New Technique of Hidden Data in PE-File with in Unused Area Two

T.Sangeetha[†] **T.Meyappan** [††]

Research Scholar Department of Comp.Sci & Engg, Alagappa University, Karaikudi
Associate \professor Department of Comp.Sci & Engg, Alagappa University, Karaikudi

ABSTRACT

The strength of the combination between hiding and encryption science is due to the non-existence of standard algorithms to be used in hiding and encrypting secret messages. Also there are many ways in hiding methods such as combining several media (covers) with different methods to pass a secret message. Furthermore, there is no formal method to be followed to discover a hidden data.For this reason, the task of this paper becomes difficult. In this paper proposed a new system of information hiding is presented. The proposed system aim to hide information (data file) in unused area 2 of any execution file (exe.file), to make sure changes made to the exe.file will not be detected by anti-virus and the functionality of the exe.file is still functioning. The system includes two main functions; first is the hiding of the information in the unused area 2 of PE-file (exe.file), through the execution of four process (specify the cover file, specify the information file, encryption of the information, and hiding the information) and the second function is the extraction of the hiding information through three process (specify the steno file, extract the information, and decryption of the information). The testing result shows; the result file does not make any conflict with anti-virus software and the exe.file still function as usual after the hiding process. The proposed system is implemented by using Java.

Keywords:

Information hiding; portable executable file; Stegnography; Statistical technique

1. INTRODUCTION

Steganography is the art of concealing the presence of information within an innocuous container. Steganography has been used throughout History to protect important information from being discovered by Enemies. A very early example of Steganography comes from the story of Demartus of Greece. He wished to inform Sparta that Xerces the King of Persia was planning to invade. In ancient Greece wax covered wooden tablets were used to record written text .In order to avoid detection by the Persians, Demartus scraped the wax from a tablet, etched the message into the underlying wood, then recovered the tabled with wax. This concealed the underlying message from the sentries who inspected the tablets as they left Persia by courier for Greece. Other historical examples of Steganography are the use of invisible inks. A common experiment conducted by young kids everywhere is to use a toothpick dipped in vinegar to write a message on a piece of paper. Once the vinegar dries, the presence of the message is not obvious to a casual inspector (aside from the smell).

Upon slight heating of the paper, a chemical reaction occurs which darkens the vinegar and makes the message readable. Other, less smelly, invisible inks have been used throughout history similarly even up until World War.

A more recently developed Steganography technique was invented by the Germans in World War II, the use of microdots. Microdots were very small photographs, the size of a printed period, which contain very clear text when magnified. These microdots contained important information about German war plans and were placed in completely unrelated letters as periods. Although Steganography is related to Cryptography, the two are fundamentally different .The quick development of multimedia and internet allows for wide distribution of digital media data. It becomes much easier to edit, modify and duplicate digital information. In additional, digital document is also easy to copy and distribute, therefore it may face many threats. It becomes necessary to find an appropriate protection due to the significance, accuracy and sensitivity of the information.

Nowadays, protection system can be classified into more specific as hiding information and encrypting information or a combination between them. Cryptography is the practice of ‘scrambling’ messages so that even if detected, they are very difficult to decipher. The purpose of Steganography is to conceal the message such that the very existence of the hidden is ‘camouflaged’. However, the two techniques are not mutually exclusive. Steganography and Cryptography are in fact complementary techniques. No matter how strong algorithm, if an encrypted message is discovered, it will be subject to cryptanalysis. Likewise, no matter how well concealed a message is, it is always possible that it will be discovered. By combining Steganography with Cryptography we can conceal the existence of an encrypted message. In doing this, we make it far less likely that an encrypted message will be found. Also, if a message concealed through Steganography is discovered, the discoverer is still faced with the formidable task of

Manuscript received May 5, 2013
Manuscript revised May 20, 2013

deciphering it.

