International Journal of Research in Computer Science
eISSN 2249-8265 Volume 2 Issue 4 (2012) pp. 23-29

www.ijorcs.org

A DATA HIDING TECHNIQUES BASED ON LENGTH OF ENGLISH TEXT USING DES AND ATTACKS

Sanjay Jadhav[1], Viddhulata Mohite[2]
[1 2] *Information Technology, Bharati Vidyapeeth College of Engineering, Navi-Mumbai,India*
Email: sanjaysaspade@gmail.com
[2]*Email: viddhulata.mohite@gmail.com*

Abstract: *The comparing recent proposal for multimedia applications network security remains an important topic for researchers. The security deals with both wired and wireless communication. Network is defined as it is a large system consisting of many similar parts that are connected together to allow the movement or communication between or along the parts or between the parts and a control center. There are the main components of the network information system such as end systems (terminals, servers) and intermediate systems (hubs, switches, gateways). Every node has its own set of vulnerabilities that can be related to hardware, software, protocol stack etc. Nodes are interconnected by physical supports in a network for example connected with cables in wired Local Area Network (LAN) or radio waves (Wi-Fi) in Wireless Local Area Network (WLAN). Some nodes are able to provide services (FTP, HTTP browsing, database access). If two nodes want to communicate together, they must be interconnected physically and logically. Network security deals with also information hiding technique. Now day's security deals with heterogeneous networks. The use of different wireless and wired network which are working on different platform is heterogeneous. So design of network security for such type of heterogeneous network is difficult task.*

Keywords: *Information hiding, DES, Encryption, Decryption.*

I. INTRODUCTION

The comparing recent proposal for multimedia applications network security remains an important topic for researchers. The security deals with both wired and wireless communication. Network is defined as it is a large system consisting of many similar parts that are connected together to allow the movement or communication between or along the parts or between the parts and a control centre. There are the main components of the network information system such as end systems (terminals, servers) and intermediate systems (hubs, switches, gateways). Every node has its own set of vulnerabilities that can be related to hardware, software, protocol stack etc. Nodes are interconnected by physical supports in a network for example connected with cables in wired Local Area Network (LAN) or radio waves (Wi-Fi) in Wireless Local Area Network (WLAN). Some nodes are able to provide services (FTP, HTTP browsing, database access). If two nodes want to communicate together, they must be interconnected physically and logically.

Network security deals with three goals:

1. Design of network security model
2. The different types of possible attacks
3. The prevention of attacks

Network security situation awareness provides the unique high level security view based upon the security alert events. Now day's security deals with heterogeneous networks. The use of different wireless and wired network which are working on different platform is heterogeneous. So design of network security for such type of heterogeneous network is difficult task. Network security policy enforcement consists in the configuring heterogeneous security mechanisms (IP Sec, gateways, ACLs on routers, stateful firewalls, proxies etc.) that are available in a given network environment. The complexity of this task resides in the number, the nature, and the the interdependence of mechanisms to consider. Although several researchers have proposed different analysis tools, achieving this task requires experienced and proficient security administrators who can handle all these parameters today. The first task in network security is only authenticate persons can access systems. Bio-metric is an emerging technology for user authentication. However, bio-metric data is generated non-revocable unlike a password (as it is not possible to change it). To overcome this problem bio-metric template protection schemes have been proposed in the last decade. Finger prints, bio-hashing, face recognition, IRIS scan are used from past years. Recently ECG based authentication is normally preferred. Web applications are an important target for security attacks. Most of these applications make use of cookies to maintain user state. Many attacks are carried out over these cookies in order to compromise network security. To design a management platform to control access to web application servers are important. Due to this simplicity and efficiency, HTTP

protocol is the primary used protocol on the World Wide Web. So, access to web based applications has become more widespread. However, most web applications contain security vulnerabilities and so, exposing web servers directly on Internet causes a rapid increase in web applications attacks. Placing a firewall in front of web servers can protect against network level vulnerabilities by filtering application traffic. Nevertheless, firewalls do not prohibit attacks employing application level vulnerabilities. Therefore, integration of reverse proxy is required to protect against application level attacks. The reverse proxy is a mandatory proxy placed in front of internal web servers. This mandatory proxy protects the access to web server resources. It deals HTTP request and response via filtering process.

