Data Hiding for HTML Files Using Character Coding Table and Index Coding Table

Yung-Chen Chou[1], Ping-Kun Hsu[2] and Iuon-Chang Lin[2]
[1] Department of Computer Science and Information Engineering,
Asia University, Taichung, Taiwan
[e-mail: yungchen@gmail.com]
[2] Department of Information Management,
National Chung Hsing University
[e-mail: kelp11211@gmail.com; iclin@nchu.edu.tw]
*Corresponding author: Yung-Chen Chou and Iuon-Chang Lin

Abstract

A data hiding scheme in HTML files is presented in this paper. Web pages are a very popular medium for broadcasting information and knowledge nowadays, and web pages are a good way to achieve the goal of secret message delivery because the different HTML coding codes will render the same screen in any of the popular browsers. The proposed method utilizes the HTML special space codes and sentence segmentation to conceal secret messages into a HTML file. The experimental results show that the stego HTML file generated by the proposed method is imperceptible. Also, the proposed method can conceal one more secret bit in every between-word location.

Keywords: Data hiding; HTML; Segment; Secret data delivery

1. Introduction

Information hiding has become a popular research issue in recent years because it can be used to transmit secret data over insecure public networks [1, 14]. The cipher text generated by a crypto system looks like random noise. Secret message delivery may fail because an unexpected user pays attention to the cipher text and might stop the transmission. Thus, Steganography is another method of achieving the goal of secret message delivery.

Steganography uses multimedia as a cover medium to conceal a secret message and generate a stego medium [4, 21, 23, 24]. A sender sends the stego medium to the receiver over public computer networks. An unexpected user will not pay too much attention to the stego medium because the stego medium is most similar to the original medium. Here, the cover medium includes Text, Image, Video, and Audio files. For instance, the LSB (least significant bits) replacement method is a simple way to conceal a secret message into a cover image. Two or three pixel LSBs are replaced by secret bits. Thus, the receiver will determine the secret message by extracting the secret message from the pixels' LSBs in a stego image. Because of the sensitivity of the human eye, it is hard for an unexpected user to notice the distortion in the stego image.

Text is a popular medium in daily internet life and because text's property is different from image, video, and audio, many researchers have been discussing methods of concealing secret data into a cover text file [6]. Text data hiding can be briefly classified as a Microsoft Word document [2, 3, 9, 15, 16, 17, 19, 20], a Portable Document Format (PDF) [12, 25], a HTML file [5, 7, 8, 11, 18, 22], E-mail [10], and program source codes [13].

In this paper, a webpage data hiding scheme is presented. The webpage can be coded by using one of several markup languages (e.g., HTML, XML, PHP, Java script, etc.). HTML is a good way to present a static webpage that introduces some information for a specified topic. An HTML file is composed of tags (e.g., "<HTML>", "<TABLE>", "<BODY>", etc.) and text. An English sentence is composed of words and the spaces between words. Lee and Tsai have presented a data hiding method which uses special space codes to replace type space characters to conceal a secret message [11].

Chen et al. presented a data hiding method by using different sentence presentations to conceal a secret message [8]. Yang and Yang proposed an HTML data hiding technique by adjusting the attributes of HTML tags to conceal a secret message [22]. Also, the case of letters of HTML tags can also be used to conceal secret data. For instance, upper and lower case letter tags can be used to represent secret bits '0' and '1', respectively [5, 18].
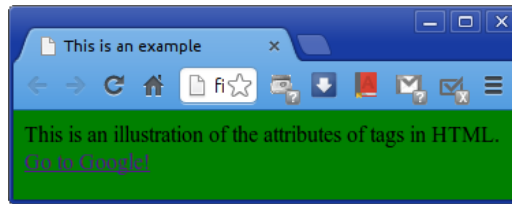
Imperceptible and high embedding capacity are two main criteria in the design of a data hiding method. The perfect solution has no distortion and very high embedding capacity. Unfortunately, distortion and embedding capacity is a trade-off problem.

The proposed method uses the special space codes, segments of between-word locations, and a pre-defined coding index to conceal a secret message. Lee and Tsai pointed out that the blank in Microsoft Internet Explorer can be coded for by using one of several different special space codes [11]. Consequently the human eye will not discern a stego HTML web page. The method described here is inspired by Lee and Tsai's method of utilizing the property of special codes with a segmentation strategy to improve the embedding capacity. The experimental results show that the proposed method can embed one more secret bits for every between-word location.

The rest of the paper is organized as follows. In Section 2, the related works about data hiding for HTML files are briefly introduced. The proposed scheme is detailed in Section 3, and the experimental result and analyses are presented in Section 4. The conclusions are drawn in Section 5.

2. Related Work

In this section, we will briefly introduce the schemes we mentioned in the previous section. Data hiding in an HTML file can be basically grouped into three categories: 1) adjusting a tag letter; 2) adjusting the attribute of a tag; and 3) adjusting the locations between words. Sui and Luo presented a data hiding method to conceal secret data in an HTML file by modifying the case of the letters used in HTML tags according to their embedding rules [18]. The stego HTML file generated by Sui and Luo's method will display the same content as the original HTML file in the browser, because the browser is insensitive to interpret HTML tags. Fig. 1 illustrates a simple example of HTML and source code. The words between the symbols '<' and '>' are called tags in an HTML file, for instance "<html>" and "<head>". Sui and Luo's method modifies the case of the tag letters to conceal the secret data, for instance tag "<html>" is modified to "<HtML>" to conceal secret bits "1011". However, the embedding capacity of Sui and Luo's method can be further improved and the peculiar case arrangement in the tags will attract an unexpected user to pay more attention to it.

