Journal of Digital Forensic Practice

ISSN: 1556-7281 (Print) 1556-7346 (Online) Journal homepage: http://www.tandfonline.com/loi/udfp20

Nostega: A Novel Noiseless Steganography Paradigm

Abdelrahman Desoky

To cite this article: Abdelrahman Desoky (2008) Nostega: A Novel Noiseless Steganography Paradigm, Journal of Digital Forensic Practice, 2:3, 132-139, DOI: 10.1080/15567280802558818

To link to this article: https://doi.org/10.1080/15567280802558818

Published online: 11 Dec 2008.

Journal of Digital Forensic Practice, 2:132–139, 2008

ISSN: 1556-7281 print / 1556-7346 online
DOI: 10.1080/15567280802558818

Taylor & Francis
Taylor & Francis Group

ARTICLE

Nostega: A Novel Noiseless Steganography Paradigm

Abdelrahman Desoky
University of Maryland, Baltimore County, Department of Computer Science and Electrical Engineering, 1000 Hilltop Circle, Baltimore, MD 21250, USA

ABSTRACT Steganography is the science and art of covert communications. When using a steganographic approach, if an adversary suspects the existence of a hidden message the approach is defeated regardless of whether or not a plaintext is revealed. Contemporary steganography approaches found in the literature often hide data by altering a text, image, audio, etc., that serves as a cover. Although, an alteration is still considered a noise that is introduced to the cover, a sender opts to make the alterations look subtle and hard to detect, in order to avert suspicion. However, recent advances in steganalysis have rendered these approaches highly vulnerable to a wide variety of attacks such as traffic, contrast, comparison, statistical, etc., which may be able to defeat the steganographic goal. This article promotes a new paradigm for covert communication, namely noiseless steganography paradigm (Nostega), that overcomes the vulnerabilities of current approaches. Nostega neither hides data in a noise nor produces noise, rendering the generated cover noiseless. Instead, it camouflages messages in a form of unquestionable data in the generated cover. Unlike all other approaches, Nostega not only camouflages a message but also its transmission. Examples of Nostega-based steganography methodologies are discussed.

KEYWORDS steganography, information security, cryptography

INTRODUCTION

Steganography is the scientific art of camouflaging the presence of covert communications. The origin of steganography is traced back to the ancient Egyptians [1, 2]. The ancient Egyptians communicated covertly using the Hieroglyphic language, a series of symbols representing a message. The message looks as if it is a drawing of a picture, although it may contain a hidden message. Hieroglyphics contained hidden information that only a legitimate person who knew what to look for could detect. After the Egyptians, the Greeks used steganography, "hidden writing," from which the name was derived [1, 3]. Fundamentally, the steganographic goal is not to hinder the adversary from decoding a hidden message but to prevent an adversary from

The original work of this paper is a large frame of academic research that is in the process to be presented as a Ph.D. dissertation, as intended, at the University of Maryland, Baltimore County, Department of Computer Science and Electrical Engineering.
Address correspondence to Abdelrahman Desoky, University of Maryland, Baltimore County, Department of Computer Science and Electrical Engineering, 1000 Hilltop Circle, Baltimore, MD 21250.
E-mail: abd1@umbc.edu

suspecting the existence of covert communications [3]. When using any steganographic technique if suspicion is raised, the goal of steganography is defeated regardless of whether or not a plaintext is revealed [3–5]. Contemporary approaches are usually categorized either based on the steganographic cover type (e.g., image, audio, graph, game, or text) [3, 6, 7] or as a linguistic and nonlinguistic steganography [15].

Most contemporary approaches camouflage data as noise in a cover that is assumed to look innocent. For example, the encoded message can be embedded as alteration of a digital image or an audio file without noticeable degradation [5, 8]. Another example is concealing a message in a text-cover by altering the format and style of an existing text [3, 9, 10]. However, such alteration of authenticated covers can raise suspicion and the message is detectable regardless of whether or not a plaintext is reveled [8, 9]. Another venue for hiding information is the unused or reserved space in computer systems, such as operating system area on a harddrive or in file headers of image, audio, etc. [11, 12]. The use of TCP/IP packets is also proposed to hide and transmit data across the Internet in packet headers [13]. However, these techniques are vulnerable to distortion attacks [4, 8]. Other approaches pursued the linguistic path. Examples include null cipher [15], mimic functions [16, 17], NICETEXT and SCRAMBLE [18–21], translation-based [22–24], confusing approach [25], and abbreviation-based [26]. These approaches are vulnerable to detection because the generated level of noise (flaws) by the hiding process [9, 22–24].