Distributed Denials of service (DDOS) attacks are persistent current and very real threats to network. Expanding upon a flexible distributed framework for network remediation utilizing multiple strategies is considered. A novel adaptive clustering method combined with features ranking for DDOS attack detection. Wavelet analysis method is considered also as one of the most efficient methods for detecting DDOS attacks. The use of client puzzles has been recognized as a preventive defense against the resource exhaustion attacks. Its original schemes however cannot be used against bandwidth attacks. To resolve this, some defense mechanisms have recently been proposed in which the puzzles are created and the answers are evaluated by the routers distributed over the network. Although interesting, these mechanisms are of high complexity and their success relies on high co-operation for core routers, a thing that is not possible in the near future. A Denial of service (DOS) attack is a malicious activity which culminates in the denial of legitimate requests for the victim's resources. A flooding attack is a DOS attack in which the attacker sends on overwhelming number of requests for a key resource to the victim. This leads to the depletion of those resources so that the legitimate requests for the same area denied. The target of a flooding attack is resource in the victim's system for example a buffer, CPU time to process requests or the bandwidth of the communication channel to the victim.

Today's security systems have been drawing great attentions as cryptographic algorithm have gained popularity due to the nature that make them suitable for use in constrained environment such as mobile sensor information applications, where computing resources and power availability are limited. Elliptic curve cryptography (ECC) is one of them, which requires less computational power, communication bandwidth, and memory in comparison with other crypto-system. In order to save pre-computing there is a trend for sensor networks to design a sensor node communicates to the end database, which indicating the needs to prevent from the man-in-middle attacking. With the rapid growth of Internet, the WWW provides an important channel for user to obtain useful information. Whereas there are more than eight billion web pages, so supplying information to user's content, is a challenging work. Fortunately, there are various web search engines, about 3500 search engines, such as Google, Yahoo, AltaVista,etc by which we can find valuable information efficiently. But possible attack is SPAM can be considered and design system immune to SPAM.

Stepping stone attacks are often used by network intruders to hide their identities. The Round Trip Times (RTT) between the sent packets and corresponding echo packets for the connection chains of stepping stones are critical for detecting such attacks. Technology never ends. Future systems are expected to defense different types of attacks as well as a mixture of service with very different and often conflicting service requirements. In these scenarios, accurate modeling is especially imperative for preventing attacks. Security issues associated with the development of the network is becoming the hot spot, high rise buildings or intelligence communities, local area networks everywhere, through the Ethernet as the communication channel. The multimedia applications such as communication of voice, sending videos, accessing e-mails; file transfer requires integration of sources like cellular/WLAN/LAN.

The integration of resources working together on single platform is called as heterogeneous network. It needs frame work for a network security in heterogeneous networks environment. Also needs separate algorithms for all types of possible attacks in network should work in heterogeneous network. For analysis purpose use of network simulator (ns-2) is taken for consideration as it works for real-time and non-real-time analysis. The comparison between designed and existing algorithm can be also carried out with network simulator. Design of network security model is also one of the important tasks. Due to a rapid progress in IT fields and increasing demand for web applications, lots of researches have focused on how to achieve network security the next generation network. Algorithms will be developed for network security for following attacks and security authentication, malware attacks, cookies security, Denial of service (DoS), cache timing attacks, Man –in-middle attack, spam, stepping stone attacks for heterogeneous networks. Out of these all information hiding techniques are more suitable and easily implementation task [1]. At present, the academic world pay mostly attention on the field that using image, video, audio as carriers and do little research on using text as carrier. It mainly because the redundant of text file is very small, it is difficult to embed, and the robustness is not well.

At the same time, it offers a wide space to the applications of data hiding system based on text document [2].

