A High Capacity Html Steganography Method

E. Satir, A. Sargin, T. Kanat, and C. Okuducu

***Abstract*—With the widespread use of the Internet and the booming growth of the computer industry, people nowadays can easily retrieve multimedia contents with their own computers or mobile phones over the Internet or mobile channels. In this case, data hiding is one of the useful schemes for delivering secret messages. Steganography refers to the science of invisible communication. In this study, we proposed a high capacity HTML steganography method that employs URL addresses. Here, URL addresses are used as steganographic cover and the HTML side of the concerning web page is used as a platform for camouflage. Accordingly, it is enough to send only the obtained URL to the recipient. Experiments were performed by investigating steganographic capacity and imperceptibility. The capacity value is increased to 8.85% for the secret message containing 600 characters. Besides, steganographic security is provided via RSA encryption and elaborating the computation by LZW.**

***Index Terms*— HTML steganography, LZW compression, steganography**

I. Introduction

WITH the widespread use of the Internet and the booming growth of the computer industry, people nowadays can easily retrieve multimedia contents with their own computers or mobile phones over the Internet or mobile channels. In this case, data hiding is one of the useful schemes for delivering secret messages. Steganography refers to the science of "invisible" communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganographic techniques strive to hide the very presence of the message itself from an observer. As broadband technologies improve bandwidth at the last-mile, multimedia content, such as still images, audio and video, have gained increasing popularity on the Internet. Given the high degree of redundancy present in a digital representation of multimedia content (despite compression), there has been an increased interest in using multimedia content for the purpose of steganography. Indeed many such techniques have been devised in the past few years [1]. Contemporary approaches are often categorized based on the steganographic cover type such as text, image, audio, or graph [2].

Textual steganography can be classified as textual format manipulation (TFM) and textual fabrication (TF) [2]. TFM modifies an original text by employing spaces, misspellings, fonts, font size, font style, colors, and non-color (as invisible ink) to embed an encoded message. However, comparing the original text with the modified text will trigger suspicion and enable adversary to pin down where the message is hidden in the text [2]. In addition, TFM can be distorted, discerned by human eye, or detected by a computer [2].

On the other hand, textual fabrication techniques generate an entire text-cover for hiding a message rather than manipulating an existing text. Examples of these approaches are null cipher [3], mimic functions [4], [5] NICETEXT and SCRAMBLE [6], and translation-based [7]-[9]. However, the text cover that is generated by these approaches often has numerous linguistic flaws that can raise suspicion. In addition, revealing the hidden message may be feasible [2].

In 2009, Desoky proposed a method called Listega which takes advantage of using textual list to camouflage data by exploiting itemized data to conceal messages. Simply, it encodes a message then assigns it to legitimate items in order to generate a cover text in a form of list. Listega establishes a covert channel among communicating parties by employing justifiably reasons based on the common practice of using textual list of items in order to achieve unsuspicious transmission of generated covers [10].

In 2010 Desoky proposed a steganographic approach that employs NLG (Natural Language Generation) and template techniques along with Random Series values (RS), e.g. binary, decimal, hexadecimal, octal, alphabetic, alphanumeric, etc., of Domain-Specific Subject (DSS) to generate a noiseless text-cover. DSS (like financial, medical, mathematical and etc.) has plenty of room to conceal data and allows communicating parties to establish a covert channel such as a relationship based on the profession of the communication parties to transmit a text-cover. Desoky's method, called Matlist (Mature Linguistic Steganography), embeds data in a form of RS values, function of RS, related semantics of RS, a combination of these, etc. He mentioned that Matlist did not preserve the meaning of text-cover every time it is used, instead it retains different legitimate meaning for each

E. Satir is with Duzce University, Faculty of Engineering, Computer Engineering Department, Duzce, 81620 TURKEY (corresponding author to provide phone: 0380-542-1100; e-mail: esrasatir@duzce.edu.tr).

A. Sargin is with Ministry of National Education, Karakopru Middle School, Sanliurfa, TURKEY (phone: 0506-675-9838; e-mail: abdurrahimsargin42@gmail.com).

T. Kanat is with Ministry of National Education, Konya, TURKEY (phone: 0535-513-3566; e-mail: tayfunkanat91@gmail.com).

C. Okuducu is with Ministry of National Education, Goger Middle School, Diyarbakir, TURKEY (phone: 0506-980-5692; e-mail: cengizoku@hotmail.com).

message while remaining semantically coherent and rhetorically sound [11].

