INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 1(27) • 2013
ISSN 1507-3858

Volodymyr Mosorov
Łódź University of Technology
e-mail: mosorow@kis.p.lodz.pl

Marian Niedźwiedziński
University of Łódź
e-mail: zie@uni.lodz.pl

HIDDEN MESSAGE TECHNIQUES IN E-COMMERCE

Abstract: The rapid growth in e-commerce applications via the Internet in recent decades is the reason why both small office and corporation users have a need to protect their data transactions through the Internet. These data transactions include sensitive document transfer, digital signature authentication and digital data storage. The use of digital steganography for information security in various e-commerce applications through the Internet are discussed in detail in this article. These applications include digital signature authentication and validation of electronic documents, digital data storage as well as secure communication of multimedia data through the open channels.

Keywords: steganography, security, e-commerce.

1. Introduction

Nowadays one of the main problems with online transactions is their lack of security. Although there exist encryption techniques, contemporary machines are able to break them, so the whole process is not confidential at all or at best only slightly. Stronger encryptions are usually forbidden by law, exposing the serious danger of improper usage by criminals. Moreover, one can suspect that something is hidden because most of the encryption methods use some hashing or bitwise operations which makes the output totally unreadable in any form by humans. When someone looks at this he/she is convinced that it contains something confidential, so they start to be suspicious and try to break the code. Because of these properties most contemporary techniques are insufficient in providing safe authentication, so let us see how is it possible to overcome them.

2. Steganography techniques

Steganography is a technique of hiding information in such a manner that it is publicly available, but still a third person would not know that any data is hidden inside [Cox et al. 2009; Wayner 2009]. Steganography is similar to cryptography. While cryptography provides privacy, steganography provides secrecy. Privacy is what you need when you do not want to hide what is sent. For this, you use cryptography and send a coded file, and only the website can decipher it. However, everyone can see that you are sending a secret message even if you do not know what that is. For true secrecy, you do not want anyone to know you are sending a message at all. Steganography makes use of a medium like text, image, sound, video or practically any type of digital content. It exploits the fact that most formats are redundant, which means that there are some parts of information that, when modified, change the original file slightly, but in such a way that it is still usable by a computer and for a human it is hard to recognize any difference (see Figure 1).

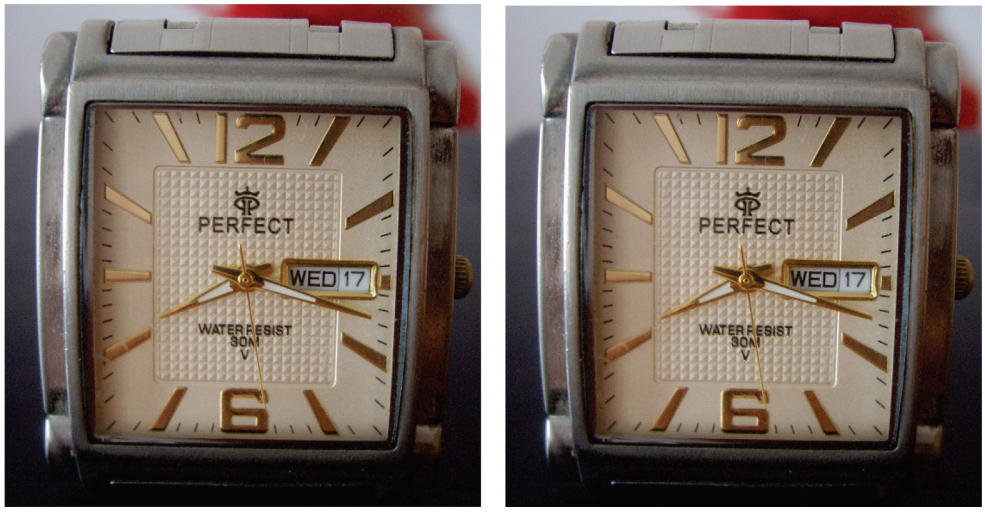

Figure 1. Original and watermarked image

Source: own source.

