International Journal of Security and Its Applications
Vol. 11, No. 4 (2017), pp.71-84
http://dx.doi.org/10.14257/ijsia.2017.10.4.06

Steganography and Data Loss Prevention: An overlooked risk?

Juan M. Gutiérrez-Cárdenas

Universidad de Lima, Peru
jmgutier@ulima.edu.pe

Abstract

Steganography is the art or science of hiding information into a carrier in such a way that the hidden data could not be detected at first sight. Steganography techniques have broadened their scope of action, from hiding information into picture media, to audio steganography and to the field of network steganography. All these methods entail a potential threat to the information security policies of any business; having into the data leakage threats its likely focus. In this scenario, business corporations cannot remain blind to these types of threats and should consider adequate policies and prevention techniques to avoid these risks. We have analyzed in this article the potential dangers that an organization could face in the light of these types of steganography techniques along with a review of current commercial software vendors to analyze their offers and mishaps on Data Leakage Prevention regarding steganography risks.

Keywords*: Steganography, Steganalysis, Data Leakage, Data Loss Prevention*

1. Introduction

In this section, we describe some basics techniques in the field of steganography. Its counterpart, steganalysis, comprises the set of procedures that allow the detection of a stego object or, which is more difficult, the disclosure of the information hidden in digital media. We will also analyze a trend known as Network Steganography in which by the manipulation of the remaining parts of packages or even by the use of covert channels in communication scenarios, it is possible to send concealed information between subjects.

The primary purpose of this research is to analyze how Steganography techniques could be used for disclosure of relevant or sensible information outside and organization frontiers without permission; and how there are little attempts to overcome this potential threat by IT security vendors related to the field of Data Loss Prevention.

This paper is divided into the following sections: First, we will make a brief description of the areas of Steganography, its variants such as Network Steganography and techniques made to overcome them known as Steganalysis. Then we will analyze the main software vendors trends related to the field of protection of Data Leakage in an organization. Also, we will show some advances made by Government parties concerned about this new form of threat and then end with some recommendations and conclusions.

1.1. Steganography and Steganalysis

Steganography deals with the conceal of information into an image that receives the name of cover image. The hidden message could be encrypted to strengthen its security, but one of its primary goals is to try to maintain the statistical properties of the cover image. In its basic form, a stego object should not bring suspicious that it is hidden some data on it [2], see Figure 1 for a succinct description of a steganographic process. In some cases, the encryption of the hidden message requires the exchange of a stego key. The transmission of this key which is made beforehand could raise suspicion of the transfer of a stego object [16].

ISSN: 1738-9976 IJSIA

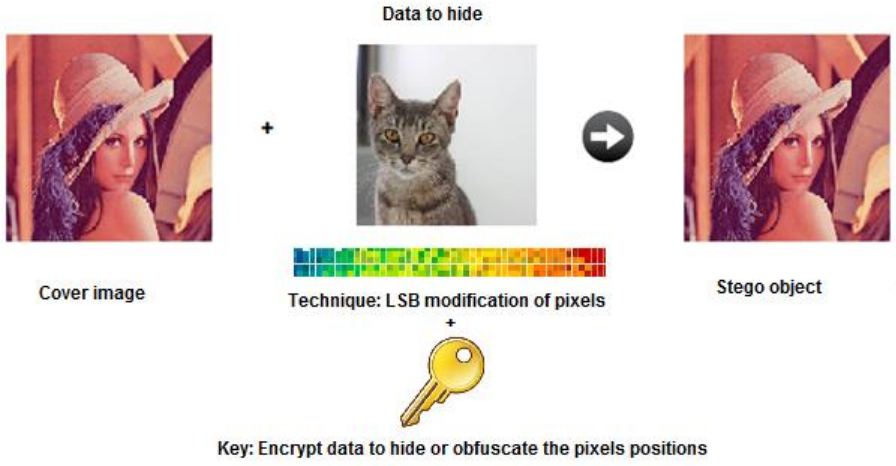

Figure 1. Steganographic Model Based on the Technique of LSB Modification. A Key is Transmitted Along with the Cover Image to a Recipient that Deploys the Hidden Message Present in the Cover Image

One of the simplest ways of generating a stego object is the modification of the Least Significant Bits (LSB) that form part of the pixels of the cover image [9, 20, 30]. In this algorithm the alteration of the LSB bits of a picture keeps the original or cover image, at mere sight, unmodified giving the impression that it does not carry any concealed information on it [2]. This technique falls into the category of a substitution method [16]. Another approach consists in lowering the values of a part of the pixels while raising the values of another set of pixels; this process is known as masking. A more robust technique uses the discrete cosine transform or wavelet transforms of part of the images [9] allowing that the statistical characteristics of the cover image are kept almost unchanged. Let us recall that minimal deviation or manipulation of the statistical properties of the cover image will result in a stronger steganography schemata, not susceptible to detection at first inspection.

