A Mixture of Timing Steganography and Series Cryptography

A Mixture of Timing Steganography and Series Cryptography

Moses Okello
Self-Employed, Gulu, Uganda
e-mail: mosesokellomoses@gmail.com

***Abstract*—This Paper presents improvement and extension of previous methodology about timing steganography based on network steganography. The previous article uses time interval between two successive transmissions mixed with cryptography prior to hiding. However this improvement tend to extend and provide new methods based on time format such as hours, minutes, second, millisecond and Nanosecond etc. It further examine how to handle effect of different time zone and high precision timing for ultrafast timing such as millisecond, Nanoseconds, picosecond, femtosecond which human action is too slow for perfect timing. In addition, the extension based on TCP-IP status codes where each elements of set of status code are index and the index represents certain numeric of combination for hiding. Finally, the cryptography method is improved and extended to series based cryptography with any defined number of different cryptographic methods combined altogether with multiple keys generated dynamically. The methods for both cryptography and steganography was integrated and each module carefully tested for their feasibility and appropriate analysis, comparisons is presented too.**

***Index Terms*—Steganography, Cryptography, Network Security, Time**

I. INTRODUCTION

Information security also refers to, as cyber security [1] is an area that deals with privacy and protection of confidential information. It sub-divides into several branches such as cryptography [2], steganography and many more. Steganography [3] is the practice of hiding information inside another information and can be categories into several sub-categories basing on the media use for hiding and transmitting or carrying hidden message.

Network Steganography: is the practise of concealing information in a network carrier by either modifying inter-arrival time for network data packet to network protocols for embedding secret message.

Multimedia Steganography: this is another type of steganography which uses Multiemedia[4] such as Images, Text, Audio and Video or motion picture for hidding secret information.

Text Steganography: this uses text for embedding secret message inside, by using method such as text formate modification such that the modification is invisible or by some form of text permutation just to embed the confidential message.

Video Steganograph: About hidding secret message in video which may include modifying motion picture information etc.

Audio Steganography just as video steganography is about hiding information in audio signal which can be noise signal to many more method describe in article.

Image Steganography. Is mostly about hiding secret information in image format such as jpg, png etc. Using some methods like Least Significant bit (LSB) Methods and many more.

II. EXISTING METHODOLOGY

There are some previously published articles in the area of timing steganography, which deals with concealing information based on timing especially in network. For the previous manuscript [5]which tend to hides bits using time interval (1) of inter-arrival of packets or events triggered in network Subject to $s.t$ (2).

$$\Delta t = t_i - t_{i-j} \quad (1)$$

$$s.t \;\; t_i \geq t_{i-j}\,;\; (i-j) \in k_1;\; k_1 \geq 0 \quad (2)$$

Where if $\Delta t \in k_2$ represents bit one else if $\Delta t \notin k_2$ represents bit zero. However, for $(i-j) \in k_1$ must always belong to the set of keys in order to keep track of the previous index of time t_{i-j}. The drawback of the method is that since each interval represents a bit, it is difficult to transmit more bits. For the case of cryptography methods, it only uses two alternating cryptography method i.e. XOR and bitwise shifting i.e. Right shift $(\ll)$ and Left shift $(\gg)$. For cryptography, method presented previous which uses bi-cryptography methods for encrypting a given piece of secret message (c) was mainly to scramble secrets information (c) prior to hiding and scramble (c) it is $e = (c \oplus k_1) \gg k_2$ In addition, to decrypt content in (e), and is $c = (e \ll k_2) \oplus k_1$.

A similar work presented in an article [6] where they slightly modify inter-arrival time of network packets. Their methods shows that the modification is untraceable as slight modification is undetected. However, due to advancement in detectability of covert timing channel it is possible to detect such slight or very small modification.

III. IMPROVEMENT OF METHODOLOGY

This section of the paper discusses and presents new concepts as an improvement of the previous article [5] and extension using TCP-IP status code. First sub-section III A introduce Unit of Time and the following sub-section after presents the improvement and extension methodology.