The concerns of contemporary linguistic steganography approaches may be summarized as follows. First, text-cover may contain unusual patterns or numerous detectable flaws (noise), such as incorrect syntax, lexicon, rhetoric, and grammar. In addition, the content may be meaningless and semantically incoherent. Obviously, such flaws can raise suspicion during the covert communications unless there is a legitimate excuse (e.g., justifiable level of common human errors, noisy text of chat room, blogger, output of machine translation). Second, the achievable bit rate is minimal. Third, most efforts are focused on how to conceal a message and not on how to hide the transmittal of a hidden message. Furthermore, if contemporary approaches can fool a computer examination, fooling a human examination may appear to be extremely difficult. A successful steganography approach must be capable of passing both computer and human examinations. These concerns motivate the development of noiseless steganography paradigm (Nostega) introduced in this article.

Nostega overcomes the issues just mentioned above by camouflaging both a message and its transmittal. Nostega achieves the steganographic goal through the following five modules: First, it determines a field that can be employed to generate a steganographic cover–(e.g.,) graphs, games, text–that is capable of concealing data while looking innocent. Basically, the embedded data should be undetectable and should keep the cover unsuspicious and noiseless. Second, it determines the parameters that can be exploited for message encoding. Examples include numerical data to plot a graph-cover, moves to generate a game-cover (e.g., chess-cover). Third, it implements a message encoder that is capable of encoding the actual messages by using the output of second module. Fourth, it implements a cover generation engine that is capable of embedding the hidden message in a form of noiseless data as an integral part of the steganographic cover. Fifth, it implements a communication protocol that is capable of covertly delivering the steganographic cover while justifying the interaction between communicating parties. Some of the main advantages of Nostega are as follows:

- It employs steganographic fields (domains) for which a tremendous amount of material, such as graphs, text, games, etc., exists in electronic and non-electronic format, rendering it impracticable for an adversary to investigate all of them. This makes a steganographic cover extremely favorable for use in covert communications.
- The high demand by a wide variety of people creates a huge volume of traffic involving these materials, making it impractical for an adversary to investigate all transmissions.
- The high volume of traffic also allows communicating parties to establish a covert channel to transmit hidden messages.
- Nostega neither hides data in a noise (errors) nor produces noise, rendering the generated cover noiseless.
- The concealment process of Nostega has no effect on the linguistics of the generated cover if text is used as a steganographic carrier, rendering such text-cover legitimate.
- Unlike other approaches–(e.g.,) translation-based [23]–it can be applied to all languages.
- The use of these materials as steganographic carriers provides plenty of room for concealing data.

The remainder of this article is organized as follows. The following section describes the Nostega paradigm. The next section demonstrates examples methodologies that adopted Nostega paradigm followed by a discussion of steganalysis validation and the final section concludes the article and highlights the direction for future work.

NOISELESS STEGANOGRAPHY PARADIGM (NOSTEGA)

Bob and Alice are on a spy mission. Bob is a medical practitioner and Alice is a market analyst consultant. Before they went on their mission, which requires them to reside in two different countries, they plot a strategic plan and set the rules for communicating covertly using their professions and friendship as a steganographic umbrella. They basically agree on concealing messages by Graphstega and Chestega methodology. When using Graphstega [6, 14] they conceal data in graphs that are usually used in their profession. On the other hand, when using Chestega [7] they conceal data in games–(e.g.), chess, checkers, crosswords, dominoes–that friends usually play. To make this work, they establish a business relationship as follows. Bob is Alice's medical doctor and Alice is Bob's market analyst consultant. In addition, they are friends. When Bob wants to send a covert message to Alice, Bob either posts medical-related documents online for authorized patients to access or he can send medical-related documents via E-mail to the intended patients. These medical-related documents conceal a hidden message. Covert messages transmitted in this manner will not look suspicious because of Bob's profession. Furthermore, Alice is not the sole recipient of Bob's messages; other non-spy patients also receive their medical documents, further warding off suspicion.