Steganalysis refers to the discovery of methods that allows the detection of concealed information inside a cover image. There are several ways in which to perform a steganalysis procedure. For example, in a hypothetical scenario, an investigator could have suspicions that a digital object has hidden material, so he deploys a set of algorithms to try to uncover it. This form of steganalysis receives the name of blind steganalysis. Targeted steganalysis refers when the person has knowledge about the probable algorithm used [2]. This type of attacks are divided in a) Chosen stego attack, when the algorithm and stego object are available. b) Chosen message, when there is the generation of a stego object in an attempt to know the algorithm that produces it; and c) Known stego object, in which the cover, stego object, and algorithm are known [16, 22]. Of the techniques mentioned earlier the one that represents quite an effort is in a blind steganalysis scenario. One of the main weaknesses that all steganography methods have is that even with a little suspicion of its presence; this could lead to the elimination of the stego object in an attempt to eliminate the threat [9]; neglecting the recovery of the concealed message which could be useful for further investigating purposes.

1.2. Network Steganography

In network steganography, the hidden information can be covered and transmitted by different protocols, such as FTP, P2P networks among others [11]. Other forms are the concealed of information inside spam messages [26], which as we know are texts easily neglected by the receiver, but nevertheless, could contain stego information inside of it

[10, 16, 20]. The characteristic of a spam message makes it a convenient subject to hide information. Mainly, because forensics investigators usually underestimate the importance of this material. The strength of using a combination of spam messaging and steganography [26] is that the cover object can out force some filtering processes. In this case, according to the authors, this converts it into a suitable way to deliver information to an external party without being noticeable by an investigator. The cases described in [26] pointed more to those related to sexual offenders, but we can argue that the same technique could be used for hiding sensitive information of an organization, and that a person could send this information by utilizing a combination of steganography and spam messages outside the borders of the institution. The damages of these actions could be moderate if the process continues for an extended period without being noticeable.

A basic form of network steganography consists in the modification of the IP headers over a network communication allowing the insertion of concealed data on them [20]. This alteration would have its simile on the simple substitution method known as LSB modification of images that we mentioned in the preceding section.

Network stego techniques rely on changes of the contents that form part of the different layers of the OSI network subdivisions. For example in the physical layer, the modifications can be performed on the communication channels or in the correction codes to hide data; while in the network layer the alteration of packages –headers or unused parts such as flags – can be used for the concealing purposes [11]. In the application layer, the information can be hidden in HTML headers or other formats [11, 16]. As we can observe, each layer can be prone to become a modifiable part for steganographic purposes.

According to Lubacz *et al.* [11], three conditions should exist so that a method could be considered in the field of Network Steganography. These conditions deal with the different levels of the OSI (Open Systems Interconnection) and are the following:

Condition 1: Modifications in the communications protocols. In this point, for example, we can consider the study of Van Horenbeeck [15]. In his study, a system was the objective of a profound control to determine which electronic devices enter or leave a security perimeter. Also, a set of safety measures was displayed such as the use of firewalls that rewrote the contents of the TCP/IP headers and the modification of the address control of DNS. Even though with all these measures, the authors found that by allowing the connectivity via HTTP for web browsing, these HTTP headers could form part of a set of probably hidden channels.

Condition 2: Modifications based on the inherent errors that can be present in the protocols; the alteration of the protocols that deal with the exchange of information or the transmission of messages.

Condition 3: The likely effects that could be brought up by these modifications should be monitored to check if they could be detected or not. According to Lubacz *et al.* [11], these triplet of conditions are essential for the existence of a network steganography based method.

Network steganography is a growing field that should raise particular attention, mainly because classical anti-malware filters and firewalls could be skipped by steganography techniques [30]. The difficulty arises when there is an absence of characteristic signatures that these threats leave. These drawbacks would also limit the set of solutions or policies that a TI in charge office would consider for their implementation into the security schemata of an organization; congregated in the lack of forensics information.

Another issue comprises the action of monitoring the communications in an organization and the limitation of bandwidth resources to the users. The former could have legal issues dealing privacy concerns from the users. Besides, the cancellation or bandwidth shortened of communication channels could diminish the transportation of information inside an organization, becoming more a nuisance than a solution.

1.3. Hidden Channels

It is valuable to consider also the case in which we two parties establish a covert mean of communication known as a Hidden Channel. In data communication, a couple of subjects, A and B, establish a protocol to start transferring data among them. The transferred data can be black of potential attacks, ranging from the message interception to the probable posterior modification of the original data. This attack is made by a third party and gives origin to an attack known as the "man-in-the-middle" attack. As a result of this problem many cryptographic algorithms to conceal and protect the data were developed, even though a potential attack can always be a matter of concern.

An alternative scenario occurs when both parties agree to start a protocol that could be censorable or even could be related to valuable information of an organization. In this case apart from the establishment of a protocol is necessary the use of what is known as a Hidden Channel of communication. In this scenario, the covert channel could be concealed within the standard bandwidth of an organization, but the use of alternative methods such as the utilization of steganography can be considered as a hidden channel [20]. If we recall the main idea behind a steganography technique is to hide information inside another digital object, this cover object acts or can also be considered as a type of hidden channel.

