A PROPOSED TEXT STEGANOGRAPHY METHOD TO ENHANCE E-GOVERNMENT SECURITY SYSTEMS

Wasan Alaa Alhamami Mohammad Reza Ahmadi

kashan University

Mohanned_almashat@yahoo.com

Abstract- **Electronic Government refers to the provision of the information and the services or the local government through the Internet or other digital means to the citizens, the companies or other government agencies. One of the main concepts in E-government is how to protect the contents of its systems and provide security to these systems. Steganography and Cryptography technologies are the most common ways to send vital information in a confidential manner. Steganography is used to hide the existences of the letter and Cryptography distorts the message itself. In this paper a proposed text steganography method is presented in order to use it with e-government systems. Non printed characters (isolation and connection characters) are used to embed the secret text bits with the cover text message. Since the non-printed characters are not appearing so the proposed method keeps the cover text similarity 100%.**

Keywords: Steganography; Cryptography; E-Government; Text Stego; Cover.

I. INTRODUCTION

Electronic Government is used to simplify the provision of relevant government information in electronic form to the citizens in a timely manner, improving the provision of services to citizens, empowering people through the access to the information without the bureaucracy, improve the productivity and cost savings in doing business with suppliers and customers in the government, and participation in decision making on public policy [1].

The more important concept in an era of fast development today is the data and information security with the fast growth of the computer networks and the advances in the technology which leads to the exchange of a large amount of information. Security has become the critical feature of the networks capability. The communications are not safe because the presence of some malicious utilizers who are waiting for the opportunity in order to get the accessing to the confidential data [2]. Encryption is aware of keeping the transmitted data safe [3]. The encryption process is applied before the sending and the application of the decryption is after the receipt of the encrypted data. Steganography is aware of writing letters hidden within the different digital content; it transfers data through hide it inside of another, such as picture or sound that the so-called cover object [4]. Cryptography encrypts the message and sends it; anyone can view the encrypted message, but it is very not easy to understand it. Steganography hides the existence of the secrete message by embedding it in a cover object [5].

In this paper a proposed text steganography method for the E-government security systems is presented. The paper arrangement as follow: section 2 presents the related work, section 3 presents the run length encoding method, section 4 presents the proposed method; section 5 presents the experimental result of the proposed method, section 6 presents the evaluation of the proposed method and section 7 presents the conclusion of the proposed method.

II. Related work

The following is a study of the works that have been done on the hide information or texts concealment [6].

A. Text Steganography in Markup Languages

In [7] they utilize one of the characteristic of the languages which based on the layouts in order to hide the information. The main characteristic of the HTML documents is their tags case insensitivity. For instance, the tag
 can be also utilized as
 and
. As a result text steganography can be applied to the HTML documents by making the changing to the lower or the upper case of the letters in the document tags. In some cases the positions of the tags are also utilized for the text steganography. For instance <B><U> </B></U> or like this <U><B> </U></B>. In order to extract the information in the first method of text steganography by comparing these words with words in normal case and in second case by comparing the tags positions. However these methods are not suitable for all the markup languages like in the WML because all the tags are case sensitive.

B. Text Steganography in Specific Characters in Words.

In [8] they identify some of the specific characters of certain words. For instance, choosing the first word of each paragraph is done in a manner during the first letters of the words side by side, as a result, extraction is confidential information or hidden. This technique requires strong mental force along with long time and requires a special text because not every type of the texts can be utilized in this method.

C. *New Text Steganography Technique by using Mixed-Case Font*

In [9] they utilize the wildcard file of the casing and not the distance between the words or the paragraphs, the non-utilize of the additions. In the proposed method the message can be hidden in just 7 characters and not 7 words and utilizing the distance between words. Therefore, it is a large amount of data compared with other methods of the preserving the exact meaning of the text in order to make it looks like these cool fonts.

III. RUN LENGTH ENCODING

Run-Length Encoding (RLE) is a very easy form of the data compression in which runs of data (which are, sequences in which the same data value occurs in many consecutive data elements) are stored as a single data value and the count of these runs rather than storing as the original run. This is the most helpful on data which contains many such runs: for instance, simple graphic images such as icons, line drawings, and animations but it is not helpful with the files that don't have many runs because it will greatly increase the size of file. RLE may also be utilized to refer to the early graphics file format supported by CompuServe for compressing the black and the white images, but was commonly supplanted by their later Graphics Interchange Format [10].