A. Unit of Time

Time units divides into several sub-units such as (3)

$$\infty \leftarrow : \text{hh} : \text{mm} : \text{ss} : \rightarrow \infty^{-1} \quad (3)$$

Smaller Units after Seconds are Millisecond (10^{-3}), Microsecond(10^{-6}), Nanosecond(10^{-9}), Picoseconds(10^{-12}), Femtosecond(10^{-15}), and can further subdivides up to infinitesimal unit (∞^{-1}). In term of seconds, it's express as (10^{-x}) where $x \in \mathbb{N}$ and if $x \to \infty$. Therefore, it is (10^{∞}) of a Second just like in [5]. It should be noted that $\infty = n^{\infty}$ for $n > 1$. Therefore, $\infty^{-1} = 10^{-\infty}$ see (3).

However for larger Units after hours are days, weeks, month, years, Decades, Century, Millennium (Kilo-Year), Mega-Year, Giga-Year, Tera-Year, eon, Supereon up to infinity(∞). Time is a special case where $\infty^{-1} \neq 0$ and $\infty^{-1} \not\approx 0$ because $\infty = \sum_{i=0}^{\infty} \infty^{-1}$.

The quest of how big is the biggest (∞) or how small is the smallest (∞^{-1}) lies beyond the realm of my understanding.

B. Time Format Steganography

In this improvement of timing using time format such as in (3) instead of using time interval like in the previous article[5] by using combination from set $V = \{0,1,2,3,4,5,6,7,8,9\}$ of numbers. However, a concepts from previous article [7] where use of Kleen Star $V^* = \{V_0 \cup V_2 \cup \ldots . \cup V_n\}$ formulae is applied for generating combination of numbers from set V using relationship$(\mapsto)$ i.e. $(a \mapsto b)$. For instance initially $V_0 = \{\emptyset\}$, and $V_1 = V;\ \ V_1 = \{0,1,2,3, \ldots . . ,9\}$ so possible combination of $V_2 = V_1 \mapsto V$: $V_2 = \{00,01,02,03, \ldots . , ,99\}$ and for $V_3 = V_2 \mapsto V$: $V_3 = \{000,001,002,003, \ldots . , ,999\}$. This continues up to a define number of combination n such that V_n can be express as in (4).

$$V_n = V_{n-1} \mapsto V \qquad (4)$$
$$s.t\ \ V_{n-1} = V_{n-2} \mapsto V$$

Hours (HH): For 12 hrs. System, the following condition must holds $1 \leq HH \leq 12$ where $V_0 = \{0,1,2,3,4, . . ,9\}$ for both AM and PM and $HH \in V_1$. For 24hrs system, it can be express as$V_2 = \{00,01,02,03, \ldots ,99\}$. Where $00 \leq HH \leq 23$ and $HH \in V_2$

Minutes (MM): In minutes, it is express numerically as $00 \leq MM \leq 59$ where $V_2 = \{00,01,02,03,04 \ldots . ,99\}$ $MM \in V_2$ And $MM \leq 59$ please see Table I for sample minutes assigned alphanumerical characters ALP and bit combinations as explains in [7] using two bit combination. Please note in Table I, the following means SP (Space), ST (Full Stop), CM (Comma). Here we use only uppercase letter and some few special character and numeric commonly use.

Seconds(SS): Second is defined as $00 \leq SS \leq 59$ and $SS \in V_2;\ SS \leq 59$ same as minutes.

Millisecond (MS): Millisecond is measure as $000 \leq MS \leq 999$. Since its maximum value is 999, from combination of set V, such that $V_3 = \{000,001,002, \ldots . ,999\}$ so $MS \in V_3$; $MS \leq 999$.

C. Time Numeric Concatenation

Given t_i, its numeric values of combination $n \geq 2$ is consider as concantenation $a||b$ [7] of set of digits index as $t_i = \{t_{i,0}||t_{i,1}|| \ldots ||t_{i,k}\}$. Suppose $t_i = V_{n,j}$ so $V_{n,j} = \{V_{n,j,0}||V_{n,j,1}|| \ldots ||V_{n,j,k}\}$. In addition $\Delta t'$ is a different between any two or more elements of set t_i or $V_{n,j}$. To find t_{i+1} for any known $\Delta t'$, t_{i+1} is express as in (5) (6) with the aid from (4) where $\Delta t'$ represents hidden contents.

