tri-bits to S.code(s)

Index	S.code	Tri-Bits	Re-Arranged Bits
0	143	000	110
1	29	001	111
2	157	010	000
3	129	011	001
4	141	100	010
5	28	101	011
6	144	110	100
7	30	111	101

C. Pre-Processing ASCII Cover Text

Shuffling of cover text content was not considered as feasible because being irrational it would create ambiguity, hence, we iterated through the cover text from start till end, searching for a 'space'. Upon finding it, a random number got generated using True Random Number Generator (TRNG) – the discussion of which is beyond the scope set for this research, in range 0 ~ 65537 and reducing it modulo 8. The outcome served as an index (Column 1st Table 6 refers) for selecting the specific S.code after which it was inserted before the said space.

D. Pre-Processing ASCII Cover Text

Since we have eight S.code(s) hence these can be arranged in 8! = 40320 unique ways (*Permutations*), an arrangement of which is shown in Table 7.

TABLE VII. 40320 Permutations for S.code(s)

R/C		28	29	30	129	141	143	144	157
1		141	144	29	143	30	129	157	28
2		30	143	129	144	28	29	157	141
3		29	141	143	157	144	28	30	129
4		144	157	129	141	143	30	29	28
5		143	30	157	28	141	144	129	29
6		129	144	28	29	157	143	141	30
...		...	...	...	...	...	...	...	...
40319		28	29	141	143	30	129	144	157
40320		141	28	30	129	29	157	143	144

E. Bit-Embedding Steps

1) Type / Select Secret Message and translate it into equivalent bits. Store message length and its corresponding file extension into four bytes (each) and translate those into equivalent binary bits. The 64-bits forms message header and is affixed before message bits.

2) Select 256-bit Stego key.

3) Process Stego Key as input through SHA-256 HASH algorithm [18].

4) Translate the outcome of Step 3 into equivalent binary bits and count the number of ON binary-bits. If the number equals or exceeds total number of binary message bits (inclusive of header bits) proceed to step 6.

5) Output of Step 3 (in place of initial Stego Key) serves as feedback to Step 3 followed by execution of Step 4.

6) Iterate cover text till end, searching for 'blank/space' by taking output of step 4 and processing one bit at a time. Mark the 'space' against ON HASH bit as secret message bit replacement position.

7) Compute a random row number for Table 7 using following equation:

$$\tau \leftarrow \left(\sum_{i=0}^{30} (Stego\ Key\ [i] * Stego\ Key\ [i + 1]) MOD\ 65537 \right) MOD\ 40320 + 1 \qquad (4)$$

8) Iterate cover text till end in search of 'space' marked for replacement (Step 6 refers), taking one tri-bit at a time. Locate S.code corresponding to those tri-bits in Table 6 that are to be treated as column head of Table 7. Replace S.code at cross section of row τ and column head of Table 7 with that affixed before the marked 'space'.

9) If no more tri-bits are to be processed, move to Step 12.

10) Increment row τ by 1. If it exceeds 40320, then set it to initial value of 1.

11) Repeat Step 8.

12) Terminate bit embedding process.

F. Bit-Extraction Steps

1) Select 256-bit Stego key.

2) Process Stego Key as input through SHA-256 HASH algorithm.

3) Translate the outcome of Step 2 into equivalent binary bits and count the number of ON binary-bits. If the number equals or exceeds 22 proceed to step 6.

4) Output from Step 3 (in place of initial Stego Key) serves as feedback to Step 2 followed by execution of Step 3.

5) Iterate stego object, searching for 'blank/space' by taking output bits, one bit at a time, of step 4. Mark the 'space' against ON HASH bit as pointer to hidden message bit.

6) Compute a random row number for Table 7 using equation (4).

7) Iterate stego 'space' characters marked as 'pointers' (Step 6 refers). Locate S.code affixed before marked 'space' in row τ of Table 7 and note down its corresponding column head. Search the column head thus for corresponding tri-bit group in 3rd column of Table 6 followed by their extraction and concatenation.

8) If first 22 bits gets processed, move to Step 11.

9) Increment row τ by 1. If it exceeds 40320, then set it to initial value of 1.

10) Of the 66 hidden bits thus obtained, the first 32 when converted into bytes gives hidden message length while the next its file extension.

11) Repeat Step 8 based on computed hidden message length vide Step 11.

