Blacknoise: Low-fi Lightweight Steganography in Service of Free Speech

Michael PAIK[1]
[1]*New York University, 715 Broadway Rm 719, New York, NY 10003, Unted States*
Tel: +1 212 998 3493, Email: mpaik@cs.nyu.edu

Abstract: Censorship of communications is a widespread, current practice in various countries with repressive governments in order to prevent or restrict speech; political speech in particular. In many cases state-run telecommunications agencies including those providing internet and phone service, actively filter content or disconnect users in defense of incumbents in the face of widespread criticism by citizens.

In this paper I present Blacknoise, a system which uses commodity low-cost mobile telephones equipped with cameras, and takes advantage of their low-fidelity, noisy sensors in order to enable embedding of arbitrary text payloads into the images they produce. These images can then be disseminated via MMS, Bluetooth, or posting on the Internet, without requiring a separate digital camera or computer to perform processing.

1. Introduction

Regimes such as China [1,2] are actively censoring content across various communications channels used by their citizens under the auspices of an effort to curb "offensive" materials, often with full cooperation from state-run agencies such as China Mobile [3].

However, reports [4] indicate that this censorship also cracks down on political speech including satire, and is triggered by, for instance, any mention of the names of political figures.

In addition, nations as varied as France and India [5] prevent encryption of SMS by regulation, ostensibly in order to ease monitoring of communications along this channel, while Iran [6] disabled the transmission of SMS entirely in the hours leading up to its 2009 presidential election in response to SMS' role in organizing protests and mass rallies as well as transmitting news outside of the country via channels such as Twitter [7].

A litany of other nations conduct routine censorship of internet traffic, including but not limited to Turkey [8], Saudi Arabia [9], Pakistan [10], and many others, which follow the pattern of limiting speech and consumption of speech on the grounds that they are protecting their citizens from harm.

2. Steganography

The aim of steganography (from the Greek *στεγανός,* for 'covered' and *γράφειν*, 'to write') as a technique is to conceal a message within some 'cover medium' in such a way that the fact that a message is being sent at all is difficult to detect and harder to prove, and recovery of any such message is harder still.

A popular historical example of such a technique is noted in Herodotus' account of Histiaeus, who shaved the head of a trusted slave and tattooed a message on his scalp, sending the slave to deliver the message once his hair had grown back in, obscuring the message.

The modern interpretation of this technique involves embedding message bits into some digital cover (most typically in images, although embedding in video, audio, and text are also practiced.) One of the most basic steganographic techniques is known as Least Significant Bit (LSB) replacement, wherein the message bits are written over the least significant bits of the carrier medium, e.g. the lowest intensity bit in each pixel in a raster image. These bits were initially assumed to contain random Gaussian noise.

