The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2021

Volume 16, Pages 209-218

IConTES 2021: International Conference on Technology, Engineering and Science

Transmission of Secret Information Based on Time Instances

Moses Oyaro OKELLO
Jiangsu University of Science and Technology

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 time instances of transmissions mixed with cryptography prior to hiding. However, this improvement tends to extend and provide new methods based on single time instance unlike the previous methodology which depend on two-time instances such as hours, minutes, second, millisecond etc. It further examines how to handle effect of different time zone and high precision timing for ultrafast timing such as millisecond, and many more which human actions is too slow for perfect timing. In addition, the extension based on Transmission Control Protocol and Internet Protocol (TCP-IP) status codes where each element 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 cryptography methods combined altogether with multiple keys generated dynamically. The methods for both cryptography and steganography were integrated and each module carefully tested for their feasibility and appropriate analysis, comparisons presented too. A brief discussion of possible extension or application of Time Interval and Instance Steganography from network based to Video and Audio time Steganography are presented which depends on time such as rate of change of features in Video, or in Audio as well. However, these video and audio Time steganography are considered as out of scope for this article which is mainly about network Steganography.

Keywords: Steganography, Cryptography, Cyber Security, Time

Introduction

Information security also known as cyber security by Von et el (2013) is an area that deals with privacy and protection of confidential information. As a result of advancement in cyber security risk, there is need to develop advanced security methods for data protection. This call for improvement of existing security methods and or coming up with novel methods that outsmart advanced technological tools used for penetrating data Security/Privacy. Cyber security sub-divides into several branches such as cryptography by Jonathan et el (2014), steganography and many more. Steganography by Wang et el (2004) 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. Steganography can be classified into several categories as given below, see figure 1.

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 see an article by Mazurczyk et el (2016).

Multimedia Steganography: this is another type of steganography which uses Multiemedia such as Images, Text, Audio and Video or motion picture for hidding secret information see paper by Papapanagiotou et el (2005) and Johnri et el (2016).

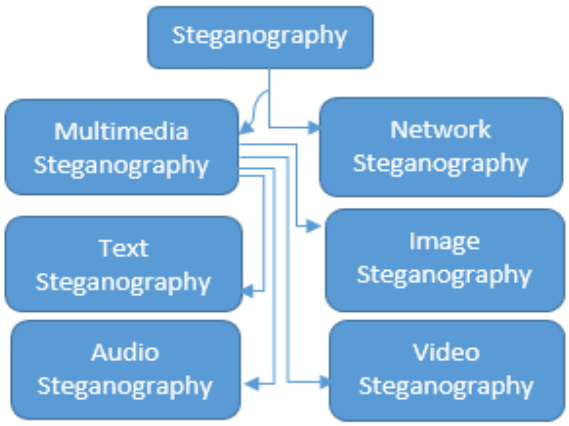
Text Steganography: this uses text for embedding secret message inside,as presented by Narayana et el (2018) based on method such as text formate modification such that the modification is invisible or by some form of text permutation just to embed the confidential message.

Video Steganograph: Is bassically about hidding secret message in video such as the one by Wang et el (2014) 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 methods fro example the one presented by Cvejic et el (2002) and Djebbar et el (2011).

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 for instance, by Kadhim el (2019).

Hybrid Steganography: this is when two or more of steganography methods is combine and used altogether for example: Image Steganography mixed with Text Steganography etc.



Figur 1. Classification of Stganography

Related Methodology

There are some previously published articles in the area of timing steganography, which deals with concealing information based on time instances especially in network. This initially appeared in preprint Okello (2020). For the previous manuscript by Okello (2018) which hides bits based on time interval (1) of inter-arrival of packets or events triggered in network Subject to $s.t$ (2).

$$\Delta t = t_i - t_{i-j} \tag{1}$$

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

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 by Liu et el (2012) where they slightly modify inter-arrival time of network packets. Their methods show 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.

Improvement of Methodology

This section of the paper discusses and presents new concepts as an improvement of the previous article by Okello (2018) and extension using TCP-IP status code. First, we introduce Unit of Time and the following sub-section after presents the improvement and extension methodology.

Unit of Time

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

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

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 an article by Okello (2018). 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 $\infty^{-1} \approx 0$ 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.

Time Instance Steganography

Table 1. 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

In this improvement of timing using time format such as in (3) instead of using time interval like in the previous article by Okello (2019) using combination from set $V = \{0,1,2,3,4,5,6,7,8,9\}$ of numbers. However, a concept from previous article Okello (2019) 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 $V_1 = V$; so $V_1 = \{0,1,2,3, \ldots . . ,9\}$. Therefore, 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 combinations n such that V_n can be express as in (4). Please Table 1 for and reference corresponding characters.

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

Hours (hh)

For 12 hrs. System, the following condition must hold $1 \leq hh \leq 12$ 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 1 for sample minutes assigned alphanumerical characters ALP and bit combinations as explain in paper by Okello (2019) using two-bit combination. Please note in Table 1, 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 $ms \in V_3$; $ms \leq 999$.