12) Translate the extracted bits into bytes and save it in a file having extension as obtained in Step 11 which is the hidden message.

13) Terminate bit extraction process.

VI. Test Results

A. Perceptibility

Figures 2, 3 and 4 are screen shorts for cover text (extracted from: http://en.wikipedia.org/wiki/Steganography), pre-processed cover text and stego object respectively which are 100% identical in appearance:

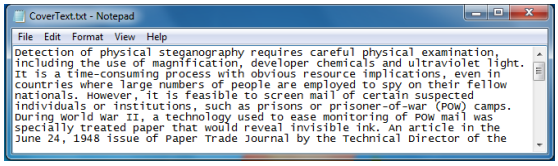

Fig. 2. ASCII Cover Text File

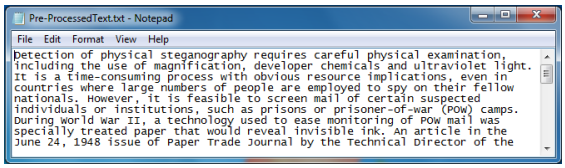

Fig. 3. Pre-Processed ASCII Cover Text File

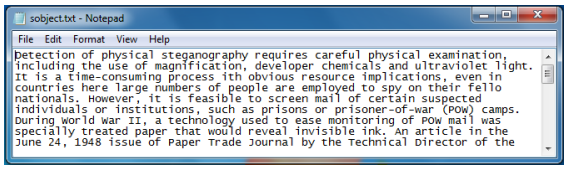

Fig. 4. Stego Object

B. File Lengths of Cover Text and Stego Object

Directory listing of the aforesaid files illustrated in Figure 5 does not show any difference unless viewed exclusively in terms of actual file size and that on persistent storage.

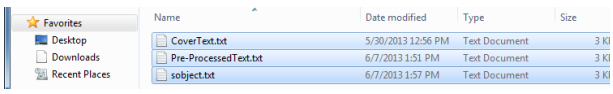

Fig. 5. Directory Listing for Cover, Pre-Processed Cover Text Files and Stego Object respectively

C. Quantified Similarity

The similarity between cover text, pre-processed text and stego object is quantified using Jro-Winkler distance [19][20]which was observed as 0.98071 while computed mean, variance and standard deviation are given in Table 8.

TABLE VIII. TABULATED MEAN, VARIENCE AND STANDARD DEVIATION

Computation	Cover Text	Pre-Processed Cover Text	Stego Object
Mean	0.09238	0.09368	0.09013
Variance	0.88189	1.18137	1.17942
Standard Deviation	0.02969	0.03437	0.03569

D. Graphical Illustration

Figures 6, 7 and 8 are graphical illustrations of probability distribution plots between ASCII cover text, pre-processed cover text and stego object respectively using MiniTab16 [21]:

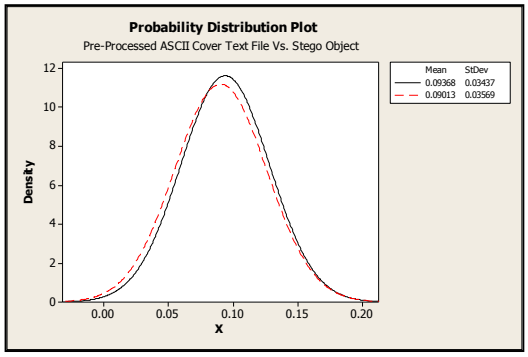

Fig. 6. Contrasting Probability Distribution Plots of Cover Text and Pre-Processed Cover Text

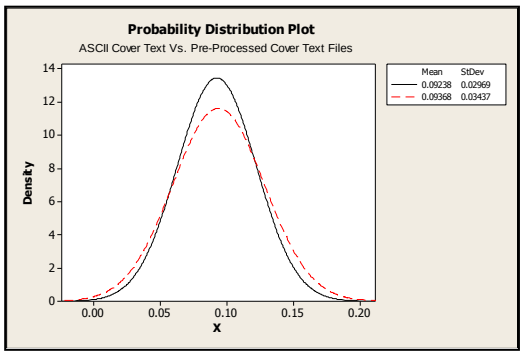

Fig. 7. Contrasting Probability Distribution Plots of Pre-Processed Cover Text File and Stego Object