When Alice decides to send Bob a message, she does it in the same manner as Bob, except she uses her profession to do so. She posts market analysis reports that Bob or anyone else can access or she sends market analysis–related documents via E-mail to a set of clients, including Bob. These market analysis reports and graphs conceal a hidden message. However, only Bob will be able unravel the hidden message because he knows the rules of the game. Alice's communication looks legitimate and nothing is suspicious because she is a market analyst and she does have a business relationship with both Bob and other non-spy clients.

Alice or Bob can use real data from their professions and their established business relationship to make their covert communications legitimate. If real data are not available, then untraceable data can be fabricated to avoid comparison attack if an adversary attempts to trace data and compare it to its original. In addition, since Bob and Alice are friends, they can employ Chestega and play games online that conceal data such as chess, checkers, crossword, dominoes, etc. The above scenario demonstrates how a Nostega paradigm can be employed. Nostega methodology is described in the remainder of this section.

The Architecture of Nostega

Nostega achieves legitimacy by basing the camouflage of both a message and its transmittal on a particular field such as education, economics, graphs, games, etc. As stated earlier, in the above example of Bob and Alice, using a particular profession or relationship gives legitimacy for camouflaging both a message and its transmittal. The core idea of the Nostega paradigm is basically camouflaging messages by embedding them in a form of noiseless data by employing either an altered authenticated data, or legitimate of untraceable data, as shown in the following section. The following is an overview of the Nostega architecture, which consisted of five modules as shown in Figure 1:

1. Steganographic Field Determination (Module 1): Determines the fields such as education, economics, graphs, games, etc., for achieving the steganographic goal. One of the major selection criteria is how the steganographic field facilitates the process of generating a noiseless cover in which the data are naturally embedded so that the cover looks innocent, raising no suspicion, and the hidden message is undetectable. Note that the process of Module 1 is only involved at the stage of constructing a Nostega-based system.
2. Steganographic Parameters Determination (Module 2): Encodes a message in an appropriate form for the camouflaging process (Module 3). The form and the component of the output of Module 1 may have an essential effect on how a message can be encoded. Therefore, studying and analyzing the output of Module 1 is necessary for determining the parameters that can be used by next module (Message Encoder). In other words, this module is responsible for determining what parameters can be

