International Journal of Informatics and Applied Mathematics
e-ISSN:2667-6990 Vol. 6, No. 1, 29-39

Steganalysis of Chat Based Steganography

Moses Oyaro Okello

Jiangsu University of Science and Technology, Zhenjiang, China
mosesokellomoses@gmail.com

Abstract. Steganalysis is the practice of identifying potential secret communication and taking appropriate action, such as deciphering to uncover the hidden contents or destroying the object containing the hidden information if it cannot be uncovered. At times, its very necessary to perform Steganalysis due to the fact that steganography is often misused by those with bad intentions, making it a platform for criminal communication. This paper presents a methodology for the detection of timing steganography. The method is based on user behavior during chat, such as the time taken to read, edit, and send text, etc. The method was tested using simulation-based chat software, and it can detect intended timing samples correctly.

Keywords: Steganalysis · Steganography · Timing · Chat

1 Introduction

Steganalysis is the practice of discovering hidden secrets within other open, clear information, as presented by [1], as well as [2]. Steganography and Steganalysis are both used to improve security because steganography hides information in the presence of an adversary, whereas Steganalysis uncovers or deciphers hidden information in the case of suspected secret communication flows among suspected criminals.

How is steganography or covert communication detected? This process involves step-by-step analysis of suspected payloads or packets, which are believed to contain hidden information. Firstly, the suspected payload or object is analyzed using any available known method for possible abnormalities such as the existence of inconsistencies or anomalies, etc., and then objects are classified accordingly. Then, those that contain some anomalies or inconsistencies are further deciphered to uncover hidden information, or if its impossible to uncover this hidden information, it is therefore destroyed to ensure that the hidden information does not reach the intended recipient.

As part of the privacy protection act enacted by most countries constitutions, an individual has a right to privacy, as presented in an article by[3] , and [4], as well as a covert communication article by [5]. However, at times such rights are violated by many, especially those with bad intentions. For example, criminals might conceal their communication while plotting to do activities that might be totally against the law or harmful to one another, as explained in a paper by [6].

Steganalysis aids in identifying and, if possible, extracting, recovering, or decrypting the suspected payload; if its impossible to decrypt, preferably destroying the suspected payload to disorient such covert communication among parties that would otherwise misuse the right to privacy, as presented in an article by [7]. By doing so, an appropriate measure can be taken early enough.

The problem arousing this research is based on the fact that most illicit activities are often coordinated activities that involve secretive communication among parties involved remotely. One of the ways through which this is done remotely is by steganography, such as network, image, text, audio steganography etc., to ensure that their communication is undetectable and remains concealed so that they bypass security systems (Steganalysis).

This paper is organized into five major sections: background studies, proposed methodology, experiments, discussion, and conclusion. Background studies are about the basics of the idea, motivation and challenges in steganalysis, organization of the paper, and related work to the proposed methodology of this research, which is mainly about timing steganography. The second section is basically concerned with the proposed methodology, which presents theoretical methods introduced to detect steganography, specifically timing steganography.

The next section presents experimental results mainly to check if the proposed methodology can detect the hidden communication flows and how well it can detect them, i.e., its percentage efficiency. After the experimental section, it is followed by the discussion section, which presents in-depth analysis, gaps, and any other findings in the paper. Conclusion, which provides a summary of what

is presented in the paper. The last section is a bibliography or reference list of relevant works.

2 Related Work

Several approaches and techniques have been proposed and are being used for the detection of information hiding. Take, for instance, an article by [8], which applies the techniques of artificial intelligence such Artificial Neural Network (ANN), deep neural networks (DNN), convolutional neural networks (CNN), etc. to tackle the challenges in steganalysis especially in image steganography, Signal-based steganography with techniques such as CNN works well for the detection of abnormalities in images, like in an article by [9] and [10], which use CNN techniques to detect images Steganography easily detects abnormalities left behind as a result of embedding confidential information in images. This same approach of using AI is also being applied in network steganalysis to detect anomalies in network traffic, for example in an article by [9] that explains how AI can be used in the detection of steganography.

This work is basically about the detection of timing steganography in networks, especially in chat based online applications. For example, a work by [11] on network timing detection uses a statistical method that detects small variations in signal noise. A sample of timing steganography work is presented by [12]. Which utilities inter-arrival time of network packets by varying the delay to hide information.