Steganography, Network Steganography and the use of Hidden Channels for transporting information, censorable or valuable for an organization, can be a potential threat increased by the difficulties that inhere their detection or prevention in an organization.

2. Data Loss Prevention

Data Leakage Prevention or Data Loss Prevention refers when the information within a corporation is by accident or intentionally spread outside the boundaries of an institution [3, 21], and is a general concern for any organization [21].

According to [3, 19], this problem suffered a growth in its spread, because of the ways that data is transmitted nowadays and by the presence of different communication networks and protocols; thus allowing even the existence of covert or hidden channels of communication [20].

A well-known and mediatic case that put on trial the consequences that a Data Leakage scenario could bring was the Wikileaks case. The Wikileaks case exposed how the sensible data of a government could be put at risk, and also to raise the discussion about media censorship; besides the transparency that a government should have related to the disclosure of information to the public was also brought into discussion [18]. This case was only a sample of the dangers that could entail the non-authorized and the efficient use of the information at higher government levels.

For example; we consider the case in which a person that has access to sensible data inside an organization can use steganography methods to conceal that information and transfer it to a third-party. It is valuable to mention that for this article, and because the third party is intentionally using a steganography technique to conceal data, we are not considering the situation of data loss due to an unexpected scenario. Of all the challenges that DLPs tools have to deal nowadays regarding: audit of data in transit and in rest, policies, social scenarios, context and content analysis and so on. We hypothesize that the use of steganography -maybe joined with cryptography techniques- could be a new issue that current and future DLPs software will have to confront [21].

We can think about the possible dangers that the use of a steganography tool could impose for an organization, and also how easy would be to bypass a DLP detection mechanism. In the case of an encrypted document, this threat could also circumvent a DLP detection tool when we sent a document, for example, by email [21]. Considering this danger, one could argue that cryptographic methods could also represent a peril for

hiding sensitive information and for transporting it to third-parties. Nevertheless, we should remember that crypto material could be spotted, at first sight, a situation that does not occur with steganographic material, which conceals the data into what we can call an "innocent" carrier or media.

A potential attacker could have at hand many techniques, such as steganography or watermarking, in which the potential threat is not easily visible on first inspection; and thus bringing up the possibility of a DLP scenario. For this reason, the strict adherence to policies, towards these steganographic risks, that could enforce and diminish the peril of Data Leakage should be a must in organization nowadays. These set of policies, for example, could refer to the elimination of data that it does not adhere to the needs of the organization [3] along with traffic control of information. In the latter case; the destruction of potential files that could content steganography information and that are not needed to be transmitted inside or outside the organization could represent a way to contain steganography risks. Even though it is somewhat impossible to keep track of all the information media that travels within and outside a corporation, and detection of modified files or even the destruction or censorship of what data is transmitted could represent legal issues for the institution that reinforces those policies. In any case, it seems very improbable that there would be a banned use of steganography tools, but the organization could put some burdens for the software that is installed by users within it [6].

According to [21] are some institutions that have studied the problem of DLP such as SANS, Securosis, and ISACA. SANS in a whitepaper [14] established the possibility that some workers could be bribed, so they will be tempted to share sensible information to a third party by using steganography means. Unfortunately, the other institutions do not mention a connection between steganography and data loss prevention, apart from some theoretical information about this method of concealing information.

A set of measures for avoiding Data Loss, related to steganography, are oriented to the use of Machine Learning or Statistical techniques [2, 3] to detect if a file has been forged hiding information on it. These techniques present their limitations, such as in the case in which it is not possible to find the alteration of statistical patterns [17]. Even machine learning techniques would need a set of modified files to be used for comparison or training purposes. In such a way, that we could perform a successful blind steganalysis attack. As we can observe the techniques are available, in some way with their limitations, but these should be in conjunction with an adequate set of policies maybe aided with the development of software stego pipelines that could perform different attacks on suspicious files that are transmitted in and out an organization.

3. Risks of Steganography Concerning DLP

The risk that entails the use of stenographic techniques are diverse. They can be use – as it was only a suspicion – to carry on terrorist attacks [2, 13, 25] or to transfer illicit media material. In the case of businesses, it could be used to steal organization information to be commercialized to potential competitors or that sensitive information could be transferred to a third-party [6]. A realistic scenario in which this procedure could take place was described by [30] by hiding information within a company logo and transfer secret information between departments in an organization. Some solutions proposed in [30] were to compare the hash values of the logo or make a surveillance of the network traffic in an organization. Other measures would be to compare the duplicate colors into a picture or to uncompress and compress an image into different formats, *i.e.*, bmp to jpeg [6]. In any case, the advent of new forms of steganography techniques can prove these attempts to be fruitless. Also, another factor to consider would be the inherent difficulty in auditing all the information traffic inside an organization along with the communication channels and so forth due to the size of business.