(a) A simple HTML file in MS IE9

```
1   <html>
2       <head><title>This is an example</title></head>
3       <body bgcolor="green">
4           <p>This is an illustration of the attributes of tags in HTML.<br>
5           <a href="http://www.google.com/" target="_blank">Go to Google!</a>
6       </body>
7   </html>
```

(b) The source code of an HTML file of (a)
Fig. 1. A simple HTML file and source code

In 2008, Huang et al. presented a webpage information hiding method by using a tag attribute permutation strategy [8] to conceal secret data. Because some HTML tags have several optional attributes that can be used to adjust a webpage's content presentation, the secret data can be embedded in a webpage by adjusting a tag's attribute values. According to Huang et al.'s method, the secret data needs to be converted to a large number before being embedded.

Yang and Yang presented a webpage information hiding method by adjusting HTML tag attributes [22]. Their main idea was to use quotation marks in the tags' attribute values. For example, a "<body "bgcolor=green">" is used to set the webpage's background color as "green"; so "<body>", "bgcolor", and "green" represent the tag, tag attribute, and the attribute's value, respectively. In Yang and Yang's method, if the secret bit is '0' then the tag

is "<body "bgcolor=green">". On the contrary, if secret bit is '1' then the tag is modified as "<body "bgcolor= "green"">". However, the embedding capacity of Yang and Yang's method is limited.

Lee and Tsai presented a data hiding scheme for HTML files by using different space codes to represent a space in an HTML file [11]. The main idea of Lee and Tsai's method is to collect all the codes that represent a white space in the Microsoft Internet Explorer browser and then use different codes to conceal secret data. Table 1 summarizes the white space codes. The key steps of Lee and Tsai's method are as follows: First, collect all space character sequences and transform them into 8-bit ASCII codes. Then encode the space character by considering its corresponding secret bits. Lee and Tsai's method has good performance in terms of embedding capacity. However, the embedding capacity of data hiding in a webpage can be further improved.
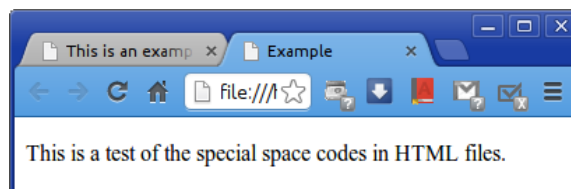
Table 1. Special space code representations in HTML [11]

No.	Name	Code type	Code inserted in HTML	Bits encoded
1	space	ASCII	typed space	000
2	space	Unicode	 	001
3	space	Unicode	 	010
4	space	Unicode	&#32	011
5	non-breaking space	Unicode		100
6	non-breaking space	Unicode		101
7	non-breaking space	Unicode	&#160	110
8	non-breaking space	HTML name		111
9	non-breaking space	HTML name	 	unused

3. The Proposed Method

3.1 The Embedding Phase

In this paper a novel data hiding scheme using HTML files is presented. The proposed method embeds secret data in an HTML file by using special space codes for between-word location segments. The main components include special space codes, a character coding table, and embedding rules. In order to improve the embedding capacity of webpage data hiding, we observed the source code in HTML files and found that codes "	" and "&#9" can also be used for concealing secret data in HTML files. Fig. 2 shows an example by testing different codes represented in Microsoft Internet Explorer. We added the special space codes "	" and "&#9" to generate a new index table, shown in Table 2.

(a) The stego HTML file viewed in MS IE9

```
1  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
2  "http://www.w3.org/TR/html4/loose.dtd">
3  <html xmlns="http://www.w3.org/1999/xhtml">
4  <head><title>Example</title></head>
5  <body>
6  <p>This is&#9;a&#9test&#x20;of&#32;the
7  &#32special space codes&#160in HTML&nbspfiles.</p>
8  </body>
9  <html>
```

(b) The source code of (a)

Fig. 2. Example of the special space codes in an HTML file

Table 2: Index coding table

index	code	index	Code
0			6	typed space
1	&#9	7	
2	 	8	
3	 	9	&#160
4	&#32	A	
5			

The proposed scheme inspired the concept of the special space codes [11] and word-segment to conceal secret data into an HTML file's content sentences. Here, the concept of word-segment is to divide a sentence into several segments. Each segment contains two between-word locations. For example, "The unanimous Declaration of the thirteen United States of America" is a sentence from the United States Declaration of Independence. The sentence can be divided into five segments as "The unanimous ", "Declaration of ", "the thirteen ", "United States ", and "of America".

Before embedding, Character codes are summarized in Table 3, which are selected from ASCII codes from 32 to 126. A new index number is assigned to every character. For instance, "30" is indexed to character 'A'. Note that, the character 'se code' is used to represent the start or the end of a secret message we embed. Because of the 'se code' notification, it is no need to remember the total length of a secret message embedded in an HTML file.