However, this proposed method is aimed at detecting chat-based timing steganography, which is presented in a paper by [13] and another paper by [14]. These papers use the time interval between two successive times of transmission or texting in the case of online chatting and a single time instance of steganography to hide secret information, which can be used in many platforms like online chat applications, video time codecs, network packet timing, audio timing, etc. In this paper, our main focus is on online chat application timing steganography.

3 Proposed Methodology

3.1 Formulation

This proposed method is based on the idea that user behaviors when chatting and attempting to perform timing with an intention to hide information are affected by their intention to send a particular text at a particular instance. Let time for receiving a message be t_1 Time for checking /reading message be t_2 Time for start typing t_3 Time for stop typing t_4 Time for sending message t_5 Total word count in a text N Total time for reading text t_6=t_3-t_2 Total time for typing t_7=t_4-t_3 Total time from end of typing to sending text $t_8 = t_5 - t_4$ For a known mean (μ) value and standard deviation(σ) of both typing speed and reading speed are (μ_1, σ_1) and (μ_2, σ_2) respectively. We can set a known average typing speed (mean) μ_1 words per second With allowable deviation of

σ_1 for very fast typist or very slow typist. So $(\mu_1 - \sigma_1)\mu_1(\mu_1 + \sigma_1)$ Since this methodology relies on typing speed, here we look into some of the few factors such as keyboard arrangements, keyboard types, etc. that affect typing speed as explained in the work by [15], which shows that typing speed using the Quartz keyboard and other keyboard types affects proficient typists with an average of 30 words per minute, whereas an inexperienced typist decreases to about 18 words per minute.

3.2 Detection Approaches

Typing Speed In this phase, we set a known mean average typing speed of word per second. Therefore, to find an average typing speed someone took to type a given number of words in a text, see equation 1.

$$t_9 = \frac{N}{t_7} \tag{1}$$

So, for a given number of words typed (N), divide by the total time spent typing t_7, we get a value that we compare against a set of known average (mean μ_1) typing speeds. But this mean value has a minimum and maximum set value to accommodate slow and very fast typists. Below is a mathematical expression (2) and code of function (1) for the above. Note: Throughout this text, the following numbers are returned based on detection status. i.e., (-1, 0, 1). However, if the returned number is (2) two, it implies that the encountered condition is outside of the listed range.

$$\delta = \begin{cases} -1 & if \frac{N}{t_4 - t_3} < (\mu_1 - \sigma_1) \\ 1 & if \frac{N}{t_4 - t_3} > (\mu_1 + \sigma_1) \\ 0 & if (\mu_1 - \sigma_1) \leq \frac{N}{t_4 - t_3} \leq (\mu_1 + \sigma_1) \end{cases} \tag{2}$$

Algorithm 1 Code 1: Returns timing Result based on equation 2

Require: $f1(N, t_3, t_2, \mu_1, \sigma_1)$
  $t_7 = t_4 - t_3$
  $t_9 = \frac{N}{t_7}$
  if $t_9 < (\mu_1 - \sigma_1)$ **then**
    $\delta = -1$
  else if $t_9 > (\mu_1 + \sigma_1)$ **then**
    $\delta = 1$
  else if $(t_9 \leq (\mu_1 - \sigma_1)) and (t_9 \leq (\mu_1 + \sigma_1))$ **then**
    $\delta = 0$
  else
    $\delta = 2$
  end if
  return δ

If the typing result is negative (-1), it implies that the typing rate is very slow, i.e., slower than the average mean value. So it can also mean that the typist is trying to slow down their typing speed in order to meet a target time. Hence the possible intent of timing and steganography detected.

But if the typing result is positive (+1), it implies that the typing rate is very fast, i.e., faster than the average mean value. So it can also mean that the typist is trying to increase the typing speed in order to meet a targeted desired time. Hence the possible intent of timing and steganography detected. In addition, if typing speed is very high, it could also mean the typist just copied and pasted text that was typed somewhere else and just waited for the perfect time to send (timing steganography) and simply copied and pasted the pre-typed text and sent it.

And lastly, if the typing result is zero (zero), it implies that the typing rate is normal, i.e., within the average mean value. So it can also mean that the typist is typing at normal speed, hence, no steganography is detected.

However, the problem with this method is that setting the average mean value can be difficult as different typists have different typing rates, which may lead to errors or inaccurate detection.