Time Numeric Concatenation

Given t_i, its numeric values of combination $n \geq 2$ are consider as concatenation $a||b$ in an article Okello (2019) 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. Please note $\bowtie$ simply represents any of this operator $+, -, *, /$
Which can be use but because $+, -$ is the only operator that can be easily use, so we omit the rest of operators.

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

$(j + l) \geq 0$ 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.

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

So, by comparing $\Delta t'$ with Table 1, or those presented by Okello (2018) to extract or hid matching content. An example of minute $t_i = 27$. So $t_{i,k} = 2$, $t_{i,k+1} = 7$ then $\Delta t' = 5$. And we take $\bowtie = -$ for the case of $n > 2$, $\Delta t'$ can be from combination of any order example in (8) and (9) or many more. Also $\Delta t' = \Delta V'$

$$\Delta V' = V_{n,j,k} || V_{n,j,k+1} \bowtie V_{n,j,k+2} \tag{8}$$

$$\Delta V' = V_{n,j,k} || V_{n,j,k+1} \bowtie V_{n,j,k} || V_{n,j,k+2} \tag{9}$$

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 $\Delta t'' \in V_n; n \geq 2$

$$\Delta t'' = \Delta t'_k \bowtie \Delta t'_{k+1} \tag{10}$$

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

$$\Delta t^w = \Delta t_k^{w-1} \bowtie \Delta t_{k+1}^{w-1} \tag{11}$$

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

$$\Delta t^* = \Delta t^w \bowtie \Delta t^{w+1} \tag{12}$$

Additional in-depth layer $\Delta t^{*'}$ can be express in many different ways such as in (13)

$$\Delta t^{*'} = \Delta t_k^* \bowtie \Delta t_{k+1}^* \tag{13}$$

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

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 in article Okello (2018) by comparing if the interval $\Delta t \in k_1$ then represents bit one else zero. However here, the improvement uses 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 1, these numbers can be compared 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). $s.t\ \Delta t \in V_n\ ; n \geq 2$

$$\Delta t' = \Delta t_k \bowtie \Delta t_{k+1} \tag{14}$$

Unlike in time instances, different time zone does not affect time interval.

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 defined 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).

$$T_s = (T_r + Z_s) - Z_r \tag{15}$$

However, to find receiver time in case 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.

$$T_r = (T_s + Z_r) - Z_s \tag{16}$$

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 just like in Okello (2018). For ultrafast timing (3), use of automated devices is highly recommended.

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 2. 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 2 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) $V_n = V_{n-1} \mapsto V$ just like in (4) so for instance when $n = 4$. So $V_4 = \{0000, 0001, 0010, \dots \dots 1111\}$ for more details see paper by Okello (2019) on how to generate combination of binary values. Please see Table 2 for sample http status code where each http status code has an index assigned to them and an equivalent bit combination allocated.

Table 2. Sample http status code (SC), index (ID), and 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

Improvement of Cryptography

From the previous bi-cryptography methods presented by Okello (2018), 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).

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

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.

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

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 represent any cryptography method known and feasible, so that their combination is use to improve on security strength.

Experimental Results

Results for Timing Steganography

In this to show that this method can work perfectly, it is performed using minutes where records of chart messages and phone time of calls from the sender to receiver located within the same time zone. Figure 2 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 2. Shows extracted time of chart messages.

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".

Results for Cryptography

To demonstrate the feasibility of the cryptography method, see Table 3 where a given text is encrypted using series-based cryptography methods.

Table 3 Shows how to encrypt contents using series Cryptography having three Cryptography methods

Functions	Initial c_0	$g_1(c_0, k_1)$	$g_2(c_1, k_2)$	$g_3(c_2, k_3)$
Cryptography Methods	Plain texts	Blowfish	AES	RSA
Key(s)		654321	65431234okello10	Public key not included here
Text to be encrypted	Hello, how are you doing today?	C2iPxDg9gInP+Pg OFX7DYjXUoWAM 6bPtQGVoFgo/qwY=	F5580164B3908025A CF548DAC94049A1A BABB225C67DE4209 7287E8FC9FB378C87 7C79C7F73DE4B5AE F01C62987BFC99	KFEzHUJ+mHIMfFn0WvfuGj+ VIM75PsVyZIuunEZ+8iRhGVY okchuEq6nyYpzY4zYocSc1MQX VwikBQrEHi9ihjklhqwxom/7clxk Q3w2KhhnIV6wGmzrutsIwOx6T Xorpylb0S6wZLZGnm/gS5ol7IHs 4c8cIYZqOixWRyGvf2g=

To decrypt the contents in Table 3 see Table 4 blow here

Table 4 shows how to decrypt contents using series Cryptography with three Cryptography methods