Ryabko and Ryabko (2011) proposed steganographic systems for the case when cover texts are generated by a finite-memory source with possibly unknown statistics. The probability distributions of cover texts with and without hidden information are the same; this means that the proposed stego systems are perfectly secure, i.e. an observer can not determine whether hidden information is being transmitted. The main idea behind the proposed stego systems is the following: Suppose that for a cover text x generated by a source, a set S of cover texts can be founded such that each cover text in S has the same probability of being generated as x. Moreover, assume that each element of S defines S, uniquely. Then, instead of transmitting the cover text x that was actually generated, the cover text can be transmitted in the set S whose number in S corresponds to the secret text which is wanted to be passed. This does not change the probabilistic characteristics of the source, provided the secret text consists of independent and identically distributed (i.i.d.) equiprobable bits. Therefore, an observer can not tell whether secret information is being passed. There are two disadvantages of the outlined stego system: first, the rate of transmission of secret text is not optimal, and second, it applies only to i.i.d. cover texts [12].

To make a steganographic communication even more secure the message can be compressed and encrypted before being hidden in the carrier. Cryptography and steganography can be used together. If compressed, the message will take up far less space in the carrier and will minimise the information to be sent. The random looking message which would result from encryption and compression would also be easier to hide than a message with a high degree of regularity. Therefore encryption and compression are recommended in conjunction with steganography [13].

Finally in 2012, Satir and Isik proposed a LZW (Lempel-Ziv-Welch) compression based [14] and an enhanced version; Huffman compression based [15] text steganography methods where capacity and security issues were considered. In the proposed methods, LZW and Huffman coding algorithms were used to increase the capacity and to contribute the security. Moreover, the proposed methods construct stego keys and employs Combinatorics-based coding in order to increase the security and to provide the desired randomness. For imperceptibility and to render the carrier medium innocent, they constructed forward mail platform as stego cover in order to conceal secret information. They obtained 7.042 % and 7.962 % capacity values for the secret message containing 300 characters (or 300·8 bits) via LZW and Huffman coding algorithms, respectively. They stated that the hidden information cannot be extracted, easily without the used stego keys. Besides, the extraction procedure was rendered more complex by means of the employed compression techniques.

In this study, a steganographic method that employs web page as the carriers, has been proposed. The purpose of this study is to obtain a significant increment ratio in the amount of secret data that is aimed to be hidden while complicating the extraction procedure and ensuring the imperceptibility. For capacity issue, secret data has been compressed via LZW coding since it is widely used in the literature and most importantly, it does not necessitates to send any additional information to the recipient for decompression. Certainly, this situation has an additional contribution to capacity. For imperceptibility issue, secret data has been camouflaged in HTML (Hyper Text Markup Language) side of the web page without making any modification. After detecting the coordinates of the secret data on the web page, RSA (Rivest-Shamir-Adleman) encryption algorithm has been applied for the purpose of security. Then, these encrypted content has been compressed again and embedded to the URL (Uniform Resource Locator) of the concerning web page. Thus, we obtain the URL that has a legitimate length. Evaluation procedure of the proposed method has been carried out by measuring steganographic capacity in terms of percent. Besides, imperceptibility has been considered as the main issue. The rest of the paper has been organized as follows:

A detailed explanation of the proposed scheme has been provided in the 2nd section. The performed experiments and the obtained results have been mentioned in the 3rd section. Finally a general outcome has been expressed in the 4th section.

II. The Proposed Method

Embedding and extracting phases of the proposed scheme will be explained in this section by mentioning the necessary calculations. It will be useful to provide a quick scenario, before a detailed explanation.

As noticed from the above sections, we proposed a steganographic scheme by employing HTML side of web pages. In the sender side, the secret message is firstly compressed. Then this obtained shorter content is hidden in source code (HTML side) of each web page in the collection, respectively. Namely we perform the same hiding operation for every web page in the collection. Here, the purpose is to find the best web page that provides the maximum capacity rate. After defining the best one, the compression operation is again applied to the achieved content as the result of hiding. Thus, capacity is increased again while the computation is being elaborated. Finally, the current content is encrypted and embedded in the URL of the concerning web page. So, it is sufficient to only send the obtained URL to the recipient since the secret message can be extracted by reaching the corresponding web page via this URL. Namely, once the recipient gets the URL, he/she can extract the secret message by applying inverse of the embedding phase.