The strength of steganography, as opposed to other techniques such as cryptography, resides in the almost impossibility to detect it at first inspection; and even with the use of statistical techniques like the ones used in blind steganography [17], the results could not be satisfactory at all.

A study made by Provos and Honeyman [17] in which they downloaded two million images from the Internet to detect if steganographic techniques have altered them in an attempt to show the importance of this technique. The tool the authors developed was named as Stegadetect and consisted of software that searches for statistical patterns or signatures that can be found on an altered image in the Discrete Cosine Transform (DCT) used in JPEG files for compression purposes [2]. The study mentioned that they did not manage to find any hidden message into the set of downloaded images tested by Stegadetect, but one can hypothesize that maybe the steganalysis technique used was not the suitable one, this reinforced by the fact that the number of steganographic methods is diverse.

Other techniques try to search if there are steganographic materials within email traveling thru and outside an organization by using a pipeline of different steganalysis techniques such as signature, blind steganalysis and LSB modifications [29]. Even though, one should consider, that some steganography algorithms are immune to statistical analysis and blind steganalysis in the lack of the source to perform an accurate comparison for checking for a payload.

Considering the use of machine learning techniques for deploying a blind steganalysis attack, what we need is a set of samples that could aid for the training stage as in any supervised learning algorithm [2]. As we mentioned before, one biggest problem that the Steganalysis techniques have to deal with is that some steganography techniques do not form patterns or make a profound alteration of the statistical properties of the image used as a cover image. In this scenario, its detection is harder and forces the analyst to use different algorithms in an attempt to detect it. The failure of these techniques resides that these algorithmic and statistical techniques are tailored solutions for specific types of steganographic tools.

The benefits for an attacker of using a steganographic technique are tempting: ranging from a set of various methods, the almost impossibility to perform blind steganalysis attacks as we established before and the assurance of the anonymity between parties [13] that could be involved in a case of DLP.

Steganography media need to be transmitted, so, for example, the measure of analyzing if a social network deviates from their usual pattern of communication [19], could also serve to block this material to travel within or outside an organization. If it is not possible to block all media material flowing outside our boundaries, the modification of the media, *e.g.*, images, on purpose could destroy any hidden message that it could conceal [27].

The work made by [24] establishes a potential threat scenario to the internal information assets of an organization. In the schemata proposed, see Figure 2, an external attacker contracts a person within the organization for its illegal purposes. The person inside the organization uses steganographic tools for concealing the data and transfers it by using a cover wireless channel. The person in charge of the information security inside the organization should deploy a set of countermeasures that range from policies, ban of certain types of IT related activities and a set of steganalysis techniques that could aid in the detection of stego material [24]. As we established before the ban of activities or the interception of communications could bring legal issues. Also, the set of steganographic content is diverse, so the uses of steganalysis techniques are made ad-hoc for some types of attacks. Nevertheless, we can observe that a potential Data Leakage scenario is somewhat possible given the right conditions: disloyalty of the personal, use of non-restricted software and use of covert channels.