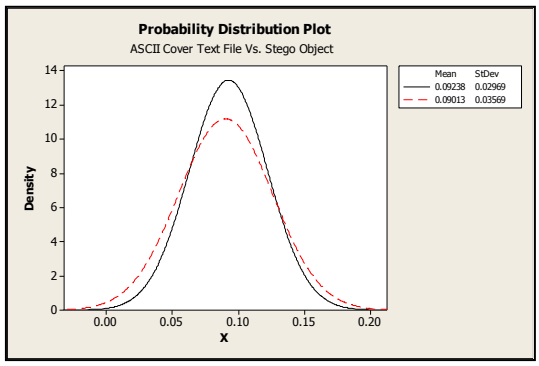

Fig. 8. Contrasting Probability Distribution Plots of ASCII Cover Text File and Stego Object

As apparent from preceding test results and graphical illustrations that Wendy will have a tough time to guess about the cover text that would have been used for information hiding purpose.

VII. THEORETICAL SUBSTANCE

Let δ be the cover text, and let α denote secret message bits that are to be hidden inside δ.Bit embedding involves searching for a blank/space in cover text and then replacing it with a double space to represent secret message bit '1' while for binary bit 0 no extra space is inserted. We may then represent bit embedding and extraction processes as follows:

Bit embedding: *if* $(\delta_j = \text{""})$ *then if*$(t = 1)\delta_j =$, *where* $t \in \alpha = \{1,0\}^*$, *j= 1, 2, 3 , … , total_ spaces &black-"", blue-"" &red-"" denotes blank/space characters respectively for clarity.*

Bit extraction: *if* $(\delta_j = \text{""})$ *thenif*$(\delta_{j+1} = \text{""})\{m \leftarrow 1; j \leftarrow j+1\}$ *else* $m \leftarrow 0; j \leftarrow j+1$, *where "j" denotes space counter which has an initial value of 1.*

From above it is obvious that Wendy can easily extract the hidden information by merely knowing the algorithm. Hence, there seems a daring need to induce some sort of uncertainty so that Wendy may not ascertain on actual cover text used in bit embedding process.

For incomprehensible steganography, stego object (**S**) must be an exact replica of cover text(**C**) – the chance of occurrence of which, however, is 1/100 as for remaining cases $\boldsymbol{S \neq C}$. Hence, security of steganographic system relates to the uncertainty involved in detection of actual cover used for whichintroduction of pre-processing stage, as in our case, will force Wendy to first confirm on the actual cover text used, then to figure out how to extract (key dependent) hidden bits from it and finally to recognize original message.

VIII. ADVANTAGES AND LIMITATIONS

Following are some of the pros and cons of our proposed data hiding scheme:

1) Advantages

- Key dependency.
- Information Theoretically Secure Solution.
- Imperceptibility of information hidden inside cover text.
- Increased bit embedding capacity per inserted byte.
- Prior information about hidden message's type and length facilitates in bit-extraction process.
- Doubles Wendy's effort towards cracking the system.

2) Limitations

- Increase in stego object's file size to a number equal to that of spaces in cover text file.
- Less 'Notepad' (default application for ASCII text files) opening the stego object through other applications may result in incomprehensible text.

IX. Future Work

Following are recommended as future work:

- Exploring new ideas to increase bit embedding capacity of text-cover.
- Compression of secret message.
- Adding another security layer via Key controlled encryption.
- Random, stego keydependent, bisectionof encrypted bitsjust before commencement of bit embedding processto illude comprehension about its starting point. OR

  Selecting random, stego keydependent, secret bit embedding starting point in text cover and then traversing cyclically just before that point.

X. Conclusion

Communicational ease that internet offers had its confronting impact when legitimate owners of information got deprived of their stake due to its illicit online copying and distribution. In addition, for many - it also appeared as a direct assault on their privacy and hence was reluctant to store, share and distribute digital contents over the internet. The situation necessitated the need to evolve copyright schemes to protect digital contents that inadvertently has given way for covert communication which is now being exploited in full especially in regions where cryptography is outlawed. With ever changing requirement for persistent storage and retrieval of data a variety of file formats like text, image, audio and video etc. have been evolved of which, excluding text file format, others offer Meta date (additional space) for storing secret information, and hence are the preferred choice for cover/carrier when it comes to information hiding. The fact of the matter, however, is that text format is the cheapest and most preferred choice for communication e.g. SMS texting, IP packets etc. and being least susceptible to be used as cover/carrier is an ideal choice for stealth communication.