A. Embedding phase

Block diagram of the embedding phase has been provided in Figure 1.

Let's explain the operations and variables in each block.

1. Compression: Secret message is compressed via LZW coding in this step. Let *M* be an array containing characters of secret message and *M'* be the content after compression. As the result, we can claim that:

$$S(\mathrm{M'}) \leq \mathrm{S(M)}$$

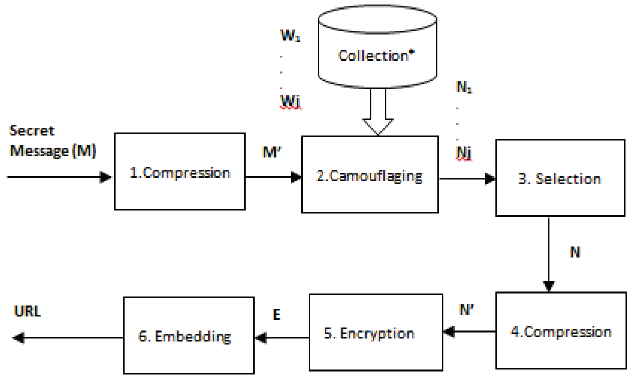

Fig. 1. Block diagram of the embedding phase

2. Camouflaging: In this step, we employ collection of web pages to enhance the capacity. Let *W* be a web page in the collection. We consider the source code, namely HTML side, of the web page for camouflaging. Thus, we can represent *W* as an array containing the symbols in the HTML side.

$$M' = (\mathrm{m}'_1, \mathrm{m}'_2, ..., \mathrm{m}'_i)$$
$$\mathrm{W} = (\mathrm{w}_1, \mathrm{w}_2, ..., \mathrm{w}_j)$$

Since HTML side consists of the symbols including letters, numbers, marks and etc. we can perform the following operations to achieve the new content *N*:

$$\begin{aligned} &\mathrm{m}'_1 = w_1 \rightarrow n_1 = 1 \\ &\mathrm{m}'_1 = w_2 \rightarrow n_1 = 2 \\ &\vdots \\ &\mathrm{m}'_1 = w_j \rightarrow n_1 = j \end{aligned} \tag{1}$$

Let's assume that $n_1=1$. This means that the first elements of *W* (the first symbol in HTML code) and *M* (the first character in secret message) are the same. After estimating the first element of *N* like that, the rest is estimated by considering the relative distances via Equation 2:

$$\begin{aligned} &\mathrm{m}'_2 = w_2 \rightarrow n_2 = 2-1 \\ &\mathrm{m}'_2 = w_3 \rightarrow n_2 = 3-1 \\ &\vdots \\ &\mathrm{m}'_2 = w_j \rightarrow n_2 = j-1 \end{aligned} \tag{2}$$

This operation is performed iteratively till all elements of *M'* is mapped. As the result we obtain a numerical array; *N* whose element number equals to the element number of *M'*.

$$S(\mathrm{N}) = \mathrm{S}(\mathrm{M'}) = \mathrm{j} \tag{3}$$

The essential point in this step is that we perform the camouflaging for every *W* in the collection by using the same *M'*. Thus, we will be able to define the best *W* in the next step.

3. Selection: In this step, we consider the steganographic capacity rate to choose the best *W* in the collection. Steganographic capacity is calculated via Equation 4 [10]:

$$C = \frac{BitsofSecretMessage}{BitsofStegoCover} \tag{4}$$

Accordingly, we can adapt this formula to our scheme as follows:

$$C = \frac{BitsofM'}{BitsofURL} \tag{5}$$

Notice that this calculation is performed for each *W* in the collection. As the result, *W* that gives the maximum *C* is chosen as the carrier to camouflage. Besides, rest of the operations are performed on *N* which corresponds to the chosen *W*.

4. Compression: The obtained *N* is compressed via LZW coding again. The purpose of this operation is to enhance steganographic capacity and elaborating the computation for steganographic security. At the end of this step, we have a new numerical array *N'*. Certainly we can claim that:

$$S(\mathrm{N'}) \leq \mathrm{S}(N)$$

5. Encryption: In this step, *N'* is encrypted via RSA encryption algorithm. Let's call this content *E*. The purpose of this operation is to ensure steganographic security in case of any observations and to render the proposed scheme resilient against attacks.

