Boosting the Capacity of Web based Steganography by Utilizing Html Space Codes: A blind Steganography Approach

M Ali Tariq[1], Aliya Tabassum Abbasi[2] Aihab Khan[3], Basheer Ahmad[4]
[1, 2, 3,4]Department of Computing and Technology, IQRA University, Islamabad Pakistan,
EMAIL: alic0803@gmail.com, aliyatabassumabbasi@gmail.com, aihab@iqraisb.edu.pk, drbasheer@iqraisb.edu.pk,

***Abstract*— Nowadays, Web Steganography is massively used for data hiding. The development of web has expanded the interest for strategies that can guarantee data security on site page. This paper utilizes the html labels (tags) to conceal the secret message. Existing schemes i.e. elements containing other element, changing case letters, line shift, word shift, line break, and changing attributes are not robust across random space modification attacks. Also, imperceptibility of the cover text gets affected. Moreover, these approaches have low embedding capacity for data concealment due to the insertion of only two bits per segment. In this paper, proposed embedding procedure is based on insertion of different space codes in the content containing expressions of web source page. Our proposed scheme hides the secret message bits in the space between the text in html tags by concealing four bits per space; thus by, improving the hidden capacity with minimal perceptivity. Also, proposed method is more secure as secret data have come across some encryption prior to embedding. The experimental result shows that proposed scheme has high capacity by taking 5 variable size texts and comparing these with different existing approaches. Moreover, imperceptibility is also analyzed experimentally by comparing the file change size of the proposed approach with previous methods.**

Keywords*— Steganography; HTML; white spaces; Special space codes; security; hidden capacity; imperceptibility.

I. INTRODUCTION

Steganography is the art and science of communicating in a way that hides the existence of the communication information. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any intruder to even detect the existence of the secret message [1], thus by achieving secure communication whereas, cryptography is the investigation of changing over the messages that are expected to be secret into some other structure, such that it is not reasonable to anybody other than the planned sender and beneficiaries [2-5]. Covert communication is transferring secret information by hiding it in a cover media such as image, audio, video, text without changing their appearances [6-8].

Due to large amount of available bandwidth in web based communication; nowadays, web pages became the research area of data hiding and secret communication. Hypertext Markup Language (HTML) is one of the scripting tools used in web development [11-17]. The secret information is embedded in HTML page, and it produces a stego-html page. It becomes part of a website, and also browsing does not find anything suspicious in the web page containing secret stream [15-23].

The ingredients of steganographic system are as follows: -

- Sender is the one who wants to communicate some information.
- Data that a user wishes to Communicate with another party is the secret message which is being embedded in the pre-selected cover object.
- Cover object is the medium which conceals the secret message.
- The resultant object after being secret message is embedded in cover medium is termed as stego media.
- A stego key is the secret key to control that particular secret communication [9-10] and aided in the extraction process.
- Embedding algorithm is the incorporated steganography method to conceal the secret message in the particular cover message.
- Receiver is the only person who knows stego key and he/she has privilege to extract secret information from stego-object.
- Extraction or decryption algorithm is essentially the embedding algorithm runs in reverse. It takes the stego-media and stego-key and produces the original plain text.

The strength of any steganography system is measured by the following parameters:

- Capacity: Capacity is the ability to hide the maximum number of external bits in a given cover file in a way that the chance of detection is negligible.
- Robustness: Robustness is an important attributes of steganography which shows the resistance against the steganalysis attacks during the digital transmission.
- Imperceptibility/Invisibility: A digital steganography is highly imperceptible if it contained unnoticeable modification in stego-message or difference in size of cover and stego-file

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

- Security: It is said that the embedded algorithm is secure if the embedded information is not subject to removal after being discovered by the attacker

Text based Steganography methods can be implemented on web page contents and plaintext [3]. World Wide Web (www) pages have turned into the fundamental approach to give data to Customers [3]. Website page content contains HTML, CSS, XML, JavaScript and so forth as substance [3, 5]. HTML codes are shown by program such as Google Chrome, Safari, and Explorer etc [3]. Web page content Steganography uses labels, properties of the labels of web record to conceal the information.