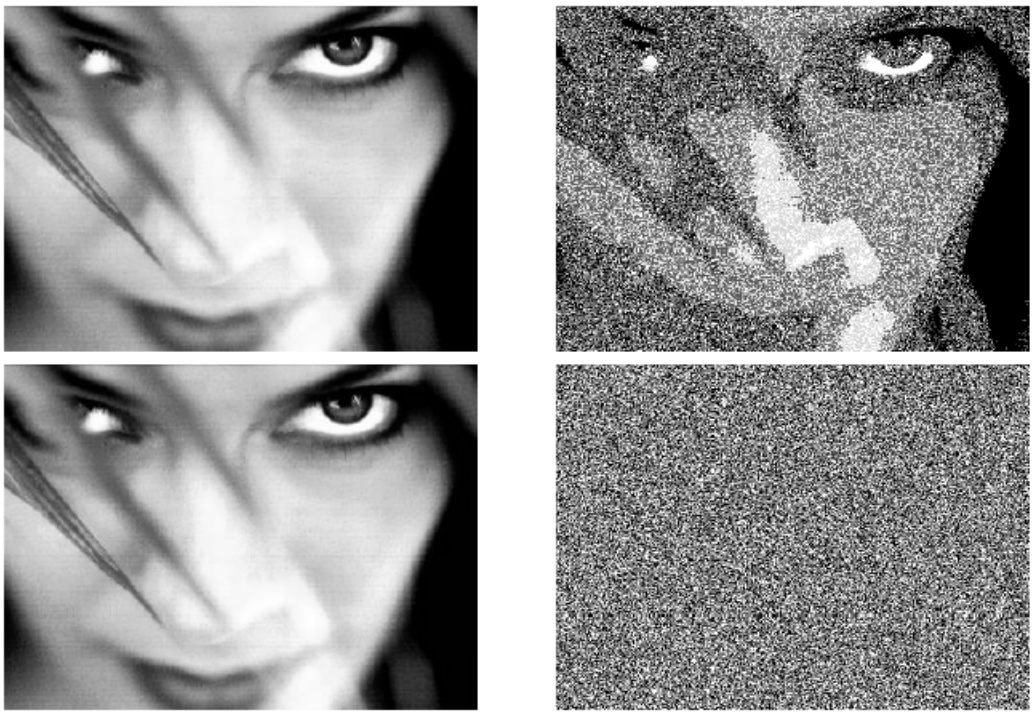

Figure 1: LSB plane example using two images. Upper left image is the original photograph, and upper right is its least significant bit plane with 0 set to black and 1 set to white. The lower left image is a message embedding with S-Tools and the lower right is its LSB plane. Images from [11].

Subsequent analysis [11] indicated that the LSBs of cover images were not, in fact, random, but statistically correlated. The outworking of this was that naive embedding of message bits was easily detectable using straightforward χ^2 analysis and, depending on embedding style, could also be detected using a "Visual Attack" [11] in which the bit plane assumed to contain the image was extracted from the cover image and visually inspected.

A somewhat more advanced technique than LSB replacement is called LSB matching [12], wherein the pixel values are modified at random by ±1 if the bit of the cover does not match the bit of the embedded image, which preserves image statistics better than the earlier method.

3. System Overview

We make the observation that low-cost embedded imaging sensors of the type typically found in early or inexpensive cameraphones exhibit high noise floors in both luminance and chrominance due to their small size, artificially increased sensitivity/ISO, and typically the lack of a flash.

Using 150 samples of images taken with a Nokia 3110c, a Chinese-made Amoi E72, and an Indian-made Micromax X280 at the default resolution for MMS (120x160 pixels), it was observed that the LSB plane did, in fact, more closely resemble random noise than image

content (illustrated in Section 4). Significantly, this also held true for each of the four least significant bit planes of each color channel, leading to significant visible noise in the resultant images.

The design of Blacknoise makes use of this fact and makes the novel contribution of extending the LSB matching technique across all three color channels of a PNG bitmap image taken with mobile phone cameras, across the four least significant bits. The result is that the embedding rate on any given bit plane is 1/12 what it would be on an equivalent grayscale bitmap image using conventional LSB matching.

Blacknoise operates, at a high level, as follows: Users Alice and Bob each have a cameraphone handset with the Blacknoise software installed. In a face-to-face encounter, the software establishes a symmetric key for communication between the two parties over Bluetooth or some other near-field communication method, e.g. Infrared, NFC. This key is used until the two parties meet face-to-face again and optionally establish a new key.

After the two parties separate, if Alice wants to send Bob a message, she takes an arbitrary, innocuous snapshot using her cameraphone, and enters the message. This message is encrypted appropriately with the symmetric key and a stream cipher, and the message is embedded into the image in a pseudorandom manner, using a pseudo-random number generator (PRNG) seeded with the last n bits of the key. When embedding the message, the system makes use, as noted above, of the four least significant bit planes of each color channel. The alpha, or transparency, channel is left untouched as it is unlikely that a mobile phone will produce an image with variable alpha, and as such images with alpha channel noise would immediately become suspect. The encoded image is then sent as a PNG bitmap using some carrier medium (MMS, Bluetooth, email, Internet posting, etc.) to Bob.