As a result, the medium with hidden information included can be shown publicly without the risk of the information being extracted. This is due to the fact that probably no one will even notice that there is any data hidden. Such a property gives this method high effectiveness in hiding the information from any intruder.

Steganography (literally meaning covered writing) has its roots in ancient Greece, where many ways of covering messages were used. One of the examples was tattooing the shaved head of a messenger, letting his hair grow and then shaving

it off again when he arrived at the destination. The magic behind steganography is its context that looks like something natural, not uncommon. It can appear as a picture, some text or article, shopping list, any object that is commonly used and stores some information. This object is called cover text, because it distracts someone from the factual meaning of the message. This meaning may be written with an invisible ink or knitted into the material (for example using Morse code like in the Second World War).

A quite common example is a special UV ink (there are even cartridges for printers in order to print higher resolution text on paper).

Such an idea is sometimes used for cheating in exams with pens equipped with UV lamps (see Figure 2). Another very simple idea is a message written on a postcard under the stamp. To most people it would look like a typical seasonal card, but the addressee knows that he/she should remove the stamp in order to read the real message (see Figure 3). Many other similar examples can be observed between two people in love when they want to hide their feelings at first glance, but leaving some signs how to decode them. One may notice that steganographic techniques resemble mysteries.

Figure 2. Hidden message written with UV ink

Source: [WWW1].

Hello, Kate,
I thank you for your last email.
Did you send the copy to Michal?
Do you think it's possible we meet again?
Every day I dream about it.
Neil

Figure 3. Example of message encoded with capital letters

Source: own elaboration.

Another most widely used kind of steganography is the so-called *digital watermarking*. A watermark, historically, is the replication of an image, logo, or text on paper stock so that the source of the document can be at least partially authenticated. A digital watermark can accomplish the same function; a graphic artist, for example, might post sample images on his/her website complete with an embedded signature so that he/she can later prove ownership in case others attempt to portray that work as their own.

2.1. The reason for steganography

The main purpose of steganography is to mislead the intruder [WWW2; WWW4]. However, usually it is done in a very basic way, so once somebody knows simple methods he/she can figure out other solutions. For that reason, it is advised to compress and encrypt data beforehand. First, compression makes the message smaller, which is better for steganography since it requires a smaller medium and secondly, data encryption ensures that the data will not be noticed using typical techniques for steganography (encrypted data looks like random information, so when propagated in the medium it looks normal (see Figure 4). Even dictionary attacks are likely to fail in decoding such a structure). There is also a dilemma here which speaks in favor of steganography. We cannot be sure that the hidden information is added to the message.

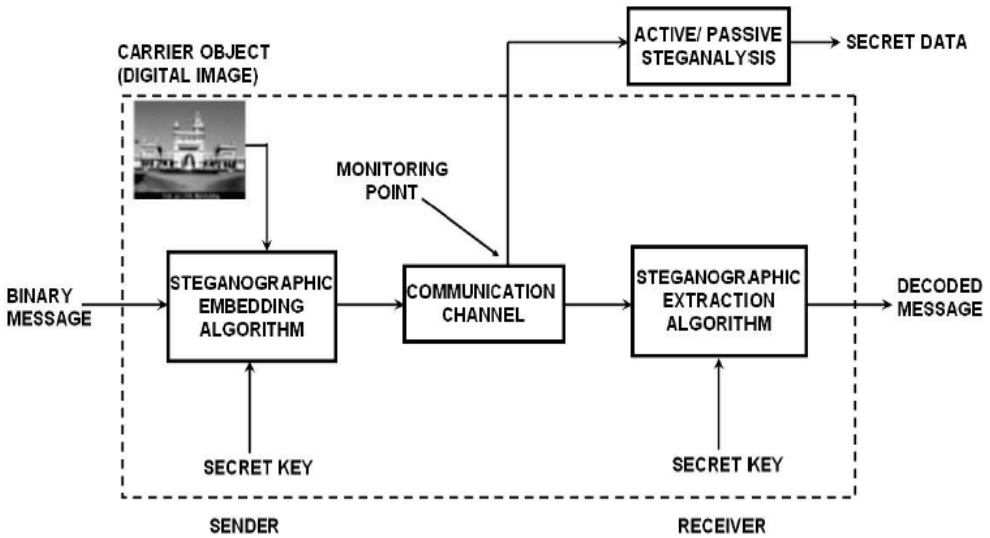

Figure 4. Typical encoding/decoding process

Source: [Meghanathan, Nayak 2010].