Utilizing properties as a part of diverse request i.e; uses labels in changing letters cases [3],whitespace in the labels are a few procedures used to conceal information in web archives [3, 4, 5, 6]. There are different types of text based steganography techniques for html document i.e. Change case of letters in tags [1], appearing order of attributes [2], changing orders of elements [3], shift rows [5], white space on tags [6], hide data using attributes etc [7,8]. Above mentioned schemes have resulted in low hidden capacity by hiding only small number of characters of steganography systems [19, 20, and 21].

Our paper is an improvement of the work incorporated in the papers [3], [12], [13]. In this paper, an enhanced technique is proposed to boost the Capacity of Web based Steganography by utilizing Html space codes. To improve the embedding capacity, our technique is hides more bits as compared to previous methods. Prior to this method, maximum of ten space codes are used to hide two bits per segments (one character takes four spaces to hide) in Html document. Also, previous methods only hide in small characters. Our proposed method incorporates ten space codes to hide four bits per Segment(one character takes two spaces to hide) in Html document, secret message is hidden in the spaces between words of a text in HTML document and the scheme is effective in achieving better capacity rates, while maximizing the Imperceptibility factor. Proposed technique utilizes blank space codes in Html Document, so originality of Html text does not change. Moreover, our scheme also eliminates the barrier by hiding in small, capital and special characters as well.

Rest of the paper is organized as follows: The Section 2 of the paper contains related work. Proposed method has been elaborated in section 3; Section 4 elaborates the incorporated algorithm; section 5 evaluates the proposed method experimentally. At last, conclusion and future work is presented in section 6.

II. RELATED WORK

There has been immense work in the field of text Steganography [1, 2, and 3]. Various techniques are in placed that hide the text inside the source code of the Html file [1, 3, and 6]. These techniques are based on hiding information in the properties of HTML elements such as; Html space codes, tags and spaces to encode/decode the secret message with two bits per segments (one character takes four spaces to hide). Some of the work related to web steganography is explained below:

Yang et a ., [8] proposed an efficient webpage information hiding method that conceals the secret message in Html file by changing the order of attributes [17].The disadvantage of this scheme is low embedding capacity as their scheme is capable of concealing only one or two bits per segment in Html document.

Another improved scheme uses random characters to hide the secret stream in an Html file [9]. The idea behind this scheme is to improve the Imperceptibility and embedding capacity, but the imperceptibility problem still persists as the hidden text document is visible on webpage.

The Approaches used by *Garg et al .,* [2] & *Zhang et al.,* [10] bits grouping attribute order are less robust, as these approaches affect the integrity of content, which intruder can easily know about the existence of secured information and tries to retrieve.

Another scheme that hide secret message in the spaces between expressions of a spread in HTML document [3]. This scheme has low imperceptibility, since embedding procedure has changed the originality of the cover message.

Also*, Junling et al.,* [11] proposed a scheme attribute order to hide secret message. This scheme is less robust against different means of attacks, as this approach affecting the integrity of contents during embedding. Another data hiding method involves the changing of the letter case to hide the secret message in HTML document [12]. However, this approach has low embedding capacity because of concealing one bit per substitution and insufficient vocabulary.

Chen et al., [13] presented character coding scheme for HTML document by hiding two bits. But, their embedding procedure don't embed large cover message. Also, secret information is directly embedded in a cover medium without any encryption which results in a rapid access of secret, if once discovered. Some approaches using Unicode Space characters, line shift and attribute to hide secret information in HTML document [18]. These approaches are less robust against different means of attacks.

Puneet et al., [19] proposed a scheme to improve the capacity data hiding in Html Document. The author use different attributes and special codes of html to improve the capacity and imperceptibility. The special codes don't work well and this approach has robustness issue because of lack of any encryption or randomization used before embedding.

The techniques used in [22] *and* [23] incorporated special characters to embed the secret information in Html documents. However, these are less imperceptible, and also have low hidden capacity, since these schemes do not compensate large size secret messages. Moreover, these approaches are less robust against different means of steganalysis.

Hence, concluding the above extensive literature, previous web based steganography approaches do not combat among the conflicting steganography parameters, which are the matter of great concerns.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

III. PROPOSED METHOD

This paper presents an improved scheme which boosts the Capacity of Web based steganography by utilizing Html space codes while minimizing the imperceptibility factor. Figure 1 shows proposed text steganography scheme.