Functions	Initial $g_3'(c_3, k_3)$	$g_2'(c_2, k_2)$	$g_1'(c_1, k_1)$	Decrypted Text c_0
Cryptography Methods	Encrypted Texts Using RSA	AES	Blowfish	Plain Text
Key(s)	Enter Public key not included	65431234okellо10654321	654321	
Text to be decrypted	KFEzHUJ+mHIMfFn0WvfuGj+ VIM75PsVyZIuunEZ+8iRhGV YokchuEq6nyYpzY4zYocSc1 MQXVwikBQrEHi9ihjklhqwx om/7clxkQ3w2KhhnIV6wGmz rutsIwOx6TXorpylb0S6wZLZ Gnm/gS5ol7IHs4c8cIYZqOix WRyGvf2g=	F5580164B39 08025A CF548DAC9 4049A1A BABB225C6 7DE4209 7287E8FC9F B378C87 7C79C7F73D E4B5AE F01C62987B FC99	C2iPxDg9gI nP+Pg OFX7DYjX UoWAM 6bPtQGVoF go/qwY=	Hello, how are you doing today?

Analysis and Comparison

Analysis of Time Instance Steganography and TCP-IP

Let sample space he defines 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).

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

In comparison to previous methods and some existing methods in timing steganography, this method including TCP/IP status code does not modify 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.

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).

$$P = 1 - (\prod_{i=0}^{n} p_i') \tag{20}$$

So as n in (20) increases, P approximately equals one, implying strength of cryptography increases with more series. However, a greater number of keys can delay 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 is (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 operations 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.

$$T = m(\sum_{i=0}^{n}(t_i)) \tag{21}$$

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.

Discussion of Possible Extension

In this sub-section, further ways of how to encode information based on both video and audio or even text-based steganography.

Video: For video, it is based on the idea that video comprises of moving pictures in which a feature in a recorded video is timed such that the instances or the interval represent the intended message just like in network steganography.

For example, in action movie where background of actors angle/positioning of reference object/Actor or even some tiny feature which is part of the video that keep changing at a varying interval or at given instances. A similar approach can be used in Audio such as timing of sentences construction, tone variation, etc. For text, it's quite difficult. However, the concept of numerical value in Time interval or Time instance steganography can also be applied in text where possible.

Conclusion

This improvement and extension of previous article by Okello (2018), 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 **Hata! Başvuru kaynağı bulunamadı.** has made it possible to hide more bits or information unlike in previous article Okello (2018) where time interval hides a single bit at each interval. 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 encrypts 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 times 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.

Scientific Ethics Declaration

The author declares that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the author.

References

Cvejic, N., & Seppanen, T. (2002, December). Increasing the capacity of LSB-based audio steganography. In *2002 IEEE Workshop on Multimedia Signal Processing.*

Djebbar, F., Ayad, B., Hamam, H., & Abed-Meraim, K. (2011, April). A view on latest audio steganography techniques. In *2011 International Conference on Innovations in Information Technology* (pp. 409-414). *IEEE Transactions on Information Forensics and Security*, *9*(5), 741-751.

Johri, P., Mishra, A., Das, S., & Kumar, A. (2016, March). 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).

Jonathan, K., & Yehuda, L. (2015). Introduction to Modern Cryptography.-2nd. http://203.162.10.101/jspui/handle/123456789/723

Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, *335*, 299-326.

Liu, G., Zhai, J., & Dai, Y. (2012). Network covert timing channel with distribution matching. *Telecommunication Systems*, *49*(2), 199-205.

Mazurczyk, W., Wendzel, S., Azagra Villares, I., & Szczypiorski, K. (2016). On importance of steganographic cost for network steganography. Security and Communication Networks, 9(8), 781-790.

Narayana, V. L., Gopi, A. P., & Kumar, N. A. (2018). Different techniques for hiding the text information using text steganography techniques. *Neurocomputing*, *335*, 299-326.

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

Okello, M. (2020). A mixture of timing steganography and series. https://www.techrxiv.org/articles/preprint/A_Mixture_of_Timing_Steganography_and_Series_Cryptography/13134992

Okello, M. A (2019). Secure and optimal method of steganography using bit combination and dynamical rotation. Over Addresses. Preprints 2019, 2019020252. https://www.preprints.org/manuscript/201902.0252/v2

Papapanagiotou, K., Kellinis, E., Marias, G. F., & Georgiadis, P. (2005, December). Alternatives for multimedia messaging system steganography. In *International Conference on Computational and Information Science* (pp. 589-596). Springer, Berlin, Heidelberg.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102.

Wang, H., & Wang, S. (2004). Cyber warfare: steganography vs. steganalysis. *Communications of the ACM*, *47*(10), 76-82.

Wang, K., Zhao, H., & Wang, H. (2014). Video steganalysis against motion vector-based steganography by adding or subtracting one motion vector value. *IEEE Transactions on Information Forensics and Security*, *9*(5), 741-751.

Author Information

Moses Oyaro OKELLO
Jiangsu University of Science and Technology Gulu,
Uganda
Contact e-mail: *mosesokellomoses@gmail.com*

To cite this article:

Okello, M.O. (2021). Transmission of secret information based on time instances. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)*, *16*, 209-218.