Upon receipt of the message, Bob opens the application and uses the established key to seed his own PRNG, selecting the correct bits to read values from, and uses the key to decrypt the ciphertext, recovering the message.

Eve, a party at the telecom or Internet provider observing the MMS message or image, may perform statistical analysis on messages passed between parties, and ideally should not be able to detect the presence of a message in the cover.

4. Implementation

A proof-of-concept implementation of Blacknoise was created on a pair of Nokia 3110c handsets in J2ME. The 3110c has the requisite J2ME APIs: JSR 205 [13] for MMS, JSR 82 [14] for Bluetooth connectivity, JSR 177 [15] for cryptographic APIs, and JSR 135 [16] for access to multimedia devices, including onboard cameras. In addition, as noted previously, the 3110c has a poor-quality image sensor which produces a high noise floor.

The software creates an RFCOMM Bluetooth connection between the two handsets using a custom UUID to distinguish the application. It subsequently establishes a symmetric key for the Salsa20 stream cipher. The implementation of this cipher is provided by the BouncyCastle [17] cryptographic library for J2ME.

A file selector is provided to load images which have been saved to the phone, allowing images to be received via any of the various communication methods the phone supports, including MMS, Internet, Bluetooth, and Infrared.

As the 3110c unfortunately does not support capture of images into a bitmap format (despite specifications indicating otherwise) a custom PNG encoder using the open source JZlib [18] library was implemented.

Once a key between two parties is established using the J2ME PRNG, the application allows capture of images via the 3110c's onboard camera, at the 120x160 pixel resolution standard for minimal MMS. After the image is captured, the user specifies a message to embed, with the same 160 character, 140 byte payload limit as an SMS message. This limit is artificial but is designed as a sensible first-cut payload size and will increase as further evaluation about the embedding capacity of these images is performed. Larger captured images also clearly offer greater embedding capacity.

The input message is encrypted using the Salsa20 cipher and the established key (with a static, predefined 64-bit initialization vector for the purpose of this proof of concept) and embedded at random using LSB matching to preserve statistical properties. The resulting image is then either saved for transmission using WAP/GPRS/EDGE/UMTS or Bluetooth, or is embedded into an MMS/SMIL message. In the latter case the user is prompted to enter any additional descriptive text, such as a caption, and the message is transmitted using JSR 205 APIs.

The message is appropriately extracted and decrypted upon receipt when the user selects the received file in the file browser and selects the symmetric key he has established with the sender, and the decrypted message is displayed to the user.

5. Dissemination Methods

5.1 – MMS

The Multimedia Messaging Service (MMS) is a service which works analogously to the better-known SMS, but can carry multimedia content (e.g. images, video, and audio) as well as text. As a result, the payload size of MMS can be much higher, albeit at a somewhat higher cost to the subscriber.

The popularity of MMS is on the increase in areas with limited data connectivity, with China Mobile, for instance, reporting a volume increase of 130% to 33.1 billion messages, representing an 83.7% increase in revenue to approximately $421 million USD in its 2008 earnings report [19].

MMS is supported on every modern cameraphone handset and has widespread API support via J2ME JSR205 [13] and lower-level phone operating systems.

This widespread and growing acceptance of MMS, its larger payload as well as its own and well-understood specification make it one of the natural choices as an obfuscated data carrier.

The use of Blacknoise over an MMS carrier is straightforward. Once the shared key is established and an appropriate message is encoded in an image shot by the cameraphone, the image is then embedded in an MMS message and conveyed to a target user, and the message extracted and decrypted on the other end using the shared key.

5.1.1 – MMS Caveats

While MMS is a natural channel for information such as this, there are certain drawbacks which must be considered.