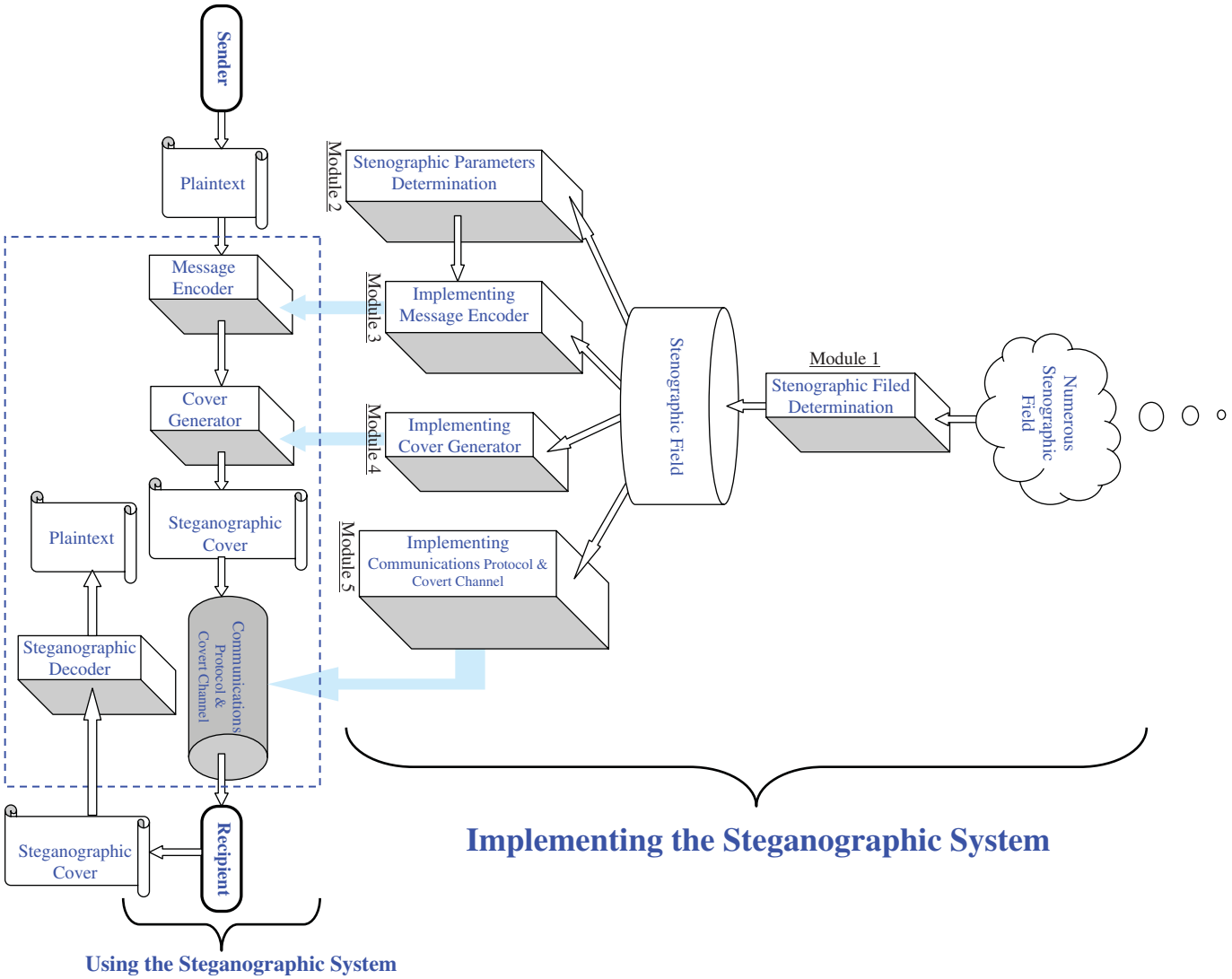

FIGURE 1 **Illustration of an overview of a Nostega paradigm showing the interaction of various stages to build a Nostega system and the configurations between communicating parties.**

employed in order to implement a steganographic code that can encode messages in an effective way. For instance, if the steganographic field is a graph, then the steganographic parameters may be numerical values to plot the graph-cover [6, 14]. On the other hand, if the steganographic field is chess games, then the steganographic parameters may be chess moves [7].

3. Implementing Message Encoder (Module 3): Implements a message encoder that is capable of accommodating the requirements of Nostega paradigm as stated earlier.
4. Implementing Cover Generator (Module 4): Constructing a cover generator or using a contemporary tool that is capable of achieving the steganographical goal. For instance, if the cover is graphs such as charts, then employing a tool that is used by a wide variety of people, such as Microsoft Excel, maybe a good option in order to generate a steganographic cover that looks like an ordinary graph. On the other hand, if the cover is chess, then chess software such as Chessmaster may legitimize the steganographic cover.
5. Implementing Communications Protocol & Covert Channel (Module 5): Configures the basic protocol of how a sender and a recipient would communicate covertly. It includes the covert channel for delivering a Nostega-based cover between the communicating parties along with the decoder scheme to unravel a hidden message. A covert channel can be based on

a justifiable reason as in the scenario of Bob and Alice.