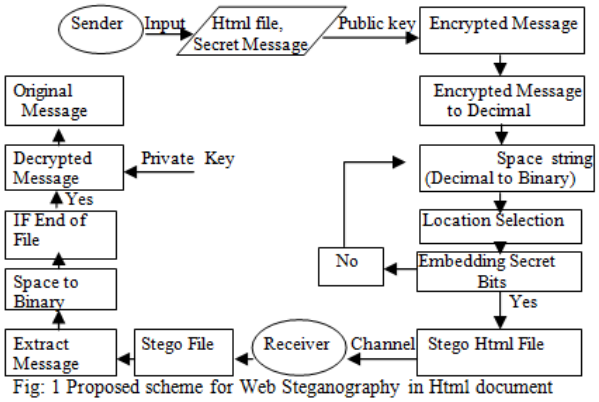

Fig: 1 Proposed scheme for Web Steganography in Html document

Fig: 1 shows our proposed model. Here we present an improved scheme, that is easy to use and can also increase the LEC (largest embedding capacity) of the cover webpage. Our proposed strategy is also hiding small, capital, special characters with four bits per segment and stow away more bits in the Web record with a largest embedded capacity and imperceptibility. The proposed method utilizes the html labels, white space and their credits to hide the secret message. It embeds in way that the properties in the html labels have no effect on the presence of the archive. These properties of html tags can be utilized to hide the secret messages effectively. The proposed scheme is divided into two main processes: embedding and extraction process. Different processes such as message encryption, space string generation, and finally concealing process are further part of the embedding process. The detail of the above mentioned processes are explained below:

A. Embedding Process

i) *Message Encryption Process:* First step towards embedding process is to encrypt the secret message prior to embedding, so as to increase the security of the proposed scheme. For encryption of the secret stream, the proposed scheme uses caser cipher.

ii) *Space Code Generation Process:* This process involves the conversion of secret message to decimal which is then undergoes through several stages to get the required space codes for embedding. These stages include:
- At first, perform the MOD operation of the decimal value by 10.
- Secondly, store the resultant quotient and remainder value. And convert these both stored values to their equivalent binaries.
- In the next step, convert these resultant binaries into four bit group or block.
- After that, search each four bit block to space code table listed in Table 3 to get the required space codes for embedding.

iii) Concealing Process: select the appropriate HTML page. And conceal these space codes in the space between the words of text in tags behind the source code of the selected web page. The resultant web page after embedding is called stego text which is being ready to be communicated.

B. Extraction Process

The strength of any steganography system is measured by the simplicity of its extraction process. The simpler is the extraction process, the more effective is the steganography system [3]. Hence, the extraction process of the proposed scheme works exactly in opposite of the embedding procedure making it quite simple and easy to implement.

Extraction process follows the following reverse procedure:

i) Extract the embedded space codes from the stego text.
ii) Convert these extracted space codes to their allotted binaries by following the Table 3.
iii) Combine each binary block and convert these to decimal.
iv) Decrypt this decimal value to get the original message.

To make the proposed steganography system more understandable; a sample example is demonstrated below:

For instance; "DR**"** is the secret message that is to be embedded and retrieve from the Html document. Secret information is first encrypted before embedding in Html Document to increase security. Once it's encrypted, secret information is converted to decimal (e.g. decimal value is 65). Calculate the decimal value by MOD 10 (Q=6, R=5 when taking mod) and store the quotient and remainder in variables. Convert the decimal value of quotient and remainder in binary (e.g. when taking mod binary value is 01100101 and binary to nibble (0110 0101). Search the space codes of quotient and remainder in special code table and encode it by using the index number of code table.   space codes are selected according to index number of fixed space codes and encode in the space between words of text in Html document. To retrieve the secret information from Html Document, we use the reverse procedure of Decoding process.