Firstly, MMS, depending on the country, can carry a significant cost, often three to ten times that of SMS or data via GPRS, EDGE, or UMTS, which can represent a major cost burden in developing nations.

Secondly, MMS messages are routed from handsets to servers controlled by the mobile service provider known as MMSCs, or Multimedia Messaging Service Centers, which then route the messages onward to their destinations. Because this carrier-controlled bottleneck exists, carriers can put filters in place which either resample or compress images in bitmapped formats, destroying the data contained within. While techniques exist to embed bits in similar ways into audio and video rather than images, these media are also susceptible to the same type of resampling or compression and offer no advantage against this bottleneck, while offering significantly increased complexity to encode on a computationally restricted mobile handset.

Finally, as in the Iranian example, during periods of dissent, mobile carriers can simply be instructed to turn off communications entirely, completely blocking this channel of communication.

5.2 – Bluetooth/Infrared

Bluetooth or Infrared file transfer, also known as OBEX, or Object Exchange, offers another channel through which Blacknoise images can be conveyed. This technique requires the communicating parties to be in very close proximity to one another - 30 meters in the case of Bluetooth, and mere centimeters in the case of Infrared. In order to perform the exchange, the properly encoded Blacknoise image merely needs to be sent, as any other image file, to the recipient which is set to receive it.

This proximity makes widespread interception and analysis difficult, as the information exchanged never spreads beyond the immediate vicinity of the sender and receiver. In addition, there is no cost associated with this transfer mechanism, as there is with MMS.

Finally, Bluetooth supports a technology called 'Piconets' in which one master can communicate with up to 7 other devices, and 'Scatternets' which are bridged Piconets, which have no effective size limit. While the exact implementation of a communication channel using these techniques is outside the scope of this paper, it's clear that in some cases, particularly where many people are massed together, (e.g. a protest) this represents an economical and secure method for dissemination of information.

5.2.1 – Bluetooth/Infrared Caveats

Again, certain drawbacks apply to this communication channel, aside from the distance restriction inherent to the technology.

Bluetooth, as a standard wireless communications medium, is susceptible to jamming on its standard frequencies. While Bluetooth uses channel hopping in order to counteract narrowband interference, a sufficiently powerful broadcaster could energize the entire Bluetooth band and prevent any communications from occurring.

Additionally, only certain payloads and scenarios make sense for Blacknoise communication with those who are already nearby vis-a-vis passing a piece of paper or having a conversation in person. However, in these specific scenarios (e.g. where the parties communicating are under direct visual observation), Blacknoise can prove indispensible in, for instance, providing plausible deniability that any communication occurred.

Finally, in the case of Piconets and Scatternets, the problem of key dissemination and control adds a significant degree of complexity to 'broadcast' type messages. While these challenges are straightforward to overcome, they do require careful redesign of certain elements of the protocol, as well as potentially imposing a larger infrastructure burden compared to the current lightweight implementation of Blacknoise.

5.3 – Internet

The Internet, for those who have access to it, is easily the most robust and simplest method of conveying Blacknoise images. While nations which carry on censorship can and do selectively block sites, it is nigh well impossible to block every site on which a Blacknoise user might post an image, and even more difficult to resample every candidate image to make it unusable, given the sheer volume of images transmitted through the Internet.

Aside from dedicated photo-sharing sites such as Flickr [20], Blacknoise images can be posted anywhere in innocuous forms from personal blogs (though Blogger [21], Tumblr [22], Livejournal [23] and Wordpress [24] are all blocked in China, myriad other services exist), and the nearly limitless number of discussion forums on the internet which support .PNG images in 'Avatar' icons or user signatures.

Use of the Internet as the medium for conveying these messages carries with it all of the advantages entailed in other Internet use, including (relative) anonymity, encryption when using TLS and, typically, low cost.

Finally, unlike either the MMS channel or Bluetooth, it is impossible for a regime to completely cut off Internet access without both incurring significant negative global publicity and crippling elements of its business mix which rely on the information economy.