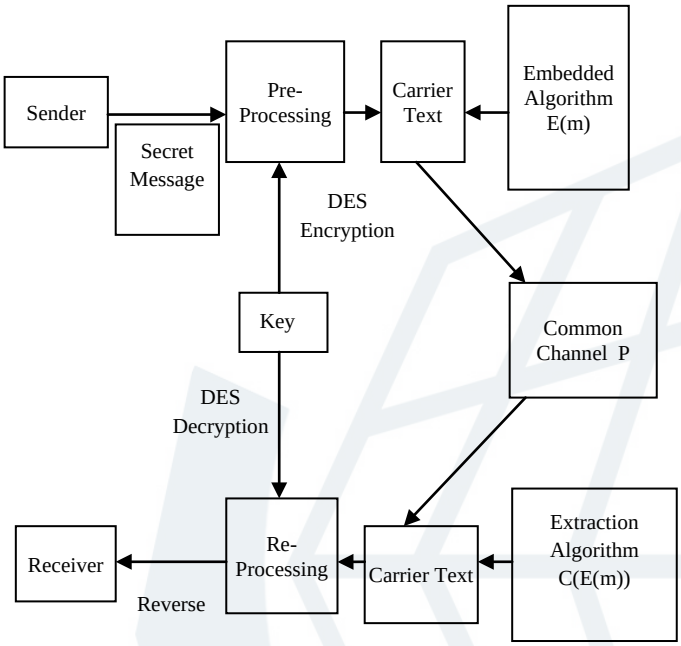


Figure 1: Structure of the hiding system

The structure of the system is shown in figure 1, it mainly includes preprocessing, embedding, extracting and post-processing five modules. The processing module is divided into encryption, grouping and formatting text three modules. The remaining paper focuses on the proposed system algorithm in section II. Section III follows flow chart whereas section VI gives result.

II. PROPOSED SYSTEM ALGORITHM

A. Using DES to encrypt the main two steps are select one appropriate encryption key KE and encrypt secret message m with KE to get the cipher text m '.

B. Creating the embedded key KE:

Step 1. Transform the encrypted file whose type is byte into binary sequence.

Step 2. Take the elements of Lk as the length of block. And cut the text into even blocks, Lk is random integers between 0 and 5, then extract the embedded key KE ={k I k E lk } .which need to be attention is that KE is generated by random function.

Step 3. Translate every block into decimal digit, and generate a decimal sequence, which will decide the embedded position with the length of the words, Pre-process carrier text. Pre-processing is adjust the colour, font size and character spacing of the carrier without change its original vector content and format, then add some colour and characters as disturbs. It mainly includes the following two steps.

1. Typesetting carrier text in mrified form.
2. In setting a few random interference using suitable algorithm, but we must ensure that these interferences will not affect the extraction of secret message. The purpose of pre-processing is to increase the accuracy of extracting and improve the ability against attacking.

C. Design of Embedded Algorithm

Preliminary definition:

1. Define stochastic nature numbers Lk, then according to Lk, divide the binary bit stream of secret message M into groups randomly and transform them into decimal number. The decimal number of M is M~{ml.m2 ... mi liE N .mi<2k-l} after being transformed.
2. Define the set of text V~ {v l.v2 ... vj I j EN} according the sequence of text
3. Define Length (x) As the function[5]. which is used to calculate length of words.
4. Define the set of decimal is D~{dl, d2, ... , di}. which is the result that transform secret message using KE.

Design of embedded algorithm:

The embedded algorithm decides the invisibility, hidden capacity, robustness of the system. Complexity of the algorithm impacts operation efficiency directly. The embedded algorithm is designed as follows:

Step 1. Select a colour which is similar to the colour of carrier as embedded characteristic, which has solved the second problem, which make the colour change of the text as a manner of embedding secret message.

Step 2. Define the embedded position in the words.

Algorithms E(M) is described as follows:

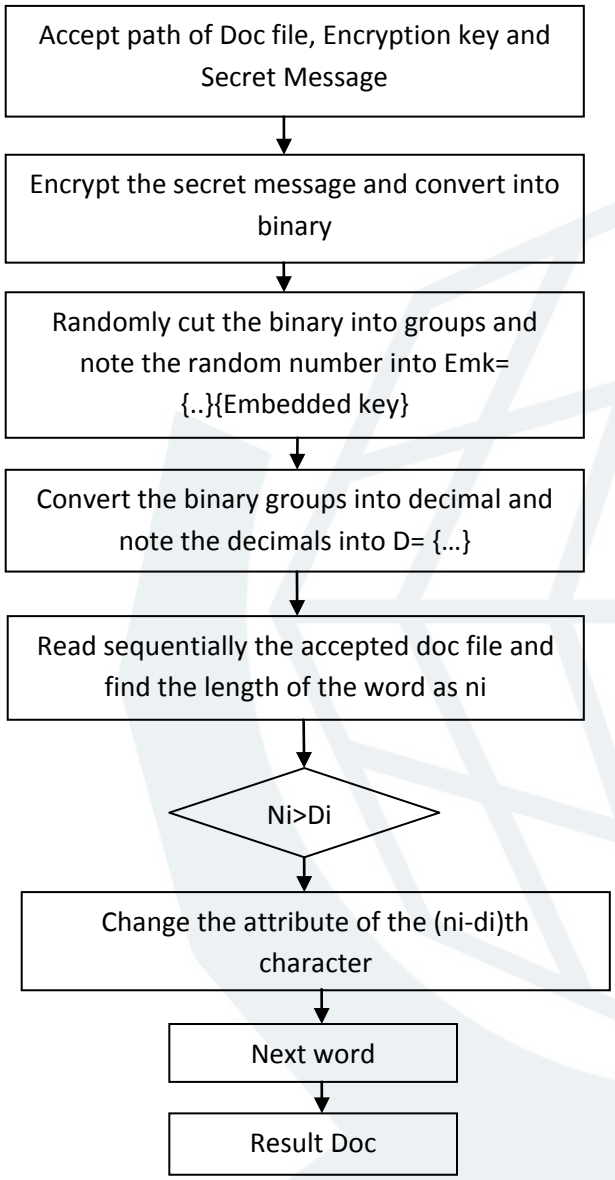
```
E (M)
{
   int x.y;
   Define x= 1, y= 1; // start embed with the
                        beginning or decide by himself
   Line1:
   If x<j and y <j then // judge the embedding
                          is complete or not.
   If Length (vy>dx) then // select the position of
                            character need to be embedded.
   Embed message into the position Length (vy)-
    mx of word vy;

     x=x+ l; y=y+ 1;
   Else jy+1

     goto linel;
   Else fail to embed;

Complete embedding.
```

III. PROPOSED SYSTEM FLOW CHART



IV. PROGRAM FOR PROPOSED SYSTEM

```
package com.sss.stegnography.text.cryptography;
import java.io.UnsupportedEncodingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.SecretKey;

public class DesEncrypter
  {
      Cipher ecipher;
      Cipher dcipher;
 public DesEncrypter(SecretKey key) {
  try {
      ecipher = Cipher.getInstance("DES");
      dcipher = Cipher.getInstance("DES");
      ecipher.init(Cipher.ENCRYPT_MODE, key);
      dcipher.init(Cipher.DECRYPT_MODE, key);
        }
   catch (javax.crypto.NoSuchPaddingException e)
        {
         }
   catch  (java.security.NoSuchAlgorithmException e)
        {
          } catch (java.security.InvalidKeyException e)
          }
         }

public String encrypt(String str) {
    try {
     // Encode the string into bytes using utf-8
        byte[] utf8 = str.getBytes("UTF8");
     // Encrypt
        byte[] enc = ecipher.doFinal(utf8);
     // Encode bytes to base64 to get a string
        return new
sun.misc.BASE64Encoder().encode(enc);
         } catch (javax.crypto.BadPaddingException e)
        {
          } catch (IllegalBlockSizeException e) {
         } catch (UnsupportedEncodingException e) {
        }
        return null;
      }

public String decrypt(String str) {
      try {
     // Decode base64 to get bytes byte[] dec = new
        sun.misc.BASE64Decoder().decodeBuffer(str);
     // Decrypt
        byte[] utf8 = dcipher.doFinal(dec);
     // Decode using utf-8
        return new String(utf8, "UTF8");
        }
     catch (javax.crypto.BadPaddingException e) {
       }
     catch (IllegalBlockSizeException e) {
       }
     catch (UnsupportedEncodingException e) {
       }
     catch (java.io.IOException e) {
       }
    return null;
     }
}
```