$$t_{i+1} = V_{n,j+l} \qquad (5)$$
$$s.t\ \ \Delta t' = V_{n,j+l,k} - V_{n,j+l,k+1} \qquad (6)$$

$(j + l) \geq 0$ In addition, $(j, l) \in \mathbb{N}$ for any given t_i, $\Delta t'$ can be obtain from (7). If $t_i \geq t_{i.+1}$, it means t_{i+1} is in the next cycle of time.

$$\Delta t' = t_{i,k} - t_{i,k+1} \qquad (7)$$

So, by comparing $\Delta t'$ with Table I, or those in [7] to extract or hid matching content. An example of minute $t_i = 27$. So $t_{i,k} = 2$, $t_{i,k+1} = 7$ then $\Delta t' = 5$. For the case of $n > 2$, $\Delta t'$ can be from combination of any order example in (8) and (9) or many more. Also $\Delta t' = \Delta V'$

$$\Delta V' = V_{n,j,k}||V_{n,j,k+1} - V_{n,j,k+2} \qquad (8)$$
$$\Delta V' = V_{n,j,k}||V_{n,j,k+1} - V_{n,j,k}||V_{n,j,k+2} \qquad (9)$$

Example is $V_{n,j} = 256$, from (8) $\Delta V' = 19$ and from (9), $\Delta V' = -1$

Further inner layer e.g. $\Delta t''$ can be as in (10). Provided $\Delta t'' \in V_n; n \geq 2$

$$\Delta t'' = \Delta t'_k - \Delta t'_{k+1} \qquad (10)$$

Supposed (w) represents total of $('''')$, so $\Delta t'''$ is Δt^w when $w = 3$. General expression of (10) is in (11)

$$\Delta t^w = \Delta t_k^{w-1} - \Delta t_{k+1}^{w-1} \qquad (11)$$

$s.t\ \Delta t^w \in V_n$, $n \geq 2$. For Δt^* is define in (12) given that $\Delta t^0 = \Delta t;\ w \geq 0$

$$\Delta t^* = \Delta t^w - \Delta t^{w+1} \qquad (12)$$

Additional in-depth layer $\Delta t^{*\prime}$ can be express in many different ways such as in (13)

$$\Delta t^{*\prime} = \Delta t_k^* - \Delta t_{k+1}^* \qquad (13)$$

Note that for values of (t) of the corresponding $\Delta t^*, \Delta t^w$ should be within range of V_n

An example: Supposed Susan sent five digits access code and Mary received $t = 256$, and to decode secrete code; it is known that Mary has to use concatenation of absolute values of $\Delta t'||\Delta t''||\Delta t^*$.

Solution: from (8) $\Delta t = 19$ and from (10) $\Delta t'' = -8$, and from (12) $\Delta t^* = 27$. Therefore, Secret Access code is 19827

D. Time Numerical Interval

Time interval Δt also ΔV in term of V since $t_i = V_{n,j}$ (1) and (2) have been previously use for hiding bits[5] by comparing if the interval $\Delta t \in k_1$ then represents bit one else zero. However here, the improvement use combination technique in (4) since Δt is numeric such that $\Delta t \in \mathbb{N}$ where $\Delta t = \{0,1,2,3, \ldots . n\}$. Therefore, just like in Table I, these numbers can be compare with

alphanumeric values or bit combination. Those numbers are then the interval.in addition Δt just like in (7), (8), and up to (13) can be as (14). $s.t\ \Delta t \in V_n\ ; n \geq 2$

$$\Delta t' = \Delta t_k - \Delta t_{k+1} \quad (14)$$

Unlike in time format, different time zone does not affects time interval.

E. Time Zone

Different time zone: Across the globe, there is possibility that sender and receiver of secret message/information are located in different time zone(Z). Therefore, if the hidden information is encoded base on sender time zone, therefore for receiver to decode the right time, they must first subtract time zone (Z) from the receiver time (3) to get the sender time T_s. Here sender time zone is define as Z_s and receiver time zone Z_r . In addition, receiver time as T_r . To find sender time in order to decode the right time from receiver time, see (15).

$$T_s = (T_r + Z_s) - Z_r \quad (15)$$

However to find receiver time incase when hidden information is to be encoded using receiver time, sender need to use (16) to find the right receiver time for encoding the right information before sending.

$$T_r = (T_s + Z_r) - Z_s \quad (16)$$

For $(T_r, T_s) < 0$ indicate previous day $t_r += 24$ and for $(T_s, T_r) \geq 24$ in 24 hrs system indicates next day $t_r -= 24$. The same applies for t_s

Same Time Zone: For the case when both sender and receiver are located within the same time zone. $Z_s = Z_r$. Therefore, from (15) and (16) $T_r = T_s$.