Let’s consider a single line of the pixels with B representing a black pixel and W representing white: WWWWWBWWWWWWBBBWWWWWBWWWWW.

If the Run-Length Encoding (RLE) data compression algorithm is applied to the above pixel line, the following sequence will be the result: 5W1B5W3B5W1B5W this is to be interpreted as five Ws, one B, five Ws and so on [11].

IV. THE PROPOSED HIDING METHOD

In the proposed method both the secret message and the cover message are in Arabic. The connection and isolation features of the Arabic letters are employed in order to hide the secret binary bits in the cover text message in a way that keeps the similarity of the cover message 100%. This will avoid the cover message from the attacker attempts to retrieve the secret message. In the proposed Method the run length encoding is used to reduce the number of the secret binary bits before embedding it in the cover text. Algorithm (1) shows the proposed method (embedding case) and Algorithm (2) shows the proposed method (extraction case).

Algorithm (1) : The proposed Embedding Method
Input: Secret text, virtual cover text.
Output: Stego text.
Begin Step1: Read Arabic text. Step1: Convert Secret text characters to English letters. Step2: Read English letters. Step3: Convert English letters to ASCII values. Step4: Convert ASCII values to binary representation. Step5: Apply Run Length Encoding. Step6: while it is not the end of the run length encoding result 6.1: Cut one counter 6.1.1: Swap it with the corresponding connection or isolation Characters. 6.2: Cut run characters(which is may be 0 or 1) 6.2.1: If the character is “0” then the merging character is isolation character (157 ASCII value). 6.2.2: If the character is “1” then the merging character is connection character (158 ASCII value). 6.3: Store the swap result in the virtual text. 6.4: Get Stego_text (virtual cover text after embedding.) Step7: Loop. Step8: End while. Step10: End.

Algorithm (2): The proposed Extracting Method
Input: Stego text
Output: secret text.
Begin Step1: For each stego text. Step2: Read stego text. Step3: While it is not the end of the stego text. 3.1: Cut 4 characters. 3.2: Swap it with corresponding decimal values. 3.3: Store the result in L. 3.4: Cut another character (run character) and swap it with corresponding run character (if isolation character it is mean ‘0’ runs otherwise it is meaning ‘1’ runs. 3.3: Store the result in L. 3.4: Loop. 3.5: End while. Step4: Apply run length decoding into the L to get binary representation. Step5: Convert binary representation to ASCII values. Step6: Convert ASCII values to English letters.

Step7: Swap English letter
Step8: Read the database.
Step9: End.

V. IMPLEMENTATION OF THE PROPOSED METHOD

The implementation of the proposed method can be illustrated as in the following steps and figures. Figure (1) shows the proposed hiding method interface.

Figure (1): The proposed hiding method interface.

Step 1: Read the secret text which wants to be hided, Figure (2) shows the reading of the secret text.

Figure (2): The reading of the secret text.

Step 2: Application of the Hiding to the secret text, Figure (3) shows the application of the hiding steps.

Figure (3): Application of the hiding steps

Step 3: After that in order to extract the secret text the virtual text (stego text) need to be read as shown in Figure (4).