Implementation Example

The aim of this subsection is to show example steganography methodologies that are based in the Nostega paradigm. Two examples are presented, namely, Graphstega [6, 14] and Chestega [7]. According to Nostega, there are five modules applied in order to implement a successful steganographic system. The first is to determine a particular domain that can be employed to achieve the steganographical goal. Graphstega uses graphs, whereas Chestega employs popular games such as chess. The second module identifies some steganographic parameters (steganographic carriers) that are capable of concealing data without creating noise. Graphstega exploits both numeric and nonnumeric values that can be easily plotted. Meanwhile, Chestega uses the chessboard, moves, popular games, name of the players, etc. In the third module, the message is encoded in a way that does not raise suspicious or constrain the generation of the steganographic cover. Graphstega and Chestega employ either authenticated data or untraceable data (private data). Fourth, contemporary tools are employed to generate the steganographic cover in such way to appear legitimate and innocent. In Graphstega a graph-cover is generated using non-steganographical tools such as MS Excel. On the other hand, in Chestega a chess-cover is generated using non-steganographical tools such as Chessmaster 8000. Thus, the generated cover appears as any ordinary graph or chess-related document. Finally, the chosen domain legitimizes the transmission of the cover; (e.g.), sharing a performance graph in Graphstega or game analysis or training session in Chestega. Figures 2 and 3 show detailed examples for Graphstega and Chestega, respectively.

STEGANALYSIS VALIDATION

The aim of this section is to show the resilience of the Nostega paradigm to possible attacks. Again, the success of steganography is qualified by its ability to avoid an adversary's suspicion of the presence of a hidden message. It is assumed that an adversary will perform all possible investigations. In addition, the adversary is also aware of the Nostega paradigm as a public paradigm, but he does not know the detailed of

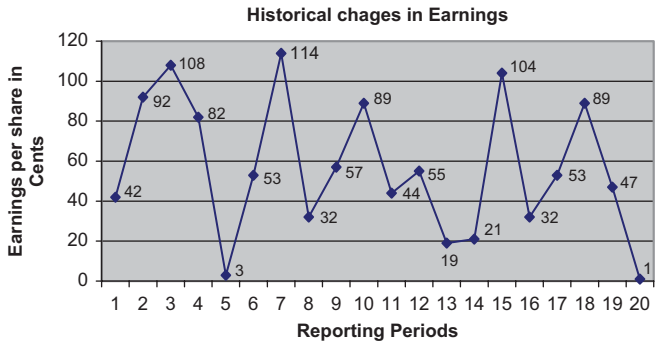

FIGURE 2 **An example graph cover that conceals the ASCII representation of the message "Use my secret key" using the earning values plotted in the graph.**

Nostega-based tool configuration that the sender and recipient employ for their covert communication.

Traffic Attack

One of the possible attacks an adversary may pursue is to analyze the communications traffic and the access patterns to publicly available or exchanged documents, images, graphs, files, etc. For example, the intelligence community has a number of tools at their disposal for analyzing traffic on the Internet, tracking access to Web sites, monitoring checked-out literature from public libraries, etc. The main goal of a traffic attack is to detect unusual or questionable association between a sender and a recipient. Traffic analysis intuitively can identify who communicates with whom. The relationship between the communicating parties will be then qualified based on the contents of the message. Traffic attacks can be applied to any contemporary steganography techniques regardless of the cover type (e.g., image, graph, audio file, text) and can achieve successful results with relatively low costs. In the context of Nostega, the subject of the cover is checked rather than its validity and consistency. If someone sends, receives, or accesses some materials without a legitimate reason for doing so, suspicion can be raised and further investigation may be warranted. The additional investigations will involve a thorough analysis of a steganographic cover, as detailed in the next subsection.

Traffic analysis is deemed ineffective with a Nostega paradigm. Nostega camouflages the transmittal of a hidden message to appear legitimate and thus suspicion is averted. Basically, Nostega ensures that the involved parties establish a covert communication channel by having a well-defined relationship with each other.

This lesson is about trading off piece(s) in order to gain a superior position. The following games demonstrate that having less material and good position can lead for winning.

Anderssen defeated Dufresne by sacrificing a piece to open the central files against the uncastled Black King, and despite his seemingly adequate development and;counterattacking chances, Black comes out a tempo short in one of the; finest combinations on record, justly known as the "Evergreen Game."

