Design for Scientific RENAISSANCE

JASER

A New Technique of Text Steganography Based on Novel Numbering System

Article Info

Received: 20/10/2016
Accepted:20/11/ 2016
Published online: 1/12/2016

Ahmed F. Albaghdadi[1a], Mustafa F. Albaghdadi[2b], Wael Jabbar Al-nidawi[3c]

Almustaqbal University college [1,3], University of Babylon IT College [2],

Ahmedfa91m@gmail.com[a], Redarrowd@gmail.com[b],
dr.waelalnidawi@gmail.com[c]

ISSN 2231-8844

Abstract

Steganography is the art of hiding information in other information in order to hiding the fact that communication is taking place. There are different types of steganography but text are the most popular because of their frequency on the Internet. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. In this paper, a new method of text steganography was applied to embed information in text by Create a new numbering system based on five characters. As which known there are five characters in ASCII table have a null size unlike other known characters which are (0129, 0141, 0143, 0144 and 0157). Anyone can test them by press a (long ALT+ Number). The proposed system can be illustrated by five steps. In the first step the user have to insert a secret message that he want to hide it and a cover message. The second step include encrypt a secret message to base64 in order to avoid unexpected symbols. The third step include convert each character in base64 to the new numbering system in order to get a three hidden character corresponding to each base64 char. The fourth step include put all the three char gropes among the words of cover text.

Keywords: **Steganography, Numbering system, Hidden characters, Hide information.**

1. Introduction

Due to the large use of internet, it is necessary to develop the security of important txt messages by proportional manner with widespread. Cryptography was created as a technique for securing the secrecy of communication and many different ways have been developed to encrypt and decrypt data in order to save the message. But it is sometimes not enough to keep the information secret, it may also be necessary to keep the existence of the message secret. This technique called steganography. Steganography is the science of invisible communication. This is implemented through hiding information in other information, thus hiding the existence of the communication. The word steganography is derived from the

Greek words “stegos” meaning “cover” and “grafia” meaning “writing” (Moerland,2003). In digital image steganography the data is hidden exclusively in images. The idea of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histories, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave’s scalp. When the slave’s hair grew back the slave was dispatched with the hidden message (Silman, 2011). there is a different between Steganography and cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret (Wang & Wang, 2004). Steganography and Cryptography are both ways to protect information of message from unwanted parties. Network socket is an endpoint of an inter process communication across a computer network of between programing electronic devices. A socket address is the combination of a port number and IP address; much like one end of a telephone connection is the combination of a phone number and a particular extension. Based on this address, internet sockets deliver incoming data packets to the appropriate application process

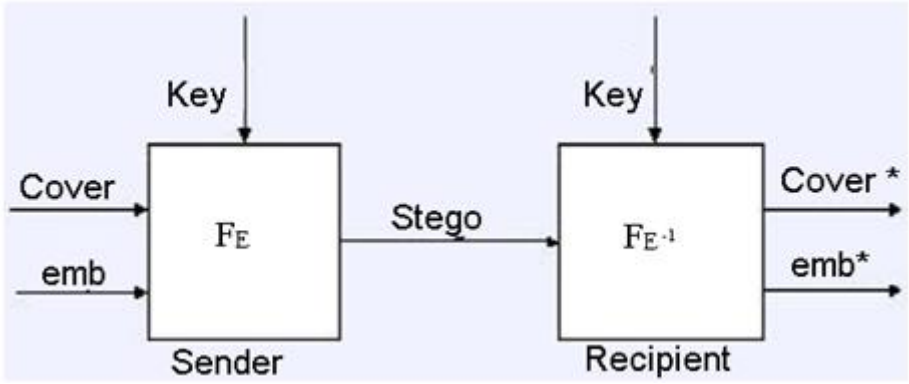

Figure 1 Graphical Version of the Steganographic System

fE : steganographic function "embedding"
fE-1 : steganographic function "extracting"
cover: cover data in which emb will be hidden
emb: message to be hidden
stego: cover data with the hidden message

2. Steganography concepts

Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner’s problem proposed by Simmons (Bandyopadhyay, 2014), where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication (Chandramouli, 2003). The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will

try to alter the communication with the suspected hidden information deliberately, in order to remove the information (Anderson & Petitcolas, 1998). There are four type of steganography as shown in figure 2 which are text steganography, image steganography, sound steganography and protocol steganography. The proposed system in this paper uses a text steganography.