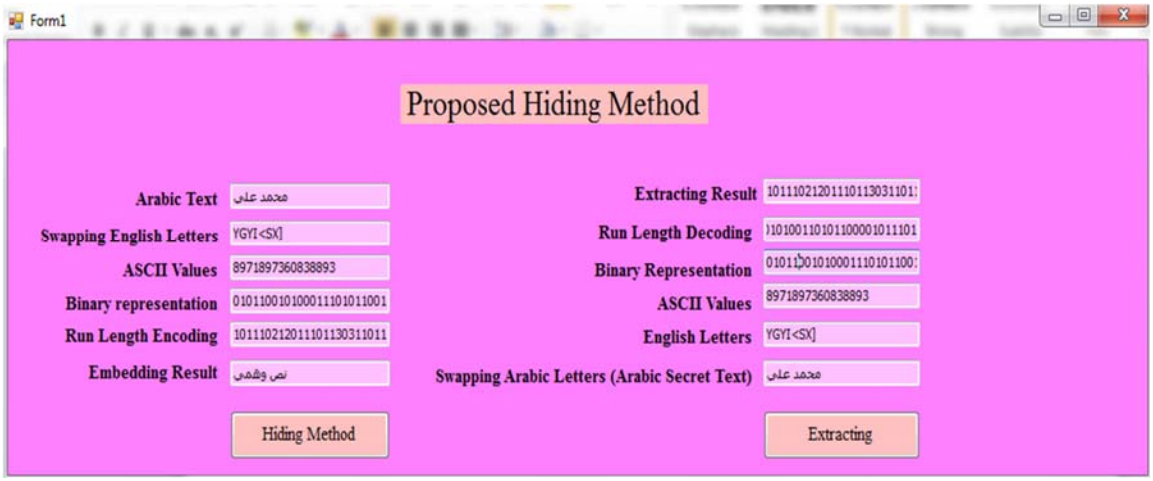

Figure (4): Extracting Process

VI. THE RESULT OF THE PROPOSED HIDING METHOD

As shown in the proposed hiding method implementation, the similarity is 100% which means that the attacker will not try to attack it. The main reason for providing this complete similarity is the using of non-printed characters (isolation character and connection character) which are used with the Arabic letters. The capacity (which is one of the hiding method measures) is good since RLE is used with these non-printed characters. Another measure of the efficiency of the hiding method is the difference; in this proposed method is 0.

VII. CONCLUSIONS

Based on the implementation of the proposed method results, the following points can be concluded:

1) 100 % similarity between the cover text and the stego text.
2) 0 difference snice no changes will be made to the form of the cover text.
3) Good capacity since the run length encoding method will be used in order to reduce the number of the secret text bits before the embedding.

References

[1] Palvia, S. C., Sharma, S., "E-Government and E-Governance: Definitions/Domain Framework and Status around the World ", (2007). Hyderabad, India: IECG.

[2] Richa D., Apurva S., Sunita G." An Innovative Data Security Techniques Using Cryptography and Steganographic Techniques", Richa Dubey et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2175-2182.

[3] Obaida M., Al-Hazaimeh A., (2013) "A New Approach for Complex Encrypting and Decrypting Data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2.

[4] Katzenbeisserc S., and Petitcolas, F.A.P. 2000, Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Boston, London.

[5] Saleh S." A Secure Data Communication System Using Cryptography And Steganography", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.

[6] Jibran A., Kamran K., Hameedullah K.," Evaluation Of Steganography For Urdu /Arabic Text.", Journal of Theoretical and Applied Information Technology.

[7] K. Bennett, "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text", Purdue University, CERIAS Tech. Report 2004-13.

[8] T. Moerland, "Steganography and Steganalysis", May 15,2003,www.liacs.nl/home/tmoerlan/privtech.pdf, last visited: 1 May 2006.

[9] Abdelmgeid A., Al - Hussein S.," New Text Steganography Technique by using Mixed-Case Font", International Journal of Computer Applications (0975 – 8887) Volume 62– No.3, January 2013.

[10] M.Vidya, J.S. Rose," Modified Run Length Encoding Scheme for High Data Compression Rate", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 12, December 2013.

[11] Mohammad H., "A Survey of Data Compression Algorithms and their Applications", Conference Paper · January 2012.

[12] Al-Hamami A. H, and Al-Hamami M.A., "Information Hiding and Watermarks", (in Arabic) Ithraa Publishing and Distribution, Amman, Jordan, 2007.

[13] Al-Hamami, A.H & Raghad Abdul-Aali, "Using natural features of letters in Text Information Hiding" Second Conference on Information Hiding, Al-Rafidain Magazine, No.10, 2003, Baghdad, Iraq.

[14] Al-Hamami, A.H & Nedhal Khoudair Abbas, "Cover Optimization for Image Steganography." Information Hiding Conference, Al-Rafidain Magazine, No. 9, PP: 68-88, 2002, Al-Rafidain University College, Baghdad, Iraq.