Table 3. Character codes table

	Char	0	1	2	3	4	5	6	7	8	9	A
						Units digits						
	0	!	"	#	$	%	&	'	(	)	*	+
	1	,	-	.	/	0	1	2	3	4	5	6
	2	7	8	9	:	;	<	=	>	?	@	A
	3	B	C	D	E	F	G	H	I	J	K	L
Tens digits	4	M	N	O	P	Q	R	S	T	U	V	W
	5	X	Y	Z	[	\	]	^	_	`	a	b
	6	c	d	e	f	g	h	space	i	j	k	l
	7	m	n	o	p	q	r	s	t	u	v	w
	8	x	y	z	{			}	!	se code			

The key steps of data embedding are as follows. First, secret data is encrypted by any encryption algorithm (e.g., DES, AES, RSA, etc.). The cipher text is then converted according to the symbols in Table 3. Next, space in the segment is encoded by using the special space

code according to the index of the cipher message's character index. For example, the index of the cipher message character 'k' is 69 (referring to Table 3), which is embed into first segment "The unanimous ", then the encoded HTML code will be "The unanimous&#160" (referring to Table 2).

For ease of explanation, let the cipher message be represented as $M = \{m_k \mid k = 1, 2, …, N_m\}$, where N_m is the number of character in M. Further, $S = \{s_i \mid i = 1, 2, …, N_S\}$ represents a set of segments in a cover HTML file H. Here N_S is the total number of segments in H. Every s_i contains two between-word locations and is denoted as s_{ij} where $j \in \{0, 1\}$. Table 4 contains a summary of the simplified descriptions of the notations used in the proposed method .

Table 4. The definition of notations

Notation	Definition
H	Cover HTML file
H'	Stego-HTML file
M	Cipher secret messages
N_m	Total number of characters in M
m_k	k-th character in M
S	A set of segments in H
N_S	Number of segments in H
s_i	The i-th segment
s_{ij}	The j-th space character of the i-th segment

In the proposed method, every segment can be used to conceal one character m_k. The following is the embedding procedure:

Data Embedding Procedure:
Input: A cover HTML file H and cipher secret messages M.
Output: A Stego-HTML file H'.
Step 1: Let $i = 1$, $k = 1$, where $i = 1, 2, …, N_s$ and $k = 1, 2, …, N_m$.
Step 2: Segment the cover text into non-overlapping segments such that every segment contains two between-word locations.
Step 3: Encode the "se code" into first segment by replacing s_{10} as " " and s_{11} as "&#xA0", respectively.
    Set $i = i + 1$.
Step 4: Encode s_{i0} and s_{i1} by using the codes in the special coding table (i.e., referring to Table 2) corresponding to m_k's tens digit and units digit, respectively.
Step 5: If M has been embedded in H, then embed the "se code" into a segment to mark the end of M and go to Step 6,
    else set $i = i + 1$, $k = k + 1$, and go to Step 4.
Step 6: Generate the remaining part of HTML code with no change. Output the stego HTML file H'.

3.2 The Extracting Phase

A receiver can extract the secret data from H' by using the extracting procedure. The extracted data is a cipher message, thus, the receiver needs to decrypt the message with a pre-associated key to obtain the original message. From this point of view, it will be very challenging for an

unexpected user to determine the hidden message without a decryption key, even if the message in H' can be extracted. The following is the extracting procedure:

The Extracting Procedure:
Input: A stego HTML file H'.
Output: Cipher message M.
Step 1: Let $i = 1$, $k = 1$, where $i = 1, 2, …, N_S$ and $k = 1, 2, …, N_m$.
Step 2: Parse the H' to find the first two codes corresponding to " " and "&#xA0" to mark the beginning of the secret message. Set $i = i + 1$.
Step 3: Parse the remaining code to find the two near codes contained in **Table 2**.
Step 4: Extract a secret character m_k by looking up **Table 3**.
Step 5: If m_k equals "se code", then all of secret characters have been extracted and go to Step 6, else set $i = i + 1$ and $k = k + 1$ and go to Step 3.
Step 6: Concatenate the extracted secret characters and output the message.

4. Experiment Result and Analysis

4.1 Experimental Results

In order to evaluate the performance of the proposed method in terms of embedding capacity, Sui and Luo's method [18], Yang and Yang's method [22], Lee and Tsai's method [11] and the proposed method were implemented using Octave software. The embedding capacity is found by counting the total number of secret characters that were embedded in a stego HTML file. We use eleven USA President inaugural addresses (listed in Table 5) to play the cover html and the "US Declaration of Independence" (i.e., total 63,456 characters) as the secret message.

The proposed method embeds eight bits for every segment. That means, each between-word location conceals four secret bits. Obviously, the proposed method conceals one more secret bit than Lee and Tsai's method for every between-word location. The embedding capacity of the proposed method and Lee and Tsai's method depend on the number of between-word locations. Fig. 3 illustrates the performance comparison. The experimental results show that the proposed method can conceal more secret data than Lee and Tsai's method.