1. e4 e5
2. Nf3 Nc6
3. Bc4 Bc5
4. b4 Bxb4
5. c3 Ba5
6. d4 exd4
7. O-O d3
8. Qb3 Qf6
9. e5 Qg6
10. Re1 Nge7
11. Ba3 b5
12. Qxb5 Rb8
13. Qa4 Bb6

The Chessmaster recommends: Knight at b1 to d2.
Analysis: You move your knight at b1 to d2, which blocks Black's pawn at d3. Black answers with a castle. You move your knight to e4, which threatens Black's pawn at d3. Black responds with the pawn to d5, which disengages the pin on Black's pawn at f7 and forks your bishop at c4 and your knight at e4. Your pawn captures pawn en passant, which pins Black's pawn at f7, protects your bishop at c4 and your knight at e4, and attacks Black's knight at e7.

Black counters with pawn takes pawn, which removes the threat on Black's knight at e7 and isolates your pawn at c3. Your bishop at a3 takes pawn, which pins Black's knight at e7, attacks Black's rook at b8, and creates a passed pawn on c3. Black responds with the bishop to h3, which threatens checkmate (queen takes pawn), pins your pawn at g2 with a partial pin, and blocks your pawn at h2. You move your knight at f3 to g5, which frees your pawn at g2 from the pin. As a result of this line of play, you win two pawns for a pawn. Additionally, your mobility is greatly increased. Also, Black's pawn structure is somewhat weakened. Finally, the pressure on Black's King is slightly increased.

14. Nbd2 Bb7
15. Ne4 Qf5
16. Bxd3 Qh5
17. Nf6+ gxf6
18. exf6 Rg8
19. Rad1 Qxf3
20. Rxe7+ Nxe7
21. Qxd7+ Kxd7
22. Bf5+ Ke8
23. Bd7+ Kd8
24. Bxe7# 1-0

==========

This brilliancy-prize game by Henry Edward Bird, one of England's premier players for half a century, features a speculative queen sacrifice with the unusual combination of two rooks and knights against queen, rook and; knight. A delight!

1. e4 e6
2. d4 d5
3. Nc3 Nf6
4. exd5 exd5
5. Nf3 Bd6
6. Bd3 O-O
7. O-O h6
8. Re1 Nc6
9. Nb5 Bb4
10. c3 Ba5
11. Na3 Bg4
12. Nc2 Qd7
13. b4 Bb6
14. h3 Bh5
15. Ne3 Rfe8
16. b5 Ne7
17. g4 Bg6
18. Ne5 Qc8
19. a4 c6
20. bxc6 bxc6
21. Ba3 Ne4
22. Qc2 Ng5
23. Bxe7 Rxe7
24. Bxg6 fxg6
25. Qxg6 Nxh3+
26. Kh2 Nf4
27. Qf5 Ne6
28. Ng2 Qc7

The Chessmaster recommends: Queen to d3.
Analysis: You move your queen to d3. Black counters by moving the rook to f8, which attacks your pawn at f2. You move your king to g1, which frees your knight at e5 from the pin and protects your pawn at f2. Black responds by moving knight to c5, which attacks your queen. You move your queen to e2, which moves it to safety. Black replies by moving the rook at f8 to e8. You move your queen to a2, which frees your knight at e5 from the pin. Black responds with rook captures knight. Your pawn captures rook, which pins Black's pawn at d5 and creates a passed pawn on e5. Black answers with rook captures pawn. As a result of this sequence of moves, you win a rook for a knight and a pawn.

29. a5 Bxa5
30. Rxa5 Rf8
31. Ra6 Rxf5

...

==========

…..

FIGURE 3 **A chess-cover that conceals the ASCII representation of the message "He doesn't love you" using a chessboard-based encoding (message is hidden using the chess moves). The bit rate is up to 7 bits per move.**

Contrast and Comparison Attacks

One of the intuitive sources of noise that may alert an adversary is the presence of contradictions in the Nostega-based cover, such as finding inaccurate information in a particular cover; (e.g.), false information about a chess game or some naïve move made by a professional player. Contradictions can also be spotted when using data that indicate a clear violation of the rules in either a chess game or a graph. The use of authenticated

or untraceable data will definitely counter such an attack as used in the graph-cover. Untraceable data means data that matter only to a particular group or are shared privately; (e.g.), a game between two unknown amateurs or numbers in a private chart that cannot be contrasted or compared. Meanwhile, noise in the context of comparison attacks reflects alteration of authenticated or previously used data. The goal is to find any incorrect and inconsistent data that may imply the manipulation of Nostega-based cover contents to include a hidden message. The vulnerability of Nostega-based cover to comparison attacks depends on how the cover is generated. Employing an unaltered authenticated data makes the cover very resilient to this type of attacks. Figure 3 demonstrates how a tool like Chessmaster has allowed the selection of appropriate games that match an encoded message and facilitated the generation of the game description and analysis. An adversary cannot detect any discrepancy in a chess-cover when examining the authenticity of the data and the consistency of the text with respect to the style of what Chessmaster usually generates.

