Asian Journal of Information Technology 15 (16): 2770-2774, 2016
ISSN: 1682-3915

Dynamic Steganography of Internet Web Pages

Rusul Amer and Wesam Bhaya
IT College, University of Babylon, Babil, Iraq

Abstract: Sending encrypted messages frequently will take the interest of intruders, maybe occur attempts to infringe and detection the secret information. Information hiding is introduce to conceal the presence of the contact via hiding a mystery message within other unsuspicious message. In this study, researcher will work with data hiding techniques in (text, image and HTML tags) of internet web pages. In particular, researcher will propose an idea of using three Steganography techniques to hide secret information in (text, image and HTML tags) of web pages dynamically. In this study, the web page will be analyzed to check the size of different contents of webpages (text, images and HTML tags). Then, researcher will hide secret data in one or more contents of web pages depend on capacity of web page contents and information which want to be hide. The propose technique characterized by highly capacity since we can hide more data when hiding in text, tags and images. Other parameters like robustness and detect-ability the propose system was considered. Fromsecurity point of view, the attackers cannot discover the concealed data of proposed techniques.

Key words: Information hiding, steganography, webpages steganography, HTML tags, concealed

INTRODUCTION

Information hiding is a scienceof concealing mystery information at digital encasement like (audio, pictures or video files), where difficult for the normal viewer to know the presence of a hiddendata in it. Information hiding is the general address to two kinds from techniques, the first kind used forsecretdatum of viewers and enemies (steganography). The second kind is used for indulgence the ideational property rights which called (Digital Watermarking). Figure 1 shows Classification of Information Hiding (Por and Delina, 2008).

Steganography is a domain from science to conceal information via inclusion a letter at another material. It is an old art from conceal information in ways a message is conceal in an innocent-appearance coverage means for this reason will not provoke an eavesdropper's notice. Steganography confirms possibility of send mystery message, during utilization of available contact means, until under conditions that are monitored. There are the option of send messages in which no one can sense the presence of mystery messages.

The hiding is done via fold some features of other media (images, texts, tags) which is called the covering. last output has equal characteristics to covering means, the covering contain the mystery message, when mystery message inside a covering image it will outcome is a steganography-image and when the mystery message inside a video will the outcome is a steganography-video and so on. Two algorithms are needed to designing steganography system, one to concealing data and other to extracts the data. Figure 2 shows general steganography view (Kumar and Pooja, 2010).

The basic terms used in the Steganography are: the secret message, cover message, the secret key and embedding process (Seidan, 2013). The covered message is the carrier of the message such as video, Image, Audio, Text, or some other digital means. The secret message is the data which is needed to be concealing in the digital means. The mystery key is generally used to embed the message depending on the concealing processes. The embedding process is the way that generally used to embed the mystery data in the cover message.

Classification of steganography: The steganography techniques can be classify according to media which can hide into it. Figure 3 exhibit steganography types.

Text steganography: Text is one of the olden means use in steganography. Text steganography propose to the established the data inwards the texts. Exist several ways to concealing data inside a text file, same like word-shift coding, line-shift coding and feature coding, Text data files like (txt, Doc, Xml and Html). Concealing information using abbreviation and space has very a few ability of including mystery information, The space steganography which is founded as well as extra white-space (such as spaces or taps) has low robustness because some electronic text editors can omit extra white-spaces automatically.