2.2. Choosing the medium

As stated before, the higher the degree of redundancy of the file the better the encoding. There are three main data types prone to contain data of less importance which are: pictures, sounds and movies (see Figure 5). There are 3*8 bits of information about each part of an image (called pixel), which give 16.7 million possible colors to be represented. It is unquestionable that slight modifications in hue will not be visible by a human without the help of specialized equipment. Thanks to this huge redundancy, images are primarily chosen as a channel of transporting data (see Figure 6). They are very popular among the Internet users, so if someone sees an image, he/she will not ask him/herself if there is any information hidden in it. He/she will just look at the picture itself and will not think about its different meaning.

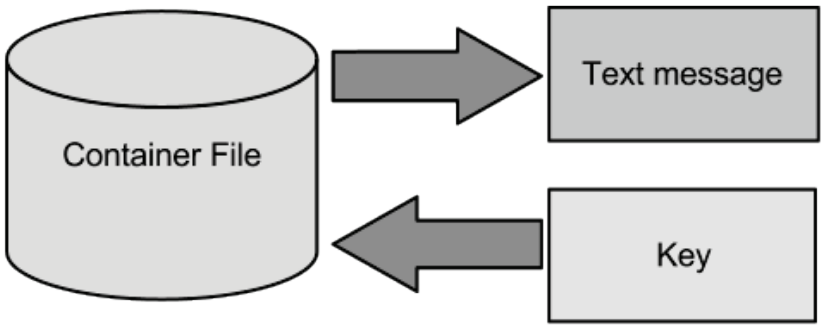

Figure 5. Basic idea of steganography using digital media (container file)

Source: own elaboration.

To hide information in audio files, similar techniques can be used as in image files. The human brain has the capability of muting quieter sounds when a stronger signal exists. This can be exploited to generate very silent noise that contains some information, which will be unnoticeable to people yet very easy to decode for some software. Such channels were also used for sending subliminal messages, because, despite the fact that our consciousness cannot recognize it, our ears still can hear it and the brain processes such information, although in an unconscious manner. Still, a human is not able to distinguish such an encoded sound.

Other redundant data is present in movies as they contain both images (whose redundancy was described earlier) and sounds, so combining it results in another way of storing encoded data. However, since audio and video files tend to be of much greater size than images, they are used for steganography much less frequently than pictures.

3. Practical application

What about its practical applications? Steganography has a wide variety of uses, especially in the Internet, where there is so much sensitive data (information that no one would like to be available to the public) [WWW5; WWW3], starting with watermarking files that are copyrighted, transactions relying on user authentication, transport of personal information, and there are many more. Talking about transactions, there is a system of authentication using an image that for most people looks just like an ordinary picture, but in reality the user's fingerprint is stored in it, together with a unique session ID to verify and authenticate the transaction session.

Sometimes some personal information has to be sent through an unsecure medium, and steganography makes a fool out of an intruder, because he/she can see the data transmitted but has no idea about the real message covered with some ordinary object. The method is so safe that one can create an offer on an auction portal (for example of used cars or books) with a message encoded into the image. Most people are not interested in thinking about the picture containing some hidden info, and since probably 99.9% of them will not, so why bother?