Table 5. Eleven cover html

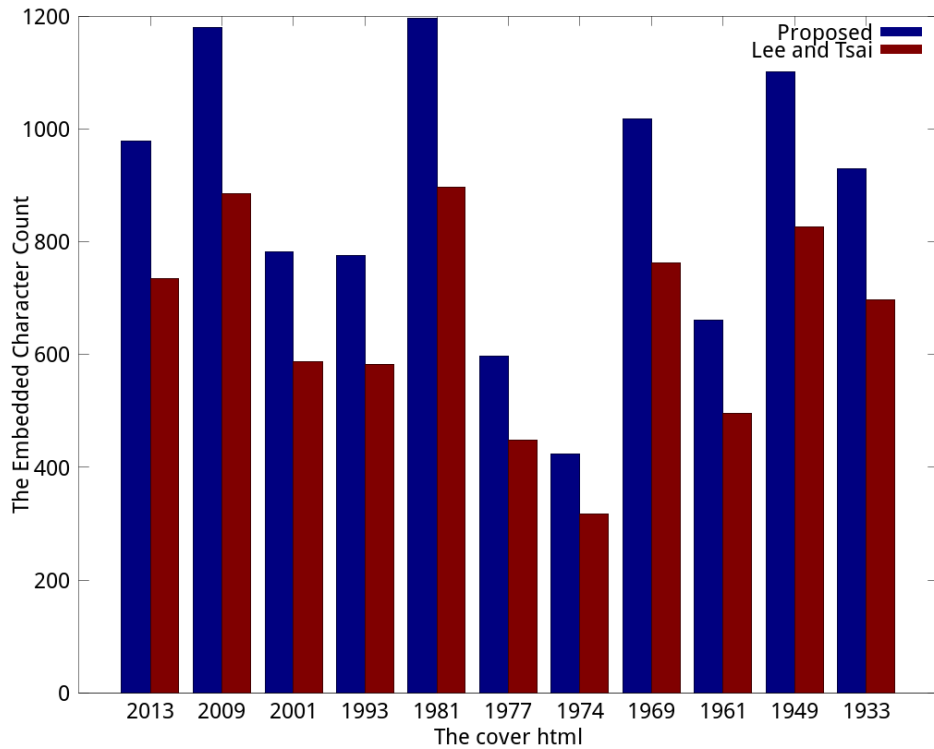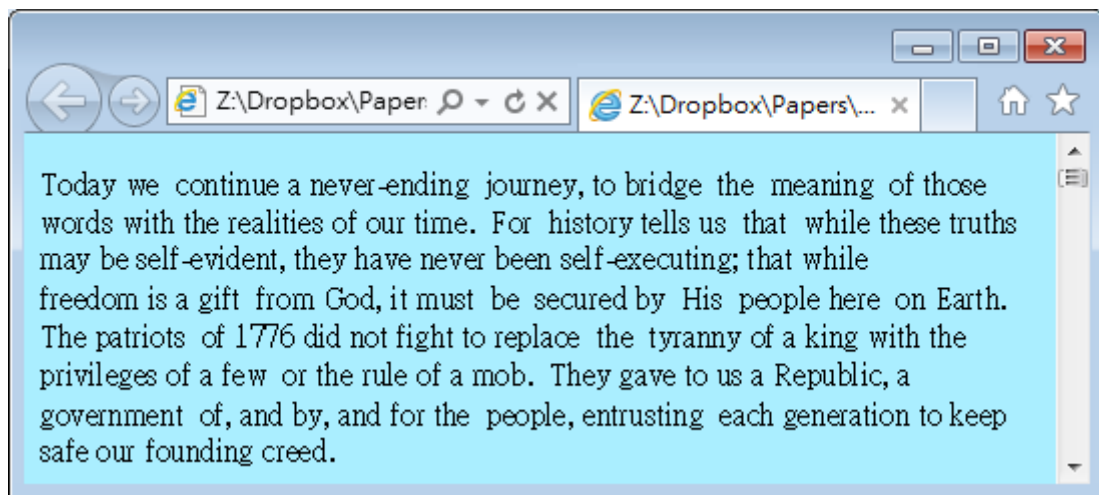| Cover html	Length (Characters)
USA President inaugural address (2013)	11232
USA President inaugural address (2009)	13295
USA President inaugural address (2001)	8997
USA President inaugural address (1993)	9030
USA President inaugural address (1981)	13760
USA President inaugural address (1977)	6887
USA President inaugural address (1974)	4786
USA President inaugural address (1969)	11586
USA President inaugural address (1961)	7605
USA President inaugural address (1949)	13660
USA President inaugural address (1933)	10938

Fig. 3. The capacity comparison of the proposed method and Lee and Tsai's method

Fig. 4 demonstrates the stego HTML generated by the proposed method. The experimental results show that it would be very challenging for a user to distinguish the difference between the original HTML and the stego HTML by using only the human eye.