Corresponding Author: Rusul Amer, IT College, University of Babylon, Babil, Iraq

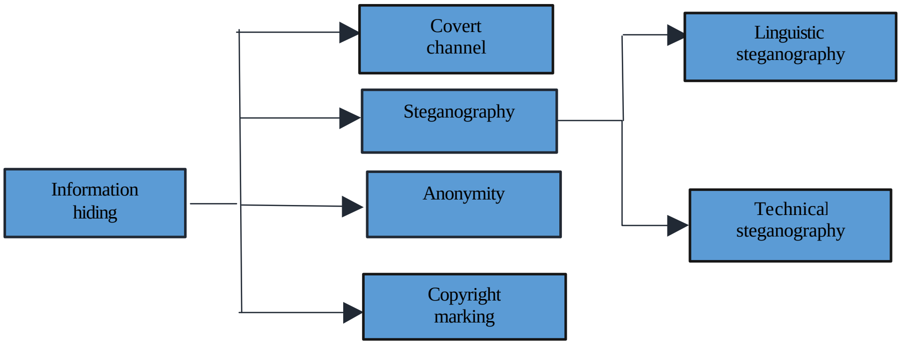


Fig. 1: Information hiding classification

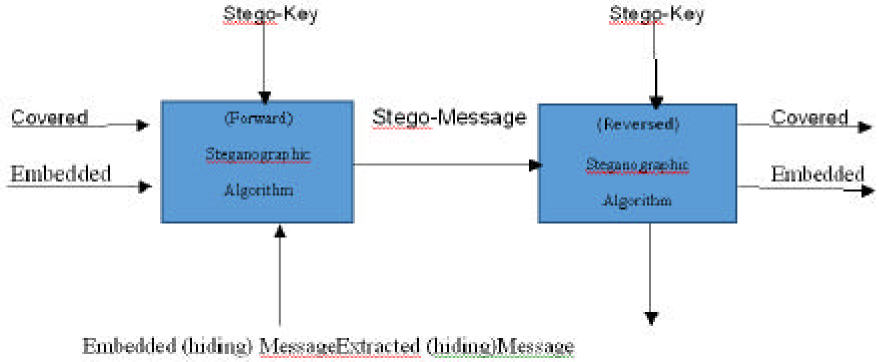


Fig. 2: Steganography system

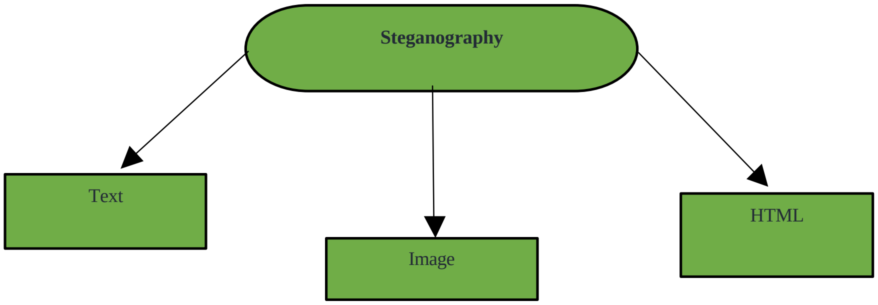


Fig. 3: Steganography type

Image steganography: The image steganography is used to conceal a secret message in an image data. The most used manner to hiding secret bit inside the image is Least Significant Bit (LSB). Thismanner uses bits of each pixel in the image. The conceal information will bring missing in the transmutation of a lossy pressure algorithm. When using a 24 bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel in this way we can use more secret bit to hide data in it.

HTML steganography: HTML or hypertext markup language is the basic programming language for web page which can be common with another languages such as Macromedia Flash and Java Script. HTML is used to make the static portion of webpages. HTML code include from two parts:“tag” which is surrounded by nook parentheses (<>) and the information between tags. Internet browsers only offer the content without tags, since tags control the look of the HTML files.

MATERIALS AND METHODS

Characteristics of steganography: Steganography techniques embedding messages within a covering. Several characteristics describe the force and frailty the of the method:

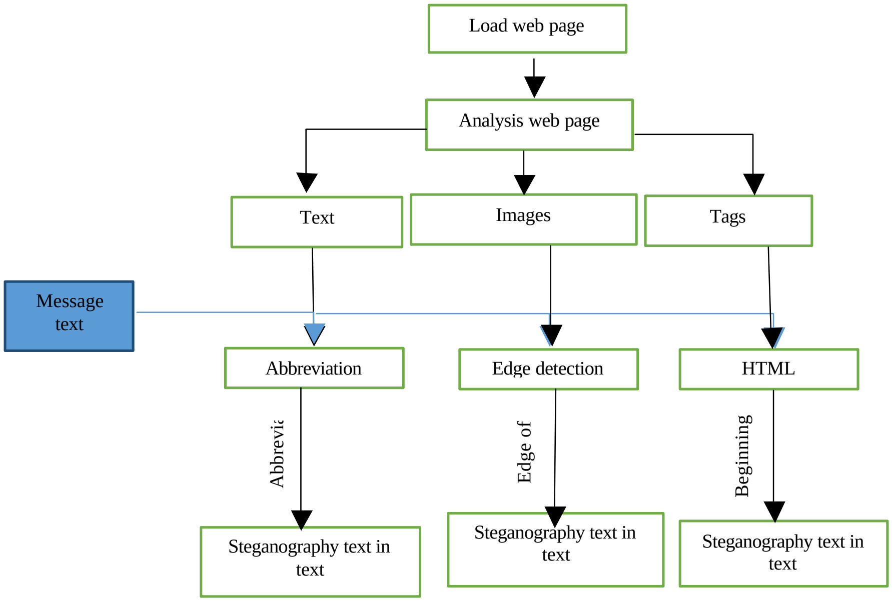


Fig. 4: General view of proposal web pages steganography

Capacity: The concept capacity at information concealing, refers to the sum numbers of bits concealing and successfully recovered via the Steganography method.