2. RELATED WORK

Steganography and cryptology are similar in the way that they both are used to protect important information [1]. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. Nowadays the term“Information Hiding” relates to both watermarking and steganography [2]. Watermarking is the technique use to hides information in a digital object (video, audio or image)
so that information is robust to adjustments or alterations[1],[2]. By watermarking, the mark itself is invisible or unnoticeable for the human vision system. In addition, it should be impossible to remove a watermark without degrading the quality of the data of the digital object [3]. The important application of watermarking is to copyright protection systems, which are intended to prevent unauthorized copying of digital media (pirating). For
example if the digital signal (audio, pictures or video) is copied, then the information is also carried in the copy [2],[3]. On the other hand, the main goal of steganography is to hide secret information in the other cover media (video, audio or image) so that other persons will not notice the presence of the information [2],[3]. This is a major distinction between this method and the other methods of covert exchange of information because, for example, in cryptography, the individuals notice the information by seeing the coded information but they will not be able to comprehend the information. However, in steganography, the existence of the information in the sources will not be noticed at all. Although
steganography is separate and different from cryptography, but they are related in the way that they both are used to protect valuable information [3]. From here emerged the urgent need to find new techniques alternative organization to overcome these weaknesses, giving rise to conceal information technology (Information Hiding), which are based on a different principle to the idea of organization, where they are buried information (Information Embedding) within other media carrier, and making them aware (Imperceptible) by hackers and attackers, and so are the public domain of information to users of the network, while the content monopoly "on the relevant agencies, which alone knows how to extract content .Nowadays, protection framework can be classified into more specific as hiding information (Steganography) or encryption information (Cryptography) or a combination between them[4].

3. PROPOSED SYSTEM

In this paper proposed a new system of information hiding using computation between cryptography and steganography is presented. The proposed system aim to hide information (data file) using computation between cryptography and steganography with in computation area which is unused area two and image page of any execution file (exe.file), to increase the degree of security and the amount of hidden data within exe file without change the size of cover file, to make sure changes made to the exe.file will not be detected by anti-virus and the functionality of the exe.file is still functioning. The system includes two main functions; first is the hiding of the information in the with in computation area which is unused area two and image page of PE-file (exe.file), through the execution of four process (specify the cover file, specify the information file, encryption of the information, and hiding the information) and the second function is the extraction of the hiding information through three process (specify the steno file, extract the information, and decryption of the information).

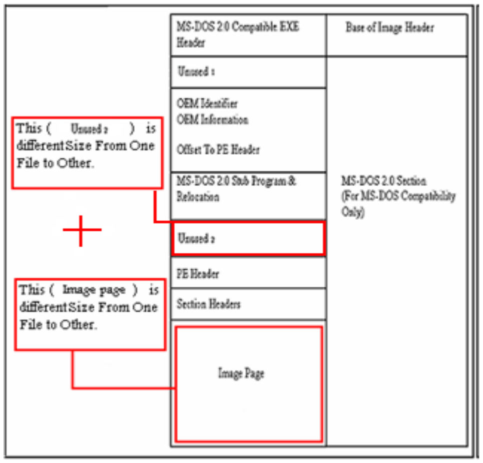
3.1 ADVANTAGE

The hiding operation within computation between unused area two and image page of EXE file, increases the degree of security for the information hiding which is used in the proposed system because the data which is embedded inside the EXE file is not embed directly of EXE file , it will be hiding within unused area two and then image page of EXE file. So the attacker cannot be guessing the information hidden.
The cover file can be executed normally after hiding operation. Because the hidden information already hide in the unused area two and image page within exe.file and thus cannot be manipulated as the exe.file, therefore, the cover file still natural, working normally and not effected, such as if the cover is EXE file (WINDOWES XP SETUP) after hiding operation it'll continued working, In other words, the EXE file can be installed of windows.

3.2 PORTABLE EXECUTABLE FILE

The characteristics of the Executable file does not have a standard size, like other files, for example the image file (BMP) the size of this file is between (2-10 MB), Other example is the text file (TEXT) the size often is less than 2 MB.
For taking advantage of this feature(disparity size) make it a suitable environment for concealing information without detect the file from attacker and discover hidden information in this file.