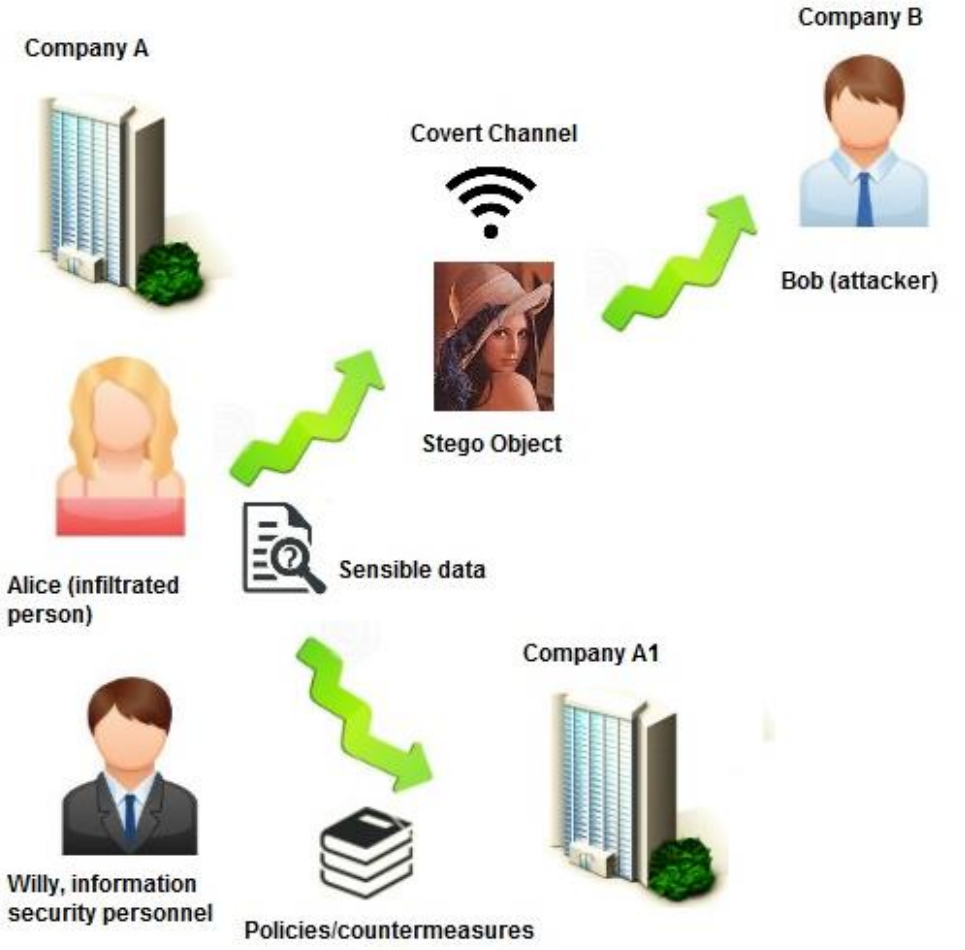

Figure 2. Schemata Showing how an Attacker (Bob) Infiltrates a Person Into a Target Organization (Alice). The Infiltrated Person Uses Steganographic Methods to Conceal Relevant Information and Sends the Stego Object to the Attacker by Using a Covert Channel. The Labour of a Security Auditor Would be to apply the Necessary Countermeasures and Use Steganalysis Techniques to avoid this Type of Attacks

At this point we should question ourselves if all the forms of steganography could possess a harm to a business organization; the straight answer would be that no. In the work of [28] Sueyosh and Tadiparthi [28], there is the proposal of using a steganography technique based on the derivation of a non-finite deterministic automaton that allows hiding a message, encoded by using Run-length encoding and using a sequence of animation frames. This technique was used in a simulated scenario in Toyota corporation, in which a designer needs to use the Internet to transfer his designs, but in such a way that if the message is intercepted the attacker would have a minimum possibility to discover them. An interesting use of what the author calls an offensive use of steganography [28].

Other ways in which steganography has proven to be useful is in a data forensics scenario, specifically in the preservation of log-files in such a way that the original version is kept unaltered by hiding it into a cover image by using a simple LSB technique [23, 31]. This scenario allows comparing the preserved log-file with a probably altered file so traces of a probable attack could be monitored.

In the following section, we will describe some major technology providers and their solutions related to DLP. We will examine if some of them consider steganography as a

threat to DLP and how they deal with it. For this analysis, we will use the Gartner Magic Quadrant of DLP, and we will observe that there has been a marked difference, related to a diminish in solutions that integrate DLP with steganography since 2013 to the current year.

3.1. Enterprise Main Players

Different solutions for DLP exist in the market that tries to ameliorate the risks for an organization of these hazards [19]. These software tools mainly inspect and audit the data when this in rest or in traffic [19], examining the content and context where the flow of data occurs, but apart from this IT sectors efforts, the real conceptualization of DLP is still vague [21].

In this section, we will analyze the leading software vendors that deal with Data Loss Prevention, for this purposes we are going to use the Gartner's Magic Quadrant for Content-Aware Data Loss Prevention [8]. We will revise the feasible DLP solutions from leaders, challengers, visionaries and niche players according to the reference mentioned above. In the following list we are reviewing a set of information security companies along with their proposals referred to the field of steganography, see Figure 3:

Figure 3. Magic Quadrant of Gartner, in this Scenario we show the Main Providers of Software Solutions in the Field of Enterprise Data Loss Prevention

In Figure 3, we can appreciate the four sections in which is divided the Magic Quadrant of Gartner related to Data Loss Prevention. Gartner divides this square into four subsections that are Leaders, Challengers, Niche Players, and Visionaries. According to Gartner [8], this division gives us some insights about the main competitors in the field. Some more details about this classification are the meaning of the subsections that we can see in Figure 2. These are: a) Leaders, which are those businesses that are well positioned in a particular area of study; b) the Challengers know the market trends and can be able to

push the market in a specific direction, but they have some drawbacks in the strategies they follow; c) the Niche players occupy a small segment of the market, but they do not represent a dominant part of it, and finally d) the Visionaries which are those companies that can manage a huge market sector, but that they present some inconsistencies related to knowledge of the different market trends.