Robustness: This is a measure from the capacity the algorithmsfor keep the information embedding in the covering even after the covering has been subject for several changes as an outcome frompressure and some kind of processing like conversion to analog and back to digital. Robustness is especially serious when the conceal data include of copyright or ownership information (the so-called Watermark). A user may compress such an image with a lossy compression method, then decompress it in an attempt to destroy any hidden watermarks.

Undetectable: An attackers probably capable for reveal the existence of conceal information at a specific file by computing some statistical properties of the file and comparing them to what is expected in that kind of file. A good stenography method must not shift the statistical features of the cover file.

Invisibility (Perceptual Transparency): This notion is based on features of the individual visible system. The embedding information is imperceptible if an average individualtopic is incapable to distinguish between carriers that do include hiding information and those that do not.

Security: It is said that the embedded algorithms is safety if the embedding data is not topic for elimination by the attacker.

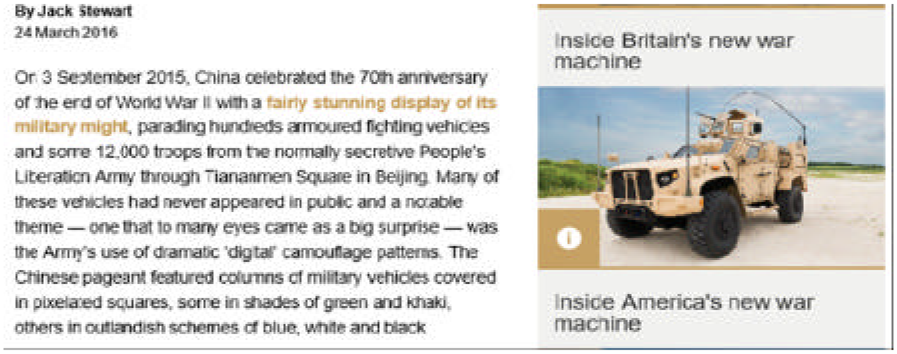
Proposed web pages steganography: We will research on analysis the web pages and checkthe contents ofthose webpages which have more percentage of text, tags and images. If the percentage of text content is high, we will use propose technique to hiding in a text or tags, elsewhere the content of image will usedto hide in it. Figure 4 shows main idea of proposal (Kumar and Pooja, 2010).

RESULTS AND DISCUSSION

Analysis web page: After analysis web page and finding the text is more in web page and secret message can be hide in it, text in text hiding must be done. Figure 5 shows Internet web page which have text.

Proposehiding text in text: Before hiding process in text, we will reduce size of secret databy using abbreviation technique. Researchers will hiding data in cover text by matching acharacters of secret text with cover text and record the sequence of matching character to produce sequence matrix as stego-key. Figure 6 shows abbreviation technique (Petter, 1992).

Propose hiding text in image: Before hiding in image, we will convert the secret text tobinary. After that researchers



By Jack Stewart
24 March 2016

On 3 September 2015, China celebrated the 70th anniversary of the end of World War II with a fairly stunning display of its military might, parading hundreds armoured fighting vehicles and some 12,000 troops from the normally secretive People's Liberation Army through Tiananmen Square in Beijing. Many of these vehicles had never appeared in public and a notable theme — one that to many eyes came as a big surprise — was the Army's use of dramatic 'digital' camouflage patterns. The Chinese pageant featured columns of military vehicles covered in pixelated squares, some in shades of green and khaki, others in outlandish schemes of blue, white and black