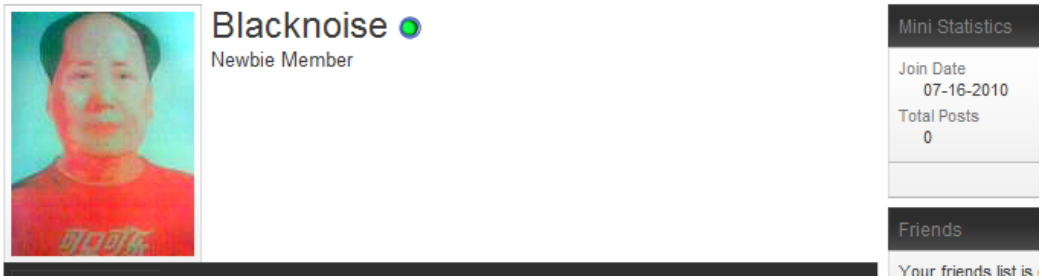

Figure 2: A Blacknoise image used as an avatar on an arbitrary web discussion forum.

5.3.1 – Internet Caveats

The Internet may be a preferred medium for dissemination of Blacknoise images, but there are obvious drawbacks to using it for this purpose. Countries which have an interest in controlling the flow of information have developed extremely sophisticated methods for tracking and tracing these flows and, while Blacknoise offers a significant degree of deniability, the burden of proof in such regimes typically lies with the accused. Thus, should an image be suspected of carrying hidden information, it is possible that the poster could be tracked and prosecuted.

In addition, it is important to note that Blacknoise images posted on the Internet as opposed to shared directly on handsets have the property that they can be accessed by anyone, a negative property if the goal is information control, and a positive one if the goal is broad dissemination.

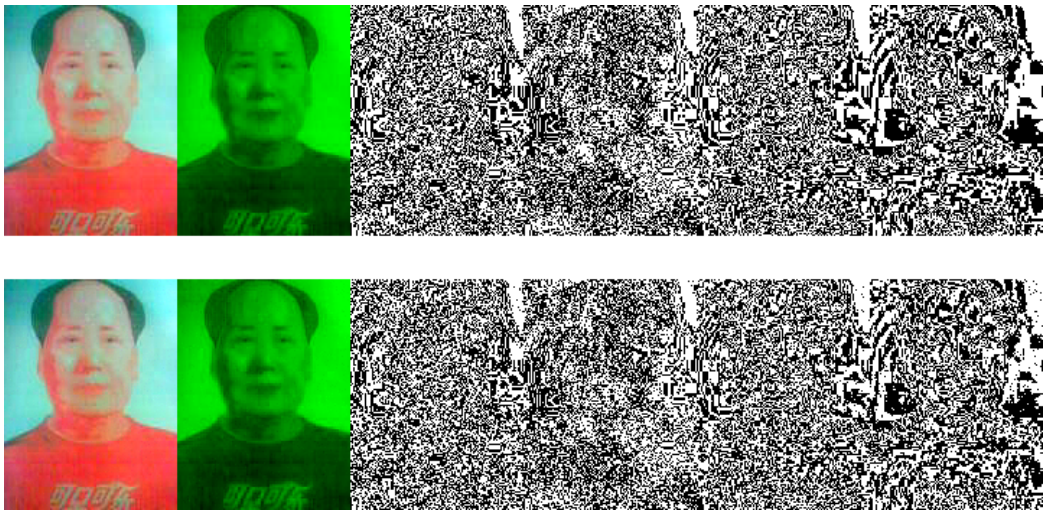

Figure 3:Examples of an image captured with the 3110c camera. The top row from left to right consists of the full color image, the green channel (selected as representative and containing the least visible noise) and the bit planes of the four least significant bits of the channel (1,2,4,8) before encoding. The bottom row contains the same images after encoding 1 message bit per pixel, a total of 19200 bits, or 2400 bytes. This represents more than 17 times the data payload of an SMS, and was selected as a reference only.