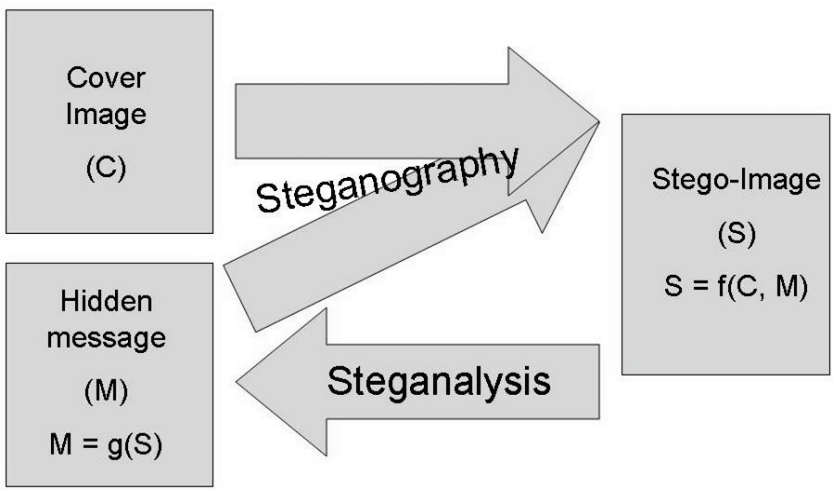

Figure 6. Creating an image with encoded message and converting back

Source: http://www.cse.wustl.edu/~jain/cse571-11/ftp/l_02cet.pdf .

The drawback of the method is that it can be also used maliciously by thieves, burglars, terrorists, hackers, gamblers, drug dealers, pornography sellers, safe crackers, etc. Because of the nature of this method it is particularly difficult to uncover such attempts.

There are a number of software packages that perform steganography on just about any software platform; readers are referred to Neil Johnson's list of

steganography tools at http://www.jjtc.com/Steganography/toolmatrix.htm. Some of the better known packages for Windows NT and Windows 2000 systems include:

- Hide4PGP (http://www.heinz-repp.onlinehome.de/Hide4PGP.htm);
- MP3Stego (http://www.cl.cam.ac.uk/~fapp2/steganography/mp3stego/);
- Stash (http://www.smalleranimals.com/stash.htm);
- Steganos (http://www.steganos.com/english/steganos/download.htm);
- S-Tools (available from http://www.webattack.com/download/dlstools.shtml).

Let us look at a quick overview of the currently available solutions in e-commerce.

StegComm is a great tool for steganographic purposes available at http://www.datamark.com.sg/. From its manual (www.datamark.com.sg/pdf/steganography.pdf) we can read: "StegCommTM is a digital steganography software package developed by DMT for confidential multimedia communication. The software allows the user to select a multimedia data file or "container" for embedding hidden text, audio sequence, video clip, or any form of data file. Many conventional steganography techniques simply incorporate a combination of cryptography and steganography. The cryptography operation is used first to scramble the hidden text. For steganography operation, the scrambled data is then inserted or "hidden" into the least significant bits (LSB) of the container data. One of the common drawbacks of these techniques is that the container file has to be of a certain size greater than the hidden file. Other limitations include the knowledge required about the exact location of the hidden text, the limited container data formats, and the export restriction of using encryption algorithms to certain countries. These difficulties are circumvented by the use of StegCommTM. First, StegCommTM utilises a patent-pending lossless algorithm (the HTTY algorithm) that does not affect the data integrity of the container file. Second, the program is completely independent of the size of the container file relative to that of the hidden file. Third, as steganography is a relatively new field, there are currently no export restrictions on products that incorporate this technology. Another key advantage of the lossless algorithm is the option to select any digital data file from a webpage on the Internet. As the algorithm does not corrupt or overwrite the container file, multimedia data posted on any webpage, such as images (JPEG, GIF), video clips (AVI, MPEG) or audio files (WAV, MIDI), can be selected as the container file. Furthermore, customized container files, such as the voices and images of the sender captured via video conferencing, can be generated very easily. Therefore, the probability of knowing which container file was used during encoding is infinitesimally small. It is almost like "finding a needle in a haystack"

The operations involved in using StegComm™ are illustrated in Figure 7. A multimedia container file is first chosen from the PC hard disk or from a webpage on the Internet. The knowledge of this container file must be pre-determined and communicated securely between the sender and receiver. The algorithm generates a hash file or stegfile from the inputs of the container file and the hidden text. The stegfile contains random data based on a number of mathematical operations between the two input files. The random data bears no data resemblance to either the container

or the hidden file. For example, if a hacker were to intercept this stegfile and perform his/her normal decoding analysis on the data, without the knowledge of the container file, it is virtually impossible for him/her to decode the stegfile. The hidden file can therefore only be decoded if both the container and the stegfile are available at the receiver end. Figure 7 illustrates a graphical user interface (GUI) for StegCommTM.