It is worth noting that the traffic analysis, discussed earlier, can also be pursued as a base for launching comparison attacks in case the data are not publicly accessible. In that case, current data are compared to a record of old data in order to search for any inconsistency over some period of time. Countering such an attack is always a challenge because it requires consistency with data that were previously used over an extended period of time. Contradictions would surely raise suspicion about the existence of a hidden message. Nostega, as demonstrated through examples, is simply made contrast-aware and comparison-aware. The flexibility in message encoding and the ability of employing more than one cover type enable Nostega to avert such attack.

Linguistics and Statistical Attacks

Linguistics and statistical attacks applies to Nostega-based methodologies–e.g., Chestega–that employ text covers. Linguistics examination distinguishes the text that is under attack from normal human language. Distinguishing the text from normal human language can be done through the examination of meaning, syntax, lexicon, rhetoric, semantic, coherence, and any other issues that can help to detect or suspect the existence of a hidden message. These examinations are used to determine whether or not the text that is under attack is abnormal. Generally, the text produced by natural language generation (NLG) systems usually meets the expected properties of a normal human language. Thus, employing NLG systems in cover generation would prevent noises caused by linguistic flaws. For example, the chess-cover shown in Figure 3 is generated by contemporary tools like Chessmaster, which makes it linguistically sound (free of errors). Furthermore, if there are errors in the NLG engine, it should not be a concern for two reasons: first, it applies to all of the generated text with and without a hidden message; second, nothing is concealed in errors. Therefore, it is obvious that a Nostega paradigm is capable of passing any linguistic attack by both human and machine examinations.

On the other hand, a statistical attack refers to tracking the profile of the used text. A statistical signature (profile) of a text refers to the frequency of words and characters used. For example, an adversary may use the statistical profile of chess text that contains no hidden message and compare it to a statistical profile of the suspected chess-cover to detect any differences. An alteration in the statistical signature of a text can be a possible way of detecting a noise that an adversary would watch for. Tracking statistical signatures may be an effective means for attack since it can be easily automated and combined with traffic analysis. Nonetheless, statistical attacks are ineffective with the Nostega paradigm since the hidden data are naturally an intrinsic part of the cover and not a noisy component that is imposed by alteration. This is also confirmed in the Chestega validation [7].

CONCLUSION

This article introduced Nostega, a novel steganography paradigm. Nostega promotes camouflaging both a message and its transmittal. Nostega neither hides data in a noise (errors) nor produces noise, rendering the generated cover noiseless. Instead, it conceals messages in a form of noiseless data in the generated cover using either unaltered authenticated data or untraceable data, thus avoiding wide varieties of attacks. The concealment process of Nostega has no effect on the linguistics of the generated cover if text is used as a steganographic carrier, rendering such text-cover legitimate. Unlike other approaches like translation-based,

it can be applied to all languages. For steganographic carriers, Nostega uses materials such as graphs, text, games, etc., that have plenty of room for concealing data. The implemented metrologies that are based on Nostega paradigm are keyless schemes. Yet, Nostega is a public paradigm, which implies that it is resilient even when an adversary is familiar with this new paradigm. It is observed that a steganographic system based on Nostega is capable of fooling both machine and human examinations. Applying Nostega to more steganographic fields is worth investigating in the future.