Furthermore, considering non-real-time system with uniform delays δt should abstract from (15) and (16) to get the actual T_r, T_s. However, $\delta t \approx 0$ in real-time transmission system, so there is no need for subtracting anything as in [5]. For ultrafast timing (3), use of automated devices is highly recommended.

F. Extension to TCP-IP Status Code

For the use of TCP-IP status code given status code set $S = \{s_1, s_2, s_3, \dots, s_n\}$ where $s_i \in S$ and index i of the status code represents bit combination as shown in example Table II. Here, combination technique presented in (4) is use. Where combination base value $V = \{0,1\}$ representing binary numbers that is equivalent of bits and for set $V = \{0,1,2,3, \dots 9\}$ represents numeric integers and a set of TCP-IP status codes. For example see Table II where set of status code for hypertext transfer protocol (http) are index numerically up to 16 index from zero to fifteen, and this number of index are assign four bits combination. So to generate a given bit combination of total (n) $V_n = V_{n-1} \longmapsto V$ just like in (4) so for instance when $n = 4$. So $V_4 = \{0000, 0001, 0010, \dots \dots 1111\}$ for more details see paper [7] on how to generates combination of binary values. Please see Table II for sample http status code where each http status code has an index assigned to them and an equivalent bit combination allocated.

G. Improvement of Cryptography

From the previous bi-cryptography methods presented[5], multiple cryptography methods is presented called series based cryptography where a given character/information is encrypted up to a defined number of cryptography method with given number of varying keys as per the cryptography method presented. Supposed function $G(c, K)$ represents set of known cryptography methods such that $\{g_1(c, k_1), g_2(c, k_2), .., g_n(c, k_n)\} \in G(c, K)$ and $k_i \in K$ are set of keys for encrypting. For parameter (c) represents character, or information for encrypting by cryptography methods. $g_i(c, k)$ Moreover, (k_i) is key for encrypting information. To encrypt character (17).

$$e = g_n(g_{n-1}(\dots g_1(c, k_1) \dots, k_{n-1}), k_n) \quad (17)$$

To decrypt encrypted contents in (e), it is the reverse of the formulae in (17) please see (18) for decrypting. We assume that the function for decrypting is $G'(e, K')$ where $\{g_1'(e, k_1'), g_2'(e, k_2'), .. g_n'(e, k_n')\} \in G'(e, K')$ and $k_i' \in K'$ are sets of keys for decrypting encrypted contents.

$$c = g_1'(g_2'(\dots g_n'(e, k_n') \dots \dots, k_2'), k_1') \quad (18)$$

In the functions for decrypting $G'(e, K')$ takes in encrypted contents (e) with keys K' for decrypting and returns decrypted contents c. From the previous methods, $e = (c \oplus k_1) \gg k_2$ can write as $e = g_2(g_1(c, k_1), k_2)$ where $g_2(c, k_2) = (\gg\ll)$ representing the bitwise shift operator and $g_1(c, k_1) = \oplus$ representing XOR operator. To decrypt e, $c = g_1'(g_2'(e, k_2'), k_1')$ the same function can represents any cryptography method known and feasible, so that their combination is use to improve on security strength.

IV. EXPERIMENTAL RESULTS

A. Results for Timing Steganography

In this to show that this method can work perfectly, it is perform using minutes where records of chart messages and phone time of calls from the sender to receiver located within the same time zone. Fig 1 shows extracted time from calls in a day from sender and decoded as "MEETING 18:18 AT GULU" please see Table I for reference on how to extract the message and in addition, this is an unencrypted hidden message. However, both sender and receiver should know Table I before sending in order to encode and decode the hidden message.