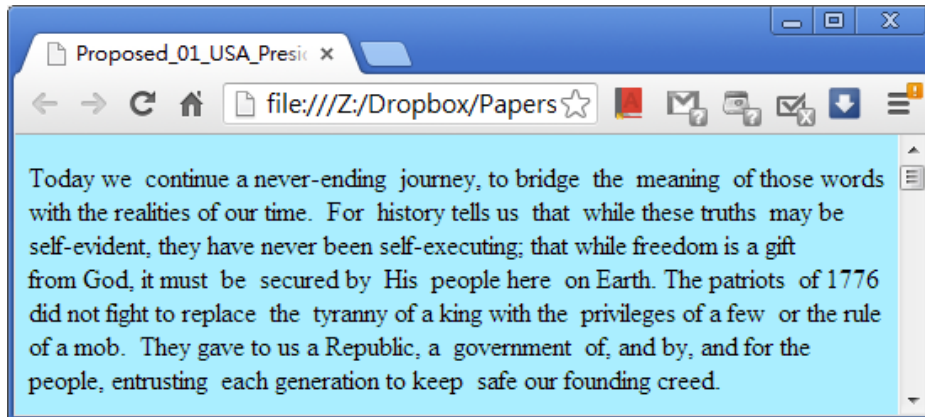(a) The stego HTML file generated by the proposed method (2013 USA President inaugural address)

```
1    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
2    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
3    <html>
4    <body bgcolor='#aaeeff'>
5    <p>Today we continue&#32a never-ending journey,&#9to
6    bridge the meaning of those&#x20;words with&#9the realities
7    of&#32our time. For history tells&#160us that 
8    while these&#x20;truths may be self-evident, they&#32;have&#x20;never
9    been&#x20;self-executing; that&#9;while freedom is a&#160gift 
10   from God, it&#160must be secured by His 
11   people&#x20;here on&#9Earth. The patriots of&#x20;1776 did&#32;
12   not fight to&#32;replace the tyranny&#9of a&#9king with&#x20;
13   the privileges&#32;of a&#x20;few or&#9the rule&#9of a&#x20;mob.
14    They&#9gave to&#9;us a&#x20;Republic,&#32;a government of,
15   &#9and by, and&#32;for&#9the people,&#x20;entrusting 
16   each&#9generation to&#32keep safe our founding&#x20;creed.</p>
17   <p>
```
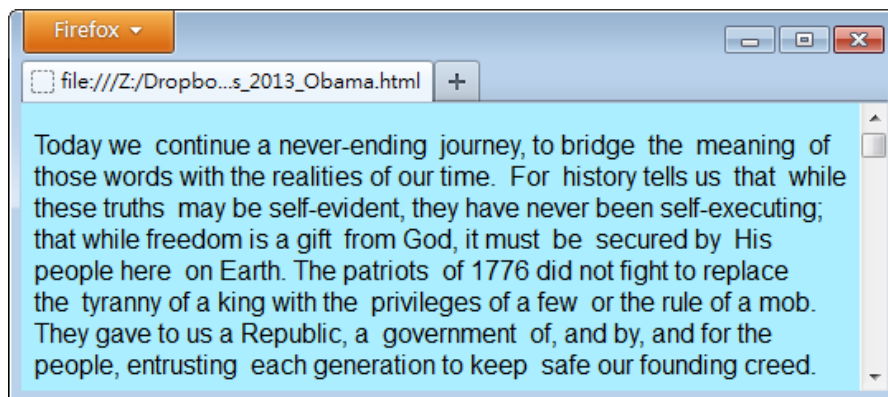
(b) The source code of the stego HTML file
Fig. 4. The visual quality of cover HTML and the source code

Fig. 5 shows the browsing results by using other popular browsers, Firefox and Google Chrome. From Fig. 5, it is hard to distinguish the difference by using the human eye.

(a) The stego HTML shown in Google Chrome

(b) The stego HTML shown in Firefox

Fig. 5. The stego HTML browsed by different bowser (2013 USA President inaugural address)

Sui and Luo's method uses the case of tag letters to conceal secret data. Thus, the embedding capacity of Sui and Luo's method is limited by the number of tags. To carry more secret data, using more redundant tags is a solution. For example, if the secret data contains 300 characters (i.e., 1 character = 8 bits) and normally a tag contains 4 letters, then it requires 300 * 8 / 4 = 600 tags to conceal the secret data.

On the other hand, Yang and Yang's method uses different quotation types to conceal secret data. Thus, the embedding capacity of Yang and Yang's method may also be limited by the number of attribute settings. To carry more secret data, using more redundant attributes is a solution. For example, if the secret data contains 300 characters (i.e., 1 character = 8 bits) and normally an attribute setting can conceal one secret bit, then it requires 300 * 8 = 2400 attribute settings to conceal the secret data.

4.2 Experimental Analysis

The perfect situation for stego html is when all the blank characters never change. However, that is impossible. So, our goal is to try to increase the secret data embedded and increase the reserved "space" characters. The proposed method conceals secret data by using the index coding table with the character coding table, thus the index coding codes utilization will be highly related to secret content. Fig. 6 demonstrates the histogram of index coding codes adopted in concealed secret data. As we see, the "type space" is higher than others.
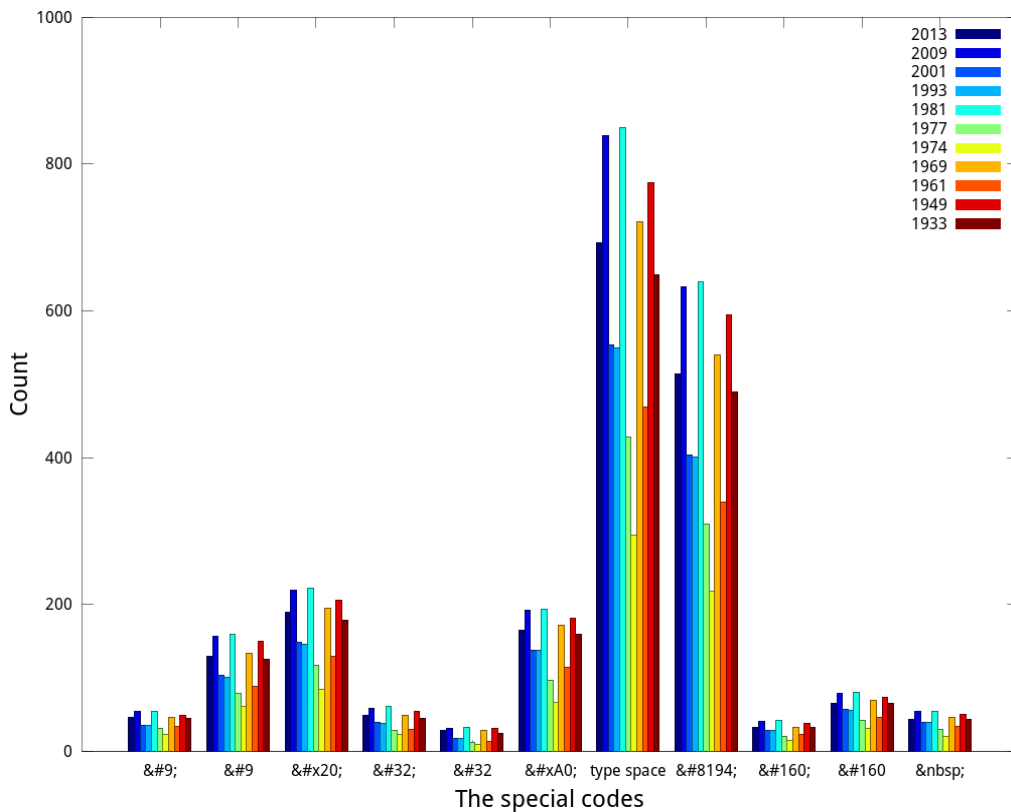