- HTML Space Codes

Hypertext Markup Language (HTML) is utilized as a steganography media, and exchange data as hypertext records through web. It depicts the structure and the semantic content of a web document. HTML supports visual pictures and different Medias. Different HTML components are used, for example, <img>, <title>, , <p> etc. These are the building squares of site page. Two sorts of spaces are used in html document, Normal Space and Non-breaking Space. The numeric character Representation of these two classes of clear characters shows up as standard space in site page. Html additionally characterizes character element references. Table 2 shows two sorts of space codes accessible in Html.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

In this situation, consider an altered number of unique space codes. As mentioned earlier, our proposed technique makes use of these altered space code. Table 3 demonstrates an illustration of 10 space codes

Table 2: Types of Space Codes

Normal Spaces	Character Representation	Character element
&#32	&#32	&#ensp
&#32	&#2000	&ensp14
&#20	&#2003	
	&#32	
	&#2005	
	&#2006	
	&#9	
		&#nbsp
	&#x8194	
	&#2007	
	&#2001	
	&#xA8194	

Table 3: Fixed Space Codes

Sr no	Space codes	Bits
1	Space	0000
2	&#9	0001
3		0010
4	&#32	0011
5		0100
6		0101
7	&#nbsp	0110
8		0111
9		1001
10	&#1v60	1010

IV. PSEUDO CODE/ALGORITHM

Pseudo code of the proposed method is generally categorized into two algorithms:

a. Embedding Algorithm
b. Extraction Algorithm

Each of these algorithms is explained under subsequent section.

A. Embedding Algorithm

Algorithm of the proposed embedding procedure is detailed below:

Input: Cover Html File (C) and Secret Message (S)
Output: Stego HTML File (C)
Step1: *Begin*
Step 2: ES [] =encrypt(S) // encrypt secret message//
Step 3: for i=1 to ES
Step 4: EB[i] = ConversionToBinary (ES[i]) // binary
Step 5: Next I //conversion of Encrypted message characters//
Step 6: for j=1toEB
Step 7: ED[j] =ConvertionToDecimal (EB[j]) //conversion to
Step 8: R[j] = Calculate ED[j] MOD10 decimal and caluclation
Step 9: Q[j] = Calculate ED[j]\10 of remainder and quotient//
Step 10: Next j
Step 11: for each R [] and Q []
Step 12: bB [] =ConversionToBinary(R&Q [])
Step13: SPC [] = Get_spacecode (bB []) //Space Codes//
Step14: While (SPC! =EOF ())
Step15: C' =Embed (SPC [], C) // Stego HTML File//
Step16: *end*

The above algorithm describes the embedding procedure in detail. Encryption of secret message (ES) takes place at step 2. At step 3-5, the encrypted secret message characters are converted to their equivalent binaries (EB_1, EB2… EBn). Each of these Binaries is then transformed to decimal (ED_1, ED2… EDn) at step 7. Remainder (R) and Quotient (Q) of each of the decimal is calculated using step 8-9. From step 11-13, each of the resultant remainder and quotient value are then converted to binary blocks (bB_1 bB_2… bB_n); i.e; each block contains 4 bits. Space code is now being searched against each of these binary blocks, which are then embedded in the cover text (C) to get the stego text (c').Thus, the proposed embedding algorithm successfully embeds four bits per space segment.

B. Extraction Algorithm

Extraction algorithm works exactly in reverse order of the embedding algorithm.
The formal algorithm for the extraction process is explained below:

Input: A Stego HTML file (C')
Output: Secret Message (S)
Step 1: *Begin*
Step 2: while (C'! =EOF ())
Step 3: SPC [] =Extract SPC // extraction of embedded space
Step 4: end while code//
Step 5: for each SPC []
Step 6: bB [] =Extract (SPC)//extraction of four bit binary blocks//
Step 7: ED [] =ConvertToDecimal (bB [])
Step 8: Next j
Step 9: For j=1 to ED []
Step 10: EB [] =ConvertToBinary(ED []) // conversion of each
Step 11: Next j decimal to their equivalent binary//
Step 12: for each EB []
Step13: ES [] =ConvertToCharacter (EB []) //Character Conversion//
Step14: S=Decrypt (ES []) //decryption of characters//
Step15: *End*

The above algorithm includes the steps of the proposed extraction process. At step 2-4, embedded space codes (SPC_1, SPC_2… SPC_n) are extracted from the stego text. Across each space code binary group of bits (bB_1, bB_2… bBn) are extracted and then converted to decimal (ED_1, ED_2… EDn), which is being listed from step 5-8. These extracted decimals are then again converted to binary (EB_1, EB_2… EBn) at step 9-11. At step 13, the encrypted characters (ES_1, ES_2… ES_n) is fetched across each binary. These encrypted characters are then reconverted by decryption algorithm to get the

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

desired secret message (S).