V. RESULT

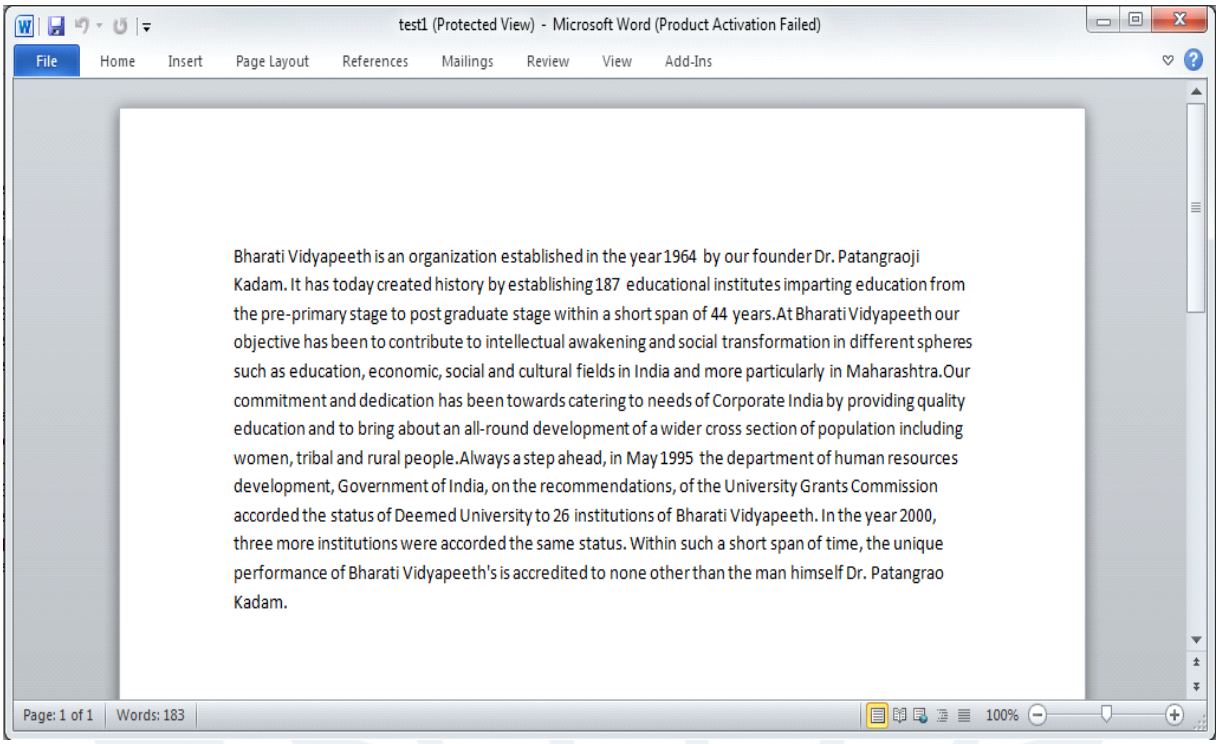


Figure 2: Original Document

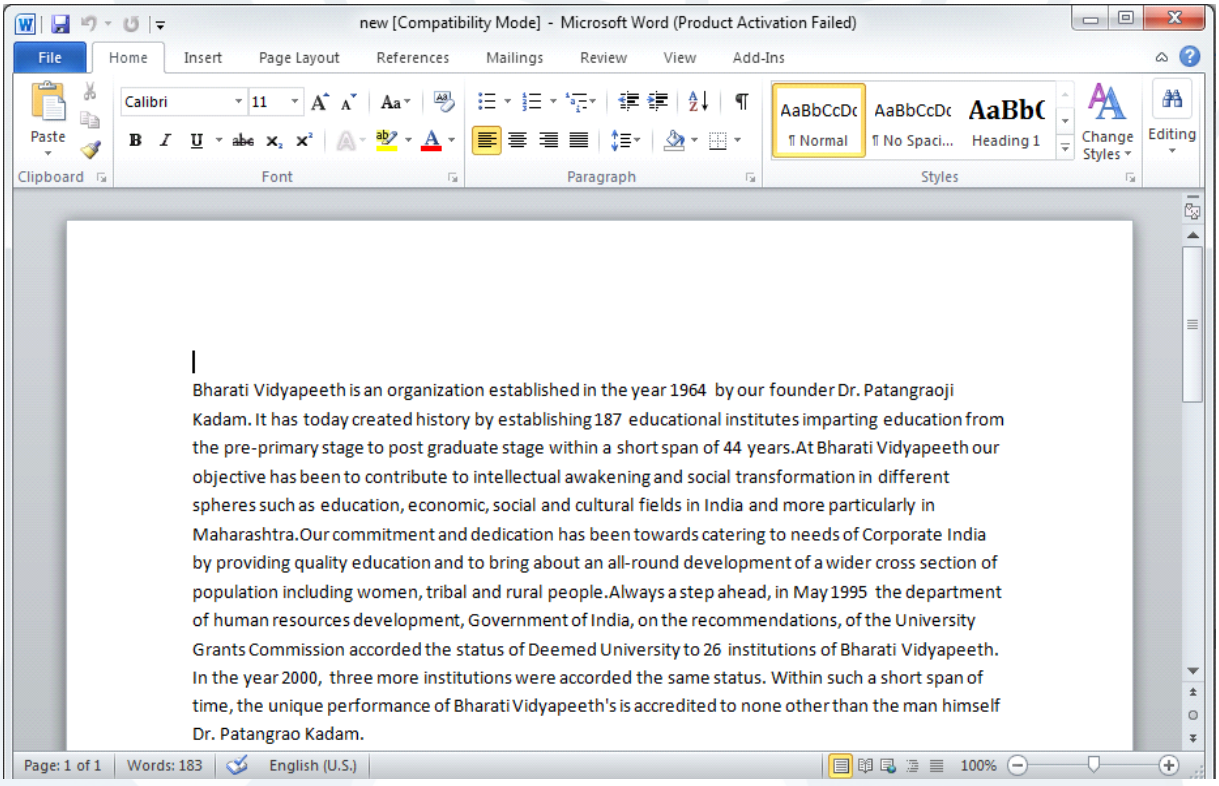


Figure 3: Encrypted Document

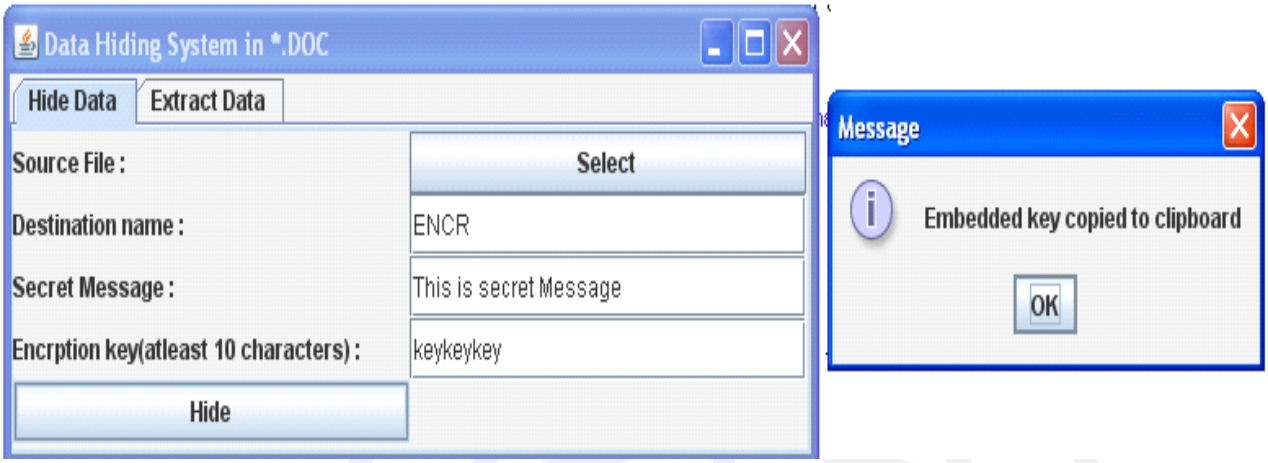


Figure 4: Screenshots – Hide Data

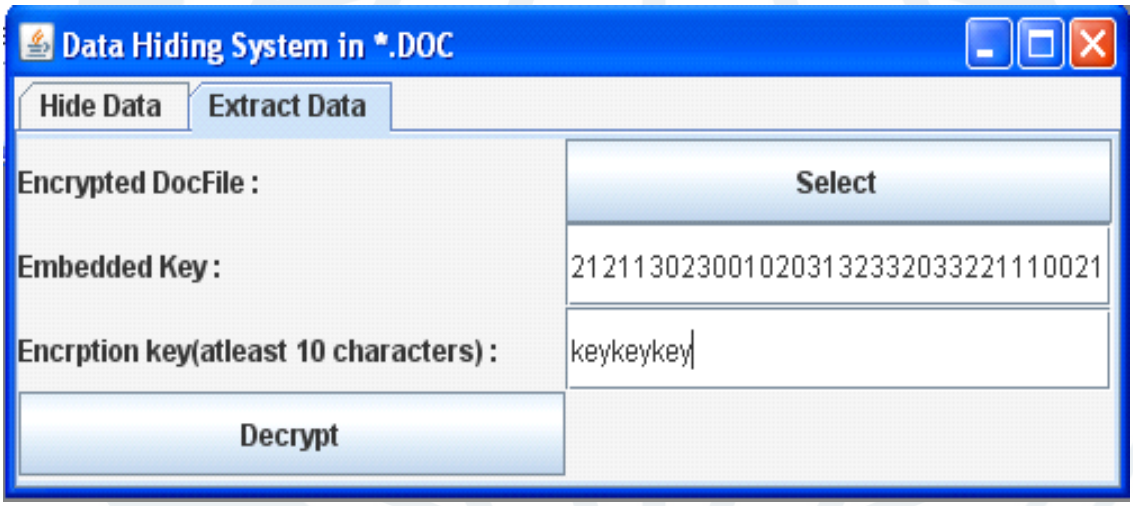


Figure 5: Screenshots – Extract Data

Encryption Key: keykeykey

Embedded Key:
02010321200210113030212320112232231333311110
01101002300333212001010031301120031030120131
23220233313032030331323001220122011002220200
23212

Result message: - This is secret message

VI. CONCLUSION

In general, the security and the capacity of the information hidden system conflict with each other, in order to solve the problem, we design and implemented a hidden system based on the length of English text document and secret message encryption. Combine randomness of the English words, DES, with the ideological of blocks, which insure the security, and the capacity are greatly improved at the same time. The proposed system used for information hiding gives several