We will analyze different organizations that appear in the four quadrants of the Gartner magic square to see if they consider steganography threats related to DLP. The analyzed results are:

Table 1. Results of the Main DLP Vendors of the Gartner Magic Square

Leaders	
Company	**Results**
Symantec	The information available relates to a question posted in a forum in Symantec about if it was possible to detect steganography in DLP (https://www.symantec.com/connect/forums/steganography-and-dlp). No official answer was given about this subject.
Forcepoint	No information available/considered.
Digital Guardian	No information available/considered.
Intel Security	No information available/considered.
Challengers	
Company	**Results**
There were no challengers in this version of the magic quadrant	No information available/considered.
Niche Players	
Company	**Results**
Clearswift	No information available/considered.
InfoWatch	No information available/considered.
Somansa	No information available/considered.
Zecurion	No information available/considered.
Visionaries	
Company	**Results**
GTB Technologies	No information available/considered.
Fidelis Security Systems	It has a partnership with Backbone Security related to software solutions that could detect which stenography tool has been used for information hiding. This information tool uses the fingerprint technique for achieving its purposes (available at http://www.prweb.com/releases/fidelis/fidelissecurity/prweb3893514.htm)

As we can conclude from the previous information, only one company has a solution that considers steganography as a threat; this decrease is marked compared to the results given by the same Gartner Magic Square of 2013 and 2011 as we will see in the Table 2 and Figure 4.

Table 2. Results of the Main DLP Vendors of the Gartner Magic Square 2 (Version of 2013 with Data Added from the Version of 2011)

Leaders	
Company	**Results**
Mcafee	It forms part of what is called a Security Innovation Alliance (SIA) in which various partners are assessed regarding technology or management to form part of their team. For steganography threats, those are enclosed into the Theft and Forensics Division with partners such as Def-Logic, Nuix, Raytheon as associate partners and HBGary and Blue Coat as their technology counterparts (available at http://www.mcafee.com/us/partners/security-innovation-alliance/sia-partner-by-solution.aspx).
CA Technologies	No information available/considered.
RSA (EMC)	No information available/considered.
Websense	Offers an AP-Data Administrator Course as part of its Triton policies, not so much information about the techniques used are mentioned (available at http://www.websense.com/content/support/library/data/v80/policy_classifier/DSSpolicyclassifier.pdf)
Verdasys/Digital Guardian	No information available/considered besides of an article that mentions steganography treats related to the extraction of non-authorized information (available at https://digitalguardian.com/blog/data-theft-exception-or-rule)
Challengers	
Company	**Results**
There were no challengers in this version of the magic quadrant	No information available/considered.
Niche Players	
Company	**Results**
Trustwave	No information available/considered apart from a blog article in which it mentions that the suspicious that Al Qaeda has used steganography content for their terrorist attacks was only a hype, because of not having enough evidence to support this claims (available at https://www.trustwave.com/Resources/SpiderLabs-Blog/Hackers-and-Media-Hype--Big-Hacks-that-Never-Really-Happened/)
Code Green Networks	No information available/considered.
Trendmicro	No information available/considered. A blog post mentions information about malware was hidden in JPEG images; this trojan was named as ZeusVM (available at http://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware-why-and-how/). Also, another blog entrance describes how an image, using steganography, can hide Command & Control instructions by obfuscating them (available at: http://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware-concealing-code-and-cc-traffic/) ; this type of actions can be a threat for data loss prevention if we consider the existence of hidden channels as we mentioned in Section 1.3
Safend	No information available/considered.
Palisade Systems	No information available/considered.
InfoWatch	See Table 1
Absolute Software	No information available/considered.
Zecurion	See Table 1
Visionaries	
Company	**Results**
GTB Technologies	See Table 1
Fidelis Security Systems	See Table 1

Figure 4. Gartner Magic Quadrant of Data Loss Prevention Providers, this Version, Circa 2013 (Available at: https://philipcao.com/2014/04/26/gartner-magic-quadrant-2013/), had a Certain Number of Organizations Concerned about Steganography as a Risk in Data Leakage Scenario (As Seen on Table 1.). The Firms Trendmicro, Safend and Palisade Systems which Appeared on 2011 have been Added to the Picture (Available at: http://www.etruserve.com.tw/gtb/GTB%20wp/rp-gartner-magic-quadrant-dlp-2011.pdf)

We can observe from the above list, Table 2, that only three companies: Mcafee, Websense, and Fidelis developed software tools and policies related to steganography risks dealing with Data Leakage Prevention. Most of the security providers only enforce the policy counterpart for avoiding the leakage of information to external sources [29]. Other companies that do not appear in the Gartner´s Magic Quadrant such as Wetstone Technologies that provide courses related to forensic analysis that deals with steganography techniques and detection [20, 30]. Among them other independent software tools that could perform steganalysis techniques such as Stegdectect [17] which uses a signature detection system; StegoSuite, which uses statistical analysis; Steganography Analyzer Signature Scanner, that searches for hexadecimal signatures or PixAlert that is used for detecting illegal images [20]. As we can see, there is a plethora of algorithms and techniques that could aid in the detection of stenographic content in various sources.

It is uncertain why steganography it is not quite seen as a risk for the cases of information theft within organizations. We believe that a reason could be that the

techniques for performing steganalysis are rather limited mainly in the cases of blind steganalysis; or just because there have not been so many documented threats that could make them represent a real risk for the vulnerable information that a company has. Also, a lack of adequate of information and training could enforce the problematic of non-awareness [20]. Even though, as we will see in the following section, this threat has raised the attention of the National Institute of Standards and Technology (NIST).