Example: "A" is the secret data which is to be embedded in Html document. Secret information is first encrypted before encoded to Html Document to increase security. Once it's encrypted, secret information is converted to decimal (e.g. decimal value is 65). Calculate the decimal value by MOD 10 (Q=6, R=5 while taking mod), and store the quotient and remainder in value. Convert the decimal value of quotient and remainder in binary (e.g. when taking mod binary value is 01100101 and binary to nibble (0110 0101). Search the space codes of quotient and remainder in special code table i.e Table 3, and encode it by using the index number of code table.   .Space codes are selected according to index number of fixed space codes and encode in the space between words of text in Html document.

V. RESULTS AND DISCUSSIONS

A progression of examinations has been taken to test the proposed method in this paper. The test environment incorporates: Core i7-2450 M CPU @ 2.6 GHz RAM is 6GB DDR3, Window 7 operating system, language is C# and Development tools are Microsoft Visual Studio 2013 and Html source. Fig.2,3 shows the screenshots of the diverse strides of Hiding Process in Html Document.

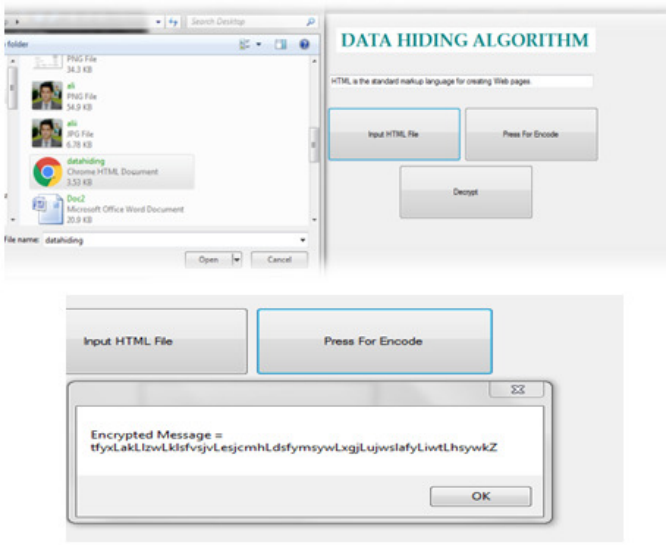

Fig 2: Encryption of Secret message

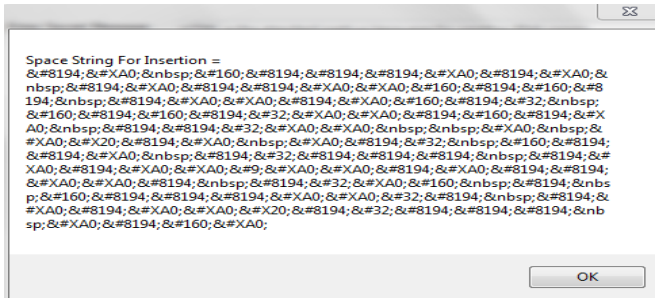

Fig 3: Embedding of Space codes

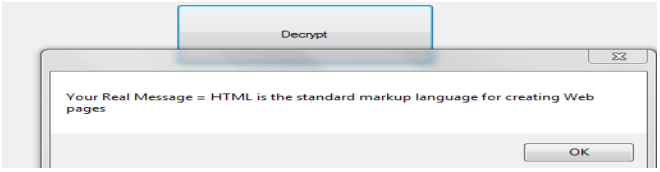

Fig 4: Decryption of reveal secret message

A. Capacity Test

Table 4 shows the experiment results of Embedding Capacity between Proposed and Existing methods. In order to evaluate the performance of the Proposed Hiding Method Capacity (PHMC) in terms of embedding capacity, existing methods LEE Hiding Method Capacity (LHMC), YANG Hiding Method Capacity (YHMC), CHOU Hiding Method Capacity (CHMC), and the proposed method were implemented using Octave software. Embedding capacity ratio of proposed method is far better than existing methods. The embedding capacity is calculated by counting the total number of secret characters that is embedded in an HTML file. Previous methods embed two bits per segment while taking only small characters for embedding; whereas, the proposed method embeds four bits per segment by taking every small, capital and special characters. The capacity performance of the proposed method can be clearly depicted in table 3. Fig 5 shows the results that our proposed method has improved the embedding capacity to larger extend as compare to existing approaches.