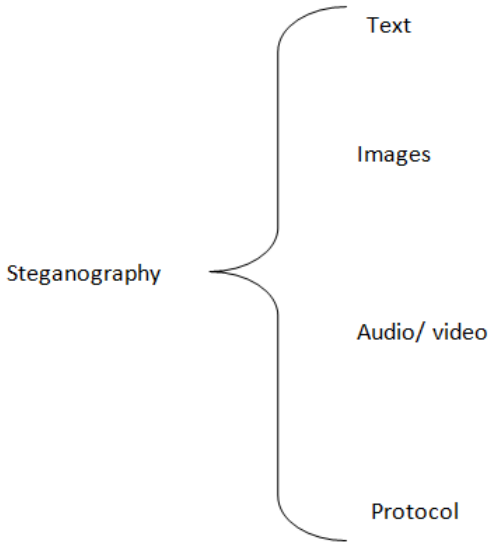

Figure 2: Kind of steganography

3. Uses of Steganography

Steganography can be a solution which makes it possible to send news and information without fear of the messages being intercepted and traced back to us. It is also possible use steganography to store information on a location. For example, some military secrets, can be stored in a cover source. When we are required to unhide the secret information, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside. Paired with existing communication methods, steganography can be used make hidden exchanges like Governments communications: those that support national security. Digital steganography provides vast potential. Businesses may have similar concerns regarding trade secrets or new product information. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them. The idea of using steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites.

4. Proposed system

The most important purpose of this proposed system is to increase the security of a message by using new technique based on new numbering system. This numbering system based on five hidden characters. Any information and be represented by these five hidden characters by convert it to base64 at first in order to avoided the unexpected symbols. The VB.NET 2015 is used to program this application shown in figure 3.

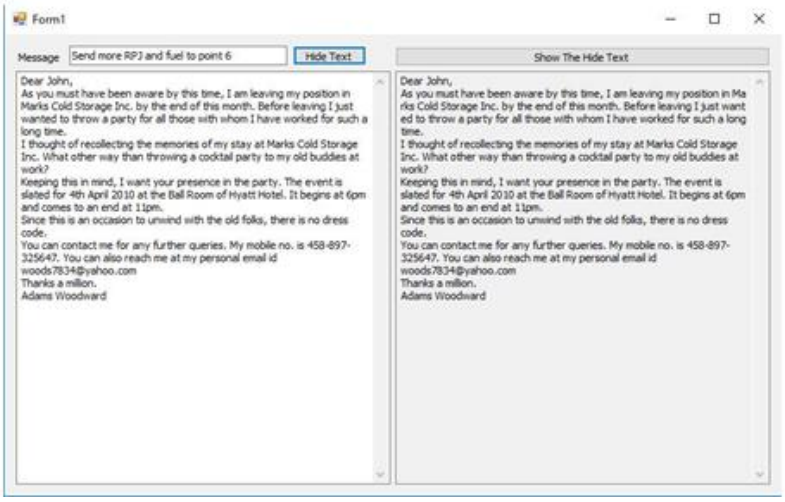

Figure 3 Hide message in cover

As its clear from the figure above in the left hand there are a secret message and cover message. In the other hand on the right, the new text that includes the secret message and cover message together. However, its lock like cover message exactly because the secret message is saved in the spaced among the words of cover message according the following flowchart in figure 4.