StegCommTM is currently being marketed in two product versions: Standard and Professional. For some corporate companies, such as banks and financial institutions, as well as government agencies, where data security is of paramount importance, the Professional version offers an additional layer of security by incorporating an encryption solution, such as DES or 3DES, to the stegfile prior to open channel communication. Passwords for both container file and stegfile are also available in the Professional version. However, for SOHO and home users, the Standard version is more than adequate for their day-to-day needs in secure data communication.

Figure 7. GUI of StegComm™ software

Source: [WWW2].

Steganography is also effective in authenticating clients in the network. An example of an application that combines steganography with digital authentication (electronic signature) is StegSign^{TM} application. This application can hide details of the company, or other confidential documents in different type files (at least in emails, text documents, etc.). Thus, if someone has tampered this will interfere with file transfers with such hidden data, those receiving and sending these files will be informed (e.g. when sending commercial information during negotiations). Figure 8 shows the main window of the StegSign^{TM} application.

StegSign^{TM} application can also be used to protect against unauthorized access to data. An example of this type of application may be e-banking, where the electronic signature authenticates both the bank and the customer.

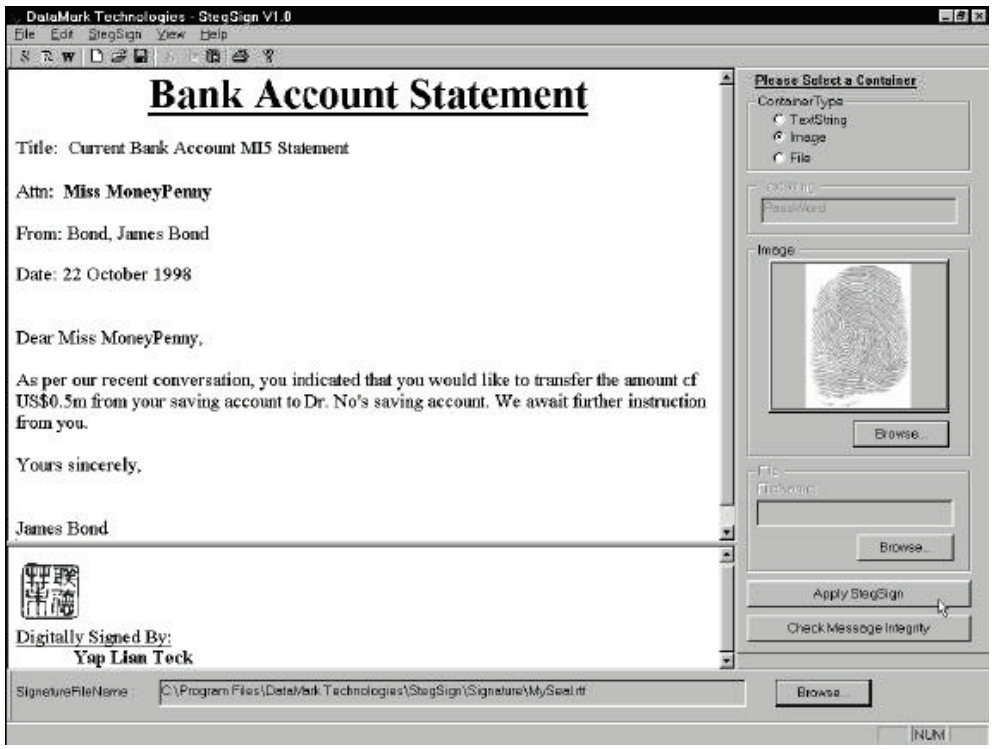

Figure 8. StegSignTM application window using in e-banking

Source: [WWW2].