Fig. 6. The count of special codes embedded in test cover htmls using the proposed method

Fig. 7 shows the histogram of special codes embedded in stego html by using Lee and Tsai's method. From Fig. 7, it can be seen that the frequency of the "space" character adopted to conceal secret data is similar to others.
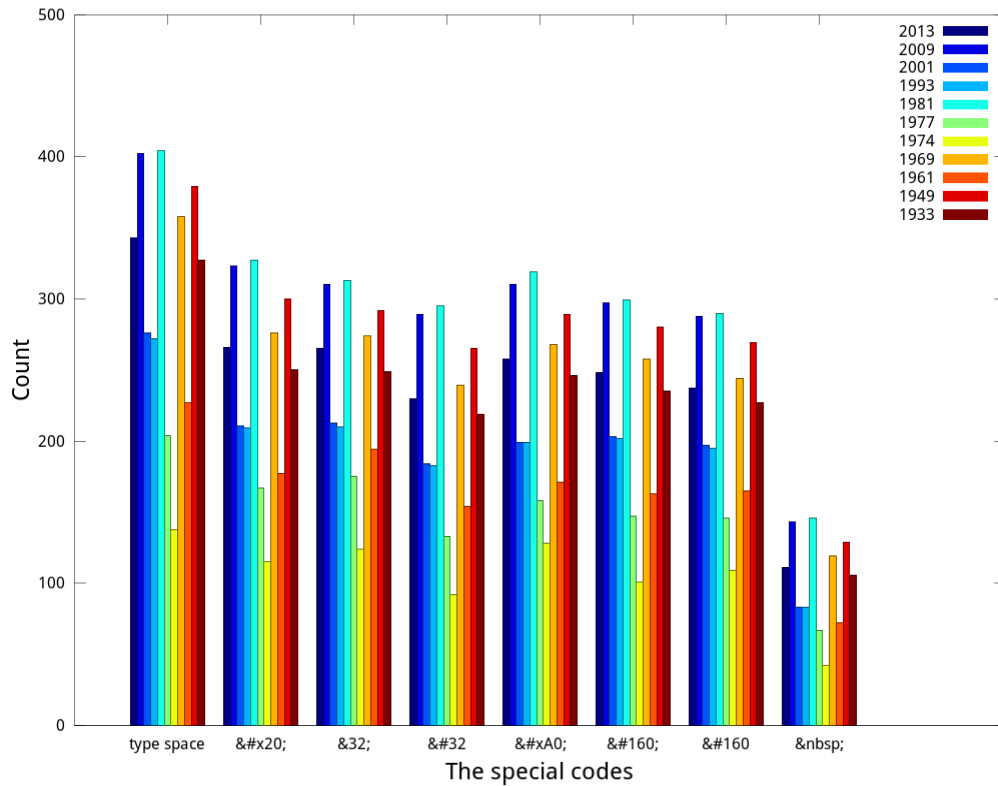
Fig. 7. The count of special codes embedded into test cover htmls using the Lee and Tsai's method

Fig. 8 demonstrates the frequency comparison of the "space" character adoption between the proposed method and Lee and Tsai's method. From this point of view the proposed method not only successfully increases the performance in terms of embedding capacity but also increases the reserved "space" characters. Also, the proposed character coding table can be permuted and pre-shared to both the sender and receiver. In the other words, the proposed method is more secure than Lee and Tsai's method.