3.2. Government Proposals

a) NIST Special Publication

The National Institute of Standards and Technology (NIST) published on 2013 a particular set of policies entitled "Security and Privacy Controls for Federal Information Systems and Organizations". Here we can find that the inclusion of a section related to steganography. This item is in the chapter concerning to "Boundary Protection-Prevent unauthorized exfiltration" [12]. In this section, steganography is considered as a threat that could devise into the extraction of information from an information systems context. The section related to "Malicious Code Protection" considers that steganography techniques could be used for hiding malware into files that could affect an information systems environment. Also, the item related to "Information Systems Monitoring" considers that steganography could be used for extracting information outside the boundaries of a given organization. The NIST organization also maintains a list of digital signatures of steganography software [16]. As we can observe there is a slow increase in the interest of the risks that these hiding techniques could address to any organization that uses information systems. Threats are related mainly to extraction or disclosure of private information thru the use of malware to infect or also to steal valuable data and transport it outside the boundaries of a corporation.

From the information gathered in this brief article, we can notice that there are only a few attempts to consider steganography like a real risk for data theft inside an organization. The interest from the NIST to include a section about this hidden technique might bring more concern into the development of new policies and software tools that could aid in the detection of altered media with the purpose of hiding information.

a) Other Regulatory Policies: BS 7799

Trcek [5] mentions Security Policies as a form that an organization has to control security inside an organization, and establishes Access Control as a sub-task within this Security Policies. Trcek considers the Access Control related to the code of practice which are a set of policies stated by the BS-7799 (available at: http://www.infosectoday.com/ Articles/27001.htm) – which later derived to the ISO ISO/IEC 27002 [7]- that if followed will help in the elaboration of sound security policies. The Access control, considered within this normative, is defined as the set of policies that enforce the security in networked services, limit connections for applications that entail a high risk among others [5]. The author also pinpoints the importance that sensitive information should not be transported to lower levels, and this should also be made in a horizontal fashion; making this form of practical information being tailored for organizations that follow a hierarchical model. It is interesting how the author mentions that steganography should be considered also as a threat in the Access Control Policies schemata. Unfortunately, no more information is given about how to implement security policies related to it.

4. Recommendations

Steganography techniques indeed could represent a risk for the information assets of an organization. It is relatively simple to hide information into another media by using any of

the available software tools that are mostly freeware over the Internet. We believe that measures related to the enforcement of policies within an organization that allows more control the transmitted media could be fruitful in the short term. The creation of software pipelines with different steganalysis algorithms should be developed and deployed to monitor the information that is transmitted inside and outside an organization, and if these solutions are not available from a private vendor, these should be developed and implemented by the corporations themselves. The risks of confidentiality breakages, derived from the inspection of transmitted items, should be explicitly specified within the companies policies in the way of avoiding legal issues between employers and employees also.

5. Conclusions

Steganography algorithms refer to the hide of information within digital media. The information concealed could be vulnerable information for an organization to malware that could endanger the systems of an institution, and at the end resulting in a Data Leakage or Data Loss scenario. Even though there have been developed many steganalysis, as a counterpart of steganographic techniques, these algorithms seem rather limited. This limitation is visible by a lack of an offer from Information Security companies that could provide them with packages in the same way as it is provided other security tools. The develop and implementation of policies and software pipelines that allow the detection of steganographic items should be considered as a vital part of avoiding the non-authorized extraction or invasion of malware software outside and inside any organization.

