ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Technology for Hiding Information using Steganography in Smartphones

Rohith V[*1], Yathiraj GR[*2], Akshaya George[*3], Aswathi M V[*4], Athul Jithendran[*5], Navanya M A[*6]

Asst. Professor, Department of CSE, Coorg Institute of Technology, Ponnampet, Karnataka, India[*1*2]

UG Scholar, Department of CSE, Coorg Institute of Technology, Ponnampet, Karnataka, India[*3*4*5*6]

ABSTRACT: Due to the technological advances of software and hardware, now a days mobile phones offering capabilities, before achievable only for desktop computers or laptops are available. By offering much better services and centralizing ahuge volume of data, modern smartphones changed theway we socialize, entertain and work. Much complex hardware/software frameworks leads to a number ofvulnerabilities, attacks and hazards to profile individuals or gathersensitive information. The majority of works evaluatingthe security of smartphones neglects steganography, which can be mainly used to: i) exfiltrate confidential data via camouflage methods, and ii) conceal valuable or personal information into innocent looking carriers. Hence the paper surveys the state of steganographic techniques for smartphones. Here we showcases the most popular software applications to embed secret data into carriers, as well as possible future directions. The different approaches are grouped according to the part of the device used to hide information, leads to different covert channels, i.e., local, object and network. Index Terms—Steganography, smartphones, covert channels, information hiding, security

I. INTRODUCTION

From last few decades, the advancement in the field of software and hardware led to mobile phone which offers capabilities earlier achievable only for desktop computers or laptops [1]. The increasing convergence of network services, computing/storage functionalities, and Graphical User Interfaces (GUIs) changed into new devices called *smartphones*, which now became the first choice to access the Internet [2]. The Bring Your Own Device (BYOD) paradigm makes them core tools in the daily working routine [3]. This popularity is mainly driven by a multi-functional flavour combining many features, such as a high-resolution camera, different air interfaces and Global Positioning System (GPS) into a unique tool. To handle the hardware, the Operating System (OS) has architecture very close to the one used on desktops [4].

The increased complexity and explosion of data volumes exchanged, dramaticallyincreasesvulnerabilities/attack- or "social" threats [7]. Therefore, smartphones are becoming an excellent partner for profiling users, or to gain sensitive information [8].Information, the hackers acquire from a system is in a form that they can read and comprehend and can be revealed to others, and can be modified to misrepresent an individual or an organization, or used to launch an attack.

One solution to this problem is, through the use of steganography, an information hiding technique in digital media.It includes various information hiding techniques for embedding a *secret message* into a carefully chosen *carrier*, while preventing the knowledge of existence of the message to a third person.

II. MOTIVATIONS

Globally, there are about 5 billions of mobilephones users worldwide, that too 1.08 billion are smartphone users [17]. Detail study made by International Data Corporation(IDC),reporting that the global market is expecting a hike growth of mobile phone users to 7.3-15% year[9]. It is important creating new data hiding paradigms for smartphones, especially for the following reasons:

• *Popularity reduces suspicions*: masking capacity becomes better by utilizing more certain carrier.

• "*opportunity makes the thief*":increased chances for hiding information within the TCP/IP stack, or smartphones services is due to the availability of several applications, services and protocols

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

While explaining the importance and timeliness of steganography we use four incidents on the exploitation of steganography as the enabler to leak information, or to conduct large-scale
Attacks:

2008—steganographic methods have proven to be useful for data *exfiltration*. It was reported that someone at the U.S. Department of Justice smuggled sensitive financial data out of the Agency by embedding information in several image files [10];

2010—steganography demonstrated that can pass unnoticed for long periods. It was discovered that the Russian spy ring of the so-called "illegal's" used digital image steganography to leak classified information from USA to Moscow [11];

2011—steganography witnessed to *scale*. The Duqu worm moved stolen data towards many botnet's C&C servers via apparently innocent pictures, thus traversing the Internet without raising any suspicion [12];

2014—steganography has its effectiveness for *signalling* purposes. When installed on user's machine, theTrojan.to the infected system Zbot downloaded a jpeg imageWithin which there is a list of banks and financialinstitutions, which network traffic has to be closely inspected[13].