Ratio of the embedded capacity is calculated by using ratio formula:

$$Embedding\ Capacity\ Ratio = \frac{Embedding\ characters\ size}{Html\ character\ Length} \quad (1)$$

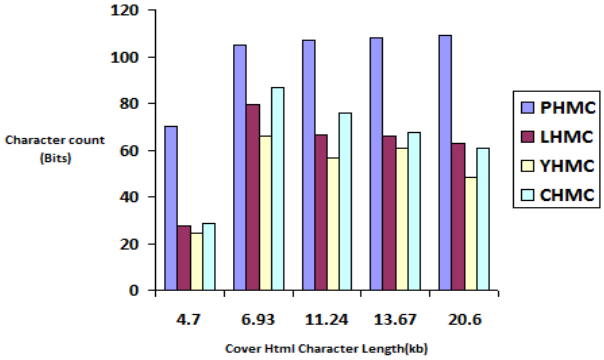

Fig 5: Comparison of Hidden capacity with Proposed and Existing methods

B. Imperceptibility

Proposed method is imperceptible as it embeds the secret message in the source code of the HTML page.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Table 4: comparison of hidden capacity between

Text	Text Size(KB)	LHMC(Bits)	LHMCR (3Bits)	YHMC (Bits)	YHMC R(2Bits)	CHMC (Bits)	CHMC R(3Bits)	PHMC (Bits)	PHMCR (4Bits)
1	**4.7**	130	27.65	115	24.46	135	28.72	330	70.21
2	**6.93**	550	79.36	458	66.08	600	86.58	728	105.05
3	**11.24**	750	66.72	630	56.04	850	75.62	1200	106.76
4	**13.67**	900	65.83	830	60.71	920	67.3	1480	108.26
5	**20.6**	1300	63.1	1000	48.54	1250	60.67	2250	109.22
Average Results	**11.428**	**726**	**60.532**	**606.6**	**51.166**	**751**	**63.778**	**1197.6**	**99.9**

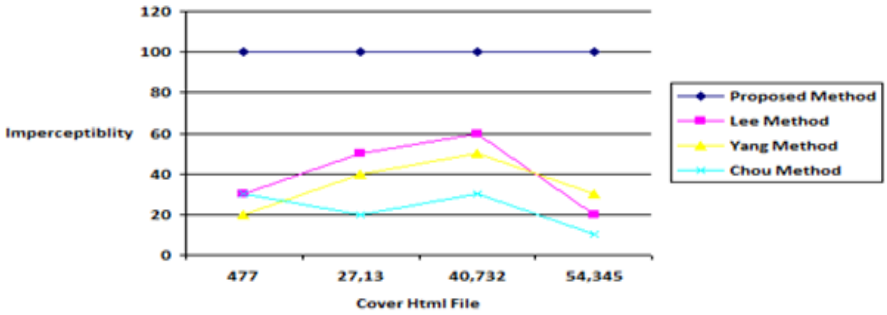

Fig 6: Imperceptibility Test

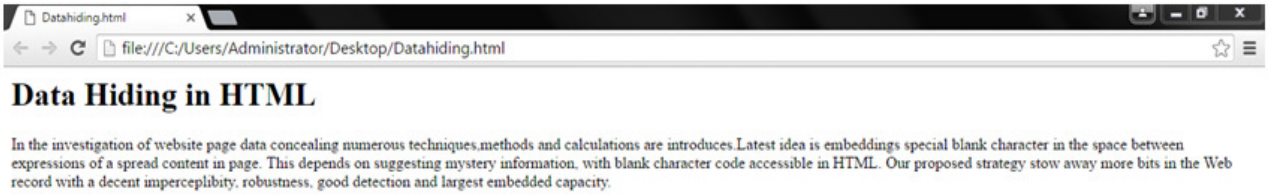

Fig 7: Html Page after embedding

Fig 8: Source code of HTML Page

In fig 6,7 and 8, imperceptibility test is conducted to check the effectiveness of the proposed approach versus previous approaches. This test is an initial attempt towards imperceptibility measures. Fig 6 shows that the proposed approach is imperceptible by showing the value of 100%. Fig 7 and 8 show the screen shot of the perceptibility test.