Time for Sending For this part we target time which a typist finishes typing t_4 to time of sending text t_5 We know that average reading speed of an individual can be set as μ_2 words per minute with a deviation of $_2$ words per minute. A mathematical expression (4) and code function (2).

$$t_8 = t_5 - t_4 \tag{3}$$

$$\delta = \begin{cases} -1 & if \frac{N}{t_5 - t_4} > (\mu_2 - \sigma_2) \\ 0 & if \quad 0 \leq \frac{N}{t_5 - t_4} \leq (\mu_2 + \sigma_2) \end{cases} \tag{4}$$

If the sending time is negative, it implies that the typist took some time or

Algorithm 2 Code 2: Returns possible timing Result based on equation 4

Require: $f2(N, t_5, t_4, \mu_2, \sigma_2)$
  $t_8 = t_5 - t_4$
  if $(t_8 \leq 0)$ and $(t_8 \leq (\mu_2 + \sigma_2))$ **then**
    $\delta = 0$
  else if $t_8 > (\mu_2 + \sigma_2)$ **then**
    $\delta = -1$
  else
    $\delta = 2$
  end if
  return δ

delayed too much after finishing typing to send the typed text. Hence, it is possible that the intention was to wait for a specific time to send a given text.

And Steganography detected. But if the sending time is zero, , implies that the sender did not delay that much to send a text after finishing typing, probably was reading to proof read the text before sending, or just sent the text without proof reading, hence no possible intention, and no steganography detected.

However, the challenges with this method are that sometimes it can be hard to differentiate a typist who, unintentionally, due to some condition, couldnt send a finished text on time. Or the one who would wish to proofread their text after finishing writing.

Reading Speed This section is only applicable for a received text in situation where there is need to reply for text and also a possible proof reading of typed text after finishing typing before sending, we know that one can spend total time t_6 reading a given text, supposed a known average/ mean for reading text is given as μ_2 with a standard deviation of σ_2 . But according to an article by[16], an average adult reading speed is about 250 words per minute. A mathematical expression (6) and code function (3) for the above on how to detect timing steganography.

$$t_{10} = \frac{N}{t_6} \tag{5}$$

$$\delta = \begin{cases} -1 & if \frac{N}{t_3 - t_2} < (\mu_2 - \sigma_2) \\ 1 & if \frac{N}{t_3 - t_2} > (\mu_2 + \sigma_2) \\ 0 & if (\mu_2 - \sigma_2) \leq \frac{N}{t_3 - t_2} \leq (\mu_2 + \sigma_2) \end{cases} \tag{6}$$

If the result is negative (-1), it implies that the reading rate is very slow, i.e.,

Algorithm 3 Code 3: Returns timing Result based on equation 6

Require: $f3(N, t_3, t_2, \mu_2, \sigma_2)$
  $t_6 = t_3 - t_2$
  $t_{10} = \frac{N}{t_6}$
  if $(t_{10} < (\mu_2 - \sigma_2))$ **then**
    $\delta = -1$
  else if $t_{10} > (\mu_2 + \sigma_2)$ **then**
    $\delta = -1$
  else if $((\mu_2 - \sigma_2) \leq t_{10}) and (t_{10} \leq (\mu_2 + \sigma_2))$ **then**
    $\delta = 0$
  else
    $\delta = 2$
  end if
  return δ

slower than the average mean value. So it can also mean that the typist is not reading, just delaying in order to meet a targeted desired time. Hence the possible intent of timing and steganography detected. But if the result is positive (+1), it implies that the reading rate is very fast, i.e., faster than the average mean

value. So it can also mean that the typist didnt read the sent text; they simply replied in order to meet the target time. In this case, there could even be a possible mismatch between the replied-to text and the received one. Hence the possible intent of timing and steganography detected. And lastly, if the result is zero (0), it implies that the reading rate is normal, i.e., within the average mean value. So it can also mean that the typist is reading at normal speed, hence no steganography is detected.

However, the problem with this method is that setting the average mean value can be difficult as different readers imply different treading rates, which may lead to a fault or inaccurate detection.

Real-time Detection From conditions (2), (4), and (6). We get a generalized condition (7), which is used after a typist taps on the send button. Which calls all the functions necessary to analyze the collected time data during typing activities. And for making a decision whether there could be a possibility of timing steganography or not, so that an appropriate action can be taken early enough before delivering the chat message to the recipient.

$$g = \begin{cases} 1 & if \delta \in \{-1, 1\} \\ 0 & else \end{cases} \tag{7}$$

Below code 4, function f4 is a code that calls functions f1, f2, and f3 at the moment when the submit or send button is pressed before a message is delivered to the recipient, so it can check if there is any possible Steganography.