08:49, 08:57, 09:01, 09:09, 09:18, 09:20, 09:39, 09:48, 10:20, 10:39, 11:18, 11:38, 11:53, 12:36, 12:41, 13:11, 13:32, 14:11

Figure 1: Shows extracted time of chart messages.

B. Results for TCP-IP Status Code

The experimental condition to verify the method base on http status code was perform on Server side and Client side where client received http status

code message from server by accessing web services from the server. The status code (S) received is then compare with information in Table II to extract the hidden contents it represents. The following extracted http status code $S = \{404, 403, 400, 503\}$, which indices are ID= {6, 5, 3, 9}. Now converting the numeric in base ten to base two binary. 6 is 110 in base two, 5 is 101 in base two, 3 is, 11 in base two, 9 is 1001 in base two. However, total bit combination is four in each base two, so adding zero in front to make four bit combination and Joining $\{0110 + 0101 + 0011 + 1001\}$, Converting from binary stream to characters ="e9" and decrypting to "Hi".

C. Results for Cryptography

To demonstrate the feasibility of the cryptography method, all $g_i(c, k_i) = c \oplus k_i$ operation see Fig 2. A console application shown in Fig 2 code written base on Series algorithm using only XOR cipher to test the algorithm and it works efficiently. However, for a mixture of more than one cryptography method like XOR and Bitwise shifting, it is required to modify the code base on (17) and (18).

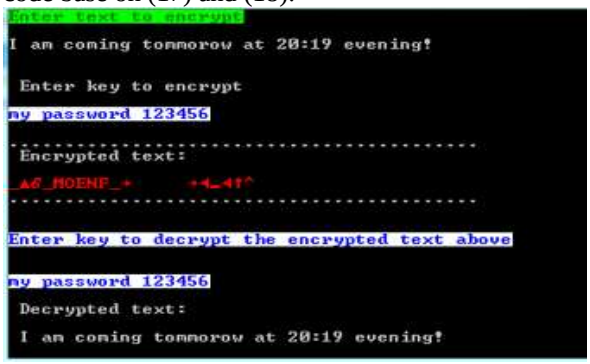

Figure 2: Shows testing XOR series algorithm.

V. ANALYSIS AND COMPARISON

A. Analysis of Timing Steganography

Let sample space be define as $n(V_i)$ (4), which is the cardinality of set V_i for both TCP/IP status code and timing steganography such as in (3). Therefore, the probability that a chosen status code or time format is the right one containing hidden information /character combinations can be express as $P = 1/n(V_i)$ and that it's not, can be express as $P' = (1 - P)$. Therefore, this implies that by making $n(V_i)$ big or large enough, it reduces the chances of guessing the hidden content as shown in the probability see (19).

$$P' = (n(V_i) - 1)\big(n(V_i)\big)^{-1} \quad (19)$$

In comparison to previous methods and some existing methods in timing steganography, this method including TCP/IP status code does not modifies the code or time for carrying hidden message as it only represents combination of bit/character to be hidden, so it is quite difficult to intercept the hidden information flow.

B. Analysis of Cryptography

This method is very hard for cryptanalyst to decrypt the encrypted contents. Let probability that $g_i(c, k_i)$ is breakable be p_i' and that it is not be p_i. Therefore, probability that at least one of $g_i(c, k_i)$ in (17) is not breakable is express as in (20).

$$P = 1 - (\prod_{i=1}^{n} p_i') \quad (20)$$

So as n in (20) increases, P approximately equals one, implying strength of cryptography increases with more series. However, more number of keys can delays execution for larger strings/text, as more cryptography methods and keys mean more series or repetitive encryption of the same character/information, so it is advisable to use fewer numbers of cryptography methods and keys with larger string where time performance is more important than security. Also repeating character in key will results into decrypting the encrypted contents like for the case of XOR cipher, which means no work done. Therefore, one should take care to avoid repeating keys.

Time performance analysis of formulae (17) and (18). Let total function of $g_n(c, k_n)$ operator in a series cryptography be (n) and time taken for each $g_i(c, k_i)$ in $G(c, K)$ operation be t_i. Therefore, total time T taken to encrypt a character a given number of operation is the summation of all t_i for using mixture of cryptography. Finally, to encrypt an entire string or text of total character"m", one has to use the formulae below (21) to find total encryption time.

$$T = m(\sum_{t=0}^{n}(t_i)) \quad (21)$$

To have higher security, element of set $G(c, K)$ should be large enough, however making these too large when "m" is large makes T extremely large, hence significantly slowing down execution time.