6. Analysis

We examine the results of embedding a message at a rate of 1 bit per pixel; in other words, an average of 1/3 bit per pixel per channel, or 1/12 bit per pixel per channel per bit plane. The resultant images of the bit planes can be seen in Figure 3.

It is clear to see that visual attacks will be difficult to execute without access to the original, unembedded cover image, as the qualitative noise pattern in the embedded and unembedded images on each of the four bit planes is very similar due to the high noise floor of the sensor masking the embedding. While differences are perceptible, particularly in fields of high intensity such as that in the upper right of the image, even these would be difficult to pick up in the absence of the original image for comparison. In addition, measures can be taken to avoid embedding 0 bits in such saturated areas during the embedding phase, or additional procedural noise can be introduced to mask saturation.

Initial attempts to classify stego and cover images using standard χ^2 techniques as well as Westfeld and Pfitzmann's sliding window [11] technique have failed to provide significantly better than random detection due to the low effective embedding rate per channel per bit plane. Histogram analysis to detect greater-than-normal symmetry in least bits due to LSB replacement is defeated by using LSB matching instead. The small image size (and therefore the small number of pixel samples) and high noise floor also contribute to creating high degrees of statistical variance between images and a difficulty in accurately characterizing a given image.

Because existing techniques for bitmap images rely upon the assumption that all bits are embedded in the LSB plane, effectiveness is reduced. It is currently unclear whether there is a simple augmentation that could be performed on these tools which would allow more robust detection of LSB matching among the 12 different bit planes used.

While there exist commercial tools to detect embedding in bitmap images, (e.g. [25]), their effectiveness is unclear as it is unknown what principles they work on. There are free and open source steganalysis tools available, but the best among them, StegDetect [26], only operates on JPEG coefficients, not bitmaps. StegSecret [27], an open-source contribution which detects various LSB schemes on bitmap images, failed to identify a single embedded image.

7. Related Work

There is a great deal of work surrounding the topic of steganography. Jessica Fridrich at Binghamton University leads a group that has produced several important papers on steganography and steganalysis [28-33].

Andreas Westfeld and Andreas Pfitzmann [11] contributed some early seminal work on steganalysis including some of the first statistical attacks on contemporary steganographic systems. Westfeld also contributed one of the first LSB encoding systems resistant to basic statistical attacks, F5 [34] for JPEG images.

Niels Provos created OutGuess [35], which used selective pseudo-random number generator seeding to deterministically offset statistical aberrations caused by steganographic embedding in JPEG images, and also created StegDetect [26], an application which detects various steganography schemes in JPEG with a high degree of reliability.

While there has been research into steganography on mobile platforms, notably by Agaian et al [36], most of the corpus consists either of implementations of 'naive' LSB or orthogonal research on algorithms which work well with constrained image sizes and low-powered processors without taking the advantages of naturally occurring noise into account.

Blacknoise builds upon various facets of the existing work, particularly making use of LSB matching and pitted against several of the published statistical steganalytic methods while contributing the underutilized principle of high-noise sources and using multiple bit planes to limit statistical perturbation of any given bit plane. In addition, the fact that Blacknoise operates preferentially on low-cost phone handsets brings steganography within practical reach for many in the developing world who own such phones but have little or no access to computers of their own.

8. Future Work

Future work on the Blacknoise system will proceed in several directions. Of primary importance is more robust analysis of the statistical properties of the cover images produced by small sensors, and how they differ from images which have been embedded. This analysis will help ascertain tight bounds for embedding capacity, allowing greater freedom in embedding text.

Orthogonal to this but of similar importance is research into generating procedural noise which carries similar statistical and visual properties for use with phones with better cameras, including smartphones.