References

[1] A. Cheddad, J. Condell, K. Curran and P. McKevitt, "Digital image steganography: Survey and analysis of current methods", Signal Process., vol. 90, **(2010)**, pp. 727-752.
[2] A. Rocha, W. Scheirer, T. E. Boult and S. Goldenstein, "Vision of the unseen: Current trends and challenges in digital image and video forensics", ACM Comput. Surveys, vol. 43, **(2011)**, pp. 1-42.
[3] A. Shabtai, Y. Elovici and L. Rokach, "A survey of data leakage detection and prevention solutions", Springer, **(2012)**.
[4] A. Siper, R. Farley and C. Lombardo, "The Rise of Steganography", Proceedings of Student/Faculty Research Day, CSIS, Pace University, **(2005)** May 6.
[5] D. Trèek, "An integral framework for information systems security management", Elsevier's Computers and Security 22, **(2003)** May 4, pp. 337-360.
[6] E. Cole and S. Ring, "Insider Threat Protecting the Enterprise from Sabotage, Spying, and Theft", Chapter 2, Elsevier, **(2006)**.
[7] E. Lachapelle and M. Bislimi, "Whitepaper: ISO/IEC 27002:2013 Information technology, security techniques, code of practice for information security management", Parabellum Cyber Security. Retrieved from: http://zih.hr/sites/zih.hr/files/cr-collections/3/iso27002.pdf, **(2016)**.
[8] Gartner: Research Methodologies. (2016). Retrieved August 30, 2016, from http://www.gartner.com/technology/research/methodologies/research_mq.jsp.
[9] H. Wang and S. Wang, "Cyber warfare: steganography vs. steganalysis", Communication of the ACM, vol. 47, no. 10, **(2004)**, pp. 76-82.
[10] J. Hally, "Steganography, what is the real risk?", SANS Institute. Retrieved from: https://www.sans.org/reading-room/whitepapers/stenganography/steganography-whats-real-risk-555 14, **(2002)**.
[11] J. Lubacz, W. Mazurczyk and K. Szczypiorski, "Principles and overview of network steganography", IEEE Commun. Mag., vol. 52, no. 5, **(2014)**, pp. 225-229.
[12] J. T. Force and T. Initiative, "Security and privacy controls for federal information systems and organizations", NIST Spec. Publ. 800, **(2013)**, 53.
[13] K. Choudhary, "Image Steganography and Global Terrorism", International Journal of Scientific & Engineering Research, ISSN 2229-5518, vol. 3, is. 7, **(2012)**, pp. 1-12.
[14] L. McGill, "Steganography: The Right Way", (2001), SANS Institute. Retrieved from: https://www.sans.org/reading-room/whitepapers/stenganography/steganography-1584.
[15] M. Van Horenbeeck, "Deception on the network: thinking differently about covert channels", Australian Information Warfare and Security Conference, (2006).

[16] M. Warkentin, E. Bekkering and M. B. Schmidt, “Steganography: Forensic, Security, and Legal Issues”, Journal of Digital Forensics, Security and Law, vol. 3, no. 2, **(2008)**, pp. 17-34.
[17] N. Provos and P. Honeyman, “Detecting Steganographic Content on the Internet”, Proc. 2002 Network and Distributed System Security Symp., Internet Soc., **(2002)**.
[18] P. Karhula, “What is the Effect of WikiLeaks for Freedom of Information?”, IFLA, (2011), February 28, Retrieved August 9, 2016 from http://www.ifla.org/en/publications/what-is-the-effect-of-wikileaks-forfreedom-of-information
[19] P. Raman, H. G. Kayacık and A. Somayaji, “Understanding Data Leak Prevention”, 6th Annual Symposium on Information Assurance (ASIA’11), **(2011)**, pp. 27.
[20] R. C. Newman, “Covert computer and network communications”, InfoSecCD ’07, **(2007)** September, pp. 1-8.
[21] S. Alneyadi, E. Sithirasenan and V. Muthukkumarasamy, “A Survey on Data Leakage Prevention Systems”, Journal Netw. Comput. Appl., vol. 62, **(2016)**, pp. 137-152.
[22] S. Katzenbeisser, “Information hiding techniques for steganography and digital watermarking”, Artech House Books, **(1999)**.
[23] S. Khan and A. Gani, “Network Forensics: Review, Taxonomy, and Open Challenges”, Journals Netw. Comput. Appl., vol. 66, **(2016)**, pp. 214-235.
[24] S. Stanev, H. Hristov and D. Dimanova, “Aproaches for Stego Defense of Sensitive Information from Inside Leakage”, Journal Science Education Innovation, vol. 1, **(2013)**, pp. 126-133.
[25] S. E. Goodman, J. C. Kirk, M. H. Kirk, “Cyberspace as a medium for terrorists”, Technol. Forecast. Soc. Chang, vol. 74, **(2007)**, pp. 193-210.
[26] S. Yu, “Covert communication by means of email spam: A challenge for digital investigation”, Digital Investigation, vol. 13, **(2015)**, pp. 72-79.
[27] T. Morkel, J. H. P. Eloff and M. S. Oliver, “An overview of image steganography”, Proc. ISSA, **(2005)**, pp. 1-11.
[28] T. Sueyosh and G. Tadiparthi, “Steganography for e-Business: An Offensive Use of Information Securit”, Asia Pacific Management Review, vol. 9, no. 5, **(2004)**, pp. 943-968.
[29] V. Stamati-Koromina, C. Ilioudis, R. E. Overill, C. K. Georgiadis and D. Stamatis, “Insider threats in corporate environments: a case study for data leakage prevention”, Proceedings of the 5th Balkan Conference in Informatics, **(2012)**, pp. 271-274.
[30] W. Eyre and M. Rogers, “Steganography and Terrorist Communications: Current Information and Trends - Tools, Analysis and Future Directions in Steganalysis in Context with Terrorists and Other Criminals”, Conference on Digital Forensics, Security and Law; Las Vegas, Nevada, USA, **(2006)**.
[31] Y. Fan and S. Wang, “Intrusion Investigations with Data-Hiding for Computer LogFile Forensics”, Proceedings of the IEEE 5th International Conference on Future Information Technology, pp. 1-6.