REFERENCES

1. Kipper, G. Investigator's Guide to Steganography. CRC Press LLC, 15–16, 2004.
2. Davern, P. and Scott, M. *Steganography Its History and Its Application to Computer Based Data Files*. School of Computing, Dublin City University. Internal Report Working Paper CA-0795. Available from http://computing.dcu.ie/research/papers/1995/0795.pdf [cited 3 August 2007].
3. Johnson, N. F. and Katzenbeisser, S. "A Survey of Steganographic Techniques." In Information Hiding, edited by S. Katzenbeisser and F. Petitcolas. Norwood, MA: Artech House, 1999, pp. 43–78.
4. Kessler, G. C. "An Overview of Steganography for the Computer Forensics Examiner." *Forensic Science Communications. Technical Report* 6(3) (2004).
5. Martin, A., Sapiro, G., and Seroussi, G. "Is Image Steganography Natural?" *IEEE Transactions on Image Processing* 14(12) (2005): 2040–2050.
6. Desoky, A. and Younis, M. "Graphstega: Graph Steganography Methodology." *Journal of Digital Forensic Practice* 2(1) (2008): 27–36.
7. Desoky, A. and Younis, M. "Chestega: Chess Steganography Methodology." *Journal of Security and Communication Networks*, in press.
8. Petitcolas, F. A. P. "Information Hiding—A Survey." *Proceedings of the IEEE* 87(7) (1999): 1062–1078.
9. Bennett, K. *Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text*. Purdue University, 2004. CERIAS Tech. Rep. 2004–13.
10. Shirali-Shahreza, M. H. and Shirali-Shahreza, M. (2006). "A New Approach to Persian/Arabic Text Steganography." *Proceedings of the 5th IEEE/ACIS International Conference on Computer and Information Science (ICIS-COMSAR 2006)*, Honolulu, Hawaii, July 10–12, 2006, pp. 310–315.
11. Anderson, R. J., Needham, R., and Shamir, A. "The Steganographic File System." *Lecture Notes in Computer Science* 1525 (1998): 73–82.
12. "ScramDisk: Free Hard Drive Encryption for Windows 95 & 98." Available from http://www.scramdisk.clara.net [cited 3 August 2007].
13. Handel, T. G. and Sandford, M. T. "Data Hiding in the OSI Network Model." *Lecture Notes in Computer Science* 1174 (1996): 23–38.
14. Desoky, A. and Younis, M. *PSM: Public Steganography Methodology*. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, 2006. Tech. Rep. TR-CS-06–07.
15. Kahn, D. The Codebreakers: The Story of Secret Writing. Rev. Ed. Scribner, 1996.
16. Wayner, P. "Mimic Functions." *Cryptologia* 16(3) (1992): 193–214.
17. Wayner, P. Disappearing Cryptography. 2nd ed. Morgan Kaufmann, 2002.
18. Chapman, M. and Davida, G. "Hiding the Hidden: A Software System for Concealing Ciphertext as Innocuous Text." *Lecture Notes in Computer Science* 1334 (1997): 335–345.
19. Chapman, M. Hiding the Hidden: A Software System for Concealing Ciphertext as Innocuous Text. Master's thesis, University of Wisconsin–Milwaukee, 1997.
20. Chapman, M., et al. "A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography." *Lecture Notes in Computer Science* 2200 (2001): 156–165.
21. Chapman, M. and Davida, G. I. "Plausible Deniability Using Automated Linguistic Steganography." *Lecture Notes in Computer Science* 2437 (2002): 276–287.
22. Grothoff, C., et al. *Translation-Based Steganography*. Purdue University, 2005. Tech. Rep. CSD TR# 05–009; CERIAS Tech. Rep. 2005–39.
23. Grothoff, C., et al. "Translation-Based Steganography." *Proceedings of Information Hiding Workshop (IH 2005)*, Barcelona, Spain, June 2005, pp. 213–233.
24. Stutsman, R., et al. "Lost in Just the Translation." *Proceedings of the 21st Annual ACM Symposium on Applied Computing (SAC'06)*, Dijon, France, April 2006, 338–345.
25. Topkara, M., Topkara, U., and Atallah, M. J. "Information Hiding Through Errors: A Confusing Approach." *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents*, January 2007, 65050V–1–65050V–12.
26. Shirali-Shahreza, M., et al. "Text Steganography in SMS." *International Conference on Convergence Information Technology* (21–23) (2007): 2260–2265.