Finally, more rigorous steganalytic tools will be brought to bear upon the images which result from Blacknoise, including RS [28] and Difference Image Histogram [37]. The standard statistical tools used in the analysis performed to date will also be examined for ways in which to augment them to detect the multiple bit plane embedding used in BlackNoise.

9. Conclusion

In this paper I have presented Blacknoise, a simple, lightweight steganographic system which takes advantage of the significant noise present in image sensors in typical inexpensive cameraphone handsets. The properties of the images produced by these cameraphones combined with contemporary embedding techniques defeat known existing first-line detection of message embedding in bitmaps.

Properly implemented, the system should allow the transmission of arbitrary text within and outside the borders of nations governed by restrictive regimes while maintaining plausible deniability and making both detection of message transmission and the recovery of messages difficult for parties not in possession of the appropriate keys.

The advantages of the Blacknoise system are clear, but significantly include a vast reduction in the amount of infrastructure required to send a hidden message: one $30 USD cameraphone as compared to a digital camera, memory card reader, computer, image editing software, etc. It is my hope that this will democratize the sending of truly private communications and increase free speech in otherwise repressive environments.

While this implementation is academic and still a work in progress, it is my hope that future development will allow for both more definitive security guarantees and practical use in China and elsewhere around the world.

10. Acknowledgments

I would like to thank Jinyang Li and those who worked on Kaleidoscope [38] for inspiration in circumventing censorship, and various friends and colleagues inside mainland China for describing the issues involved.

I would also like to thank Bill Thies, Ashlesh Sharma, and Jay Chen for feedback and input during the course of designing the Blacknoise system and the preparation of this paper for publication.

References

[1] China officials to censor SMS messages. http://www.zdnetasia.com/china-officials-to-censor-sms-messages-39142104.htm, July 2003.

[2] A Brief History of: Chinese Internet Censorship. TIME Magazine, March 18, 2009.

[3] AFP. China mobile users risk SMS ban in porn crackdown. http://www.google.com/hostednews/afp/article/ALeqM5jF6dl0QS_1q8Eub7W73BSRNwdJWQ , January 2010.