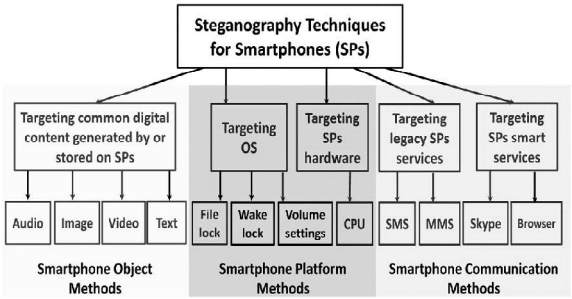


Fig.1 Taxonomy used in survey to organize the main information hiding techniques targeting smartphone's components and possible examples.

the taxonomy depicted in Fig. 1, which is composed of three different classes. Each one results into a method and a related hidden channel with a well-defined scope

III. STEGANOGRAPHY FUNDAMENTALS AND ITS EVOLUTION

Definitions And Goals: Steganography means invisible communication.The techni*que* is hiding information in other information, thus hiding the information that is to be communicated. The word steganography is derived from the Greek words "*stegos*" and "grafia" which means "cover" and "writing" respectively [1] which defines it as "covered writing". In image steganography, as the name implies the information is hidden in images. In *Histories* the Greek historian Herodotus , Histaeus, who needed to communicate with his daughter's husband in Greece. He shaved the head of one of his slaves and punched the message onto his scalp. When the hair grew back the slave was send with the hidden message [2]. The Microdot technique was developed by the Germans during world war II. Information, especially size of photographs was reduced until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent through an insecure channel in which one of the paper containing hidden information [3].

Steganography s being used in most of the computers where the carriers being digital data and networks being the high speed delivery channels. Steganography combined with cryptography helps in amplifying the strength. Typically, steganography is used to achieve one of the following goals:

- To hide a valuable information in a carefully chosen carrier to keep a secret safe.
- To hide the existence of communication if the carrier is transmitted between the parties involved in steganographic data exchange.

Eventually, hence this helps us in keeping the third-party unaware of the its presence. The two important properties for a carrier are:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

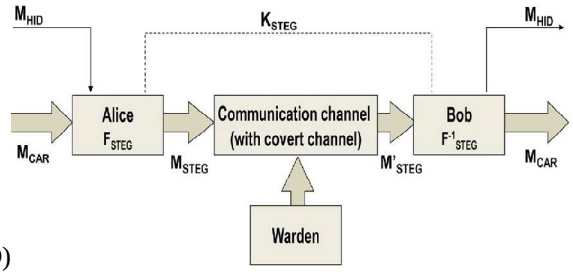
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

- *Popularity*: the used vector should be not considered as ananomaly itself, by unmasking the existence of the hidden communication potentially;
- *Unawareness*: modifications needed to embed a secret data should be not "visible" to a third party who is unaware of the steganographic procedure.

Model and Scenarios: The hidden communication model underlying Steganography is based on the famous "prisoners' problem" [15], firstly formulated by Simmons in 1983, and graphically represented in Fig. 2.
The model considers two prisoners, Alice and Bob, jailed in different cells, to prepare an escape plan they tried to communicate with each other. Their messages passed were inspected by theWarden: if any conspiracy is identified, he will put them into solitary confinement to succeed in the escape, Alice and Bob were forced to find a way to communicate. To be more formal, denote as *MHID* the hidden message, and as *MCAR*the innocent looking carrier. To bypass the Warden, both Alice and Bob must agree on a steganographic method: this is the pre-shared knowledge denoted as *KSTEG*. Then, to hide and unhide the secret, they use *FSTEG*(·) and *F*−1*STEG*(·), respectively. To create a covert communication channel, the sender alters *MCAR*by applying *FSTEG*(·) to have a *MSTEG*:



MSTEG=FSTEG(MCAR,MHID)

Fig.2.Model for hidden communication based on the Simmons' prisoners problem

Similarly, the receiver will use *F*−1*STEG*(·) with *MSTEG*tohave *MHID*, as well as the original *MCAR*:

(*MHID*,*MCAR*) = *F*−1*STEG*(*MSTEG*)

However, the channel (the Warden in the scenario ofSimmons) may alter the hidden message *MSTEG*, for instancedue to noise, resulting into *M'STEG*. This can be also theoutcome of an intentional data morphing/alteration to impede Steganography As a consequence, the steganographic communication could be voided due to difficulties in computing the *F*−1*STEG*(·).