6. Embedding: In this step, the encrypted array; *E* is embedded into the URL of the chosen *W* (in step 3). Here, the most important point is not to have any error message when the modified URL is typed on the browser. Therefore, collection consists of the web pages which can be adapted to our scheme. Thus, for the sender, it is enough to send this URL to the recipient. There is no other content that has to be sent since the URL correctly directs the recipient to the chosen web page (*W*).

B. Extracting phase

Block diagram of the extracting phase has been provided in Figure 2.

Again, let's explain the operations in each block.

1. Separation: In this step, the embedded part is separated from the URL, to apply the operations of the embedding phase in the reverse order. Thereby, we obtain array *E*.
2. Decryption: *E* is decrypted via RSA. Thus, we obtain *N'*; namely the compressed array that corresponds to the selected *W*.
3. Decompression: In this step, we decompress *N'* to reach array *N* which is obtained after camouflaging (step 2) in embedding phase.

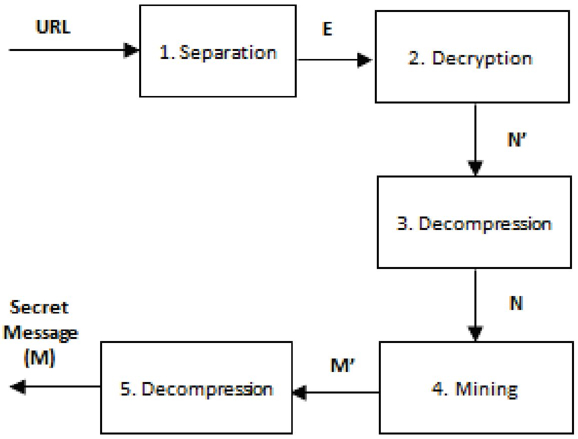

Fig. 2. Block diagram of the extracting phase

4. Mining: We have an URL that comes from the sender and we have N from the previous step. Thus, we can achieve M'; the compressed form of the secret message. Notice that the URL correctly directs us to the web page (W) used for camouflaging. We can obtain M' by performing the following mappings on the HTML side of the concerning W.

$$\begin{aligned} m'_1 &= w(\mathrm{n}_1) \\ m'_2 &= w(\mathrm{n}_1+\mathrm{n}_2) \\ &\vdots \\ m'_j &= w(\mathrm{n}_{j-1}+\mathrm{n}_j) \end{aligned} \tag{6}$$

That is to say, m'_1 equals to the element of W indexed as n_1, m'_2 equals to the element of W indexed as $\mathrm{n}_1+\mathrm{n}_2$ and so on.

5. Decompression: In this step, we decompress M'. Thus, we obtain M, the secret message by only employing the sent URL. Unlike the embedding phase, we neither used the collection, nor performed a selection since the URL provides us the carrier; namely the chosen web page.

III. Experimental Results

In this section, the experimental procedure and the obtained results have been explained. The experiments have been carried out via a software written in C# language. For an unbiased evaluation, secret messages (*M*) have been produced by employing Lorem Ipsum texts (http://www.tr.lipsum.com/feed/html)[16]. Besides, for a wide-range observation, investigation phase has been carried out by considering different lengths of secret messages. Length of each secret message has been incremented 50 by 50 beginning from 50 to 600.

For evaluation, steganographic capacity has been considered in terms of percent. Capacity rate has been calculated for each secret message by using Equation 5. Results of the performed experiments and comparison results