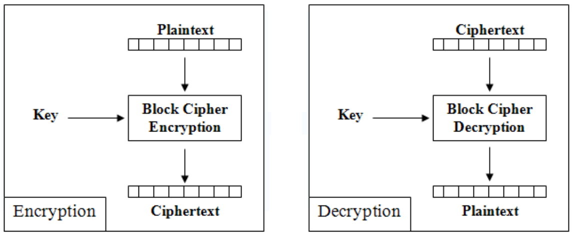
3.5 PE FILE LAYOUT


MS-DOS 2.0 Compatible EXE Header
Base of Image Header
Unused 1
OEM Identifier
OEM Information
Offset To PE Header
MS-DOS 2.0 Stub Program & Relocation
MS-DOS 2.0 Section (For MS-DOS Compatibility Only)
Unused 2
PE Header
Section Headers
Image Page
This (Unused 2) is different Size From One File to Other.
+
This (Image page) is different Size From One File to Other.

3.6 BLOCK CIPHER

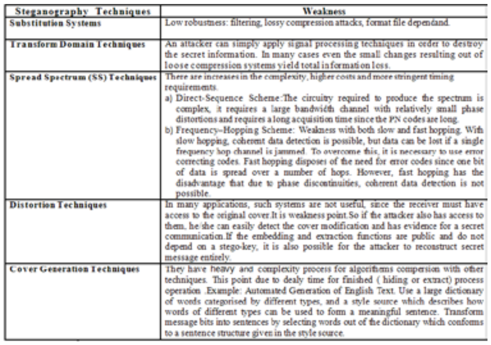
In cryptography, a block cipher is a symmetric key cipher. Which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation. When encrypting, a block Mcipher might take a (for example) 128-bit block of plaintext as input, and outputs a corresponding 128-bit block of cipher text. The exact transformation is controlled using a second input — the secret key. Decryption is similar: the decryption algorithm takes, in this example, a 128-bit block of cipher text together with the secret key, and yields the original 128-bit block of plaintext. To encrypt messages longer than the block size (128 bits in the above example), a mode of operation is used.

A message longer than the block size(128 bits) can still be encrypted with a block cipher by breaking the message into blocks and encrypting each block individually, however in this method all blocks are encrypted with the same key



3.3 STATISTICAL TECHNIQUE

Statistical Steganography techniques utilize the existence of "1-bits" Steganography schemes, which embed one bit of information in a digital carrier. This is done by modifying the cover in such a way that some statistical characteristics change significantly if a "1" is transmitted. Otherwise, the cover is left UN changed. So the receiver must be able to distinguish unmodified covers from modified ones. A cover is divided into l (m) disjoint blocks B1...B l (m). A secret bit, mi is inserted into the ith block by placing "1" in to Bi if mi=1.Otherwise, the block is not changed in the embedding process. Table 1: Weakness of Steganography Techniques



Steganography Techniques	Weakness
Substitution Systems	Low robustness: filtering, lossy compression attacks, format file dependand.
Transform Domain Techniques	An attacker can simply apply signal processing techaiques in order to destroy the secret information. In many cases even the small changes resulting out of loose comperssion systems yield total information loss.
Spread Spectrum (SS) Techniques	There are increases in the complexity, higher costs and more stringent timing requirements. a) Direct-Sequence Scheme:The circuitry required to produce the spectrum is complex, it requires a large bandwidth channel with relatively small phase distortions and requires a long acquisition time since the PN codes are long. b) Frequency–Hopping Scheme: Weakness with both slow and fast hopping. With slow hopping, coherent data detection is possible, but data can be lost if a single frequency hop channel is jammed. To overcome this, it is necessary to use error correcting codes. Fast hopping disposes of the need for error codes since one bit of data is spread over a number of hops. However, fast hopping has the disadvantage that due to phase discontinuities, coherent data detection is not possible.
Distortion Techniques	In many applications, such systems are not useful, since the receiver must have access to the original cover.It is weakness point.So if the attacker also has access to them, he/she can easily detect the cover modification and has evidence for a secret communication.If the embedding and extraction functions are public and do not depend on a stego-key, it is also possible for the attacker to reconstruct secret message entirely.
Cover Generation Techniques	They have heavy and complexity process for algorithms compersion with other techniques. This point due to dealy time for finished (hiding or extract) process operation .Example: Automated Generation of English Text. Use a large dictionary of words categorised by different types, and a style source which describes how words of different types can be used to form a meaningful sentence. Transform message bits into sentences by selecting words out of the dictionary which conforms to a sentence structure given in the style source.