C. File size change

Table: 5 show the size analysis of Html source file between Proposed and Existing Methods. FSC (file size change) is Another way to measure the imperceptibility of the steganography System. The estimation of FSC underneath the value of 5% is acceptable i.e; below this value system perceptibility is acceptable. Fig 9 shows the results that our proposed method works better than previous methods in terms of file size change

FSC= File size change/Actual file size *100 ..... (2)

File size change= Fc Actual file size= Fs

File size change = $Fc - Fs$ ..... (3)

For example to find out the value of FSC Proposed method (PS):

File size change= 480- 477=3

FSC = $\frac{3}{477} * 100$= 0.62% =100 – 0.62= 99.62

Table 5: Analysis Results of Html Source File between Proposed and Existing Methods

Html Document	Number of Characters in Secret message	Number of Space codes (Lee 3 bit, Yang 2 bit, Chou 3 bit and proposed Method is 4 bit per space)					File Size change (FSC %) After Inserting Secret message (Bytes)					
		Lee Method	**Yang Method**	**Chou Method**	**Proposed Method**	**Actual FileSize**	**Lee & Chou**	**Yang**	**Proposed**	**FSC lee & Chou**	**FSC Yang**	**FSC Proposed**
Doc 1	10	30	40	30	20	477	523	525	480	90.64	89.93	99.62
Doc 2	100	300	200	300	400	20,27	20,40	23,00	20,60	89.5	86.53	99.38
Doc 3	846	2538	1692	2538	3384	27,13	31,9	32,01	27,65	82.41	82.01	98.08
Doc 4	1409	4227	2818	4227	5636	40,73	58,96	50,15	41,75	79.78	76.86	97.50
Doc 5	2253	6759	4506	6759	9012	54,34	68,30	69,10	55,70	74.32	72.83	97.32
Average Results	923.6	2770.8	1851.2	2770.8	3690.4	2944.8	523	525	480	83.33	81.632	98.38

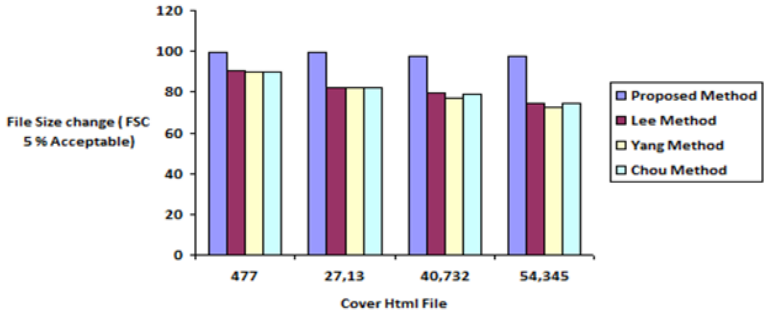

Fig 9: Comparisons of the change in file size

VI. CONCLUSION AND FUTURE WORK

Steganography with html documents is widely used nowadays. There are several methodologies to hide data in Html document. This paper presents an improved steganography system that is capable of hiding four bits per segment, thus by achieving higher capacity and which has also been measured and evaluated experimentally. Moreover, proposed method is more secure due to the encryption of secret message prior to its embedding. Also, proposed technique is more imperceptible and evaluated experimentally by using two methods i.e; imperceptibility test and file size change. Hence, our proposed method guarantees the imperceptibility parameter also. In future, this research may be extended to further improve the robustness of the proposed steganography system.

REFERENCES

[1] Sabu M Thampi," Information Hiding Techniques: A Tutorial Review", ISTE-STTP on Network Security & Cryptography, LBSCE 2004.