So that appropriate action such as delay can disorient the timing or even block the message from being delivered to the intended recipient(s).

Algorithm 4 Code 4: Returns timing Result based on equation 7

Require: $f4()$
  if $f3(N, t_3, t_2, \mu_2, \sigma_2) \in \{0, 2\}$ and $f2(N, t_5, t_4, \mu_2, \sigma_2) \in \{0, 2\}$
   and $f1(N, t_3, t_2, \mu_1, \sigma_1) \in \{0, 2\}$ **then**
    ♯ Steganography not detected
  else
    ♯ Steganography detected,take appropriate action
  end if
  return δ

4 Experiment

4.1 Test Procedure

In this sub-section, a procedure on how to detect possibility of steganography and sample data are presented from two different approach. The first one in table

1 is when typist composes a text to send to someone, and we try to detect this typist typing behavior based on typing abnormalities as a result of their behavior. For testing purposes, we used data from a website blog which indicates different typing speed based on profession, gender, age etc. The average typing speed used here is 50 words per minute or 5/6 words per second in table 1 &2 just for testing purposes. A deviation of about 15 words was used to get the boundary limits A range of (35∼ 65) words per minute about (0.5833∼1.0833) words per second. For reading speed, an average of 250 words per minute with a deviation of about 30 words. About (220∼270)words per minute and approximately (3.6667∼4.5) words per second. For the highlighted cell in both table 1 and 2 indicates detected possible timing.

4.2 Test Data Presentation

In this sub-section, test data which were gathered from automated software are presented in table 1 and table 2. The first one in table 1 is when typist composes a text to send to someone, and we try to detect this typist typing behavior based on typing abnormalities as a result of their behavior. And in the second

Table 1. Recorded time activities for Text based Chat and Steganalysis

S/N	t_3	t_4	t_5	N	t_7	t_8	t_9
01	09:20:02	09:03:12	09:03:14	75	70	2	75/70
02	10:15:11	10:15:21	10:16:30	63	10	69	63/10
03	15:00:23	15:12:04	15:14:03	327	701	119	327/701
04	15:24:34	15:24:46	15:24:49	89	12	3	89/12
05	16:00:13	16:01:44	16:01:59	65	91	15	65/91

table 2, here the target is on someone who received a text message on an online application and replied the text. We also detect the typist behavior to identify any abnormality. Table Cell where its highlighted gray is the one with some extreme abnormality hence forming a basis of detection.

Table 2. Detection of timing for a Received text and reply

S/N	t_1	t_2	t_3	t_4	t_5	N	t_6	t_7	t_8	t_9
01	8:30:11	8:50:01	8:52:23	8:52:58	8:53:29	20	142	35	32	20/35
02	9:10:07	9:10:28	9:10:30	9:11::01	9:11:08	132	02	31	07	132/31
03	10:02:25	10:20:11	10:21:52	10:21:54	10:21:56	57	41	62	2	57/62
04	12:10:17	12:15:01	12:15:20	12:15:38	12:15:41	14	19	18	3	14/18
05	12:31:23	12:31:28	12:32:09	12:35:42	12:36:26	217	41	213	44	217/213

4.3 Analysis of Data

In this subsection, analysis of the process is made step by step on how to detect steganography in both Table 1 and Table 2. Throughout S/N, one up to five are in each table.

In table 1, there are five rows of collected time spent sending text from typing, editing, and sending; each time is extracted by an automated software program, which is then compared with known average mean values for typing speed, reading speed, etc. When there is deviation, or the gathered data is not within range, it is then, concluded as detected possible steganography else, it is concluded as no possible steganography In S/N, 1, the total time from the end of typing to sending text is two, which is less than the given normal range for reading, i.e., it is assumed that the reader has proofread their text before sending. 3.6667∼4.5 Throughout the table, S/N 1 to 5, values are compared with the given normal range in sub-section 3.1, and if they are within that range, it is concluded that there is no steganography; otherwise, there is a possibility of steganography.

Similarly, just like in the analysis of table 1, in table 2 there are 5 rows for each action taken from receiving text to replying to the sender. For example, in S/N 1, total time for reading text, total time for typing, total time from the end of typing to sending text, and an average typing speed someone took to type a given number of words in a text respectively, which are totally out of the range given in sub-section 3.1, hence, possibility of steganography. The same analysis is made throughout Table 2, S/N 2 to 5, and its compared with the values given in Subsection 3.1 to classify whether there is a possibility of steganography or not.