Fig. 9 shows the result of run time comparison, the proposed method takes more time to conceal secret data than Lee and Tsai's method. The reason for this is that the proposed method is required to scan the character coding table to determine the corresponding tens digits and units digits. However, due to the computational power of web servers, the run time of the proposed method is still acceptable.
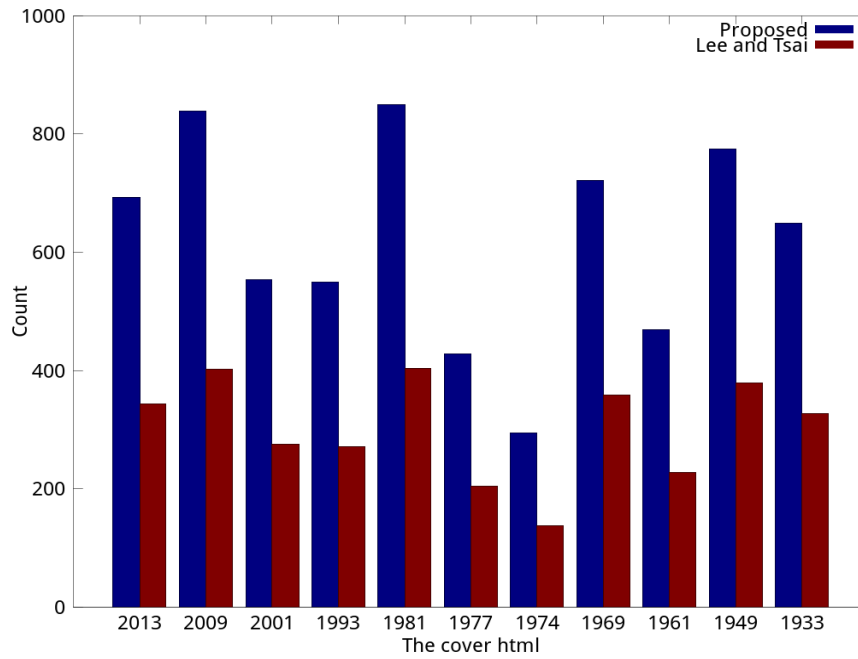
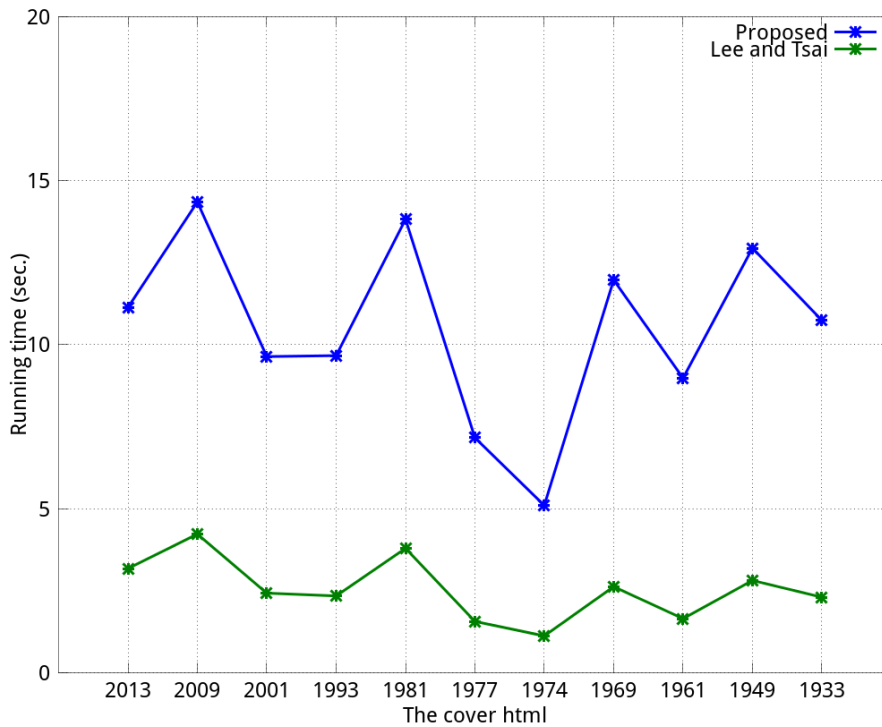**Fig. 8.** The comparison of the count of "Type space" between the proposed method and Lee and Tsai's method

Fig. 9. The run time comparison between the proposed method and Lee and Tsai's method

5. Conclusion

Employing a web page as a cover medium is a good method of secret message delivery, because the web page is a very popular way of sharing knowledge and advertising a

company's information. According to the property of encoding English sentences in a web page, the type space can be represented by several different special codes. Lee and Tsai's method uses eight different special codes to represent the "type space" and conceal the secret message. The proposed method described here improves the embedding capacity of web page data hiding. The proposed method utilizes eleven special space codes and sentence segmentation to increase the embedding capacity. In the proposed method, every between-word location can conceal one more secret bit than in Lee and Tsai's method.

References

[1] M. Barni and F. Bartolini, "Data Hiding for Fighting Piracy," *IEEE Signal Processing Magazine*, vol. 21, no. 2, 2004, pp. 28-39.Article (CrossRef Link)

[2] C.C. Chang, C.C. Wu, and I.C. Lin, "A Data Hiding Method for Text Documents Using Multiple-Base Encoding," *High Performance Networking, Computing, Communication Systems, and Mathematical Foundations*, (Yanwen Wu, Qi Luo Eds.), Springer-Verlag Berlin Heidelberg, Sanya, Hainan Island, China , vol. 66, 2010, pp. 101-109.

[3] C. Chen, S.Z. Wang, and X.P. Zhang, "Information Hiding in Text Using Typesetting Tools with Stego-Encoding," in *Proc. of the First International Conference on Innovative Computing, Information and Control*, Beijing, China, vol. 1, Aug. 2006, pp. 459-462.

[4] I.J. Cox, J. Kilian, F. Thomson Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, 1997, pp. 1673-1687.Article (CrossRef Link)

[5] S. Dey, H. Al-Qaheri, and S. Sanyal, "Embedding Secret Data in HTML Web Page," *Image Processing & Communications Challenges,* (Ryszard S. Choraœ, Antoni Zabludowski Eds.), Academy Publishing House EXIT Warsaw, 2009, pp. 474-481.

[6] M. Grosvald and C. Orhan Orgun, "Free from the Cover Text: A Human-generated Natural Language Approach to Text-based Steganography," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 2, 2011, pp. 133-141.