From the above table, most of the techniques are very complex and not suitable to be used with exe.file. In order to use exe.file. Thus, we choose to apply statistical technique because it is not complex and suitable to be implemented with the structure and characteristic of the exe.file.

3.4 ADVANCE ENCRYPTION STANDARD

In 1997, the NIST called for submissions for a new standard to replace the aging DES. The contest terminated in November 2001with the selection of the Rijndael cryptosystem as the Advanced Encryption Standard (AES). The Rijndael cryptosystem operates on 128-bit blocks, arranged as 4 × 4 matrices with 8-bit entries. The algorithm can use a variable block length and key length. The latest specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128,192, or 256 bits. AES may, as all algorithms, be used in different ways to perform encryption. Different methods are suitable for different situations. It is vital that the correct method is applied in the correct manner to each and every situation, or the result may well be insecure even if AES as such is secure. It is very easy to implement a system using AES as its encryption algorithm, but much more skill and experience are required to do it in the right way for a given situation. To describe exactly how to apply AES for varying purposes is very much out of scope for this short introduction.

4. IMPLEMENTATION:

Implementation is the stage of the project when the theoretical design is turned out into a working system.

Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

4.1 Key generation

In this module, the data owner produces key using pseudo-random key generator. The key is a secret parameter for encrypting or decrypting a specific message exchange context. Keys are important, as ciphers without keys are trivially breakable and therefore less than useful for most purposes.

4.2 Block cipher encryption

In this module the plaintext will be encrypted using an aes encryption algorithm and it will be stored in the data sharing centre. The encryption will be based on the encryption algorithm and the data will be encrypted. Encryption is the process of
transforming information using an aes algorithm to make it unreadable to anyone except those possessing a key.

4.3 Stegnography

In this module stegnography is applied for embedding the encrypted information with an exe file.

4.4 Cover object

In this module, the user has to select a portable exe as a cover object. one particular advantage of steganography, as opposed to other information hiding techniques, is that the embedded has the freedom to choose a cover object that results in the least detectable stego object.

4.5 Applying stegnography embedding

In this module the encrypted data is taken as a stego object and the exe is taken as the carrier object. Embedding data in steganographic system can be carried out without use of a key or with use of a key. To improve steganographic robustness key can be used as a verification option. It can make an impact on the distribution of bits of a message within a container, as well as an impact on the procedure of forming a sequence of embedded bits of a message.

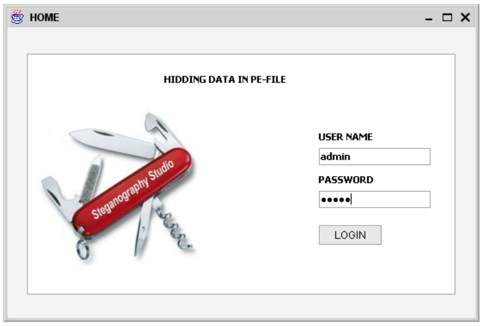
4.6 Applying reverse stenography algorithm

While information can be hidden inside exe in such a way that the presence of the message can only be detected with knowledge of the secret key. using the reverse process of the stenography algorithm we can separate the exe object with the encrypted data. Later the information is decrypted.

4.7Decryption

Decryption is the reverse operation of encryption. In this module the decryptor will use the encryption key for decrypting the information.