[2] Mohit Garg,"A Novel Text Steganography Technique Based on Html Documents", International Journal of Advanced Science and Technology, Vol. 35, (2011)

[3] Chaitali Patel," A SURVEY PAPER ON INFORMATION HIDING ON WEB PAGES", Department of Computer Engineering, International Journal of Smart Device and Appliance Vol.3, No.1 (2015)

[4] Sahil Kataria1, "An Efficient Text Steganography using Digit Arithmetic", Department of Computer Engineering, © Elsevier, 2013

[5] Xiaojun GUO,"Make Your Webpage Carry Abundant Secret InformatinUnawarely", International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, page 541-548.

[6] Puneet Kumar "Adaptive approach for Information Hiding in WWW Pages", Aggarwal HMR, Delhi (INDIA), 978-1-4799-2900-9/14©2014 IEEE

[7] SandipanDey," Embedding Secret Data in Html Web Page", School of Technology and Computer Science Tata Institute of Fundamental Research, Bhabha Road, Mumbai - 400005, India, 1004.0459v1 ,3 Apr 2010

[8] Yujun Yang, Yimei Yang, "An efficient webpage information hiding method Based on tag attributes", Proceedings of the 7th International Conference on Fuzzy Systems and Knowledge Discovery, IEEE, 2010, vol.3, pp. 1181–1184.

[9] SandipanDey," Embedding Secret Data in Html Web Page", School of Technology and Computer Science Tata Institute of Fundamental Research, Bhabha Road, Mumbai - 400005, India, 1004.0459v1, 3 Apr 2010.

[10] Xiaoming Zhang, "A Novel Approach of Secret Hiding in Webpage by Bit Grouping Technology", Department of Computer, Beijing Institute of Petro -chemicalTechnology,Beijing,China,DOI:10.4304/ISSN2614-2621

[11] Junling, Ren, "A Webpage Information Hiding Algorithm Based on Tag Dictionary", International Conference on Computer Science and Electronics Engineering, 978-0-7695-4647-6©2012 IEEE

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[12] Yung-Chen Chou, "A Reversible Data Hiding Scheme Using Cartesian Product for HTML File", Sixth International Conference on Genetic and Evolutionary Computing, 978-0-7695-4763-3/12 © 2012 IEEE

[13] Yung-Chen Chou, , "Data Hiding for HTML Files Using Character Coding Table and Index Coding Table", KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 7, NO. 11, Nov. 2013 2913 Copyright ⓒ 2013

[14] Xiaojun GUO," Make Your Webpage Carry Abundant Secret InformatinUnawarely", 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, page 541-548.

[15] Monika Agarwal, "TEXT STEGANOGRAPHIC APPROACHES: A COMPARISON", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013

[16] Sahil Kataria1, "An Efficient Text Steganography using Digit Arithmetic", Department of Computer Engineering, Govt. Engineering College, Bikaner, India , Proc. of Int. Conf. on Advances in Computer Science, AETACS, © Elsevier, 2013

[17] AnandaprovaMajumdera, "A Novel Approach for Text Steganography: Generating Text Summary using Reflection Symmetry" , Department of Computer Science &Engineering, Dr. B. C. Roy Engineering College, Durgapur, India, 2212-0173 © Elsevier, 2013

[18] Dhammjyoti V. Dhawase, "WEBPAGE INFORMATION HIDING USING PAGE CONTENTS", International Journal of Advanced Research in Computer Engineering&Technology (IJARCET) Volume 3, Issue 1, January 2014

[19] Puneet Kumar "Adaptive approach for Information Hiding in WWW Pages", Aggarwal HMR, Delhi (INDIA), 978-1-4799-2900-9/14©2014 IEEE

[20] Mr. Falesh M. Shelke," Comparison of different techniques for Steganography in images", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 2, February 2014

[21] MitaliGarg," Data Security with Image Clustering using Hopping Neighbour Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 9, September 2014 ISSN: 2277 128X

[22] Yung-Chen Chou, "A Webpage Data Hiding Method by Using Tag and CSS Attribute Setting", Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 978-1-4799-5390-5/14 © 2014 IEEE DOI 10.1109/IIH-MSP.2014.37

[23] Sruthi. E, "Lossless Data Hiding Method Using Multiplication Property for HTML File", IJIRST –International Journal for Innovative Research in Science & Technology| Volume 1 | Issue 11 | April 2015

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731