TABLE I
Capacity Values till 600 Characters

n	Secret Message	C(%)
50	Lorem ipsum dolor sit amet, consectetur cras amet.	6.257
100	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam tristique nunc lectus, eu cras amet.	6.464
150	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer consequat eleifend orci sed mollis. Vestibulum lobortis malesuada purus nec volutpat.	7.038
200	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas erat massa, elementum at orci sed, feugiat dignissim urna. Nunc fringilla fermentum tempus. Donec feugiat neque lacus, sit amet metus.	7.532
250	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam gravida et erat ac ornare. Sed lectus dolor, iaculis nec nulla non, feugiat vehicula orci. Vivamus gravida dapibus enim sed elementum. Cum sociis natoque penatibus et magnis dis nullam.	7.727
300	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi tellus turpis, vulputate at bibendum sed, volutpat vitae leo. Phasellus vel nulla at leo accumsan volutpat sed vitae arcu. Ut id aliquam velit, et tristique metus. Sed laoreet ex vitae odio pulvinar ultricies. Ut sit amet augue volutpat.	7.947
350	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec est turpis, dapibus in felis in, euismod molestie ex. Mauris quis sapien in est tincidunt pulvinar quis nec arcu. Aliquam sit amet mattis lorem. Praesent volutpat, sem ac aliquam scelerisque, purus ligula tristique mi, at hendrerit nunc orci sed est. Vestibulum ante ipsum primis in sed.	8.241
400	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam sed vehicula est. Vestibulum dignissim a neque a blandit. Aenean auctor odio sit amet nibh faucibus facilisis. Quisque a tortor hendrerit diam sagittis mattis. Etiam ullamcorper ipsum finibus, pretium justo id, ullamcorper odio. Aliquam dapibus est in tincidunt facilisis. Nulla luctus scelerisque diam, et vulputate elit ultricies amet.	8.398
450	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent quis fringilla leo. Nam ut rhoncus ante. Sed venenatis ut nunc vitae bibendum. Phasellus vel urna ultricies, maximus lectus ut, porttitor metus. Curabitur luctus, mi sed iaculis accumsan, urna mi vestibulum lacus, nec luctus arcu tellus aliquam nisi. In ac finibus quam. Nulla facilisi. Cras hendrerit ante a est rhoncus malesuada. Vivamus eget ultrices augue. Proin at faucibus amet.	8.422
500	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut non tortor tempor, pharetra sapien non, fringilla erat. Sed at eleifend ex, at finibus massa. Etiam quis scelerisque metus. Duis est tellus, imperdiet et lorem sit amet, placerat elementum magna. Proin egestas, libero a varius gravida, est leo porttitor lorem, sit amet imperdiet sapien augue quis eros. Nam sit amet est malesuada, tempor purus eget, euismod ex. Vestibulum eget turpis id ex tempus maximus consectetur eget ante massa nunc.	8.557
550	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi rhoncus eu lacus non convallis. Nunc consectetur congue viverra. Phasellus vitae ligula eu justo sodales venenatis in ac nulla. Ut ornare consequat facilisis. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aliquam in lacinia nunc, vel vehicula lorem. Suspendisse convallis tempor ipsum. Nullam vitae condimentum ex. Etiam magna ipsum, viverra eget velit nec, maximus condimentum lectus. Suspendisse aliquam egestas ligula, nec blandit metus.	8.712
600	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris ac urna eu lorem lobortis malesuada fermentum non enim. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Praesent id lobortis neque. Curabitur a commodo ipsum. Ut porttitor felis felis, eget imperdiet velit efficitur in. Nulla suscipit elit lacus, ac tincidunt turpis pulvinar sed. Nunc ultrices faucibus pulvinar. Pellentesque mattis dui id lorem sodales dapibus. Praesent semper, metus ut suscipit congue, neque orci tempus urna, vitae placerat purus nisl quis augue. Curabitur non volutpat.	8.850

in the literature have been indicated in Table 1, Table 2, respectively.

In Table 1, details about the performed experiments have been presented. Character length (n) of each secret message, the employed secret message produced via Lorem Ipsum and the obtained capacity rate have been provided. Graphical result of the performed experiments has been demonstrated in Figure 3.

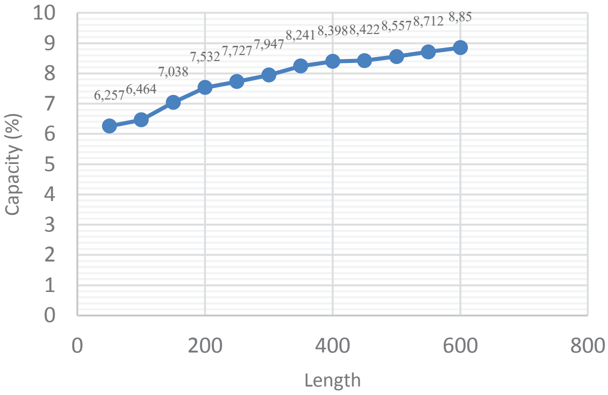

Fig. 3. Graphical result

In the given graph, we can see that there were small swings, but they are negligible. Namely, by basing on Figure 3, we observe that steganographic capacity continued to increase. The obtained maximum capacity value is 8.85% and the corresponding length is 600 characters. By basing on the given graph in Figure 3, we can claim that generally capacity increased as the length increased.