5. EXPERIMENTAL RESULT

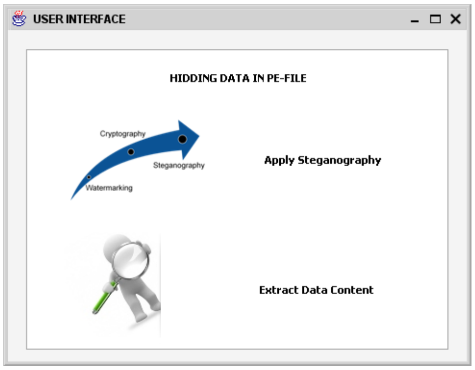


HOME

HIDDING DATA IN PE-FILE

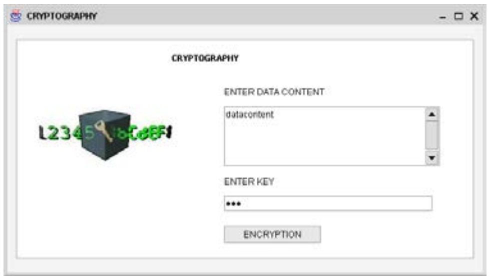
USER NAME: admin

PASSWORD: •••••



USER INTERFACE

HIDDING DATA IN PE-FILE

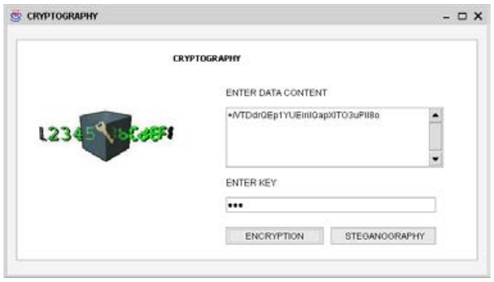


CRYPTOGRAPHY

CRYPTOGRAPHY

ENTER DATA CONTENT: datacontent

ENTER KEY: •••

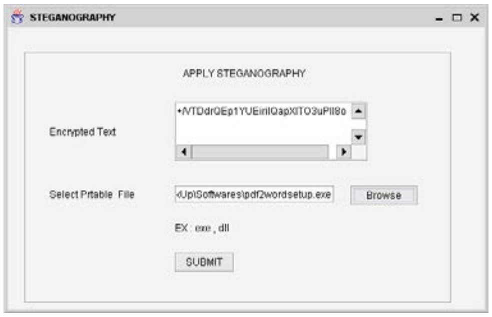


CRYPTOGRAPHY

CRYPTOGRAPHY

ENTER DATA CONTENT: +/VTDdrQEp1YUEinlQapXITO3uPIl8o

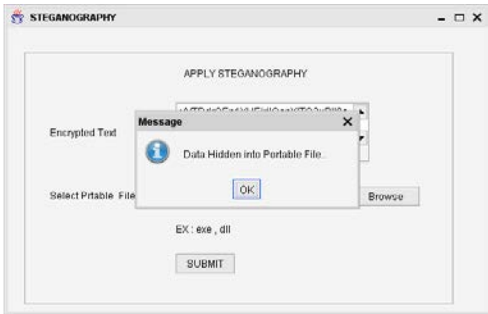
ENTER KEY: •••



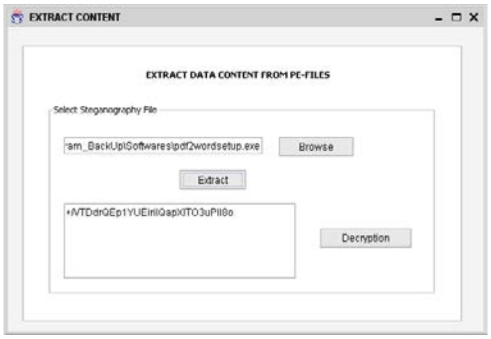
Encrypted Text: +/VTDdrQEp1YUEirilQapXITO3uPIl8o