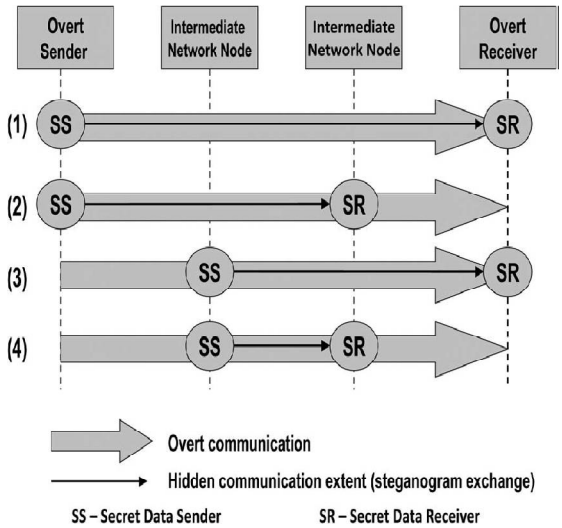


Fig.3. Hidden communication scenarios for steganography generalizing covert/overt channels

Fundamental Properties

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Steganographic methods transferring informs between two ends can be characterised by the following properties
• *Steganographic bandwidth* (or *capacity*): it is the amount of secret data that can be sent per time unit by using a given method;
• *Undetectability* (or *security* [14]): it is the inability of a certain carrier to detect a steganogram
• *Robustness*: it is the count of alterations a steganogram can withstand without destroying the embedded secret data.

Ideally, when applying highest possible bandwidth if they are robust and hard to detect then we say that it is a perfect steganographic method. The relation ruling the interdependence of themetrics is often called *magic triangle*, and depicted in Fig. 4.Put briefly, its rationale is that is not possible to increase a performance index without lowering the other two. For the sakeof completeness, we just mention the *magic hexagon*, which describes a more enhanced space [18], but it is seldom adopted.

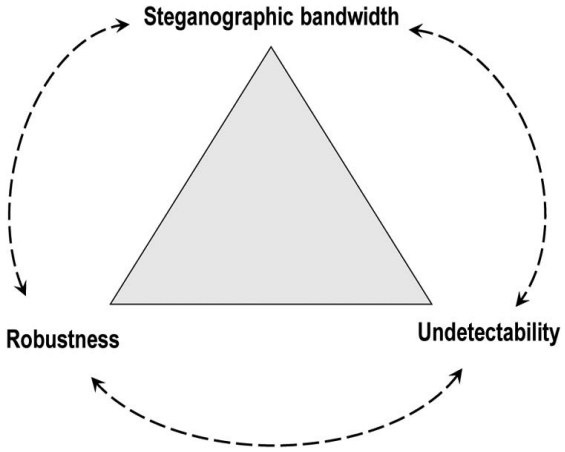


Fig.4.The trade-off relation between the three performance indexescharacterizing a covert channel.

Evolution of Digital Steganography:
Now we review on the most relevant techniques for theevolution of steganography, spawned by the advent of digital information and networking. In this perspective, the cutting edge research on data hiding for smartphones focuses on:
• *Digital media*;
• *Linguistic*(or *text*);
• *Device resources*;
• *Network*.