Comparison of the proposed method with the other contemporary methods in the literature has been presented in Table 2, in terms of capacity. Capacity of mimic function method that produces grammatically correct but meaningless texts has been calculated by employing Lorem Ipsum patterns via the given link. Capacities of Nicetext and Listega methods have been provided by basing on the samples in the cited articles. Capacities of translation based, Satir and Isik's schemes have been provided by considering the cited articles and thesis. Finally, capacity of Matlist method has been calculated statistically (averagely) by considering the given values in the cited article since this method is highly subject dependent. As seen in Table 2, the proposed method increased the capacity value to 8.85%. It has been calculated by employing the Lorem Ipsum Patterns via Eq. (5). This is a significant rate when the secret message containing 600 characters is considered.

For instance, the obtained URL for the secret message that has 10 characters, has been given below:

M = (L, o, r, e, m, ,i, p, s, u)

URL:
http://www.selcuk.edu.tr/index.php?id=&NzYyLzExMDYvMjEvMzYvMzYvMzYvMjEvMzYvMzYvMTc2OS8yMS8zNi8zOC8zNi8yMS8zNi8zOC8xNDUvMjEvMzYvMzgvNjk2LzIxLzM2LzM2Lzc2NC8yMS8zNi8zNi82OTYvMjEvMzYvMzYvNzYyLzIxLzM2LzM4LzE0NS8yMS8=

TABLE II
COMPARISON RESULTS

Method	Capacity (%)	Explanation
Mimic functions[4],[5]	1.143	Calculated by employing Lorem Ipsum Patterns (http://www.spammimic.com/)
NICETEXT [6],[17],[18]	0.29	Provided by basing on the samples in the referred articles
Translation based [9]	0.33	Noted in by the authors the referred article
Listega [10]	3.87	Provided by basing on the example in the referred article
Satir and Isik [14]	6.92	Reported in the cited article
Satir and Isik [15]	7.017	Reported in the cited article
Satir and Isik in 2013 [19]	8.15	Reported in the cited thesis
Matlist [11]	8.74	Calculated averagely via the reported values in the referred article since it is subject dependent.
The proposed method	8.85	Calculated by employing Lorem Ipsum Patterns

This URL is the steganographic cover that is sent to the recipient. When the recipient gets this URL, he/she types this on the browser and then he/ she can extract the secret message by applying inverse of the embedding procedure. However, we observed that length of the obtained URL increased, too. This situation can conflict with the imperceptibility issue, since a very long URL address can raises suspicion.

IV. Conclusion

In this study, we proposed an HTML steganography method that employs URL addresses. Here, URL addresses have been used as steganographic cover and the HTML side of the corresponding URL has been used as a platform for camouflaging. Accordingly, it is enough to send only the obtained URL to the recipient.

Experiments have been performed by investigating steganographic capacity and imperceptibility. The capacity value is increased to 8.85% for the secret message containing 600 characters. Besides, it is observed that capacity increased as the character length increased. But it is observed that the length of the obtained URL increased, too. Since very long URL addresses can raise suspicion while communication, the balance between capacity and imperceptibility should be protected. Accordingly, hiding very long secret messages can endanger imperceptibility. For this situation we employed LZW coding. Besides, in case of making the algorithm public, we employed RSA encryption to provide security. Using LZW compression also supports steganographic security since it complicates the extraction procedure. For future studies, we aim to investigate the effects of other encryption-compression combinations to hide longer secret messages and thus, we will be able to render the proposed scheme more functional.

REFERENCES

[1] R. Radhakrishnan, M. Kharrazi, and N. Memon," Data Masking: A new approach for steganography?," *Journal of VLSI Signal Processing* vol. 41, no.3, pp. 293-303, 2005.

[2] A. Desoky, M. Younis, "Chestega: chess steganography methodology," *Security and Communication Networks,* vol. 2, no. 2, pp. 555-566, 2009.

[3] D. Kahn, *The Codebreakers: The Story of Secret Writing*, Revised ed., Scribner, New York, 1996.

[4] P. Wayner, "Mimic Functions," *Cryptologia*, vol. 16, no. 3, pp. 193-214, 1992.