advantages form a technical viewpoint: flexibility and portability is very well, but robustness and operational efficiency of the system are deficiency, which need to improve and perfect.

VII. REFERENCES

[1] Stefan Katzenbeisser,Fabien A P Petitcolas. “Information hiding techniques for stegnography and digital watermarking” Artech House Publishers, 2000.

[2] Peticolas F.A.P, Anderson R.J.Kuhn M.G.information Hiding –Asurvey,Proceedings of the IEEE, 1999, 87(7), PP:1062-107.

[3] Cachin,C, “An information Theoretic model for stegnography”, in proceeding of the second international workshop on information hiding,vol.1525 of lecture notes in computer science, Springer, 1998, pp.306-308.

[4] Jeremiah J. Haarmsen, William A.Pearlman “Steganalysis of additive noise modelable information hiding” Electrical Computer and systems Engineering Department,Rensselar Polytechnic Institute, Troy,NY.

[5] Neil F.Jhonson and Sushil Jajodia “Steganalysis: The investigation of hidden information” The 1998 IEEE Information Technology Conference. September 1st-3rd,1998.

[6] Jonathan Watkins “Steganography-Message Hidden in Bits” Multimedia Systems Coursework, Department of Electronics and computer Science, University of Southampton. 15th December 2001.

[7] Leonid Reyzin and Scott Russell "More efficient provably Secure Stegnography" Department of computer science Boston University, May 15,2003.

[8] P.Davern, M.Scott "Steganography: its history and its application to computer based data files" Dublin City University.

[9] Liu Cuilin,Shen Yongiun,Zhang Guidong,Di Changyan "A Data Hiding System Based on Length of English Text" 2010 first ACIS International Symposium on Cryptography, and Network Security,Data Mining and Knowledge Discovery, E-Commerce and Its Applications, and Embedded Systems.

How to cite

Sanjay Jadhav, Viddhulata Mohite, "A Data Hiding Techniques Based on Length of English Text using DES and attacks". *International Journal of Research in Computer Science*, 2 (4): pp. 23-29, July 2012. doi:10.7815/ijorcs.24.2012.036