1) Digital Media Steganography: It is the most established part of the information hiding, algorithms were developed by the researchers to secretly embed a signature in digital pictures. During the years, different methods have been proposed, rangingfrom Least Significant Bit (LSB) modifications, to texture blockcoding [16]. Videos can also be manipulated by modern smartphones, thus many techniques were created to embed data within a Moving Picture Experts Group (MPEG) video carrier[10], e.g., secrets can be stored within video artifacts, or in themetadata describing the compressed media [18]. Similar approach is used for audio, since the human auditory system can be eluded through its "masking property," i.e., noise or strongertones make weaker ones inaudible [12]. Besides, smartphones are also digital jukebox, thus many works consider audio specific compressed formats, like MPEG—Layer III (mp3)in a way similar to the video counterpart.

2) Linguistic (or Text) Steganography: It exploits various aspects of the written word, hence the carrier is the syntactic and/or the semantic structure of the text. The most popular techniques used are: word-spacing alteration, displacement of punctuation marks, word order manipulation or patterns built on thechoice of synonyms [16]. Currently, owing to the large volume of daily spam messages, an emerging field investigates their adoption for steganographic purposes [17].

Object Covert Channel: Techniques that belong to 1) and2) allow to create an *object covert channel* that can be utilized to *i*) conceal the users' secrets with the intent of storing them locally on the device, or *ii*) if a modified file is sent to a party aware of the applied steganographic scheme, to hide the very existence of the communication.

3) Device Resources Steganography: It accepts techniques to form a covert channel within the same physical entity. Device resources steganography includes methods that allow inter-processes data exchanges within the single host. The quintessential carrier is a system-wide resource, e.g.,the CPU load [18], the level of a buffer, memory zones, or storage

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

resources. Such techniques have been recently becoming en vogue, hence commonly used to achieve steganography in cloud computing environment [19].

Local Covert Channel: These kinds of methods used in steganography helps us to create a local hidden path among entities within the same device.

4) Network Steganography: It is the latest but fast developing branch of information hiding nowadays. It utilizes one or more protocols simultaneously, for exploiting relationships between different layers of the ISO/OSI stack. More advanced methods include steganography inreal-time services like IP telephony [19], or in peer-to-peer(p2p) services such as, Skype [15] or BitTorrent [20]. Recently,Online Social Networks (OSNs) like Facebook [21] can be considered as a possible carrier of hidden data. Specific techniques exploiting emerging network protocols, likethe Stream Control Transmission Protocol (SCTP) [12] are partof the ongoing research.

Network Covert Channel: Network steganography techniques allows to create a channel for communicating in a hidden manner from/to a device, and typically this is done through a communication network.

IV. STEGANOGRAPHY VS CRYPTOGRAPHY

As we all know, steganography and cryptography are used for secret exchange of data. But both are different with its functions. Cryptography hides the contents of a secret message, whereas steganography conceals the existence of the message. Steganography must not be confused with cryptography, where we transform the message so as to make it meaning obscure to a malicious people who intercept it. Therefore, the definition of breaking the system is different [6]. In cryptography, the system is broken when the attacker can read the secret message. For breaking a steganographic system the attacker need to detect that steganography has been used and he is able to read the embedded message.

In cryptography the original message is altered to make it meaningless and it cannot be decrypted unless the decryption key is available. Since it is only altering the structure attacker can easily make sense that it contains some secret data. Basically, it offers the ability of transmitting information between persons preventing it from a third party. Cryptography can also provide authentication for verifying the identity of someone or something.

In contrast to cryptography it hides the secret message inside a *cover-image* so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an “invisible” message created with steganographic methods will not.In addition, the security of classical steganography system relies on secrecy of the data encoding system [4]. Once the encoding system is known, the steganography system is defeated.

Advantages and disadvantages comparison

Steganography	Cryptography
Unknown message passing	Known message passing
Little known technology	Common technology
Technology still being developed for certain formats	Most algorithms known to government departments
Once detected message is known	Strong algorithm are currently resistant to brute force attack
Many Carrier formats	Large expensive computing power required for cracking

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

V. SMARTPHONE COMMUNICATION METHOD

It is possible to theoretically exploit the majority of the network steganography methods already proposed for desktops (see, [9], [15], and [16] for surveys on the topic).