[5] P. Wayner, *Disappearing Cryptography (2nd edn*). San Francisco, California, USA: Morgan Kaufmann, 2002, pp. 81-128.

[6] M. Chapman, G. Davida, "Hiding the Hidden: A Software System for Concealing Ciphertext as Innocuous Text," in *Proc. International Conference on Information and Communications Security, Lecture Notes in Computer Science,* vol. 1334, Springer, Beijing, P.R. China, 1997, pp. 335-345.

[7] C. Grothoff, K. Grothoff, L. Alkhutova, R. Stutsman, and M. Atallah, "Translation-based steganography," *CERIAS Tech Report 2005-39,* West Lafayette, IN: Purdue University, 2005.

[8] C. Grothoff, K. Grothoff, L. Alkhutova, R. Stutsman, and M. Atallah, "Translation-based steganography," In *Proc. Information Hiding Workshop (IH 2005)*, Barcelona, Spain: Springer-Verlag, June 2005, pp. 213-233.

[9] R. Stutsman, C. Grothoff, M. Atallah, and K. Grothoff, "Lost in Just the Translation," In *Proc. The 21st Annual ACM Symposium on Applied Computing (SAC'06),* Dijon, France, April 2006, pp. 338-345.

[10] A. Desoky, "Listega: list-based steganography methodology," *International Journal of Information Security,* vol. 8, no. 4, pp. 247-261, 2009.

[11] A. Desoky, "Matlist: Mature linguistic steganography methodology," *Security and Communication Networks,* vol. 4, no. 6, pp. 697-718, 2010.

[12] B. Ryabko, D. Ryabko, "Constructing perfect steganographic systems," *Information and Computation,* vol. 209, no. 9, pp. 1223-1230, 2011.

[13] K. Bailey, K. Curran, "An evaluation of image based steganography methods using visual inspection and automated detection techniques," *Multimedia Tools and Applications*, vol. 31, no. 3, p. 327, 2006.

[14] E. Satir, H. Isik, "A compression-based text steganography method," *The Journal of Systems and Software*, vol. 85, no. 10, pp. 2385-2394, 2012.

[15] E. Satir, H. Isik, "A Huffman compression based text steganography method," *Multimedia Tools and Applications*, vol. 70, no. 3, pp. 2085-2110, 2014.

[16] (2014, Jul. 29) [Online].
http://www.tr.lipsum.com/feed/html

[17] M. Chapman, G. I. Davida, and M. Rennhard, "A practical and effective approach to largescale automated linguistic steganography," in *Proc. Information Security Conference (ISC'01), Lecture Notes in Computer Science,* vol. 2200, Springer, Malaga, 2001, pp. 156-165.

[18] M. Chapman, G. I. Davida, "Plausible deniability using automated linguistic steganography," in *Proc. International Conference on Infrastructure Security (InfraSec'02), Lecture Notes in Computer Science,* vol. 2437, Springer-Verlag, Berlin, 2002, pp. 276-287.

[19] E. Satir, "Bilgi Güvenligi Icin Metin Steganografisinde Yeni Bir Yaklasim," Ph.D. dissertation, Dept. Computer Eng., Selcuk Univ., Konya, Turkey, 2013.

E. Satir was born in Konya/Turkey 1983. She completed her undergraduate degree in Gazi University, Technical Education Faculty, Computer and Electronic Education Department, in 2005. She completed her graduate degree in Selcuk University, Technical Education Faculty, Computer and Electronic Education Department, in 2009. her doctorate degree in Selcuk University, Faculty of Engineering, Computer Engineering Department in 2013. Currently, she is working as an assistant professor in Duzce University, Faculty of Engineering, Computer Engineering Department.

A. Sargin was born in Konya/Turkey 1990. He completed her undergraduate degree in Selcuk University, Technical Education Faculty, Computer and Electronic Education Department, in 2013. Currently, He is working as a teacher in Karakopru Middle School in Sanliurfa.

T. Kanat was born in Nigde/Turkey 1991. He completed her undergraduate degree in Selcuk University, Technical Education Faculty, Computer and Electronic Education Department, in 2013. Currently, He is working as a teacher in Konya.

C. Okuducu was born in Karaman/Turkey 1991. He completed her undergraduate degree in Selcuk University, Technical Education Faculty, Computer and Electronic Education Department, in 2013. Currently, He is working as a teacher in Goger Middle School in Diyarbakir.