4.4 Discussion

Typing speed varies from one person to another depending on several factors, such as whether someone is still learning to type, is a slow typist, or an external factor affecting typing speed, etc. Hence, this may lead to false detection as it will be difficult to set an accurate mean value and range for normal typing activities. Similarly, the reading speed of an individual varies depending on their individual familiarity with the language being read, their age, the complexity of the text (such as fiction), and other outside factors that affect readers. The method is also restricted to only online text-based chat applications, and the use of timing in different scenarios or platforms, such as video-based timing and other network-based timing, may render this method ineffective.

Overall, this method is not a very robust one due to some reasons. For instance, it only works well with text-based chat applications, and there are many factors that affect the typing and reading speed of an individual as well as their behavior during chat. These often make the method susceptible to false detection as it is not easy to set an accurate mean value and deviation to accommodate different typists' normal behavior, which appears as intended timing.

5 Conclusion

This paper presents a methodology for steganography analysis that focuses on chat-based timing steganography. The method that relies on user or typer behaviors during typing when chatting, such as a recorded time taken to type a given total number of words in a text, time taken after finishing typing to send a text, time taken to read a given text, etc. The method was tested with sample chat on simulated application software, and it proved effective as presented, although there are some challenges that hinder the effectiveness of the method, which are also discussed in sub-section "Discussion."

I hope that as more work on this advances, a more accurate average mean value for both typing speed and reading speed can be achieved, and also that the use of artificial intelligence or any other method to detect correlation between two chat texts replying to one another will further enhance the detection of this method. At this stage, the method is still not 100 percent perfect at detection but is at least above average.

References

1. A. Nissar and A. H. Mir. Classification of steganalysis techniques: A study. *Digital Signal Processing*, 20(6):1758–1770, 2010.
2. N. F. Johnson and S. Jajodia. *September).* Steganalysis: The investigation of hidden information, 1998.
3. R. Kakungulu-Mayambala. Phone-tapping the right to privacy: A comparison of the right to privacy in communication in uganda canada. In *BILETA Conference*. 2008.
4. E. Atuhaire. *(2021).* Artificial intelligence and the right to privacy in Uganda (Doctoral dissertation, Makerere University).
5. M. O. Okello. (2022). *Optimal Covert Communication Techniques. International Journal of Informatics and Applied Mathematics*, 5(1):1–26.
6. Muawia Elsadig and Ahmed Gafar. (2022). *PACKET LENGTH COVERT CHANNEL DETECTION: AN ENSEMBLE MACHINE LEARNING APPROACH. Journal of Theoretical and Applied Information Technology. 100*, 100.:7035–7043.
7. K. Mivule and C. Turner. Applying data privacy techniques on published data in uganda. In *Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE)*, page 1. 2012.
8. Y. Zhang, W. Zhang, K. Chen, J. Liu, Y. Liu, and N. Yu. *June).* Adversarial examples against deep neural network based steganalysis, 2018.
9. Reinel Tabares-Soto, Ra l Ramos-Poll n, Gustavo Isaza, Simon Orozco-Arias, Mario Alejandro Bravo Ort z, Harold Brayan Arteaga Arteaga, Alejandro Mora Rubio, and Jesus Alejandro Alzate Grisales.
10. S. Tan and B. Li. *December).* Stacked convolutional auto-encoders for steganalysis of digital images, 2014.
11. S. Gianvecchio and H. Wang. *October).* Detecting covert timing channels: an entropy-based approach, 2007.
12. G. Liu, J. Zhai, and Y. Dai. Network covert timing channel with distribution matching. *Telecommunication Systems*, 49(2):199–205, 2012.

13. M. Okello. A new timing steganography algorithm in real-time transmission devices. *IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, China*, 10.:880–884, 2018.
14. M. O. Okello. (2021). *Transmission of Secret Information Based on Time Instances. The Eurasia Proceedings of Science Technology Engineering and Mathematics*, 16:209–218.
15. William Soukoreff, R., Scott Mackenzie, and I. Theoretical upper and lower bounds on typing speed using a stylus and a soft keyboard. *Behaviour Information Technology*, 14(6):370–379, 1995.
16. M. Brysbaert. How many words do we read per minute? A review and meta-analysis of reading rate. *Journal of memory and language*, 109:104047., 2019.