Another application with the task of protection of copyright is a DRM (Digital Rights Man-agement). This system enables the following actions:

- protection of various multimedia content from users who are using them in a manner inconsistent with the objectives of the supplier,
- controlling the accesses to the digital data.

Rights that are granted by the authors of various multimedia content, among others, are:

- change of file formats,
- the possibility of replay,
- copying.

Before transferring the media file to the recipient, it already is in the DRM system protected against reading. Only having a license gives the possibility of its restoration. To obtain a license and generate the decryption key, use the program used to play media files. To prevent the restora-tion process and preserve the secrecy of its details, you should use a number of safeguards that make it difficult to know how the program works. It is only guaranteed safe at the end, as evidenced by programs that easily allows you to bypass the security features of DRM systems. In order that a user can get a license he/she must satisfy many fixed conditions. The most commonly used condition is the payment of charges for the file.

On the market there are many applications that allow you to implement the DRM system hindquarters. An example of such an application is a Microsoft product called Windows Media DRM. This platform allows for the security and protection of multimedia content that are sent to customers. It also allows you to play multimedia content on the web and mobile devices, as well as the usual PC-type computers.

4. Conclusion

Steganography has a significant application in e-commerce. It allows the security of data, which may be generally available (e.g. promotional mp3 encouraging one to buy the whole CD audio). Hiding information also gives a new effective method of protecting and enforcement of copyrights and licenses. Hidden information can be used to confirm important business transactions and user authentication. Using steganography, one can secure data without arousing suspicion that something important is in the file – in contrast to cryptography, where if something is encrypted, it must be important.

References

Cox I., Miller M., Bloom J., Fredric J., Kalker T., *Digital Watermarking and Steganography*, 2nd edi-ton, 2009, electronic free book http://www.freeebookdownload.co.in/ebooks/free-ebook-Digital-Watermarking-and-Steganography-2nd-Ed-The-Morgan-Kaufmann-Series-in-Multimedia-Information-and-Systems--download.

Meghanathan N., Nayak L., Steganalysis algorithms for detecting the hidden information in image, audio and video cover media*, International Journal of Network Security & Its Application* (IJNSA) 2010, Vol. 2, No.1, January.

Wayner P., *Disappearing Cryptography. Information Hiding: Steganography & Watermarking*, 3rd edi-tion, MK/Morgan Kaufmann Publishers, Amsterdam 2009.

Websites

[WWW1] http://www.bdebuy.com/print_page_p1298
[WWW2] www.datamark.com.sg/pdf/steganography.pdf
[WWW3] http:\\users.finemedia.pl/dloogie/bezpieczenstwo/stegangrafia.pdf
[WWW4] http://www.microsoft.com/poland/msp/dobierz-licencje.aspx
[WWW5] http://www.pcmag.com/encyclopedia_term/0,2542,t=Windows+Media+Rights+Manager&i=54664,00.asp

TECHINIKI UKRYWANIA DANYCH W E-HANDLU

Streszczenie: Rozwój informatyki i sprzętu komputerowego w drugiej połowie XX wieku spowodował, że sposób przekazywania informacji stał się prostszy, wygodniejszy oraz bardziej niezależny. Przykładem tego postępu jest handel elektroniczny (*e-commerce*), który dzięki rozwojowi sieci komputerowych, a zwłaszcza Internetu, stał się bardzo popularnym sposobem przeprowadzania różnych transakcji. O zabezpieczanie tych transakcji muszą dbać zarówno użytkownicy małego biura, jak i wielkiej korporacji. W artykule omówiono szczegółowo zastosowanie cyfrowej steganografii dla zapewnienia bezpieczeństwa informacji w różnych aplikacjach *e-commerce* działających za pośrednictwem Internetu. Aplikacje te realizują tak ważne zadania, jak: poufne przekazywanie dokumentów, uwierzytelnianie podpisu cyfrowego i zatwierdzanie elektronicznych dokumentów, przechowywanie cyfrowych danych oraz bezpieczne przekazywanie multimedialnych danych za pośrednictwem otwartych kanałów.

Słowa kluczowe: steganografia, bezpieczeństwo, handel elektroniczny.