This paper presented a novel stegokey dependent insertion-based steganographic scheme for ASCII cover text files. Salient characteristic of the scheme included increased bit embedding capacity per byte (i.e. in place of 1/8 bits per inserted byte, the embedding capacity has raised to 3/8 bits) in contrast to other prevalent text–cover centric steganographic schemes. Pre-processing of ASCII cover text before bit embedding has added an additional security layer which would double the amount of efforts Wendy may now need to get the hidden secret excavated out of the stego object.

References

[1] Chincholkar A.A. and Urkude D.A. (2012) Design and Implementation of Image Steganography. Journal of Signal and Image Processing, ISSN: 0976-8882 & E-ISSN: 0976-8890, Volume 3, Issue 3, pp.-111-113.

[2] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, Information Hiding: A Survey, Proc. IEEE, 1999

[3] Donovan Artz, Digital Steganography: Hiding Data within Data, IEEE Internet Computing 1089-7801/ 01/$10.00, 2001 IEEE http://computer.org/internet/ MAY • JUNE 2001, p. 75-80

[4] Al.Jeeva,V.Palanisamy and K. Kanagaram, Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com, Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037.

[5] Kipper, G.: Investigator's guide to steganography. Auerbach Publications, 2004 (240 p.), ISBN: 0849324335

[6] Michael F. Deering,The Limits of Human Vision, Sun Microsystems; http://www.swift.ac.uk/about/files/vision.pdf

[7] Ashraf Seleym and Dina Darwish, Real-time Covert Communications Channel for AudioSignals, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 3, September 2012, ISSN (Online): 1694-0814

[8] Shirali-Shahreza, M.H. Text Steganography in chat, 3rd IEEE/IFIP International Conference in Central Asia on Internet, (ICI 2007), 2007, pp. 1-5.

[9] Shirali-Shahreza, M.H, A New Synonym Text Steganography, International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP '08), 2008, pp. 1524-1526.

[10] Shirali-Shahreza, M., Text Steganography by Changing Words Spelling, 10th International Con-ference on Advanced Communication Technology (ICACT), 2008. 17-20 Feb. 2008, Volume: 3 Page(s): 1912 - 1913

[11] Mercan Topkara, Umut Topkara, Mikhail J. Atallah. Information Hiding through Errors: A Con-fusing Approach.2007. Internet: http://umut.topkara.org/papers/ToToAt_SPIE07.pdf, [July 12, 2012]

[12] Bender, W., Gruhl, D., Morimoto, N. & Lu, A. "Techniques for data hiding", IBM Systems Journal, Vol 35, pp. 313-336.1996.

[13] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal, A Novel Approach of Secure Text Based Steganography Model Using Word Mapping Method (WMM). International Journal of Computer and Information Engineering 4:2, p 96-102, 2010. Shirali-Shahreza, M.H. Text Steganography in chat, 3rd IEEE/IFIP International Conference in Central Asia on Internet, (ICI 2007), 2007, pp. 1-5.

[14] Caching, C. (1998). An information-theoretic model for Steganographic. Proc. of 2nd Workshop on Information Hiding, vol. 1525, Lecture Notes in ComputerScience.

[15] Khan Farhan Rafat, Muhammad Sher. On the Limits of Perfect Security for Steganography System. International Journal of Computer Science issues (IJCSI), Issue 4, May 2013.*Under publication*.www.ijcsi.org

[16] G. J. Simmons, "The prisoners' problem and the subliminal channel," inAdvances in Cryptology:Proceedings of Crypto 83(D. Chaum, ed.), pp. 51–67, Plenum Press, 1984.

[17] J.Z lner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G.Wicke, G.Wolf. Modeling the security of steganographic systems. Proc. 2nd Workshop on Information Hiding, April 1998, Portland, LNCS 1525, Springer-Verlag, 1998, pp. 345-355.

[18] T Hansen - 2006, US Secure Hash Algorithms (SHA and HMAC-SHA), http://tools.ietf.org/html/rfc4634

[19] Jaro, M. A. 1989. Advances in record-linkage methodology as applied to matching the 1985 census of Tampa, Florida. Journal of the American Statistical Association 84:414–420.

[20] Winkler, W. E. 1999. The state of record linkage and current research problems. Statistics of Income Division, Internal Revenue Service Publication R99/04.

[21] Minitab 16. http://www.facebook.com/Minitab [June 6, 2012]