[7] H.J. Huang, X.M. Sun, Z.S. Li, and G., Sun, "Detection of Hidden Information in Webpage," in *Proc. of the Fourth International Conference on Fuzzy Systems and Knowledge Discovery*, Haikou, China, vol. 4, Aug. 2007, pp. 317-321.Article (CrossRef Link)

[8] H.J. Huang, S.H. Zhong, and X.M. Sun, "An Algorithm of Webpage Information Hiding Based on Attributes Permutation," in *Proc. of the Fourth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Harbin, China, Aug. 2008, pp. 257-260.Article (CrossRef Link)

[9] Y.W. Kim, K.A. Moon, and I.S. Oh, "A Text Watermarking Algorithm Based on Word Classification and Inter-word Space Statistics," in *Proc. of the Seventh International Conference on Document Analysis and Recognition*, Edinburgh, Scotland, Aug. 2003, pp. 775-779.

[10] I.S. Lee and W.H. Tsai, "Data Hiding in Emails and Applications Using Unused ASCII Control Codes," *Journal of Information Technology and Applications*, vol. 3, no. 1, 2008, pp. 13-24.

[11] I.S. Lee and W.H. Tsai, "Secret Communication through Web Pages Using Special Space Codes in HTML Files," *International Journal of Applied Science and Engineering*, vol. 6, no. 2, 2008, pp. 141-149.

[12] I.S. Lee and W.H. Tsai, "A New Approach to Covert Communication via PDF Files," *Signal Processing*, vol. 90, no. 2, 2010, pp. 557-565.Article (CrossRef Link)

[13] I.S. Lee and W.H. Tsai, "Security Protection of Software Programs by Information Sharing and Authentication Techniques Using Invisible ASCII Control Codes," *International Journal of Network Security*, vol. 10, no. 1, 2010, pp. 1-10.

[14] B. Li, J. He, J. Huang, and Y.Q. Shi, "A Survey on Image Steganography and Steganalysis," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 2, 2011, pp. 142-172.

[15] I.C. Lin and P.K. Hsu, "A Data Hiding Scheme on Word Documents Using Multiple-base Notation System," in *Proc. of the Sixth International Conference on Intelligent Information Hiding and*

Multimedia Signal Processing, Darmstadt, Germany, Oct. 2010, pp. 31-33.Article (CrossRef Link)

[16] T.Y. Liu and W.H. Tsai, "A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, 2007, pp. 24-30.Article (CrossRef Link)

[17] M.A. Qadir and I. Ahmad, "Digital Text Watermarking: Secure Content Delivery and Data Hiding in Digital Documents," *IEEE Aerospace and Electronic Systems Magazine*, vol. 21, no. 11, 2006, pp. 18-21.Article (CrossRef Link)

[18] X.G. Sui and H. Luo, "A New Steganography Method Based on Hypertext," in *Proc. of Asia-Pacific Radio Science Conference*, Qingdao, China, Aug. 2004, pp. 181-184.

[19] X.M Sun, G. Lou, and H.J. Huang, "Component-based Digital Watermarking of Chinese Texts," in *Proc. of the Third International Conference on Information Security*, Shanghai, China, Nov. 2004,vol. 85, pp. 76-81. Article (CrossRef Link)

[20] Z.H. Wang, C.C. Chang, C.C Lin, and M.C Li, "A Reversible Information Hiding Scheme Using Left-Right and Up-Down Chinese Character Representation," *Systems and Software*, vol. 82, no. 8, 2009, pp. 1362-1369.Article (CrossRef Link)

[21] S. Weng, Y. Zhao, J.S. Pan, and R. Ni, "Reversible Watermarking based on Invariability and Adjustment on Pixel Pairs," *IEEE Signal Processing Letters*, vol. 15, 2008, pp. 721-724.Article (CrossRef Link)

[22] Y.J. Yang and Y.M. Yang, "An Efficient Webpage Information Hiding Method Based on Tag Attributes," in *Proc. of the Seventh International Conference on Fuzzy Systems and Knowledge Discovery*, Yantai, China, Aug. 2010, pp. 1181-1184.

[23] X.P. Zhang and S.Z. Wang, "Steganography Using Multiple-Base Notational System and Human Vision Sensitivity," *IEEE Signal Processing Letters*, vol. 12, no. 1, 2005, pp. 67-70.Article (CrossRef Link)

[24] Y. Zhao, R. Ni, and Z. Zhu, "RST Transforms Resistant Image Watermarking based on Centroid and Sector-shaped Partition," *Science in China: Series F Information Science*, vol. 55, no. 3, 2012.

[25] S.P. Zhong, X.Q. Cheng, and T.R. Chen, "Data Hiding in a Kind of PDF Texts for Secret Communication," *International Journal of Network Security*, vol. 4, no. 1, 2007, pp. 17-26.

Yung-Chen Chou received Master degree from Chaoyang University of Technology in 2002, and the Ph.D. degree form National Chung Cheng University in 2008. He has presented the assistant professor of Department of Computer Science and Information Engineering in Asia University since February 2009. His research field contains digital Watermarking, Image Retrieval, Steganography, Information Security and Image Processing.

Ping-Kun Hsu received the MS degree in Management Information System in June 2011 from National Chung Hsing University, Taichung, Taiwan. His major in school was data hiding, and his research interests included information security and cloud computing. He works currently in the research and development department of the voice recognition company, Taichung, Taiwan.

Iuon-Chang Lin received the Ph.D. in Computer Science and Information Engineering in March 2004 from National Chung Cheng University, Chiayi, Taiwan. He is currently a professor of the Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan. His current research interests include electronic commerce, information security, RFID Information Systems, and cloud computing.