Inside Britain's new war machine

Inside America's new war machine

Fig. 5: Web page of text

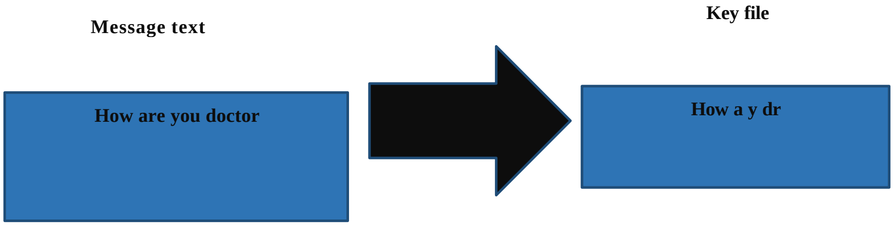


Fig. 6: Example of abbreviation technique

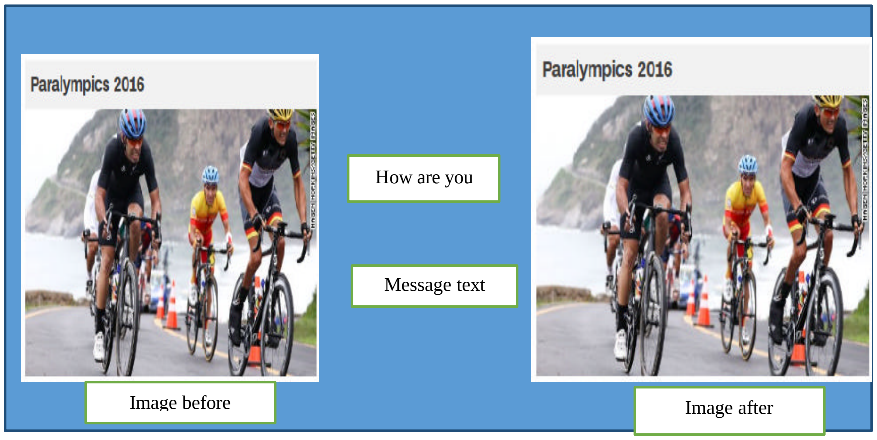
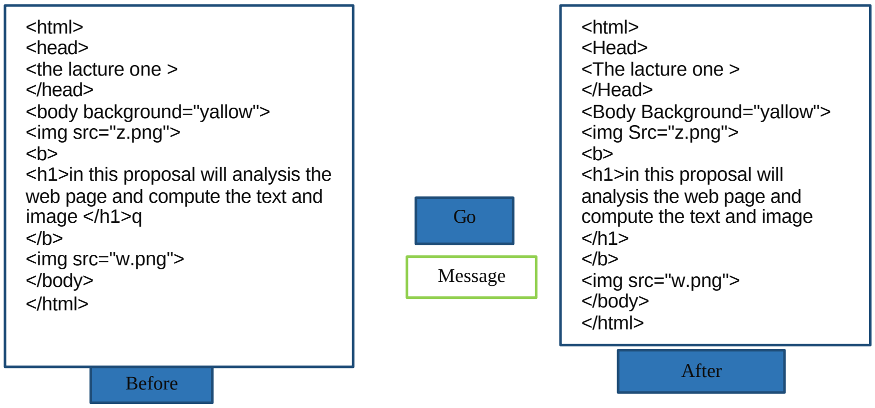


Fig. 7: Text in image steganography



```
<html>
<head>
<the lacture one >
</head>
<body background="yellow">
<img src="z.png">
<b>
<h1>in this proposal will analysis the
web page and compute the text and
image </h1>q
</b>
<img src="w.png">
</body>
</html>
```

```
<html>
<Head>
<The lacture one >
</Head>
<Body Background="yellow">
<img Src="z.png">
<b>
<h1>in this proposal will
analysis the web page and
compute the text and image
</h1>
</b>
<img src="w.png">
</body>
</html>
```

Fig. 8: Example text in tags steganography

will conceal the secret bits in cover image through generate edge frame similar to edge of original image changed by +1 or -1 according to hidden bit of 1 or 0. Figure 7 shows propose web page text in image steganography (Rani and Chaudhary, 2013).

Propose hiding text in HTML tags: Before hiding process, we will hiding text in tags of the webpage through convert the secret text to binary (1) and (0). After that, we will check whether 0 or 1. If (1) made the first letter of tag uppercase letter while (0) made the first letter is lowercase. Figure 8 showspropose text in tags steganography (Dhanani, 2014).

CONCLUSION

This study introduce proposesteganography techniques for Internet web pages. Each of these techniques attempting to satisfy the three most main features of steganography (capacity, detectability and robustness) for hiding secret information in webpages.

It has been tested few Web Pages with different sizes of text to be hidden andwe found that the resulting stego webs do not have any noticeable changes. In addition, we found that for all Web Pages, the propos altechniques work efficiently. Thus, those new steganography approachesare robust and efficient for hiding.

REFERENCES

Dhanani, C., 2014. HTML steganography using relative links and multi web-page embedment. Int. J. Eng. Dev. Res., 2: 1960-1965.

Kumar, A. and K. Pooja, 2010. Steganography-A data hiding technique. Int. J. Comput. Appl., 9: 19-23.

Por, L.Y. and B. Delina, 2008. Information hiding: A new approach in text steganography. Proceeding of the 7th WSEAS International Conference on Mathematics and Computers in Science and Engineering, April 6-8, 2008, World Scientific and Engineering Academy and Society, Hangzhou, China, ISBN:978-960-6766-49-7, pp: 689-695.

Rani, N. and J. Chaudhary, 2013. Text steganography techniques: A review. Int. J. Eng. Trends Technol., 4: 3014-3015.

Seidan, Y.A.H., 2013. Enhancement of a steganographic algorithm for hiding text messages in images. Ph.D Thesis, Middle East University, Beirut, Lebanon.