Legacy Services*:* The functions related to the telephonic portion of the smartphone, such as SMS and MMS, which are relevant carriers for steganography. According to [22], in the second quarter of 2007, Verizon Wireless alone delivered 14.4 billion of text messages. Specifically, *three* base methods, which can be mixed to enhance the throughput of secret data, are proposed:

• *acronym patterns*: words are substituted by means of acronyms (e.g., "CM" stands for "call me," or "C" stands for "see") to build a binary pattern of 1 if the acronym is used, and 0 otherwise, as to embed secret data;

• *Alternate spelling*: similar to the previous one, but uses known alternate spellings of a word (e.g., "center" instead of "centre");

• *Whitespaces*: well-known patterns of spaces among the words are used to represent secret data (e.g., Hi how are you?). An equivalent method uses line skipping.

Smart Services*:* OSNs are largely accessed from smartphones and mobile devices, we address in more details steganographic methods. In [24] the Extensible Messaging and Presence Protocol (XMPP), which is at the basis of many OSNs like Facebook or Google+, as well as many Instant Messaging (IM) services also available for smartphones, like Google Talk and Live Journal Talk. In this case, the steganographic channel is created by encoding data within attributes exchanged by the protocol.

Methods Potentially Targeting Smartphones: The availability of many desktop-grade applications multiply, at least theoretically, the number of network covert channels to be used on smartphones. To mention the most popular applications used on mobile devices, we cite Skype, generic VoIP client interfaces, Facebook (see, e.g., the popular tool discussed in [21]) or the Bit Torrent file-sharing service. Therefore, as desktops and smartphones progressively converge into a unique platform.

Modern devices have enough power to run full-featured/desktop-class games, and their enhanced connectivity makes them a very powerful platform for online gaming. An effective approach, which could be easily borrowed from desktops, is based on embedding secret data in the traffic used by First Person Shooters (FPSs) to sync the client(s) and the server.

VI. SECURE INFORMATION HIDING SYSTEM (SIHS)

for confidentiality information hiding system has been developed. However, in this paper, we are using an image file as a carrier to hide message. For embedding the data into an image, we require two important files. The first is the original image so called *cover-image*. The image which in and *gif* format will hold the hidden information. The second file is the *message* itself, which is the information to be hidden in the image. In this process, we use a plaintext as the message.

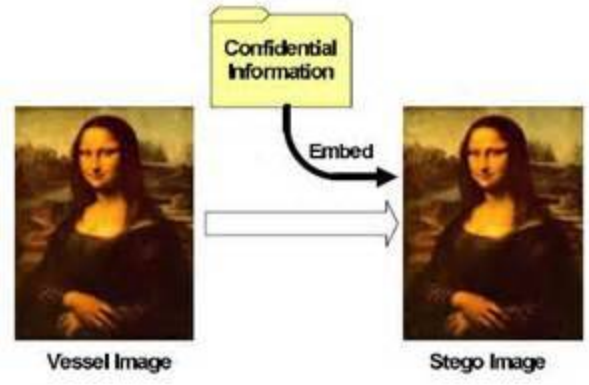


Figure stegno image

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

The *cover-image* will be combined with the message. This will produce the output called *stegoimage* ie, carrier file with hidden message. as we see, both are identical. However, there are hidden message that imperceptible.

VII. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

Modern smartphones are an excellent playground for the development of new steganographic methods, and they will be likely to become one of the most targeted platforms for data exfiltration. To classify the work done, we developed taxonomy to partition methods in three covert channels, and we also evaluated possible countermeasures.

Currently the most active trend is the one aiming at the creation of local covert channels for Android-based devices. In the near future, new low-bandwidth methods will be introduced, as well as the willingness of their search community of starting some active development over iOS or Windows Phone.

Digital media steganography for Smartphone's does not add any novelty compared to desktops, apart some works on QR codes. Nevertheless, video steganography applied to mobile devices is still a largely underestimated research area.