[4] R. MacKinnon. Censorship Foreigners Don't See - Stuff that didn't fit in my Op-Ed. http://rconversation.blogs.com/rconversation/2008/08/censorship-fore.html, August 2008.
[5] DeCryption. https://svn.berlin.ccc.de/projects/airprobe/wiki/DeCryption, 2009.
[6] Iran 'lifts block on SMS texting'. http://news.bbc.co.uk/2/hi/middle_east/8131095.stm, July 2009.
[7] L. Grossman. Iran Protests: Twitter, the Medium of the Movement. http://www.time.com/time/world/article/0,8599,1905125,00.html, June 2009.
[8] Önderoglu, Erol. Youtube, Kliptube ve Geocities Kapalı, Dailymotion Açıldı. http://bianet.org/bianet/kategori/bianet/109452/youtube-kliptube-ve-geocities-kapali-dailymotion-acildi, September 2, 2009.
[9] Internet Services Unit. Introduction to Content Filtering. http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm, 2006.
[10] Reporters Sans Frontières. Access to YouTube blocked until further notice because of "non-Islamic" videos. http://en.rsf.org/pakistan-youtube-access-unblocked-after-27-02-2008,25889.html. February 23, 2008.
[11] A. Westfeld and A. Pfitzmann. Attacks on Steganographic Systems. In *Proceedings of the Third International Workshop on Information Hiding*, Dresden, Germany, September 1999.
[12] T. Sharp. An implementation of key-based digital signal steganography. In *IHW '01: Proceedings of the 4th International Workshop on Information Hiding*, pp. 13-26, London, UK, 2001.
[13] JSR 205: Wireless Messaging API 2.0. http://jcp.org/en/jsr/detail?id=205, June 2004.
[14] JSR 82: Java APIs for Bluetooth. http://jcp.org/en/jsr/detail?id=82, March 2010.
[15] JSR 177: Security and Trust Services API for J2ME. http://jcp.org/en/jsr/detail?id=82, August 2007.
[16] JSR 135: Mobile Media API. http://jcp.org/en/jsr/detail?id=135, June 2006.
[17] bouncycastle.org. http://www.bouncycastle.org/latest_releases.html.
[18] JZlib – zlib in pure Java. http://www.jcraft.com/jzlib/.
[19] China Mobile, Ltd. 2008 Annual Results. http://www.chinamobileltd.com/images/present/20090319/pp02.html, March 2009.
[20] Flickr. http://www.flickr.com, July 2010.
[21] Beijing Notebook: Blogspot blocked in China. http://beijingnotebook.blogspot.com/2007/11/blogspot-blocked-in-china.html, November 27, 2007.
[22] Tumblr gets blocked by China for the 20th anniversary of the Tiananmen Square crackdown. http://answers.tumblr.com/post/118588176/tumblr-gets-blocked-by-china-for-the-20th-anniversary, June 5, 2009.
[23] Q. Norton. China Blocks LiveJournal. http://www.wired.com/politics/onlinerights/news/2007/03/72872, March 5, 2007.
[24] WordPress.com Still Blocked in China. http://foolswisdom.com/wordpresscom-still-blocked-in-china/, June 6, 2009.
[25] WetStone Technologies, Inc. Stego Suite. http://www.wetstonetech.com/cgi-bin/shop.cgi?view,1, 2010.
[26] N. Provos. OutGuess – Steganography Detection. http://www.outguess.org/detection.php.
[27] A. Muñoz. StegSecret. A simple steganalysis tool. http://stegsecret.sourceforge.net/, December 2007.
[28] J. Fridrich, M. Goljan, and R. Du. Reliable Detection of LSB Steganography in Color and Grayscale Images. In *Proceedings of the ACM Workshop on Multimedia and Security*, Ottawa, Canada, October 2001.
[29] J. Fridrich and M. Goljan. Practical steganalysis-state of the art. In *Proceedings of SPIE Photonics West*, *Electronic Imaging 2002*, San Jose, CA, 2002.
[30] J. Fridrich and M. Goljan. Digital image steganography using stochastic modulation. In *Proceedings of SPIE Photonics West*, *Electronic Imaging 2003*, Santa Clara, CA, 2003.

[31] J. Fridrich, M. Goljan, and D. Hogea. Attacking the OutGuess. In *Proceedings of the ACM Workshop on Multimedia and Security*, Juan-les-Pins, France, 2002.
[32] J. Fridrich and M. Goljan and D. Hogea. Steganalysis of jpeg images: Breaking the f5 algorithm. In *IHW '02: Proceedings of the 5th International Workshop on Information Hiding*, Noordwijkerhout, The Netherlands, October 2002.
[33] J. Fridrich and R. Du and L. Meng. Steganalysis of lsb encoding in color images. In *Proceedings of ICME 2000*, New York, 2000.
[34] A. Westfeld. F5-a steganographic algorithm: High capacity despite better steganalysis. In *IHW '01: Proceedings of the 4th International Workshop on Information Hiding*, London, UK, 2001.
[35] N. Provos. Defending against statistical steganalysis. In *Proceedings of the 10th USENX Security Symposium*, Washington D.C., August 2001.
[36] S. Agaian, R. Cherukuri, R. Sifuentes. Secure steganography designed for mobile platforms. In *Proceedings of the SPIE*, Volume 6250, pp. 62500E, 2006.
[37] T. Zhang and X. Ping. Reliable detection of LSB steganography based on the difference image histogram. In *Proceedings of the International Conference on Acoustics, Speech, and Signal Processing*, Hong Kong, April 2003.
[38] Y. Sovran, A. Libonati, and J. Li. Pass it on: Social networks stymie censors. In *Procedings of the 7th International Workshop on Peer-to-Peer Systems*, Toronto, Canada, February 2008.