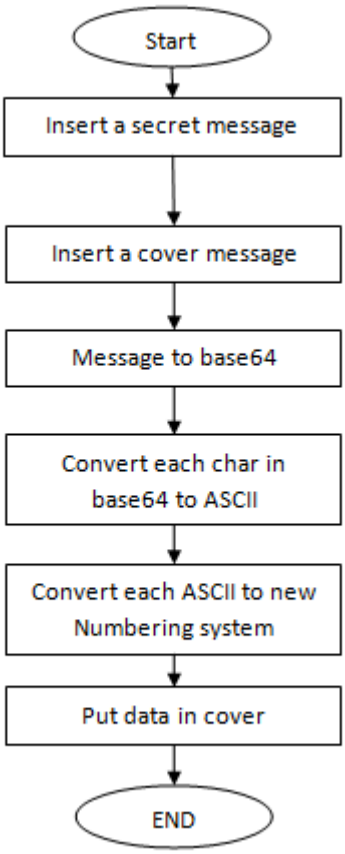

Figure 4 Flowchart operation

The proposed system can be illustrated by five steps. In the first step the user have to insert a secret message that he want to hide it and a cover message. The second step include encrypt a secret message to base64 in order to avoid unexpected symbols. The third step include convert each character in base64 to the new numbering system in order to get a three hidden character corresponding to each base64 char. The fourth step include put all the three char gropes among the words of cover text. The code bellow explain the main part of text steganography based on new numbering system

```
Private Sub HideBtn_Click(sender As Object, e As EventArgs) Handles HideBtn.Click
    Dim words() As String = Split(Covertxt.Text, Space(1))
    Dim Message As String = Convert.ToBase64String(System.Text.Encoding.UTF8.GetBytes(Messagetxt.Text))
    Resulttxt.Text = String.Empty
    If words.Length >= Message.Length Then
        For i As Integer = 0 To words.Length - 1
            If i < Message.Length Then
                Resulttxt.AppendText(words(i))
                Resulttxt.AppendText(IntToString(AscW(Message(i)), ChrW(0129) & ChrW(0141) _
                                    & ChrW(0143) & ChrW(0144) & ChrW(0157)))
                Resulttxt.AppendText(ChrW(0160))
            Else
                Resulttxt.AppendText(words(i))
                Resulttxt.AppendText(Space(1))
            End If
        Next
    Else
        MessageBox.Show("Cover words shoud be larger or equal  message char Length ")
    End If
End Sub
Public Function IntToString(value As Integer, baseChars As String) As String
    Dim result As String = String.Empty
    Dim targetBase As Integer = baseChars.Length
    Do While value > 0
        result += baseChars(value Mod targetBase)
        value = value \ targetBase
    Loop
    Return result
End Function
```

In the other hand we have to inverse the steps above in order to get the information from the cover. The VB.NET2015 is used to program this code bellow

```
Private Sub ShowBtn_Click(sender As Object, e As EventArgs) Handles ShowBtn.Click
    Dim words() As String = Split(Covertxt.Text.Replace(vbNewLine, Nothing), ChrW(0160))
    Dim Result As String = String.Empty
    Dim c As Integer
    For i As Integer = 0 To words.Length - 2
        c = StringToInt(words(i)(words(i).Length - 3) & words(i)(words(i).Length - 2) _
                & words(i)(words(i).Length - 1), ChrW(0129) & ChrW(0141) & ChrW(0143) _
                & ChrW(0144) & ChrW(0157))
        Result += ChrW(c)
    Next
    Resulttxt.Text = System.Text.Encoding.UTF8.GetString(Convert.FromBase64String(Result))
End Sub
Public Function StringToInt(ByVal value As String, ByVal baseChars As String) As String
    Dim result As Integer
    Dim targetBase As Integer = baseChars.Length
    Dim i As Integer
    For i = 0 To value.Length - 1
        result += Val((targetBase ^ i) * Array.IndexOf(baseChars.ToCharArray, value(i)))
    Next
    Return result
End Function
```

5. Conclusion

- Using steganography to hide text information is applicable and provide another level of security.
- Using the new numbering system increase the ability to hide the message without any change of cover message.
- Base64 coding is very useful to avoid any unexpected symbol.

- The number of letters in the secret message must be equal or less than the number of words in cover message.

References

Anderson, R. J., & Petitcolas, F. A. (1998). On the limits of steganography. *IEEE Journal on selected areas in communications*, *16*(4), 474-481.

Bandyopadhyay, D., Dasgupta, K., Mandal, J. K., & Dutta, P. (2014). A novel secure image steganography method based on Chaos theory in spatial domain. *International Journal of Security, Privacy and Trust Management (IJSPTM)*, *3*(1), 11-22.

Chandramouli, R., Kharrazi, M., & Memon, N. (2003, October). Image steganography and steganalysis: Concepts and practice. In *International Workshop on Digital Watermarking* (pp. 35-49). Springer Berlin Heidelberg.

Moerland, T. (2003). Steganography and steganalysis. *Leiden Institute of Advanced Computing Science*.

Silman, J., (2001) "Steganography and Steganalysis: An Overview", SANS Institute,.

Wang, H., & Wang, S. (2004). Cyber warfare: steganography vs. steganalysis. *Communications of the ACM*, *47*(10), 76-82.