REFERENCES

[1] X. Li *et al.*, "Smartphone evolution and reuse: Establishing a more sustainable model," in *Proc. 39th ICPPW*, San Diego, CA, USA, Sep. 2010, pp. 196–484.
[2] "Mobile traffic forecasts 2010–2020," Zürich, Switzerland, Jan. 2011. [Online]. Available: http://www.umts-forum.org/component/option, com_docman/task,doc_download/gid,1137
[3] G. Thomson, "BYOD: Enabling the chaos," *Netw. Security*, vol. 2012, no. 2, pp. 5–8, Feb. 2012.
[4] F. Maker and Y.-H. Chan, "A survey on android vs. Linux," University of California, Davis, CA, USA, pp. 1–10, 2009.
[5] R. A. Botha, S. M. Furnell, and N. L. Clarke, "From desktop to mobile: Examining the security experience," *Comput. Security*, vol. 14, no. 3/4, pp. 130–137, May/Jun. 2009.
[6] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 166–122, 2013.
[7] L. Caviglione and M. Coccoli, "Privacy problems with web 2.0," *Comput. Fraud Security*, vol. 2011, no. 10, pp. 16–19, Oct. 2011.
[8] M. Landman, "Managing smart phone security risks," in *Proc. InfoSecCD Conf.*, Kennesaw, GA, USA, 2010, pp. 117–155.
[9] International Data Corporation (IDC) Worldwide Quarterly Mobile Phone Tracker. [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS10301413, last accessed Jan. 2014
[10] S. Adee, "Spy vs. spy," *IEEE Spectr. Mag.*, Aug. 2008. [Online]. Available:http://spectrum.ieee.org/computing/software/spy-vs-spy, last accessed Jan. 2014
[11] N. Shachtman, FBI: Spies Hid Secret Messages on Public Websites, ser. Wired, Jun. 2010. [Online]. Available: http://www.wired.com/dangerroom/2010/06/alleged-spies-hid-secret-messages-on public websites, last accessed Jan. 2014
[12] D. Goodin, "Duqu spawned by 'well-funded team of competent coders'—World's first known modular rootkit does steganography, too," The Register, Nov. 2011.
[13] J. Gumban, "Sunsets and cats can be hazardous to your online bank account," TrendLabs Security Intelligence Blog, Mar. 2014. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/ sunsets-and-cats-can-be-hazardous-to-your-online-bank-account/, last accessed June 2014
[14] J. Fridrich, *Steganography in Digital Media—Principles, Algorithms, Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[15] G. J. Simmons, "The prisoner's problem and the subliminal channel," in *Proc. CRYPTO*, 1983, pp. 20–67.
[16] K. Bennett, "Linguistic steganography: Survey, analysis, robustness concerns for hiding information in text," Purdue Univ., West Lafayette, IN, USA, CERIAS Tech. Rep. 13, May 2004.
[17] A. Castiglione, A. De Santis, U. Fiore, and F. Palmieri, "An asynchronous covert channel using SPAM," *Comput. Math. Appl.*, vol. 63, no. 2, pp. 437–167, Jan. 2012.
[18] J. C. Huskamp, "Covert communication channels in timesharing system," Univ. California, Berkeley, Berkeley, CA, USA, Tech. Rep. UCB-CS-78-02, 1978.
[19] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, 2009, pp. 199–212
[20] P. Kopiczko, W. Mazurczyk, and K. Szczypiorski, "StegTorrent: A steganographic method for the P2P file sharing service," in *Proc. IEEESecurity Privacy Workshops*, San Francisco, CA, USA, May 2013, pp. 120–157.
[21] S. Nagaraja *et al.*, "Stegobot: A covert social network botnet," in *Proc. 13th Inf. Hiding Conf.*, Prague, Czech Republic, May 2011, pp. 299–313.
[22] J. Brown, B. Shipman, and R. Vetter, "SMS: The short message service," *Computer*, vol. 40, no. 12, pp. 106–110, Dec. 2007.
[23] S. Coulombe and G. Grassel, "Multimedia adaptation
[24] P. Reshad and J. Hernandez-Castro, "Steganography using the Extensible Messaging and Presence Protocol (XMPP)," Computing Research Repository (CoRR) 2013, arXiv.org E-print Archive, Cornell University, Ithaca, NY, USA.