Therefore, to make time of execution T small, for larger value of m total of $G(c, K)$ elements should be as small as possible. However, by making $G(c, K)$ elements small means less keys. Therefore, security strength diminishes too. The equation (21) can embed directly into the algorithm (17) and (18) to calculate total time taken for encrypting a given set of text or string of character.

VI. CONCLUSION

This improvement and extension of previous article [5], which hides bits or information by using time format such as in (3). Moreover, TCP-IP status code using numeric index and combination technique that is in paper [7] has made it possible to hide more bits or information unlike in previous article [5] where time interval hides a single bit at each intervals. In addition, time being very reliable and also status code in TCP is very convenient unlike UDP where packets are delivered without acknowledgements or status updates or no delivery feedback makes TCP very desirable to use in the method due to the prompt status feedback.

The method further encrypt information prior to hiding to improve on un-detectability and making it hard to decrypt by improving the previous encryption methods to series base cryptography where contents to be hidden is first encrypted up to a given number of time with different encryption methods and different keys generated dynamically. The use of $\Delta t^{w}, \Delta t^{*}, \Delta t^{*\prime}$ for $w \gg 1$ remains a theoretical work and its practical application are beyond the scope of this work.

VII. REFERENCES

[1] Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." *computers & security* 38 (2013): 97-102.

[2] Katz, Jonathan, and Yehuda Lindell. *Introduction to modern cryptography*. CRC press, 2014.

[3] Wang, Huaiqing, and Shuozhong Wang. "Cyber warfare: steganography vs. steganalysis." *Communications of the ACM* 47, no. 10 (2004): 76-82

[4] Johri, Prashant, Amba Mishra, Sanjoy Das, and Arun Kumar. "Survey on steganography methods (text, image, audio, video, protocol and network steganography)." In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 2906-2909. IEEE, 2016.

[5] M. Okello, "A New Timing Steganography Algorithm in Real-Time Transmission Devices," *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, Chongqing, 2018, pp. 880-884.

[6] Liu, Guangjie, Jiangtao Zhai, and Yuewei Dai. "Network covert timing channel with distribution matching." *Telecommunication Systems* 49.2 (2012): 199-205.

[7] Okello, M. A Secure and Optimal Method of Steganography Using Bit Combination and Dynamical Rotation over Addresses. Preprints 2019, 2019020252

TABLE I: SHOWS ALPHANUMERICAL (ALP) AND BINARY COMBINATION (BC) ASSIGNED TO MINUTES (MM)

MM	ALP	BC	MM	ALP	BC
00	M	00	30	SP	10
01	E	01	31	X	11
02	8	10	32	L	00
03	S	11	33	4	10
04	3	00	34	0	10
05	N	10	35	I	11
06	G	01	36	SP	00
07	SP	11	37	B	01
08	Q	00	38	A	10
09	T	10	39	8	11
10	.ST	01	40	CM	00
11	U	11	41	G	01
12	Y	00	42	W	10
13	B	10	43	V	11
14	H	01	44	3	00
15	D	11	45	?	10
16	J	00	46	A	01
17	P	01	47	,CM	11
18	SP	10	48	:	00
19	O	11	49	M	10
20	1	00	50	C	01
21	J	10	51	N	11
22	R	01	52	6	00
23	K	11	53	T	10
24	2	00	54	5	01
25	W	10	55	S	11
26	9	01	56	F	00
27	Z	11	57	E	10
28	7	00	58	5	01
29	C	01	59	B	11

TABLE II: SAMPLE HTTP STATUS CODE (SC), INDEX (ID), BIT COMBINATION (BC)

ID	BC	http	ID	BC	http
0	0000	301	8	1000	411
1	0001	304	9	1001	503
2	0010	307	10	1010	204
3	0011	400	11	1011	205
4	0100	401	12	1100	302
5	0101	403	13	1101	308
6	0110	404	14	1110	405
7	0111	408	15	1111	410