Select Prtable File: ‹Up\Softwares\pdf2wordsetup.exe

EX : exe , dll

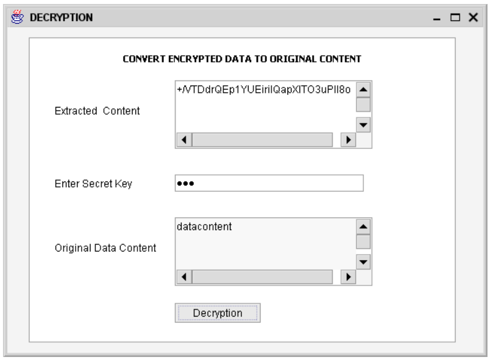


Data Hidden into Portable File.



Select Steganography File: ram_BackUp\Softwares\pdf2wordsetup.exe

+/VTDdrQEp1YUEirilQapXITO3uPIl8o



Extracted Content: +/VTDdrQEp1YUEirilQapXITO3uPIl8o

Enter Secret Key: ●●●

Original Data Content: datacontent

6. CONCLUSION

The EXE files are one of the most important files in operating systems and in most systems designed by developers (programmers/software engineers), and then hiding information in these file is the basic goal for this research, because most users of any system cannot alter or modify the content of these files. We get the following conclusions: PE files structure is very complex because they depend on multi headers and addressing, and then insertion of data to PE files without full understanding of their structure may damage them, so the choice is to hide the information beyond the structure of these files. Most antivirus systems do not allow direct write in executable file, so the approach of the proposed system is to prevent the hidden information to observation of these systems. One of the important conclusions in implementation of the proposed system is the solving of the problems that are related to the size of cover file, so the hiding method makes the relation between the cover and the message independent. The encryption of the message increases the degree of security of hiding technique which is used in the proposed system. The proposed hiding technique is flexible and very useful in hiding any type of data for files (message) because there are no limitations or restrictions on the type of the message (image, sound, text).

REFERENCES

[1] A.A.Zaidan, B.B.Zaidan, M.M.Abdulrazzaq, R.Z.Raji andS.M.Mohammed, “Implementation Stage for High Securing Cover- File of Hidden Data Using Computation between Cryptography and Steganography”. International Association of Computer Science and Information Technology (IACSIT), indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, Volume 20, 2009, Manila, Philippines.

[2] A.W.Naji, A.A.Zaidan, B.B.Zaidan, Shihab A, Othman O. Khalifa, “ Novel Approach of Hidden Data in the (Unused Area 2 within EXE File) Using Computation Between Cryptography and Steganography ”, International Journal of Computer Science and Network Security (IJCSNS) , Vol.9, No.5 , ISSN : 1738-7906, pp. 294-300, May 30 (2009), Seoul, Korea.

[3] B.B.Zaidan, A.A.Zaidan, Fazidah Othman “Enhancement of the Amount of Hidden Data and the Quality of Image", Malaysia Education Security (MyEduSec08), Grand Continental Hotel, 2008, Kuala Trengano, Malaysia

[4] Avedissian, L.Z," Image in Image Steganography System”, Ph.D.Thesis, Informatics Institute for Postgraduate Studies (IIIPS), University of Technology, Baghdad, Iraq, 2008.

[5] C. J. S. B,” Modulation and Information Hiding in Images”, of Lecture Notes in Computer Science, University of Technology, Malaya, Vol. 1174, pp.207-226, 2007.

[6] Clelland, C.T.R, V.P & Bancroft, “ Hiding Messages in DNAMicroDots ” , International Symposium on Industrial Electronics (ISIE) , University of Indonesia , Indonesia, Vol. 1, pp.315-327, 2007.

[7] Davern, P.S, M.G, “Steganography It History and Its Application to Computer Based Data Files”, School of Computer Application (SCA), Dublin City University. Working Paper. Studies (WPS), Baghdad, Iraq, 2007.

[8] Dorothy, E.R, D.K, “Cryptography and Data Security”, IEEE International Symposium on Canada Electronics (ISKE), University of Canada, Canada, Vol.6, pp.119-122, 2006,