Steganographic Communication using Multiplayer Online Game

Mohd. Akram[1], Jasbir Singh[2], Lalit Sen Sharma[3]

[1]M. Tech. Final Year Student, [2]Assistant Professor, [3]Professor
[1, 2, 3] Department of Computer Science and IT, University of Jammu

---***---

Abstract: Steganography is the technique of hiding secret data in innocuous-seeming object, so that the existence of secret is undetectable to the third party observer. In this paper we proposed a covert timing channel to transmit the covert data through the game,"8 Ball Pool", as 8 ball pool is a very popular game in standalone system and is also available to be played online against other players & friends in 1-on-1 matches. This game has several properties, using which, Steganography can be performed. Here the time of 30 seconds (given to every player to play their shot) is divided into four different intervals each communicating two bits of information. Theoretical proof and experimental result are provided to shows that if steganography driven games are played in between normal games, it becomes difficult to detect.

Keywords: Steganography, 8 Ball Pool, Steganalysis.

1. INTRODUCTION

Steganography is an art of secret communication in which the information of users is concealed by users themselves with the utilization of a range of varieties of cover media. In the last decade, text, images, audio etc. are become the well-known cover media for concealing the information. Games are deployed in discovering numerous recent studies for performing steganography. (e.g. Hernandez-Castro et al., 2006; Desoky and Younis, 2009; Farn and Chen, 2009a, 2009b; Kieu et al., 2009; Lee et al., 2008, 2010; Ou and Chen, 2014; Sushmita, Dalip and Danish, 2016).

2. LITERATURE REVIEW

Hernandez-Castro et al. (2006) suggested asteganographic technique for hiding the secret message on the basis of moves in a game. The suggested technique supposed that a winning score was obtained for each move with a searching algorithm. A move which assisted in generating better score was taken into consideration as the more favorable move. The score produced during the game was a basis technique using which a sorted-move sequence was obtained. Ifa player wanted to launch a secret message 'i', the ith move was selected by the player in the sorted move sequence for demonstrating a secret 'i'. Sometimes, the selection of optical move was not done in which the abnormal move employed as 'i' was present in between 1 and n. Therefore, the abnormal move had potential for detecting the steganographic technique that assisted in concealing the data. Moreover, distinct searching algorithms were needed in several expensive-forms of games and it was complicated task to construct these kinds of algorithms.

Kieu et al. (2009) recommended a Sudoku-based image hiding technique for which spatial domain was employed. Secret number S Ɛ {1, 2 . . . , 9} was concealed utilizing every pixel pair (i, j) in a cover image. The recommended technique enlarged a solved Sudoku having 9 × 9 matrix to 261 × 261 look-up table. The values v_i and $v_j$were taken as the gray value of a pixel pair (i, j). Anindex for the look-up table was represented using (v_i ,v_j). The nearest element (v'_i,v'_j) was searched through the hiding method in the look-up table for number S at time of mismatching of (v_i ,v_j) with the secret number S. The replacement of gray values of pair (i, j) was done with (v'_i,v'_j) as the property value of the Sudoku matrix was changed (v_i-v'_i,v_j-v'_j) that was found approximately very less (±2, ±2).But, the similar Sudoku grid information was shared between the sender and receiver. Conversely, the recommended technique was unable of enduring compression attack.

Farn and Chen (2009a, 2009b) intended 2stegano-graphic schemes in two kinds of puzzle games. In the first scheme, secret message was hidden within every attached semi-cycle on the basis of its positions and kinds on a jigsaw puzzle image. The piece permutation was executed in a jig-swap puzzle game to conceal a secret message in second scheme as pixel value was not taken in account for embedding the secret message; these schemes had robustness for resisting the compression attacks. But, the puzzle image's size restricted the intended schemes because the size of a puzzle piece was decipherable to the players.

Desoky and Younis (2009) investigated asteganographic technique for which Chess game was deployed. This technique concealed the message in chess related covers which had not developed the noise or generated a detectable noise. As there was not any utilization of approach key in this technique, approach was carried out. The position of chess board, pieces and outcomes etc. had contained in chess data. However, chess-stega was aware an adversary as the contradictions were available in the chess cover including the discovery of regarding a game which was not accurate or few naive moves made through a professional player.

Lee et al. (2010) presented asteganography technique for hiding the secret data. For this, a perfect maze game in which cells, walls, a starting cell and an end cell included was implemented. In general, this game was a puzzle having complex multipath network that comprised a player who had to discover a path between the starting cell and the end cell. A perfect maze was a rectangular maze of m × n cell that included only one path amid any two cells. Thus, an enhanced algorithm was suggested for boosting the embedding capacity and for preserving the perfect property. The prefect mazes were produced that was not easily distinguished in visual form by human from other prefect mazes whose deployment was not done.

Ritchey and Rego (2012) designed a general framework to utilize the covert channels in combinatorial games. The authors demonstrated that the stego-games were not differentiated from clean games with application of the strict requirement that forced the perfect play. The experimental analysis was conducted applying Tic-Tac-Toe game. The presented framework was proved adaptable to other multiplayer games such as Dots and Boxes, Battleship etc.

Ou and Chen (2014) suggested asteganographic technique on basis of online Tetris game that embedding the secret message in the termino sequences. Based on this message, a Tetris game was uploaded on the Internet with the embedding technique and the secret message was provided by the receiver by means of the extracting algorithm. There was a necessity of transmission of pre-shared secret key for which a secure communication channel was employed.

Sushmita, Dalip and Danish (2017) recommended a novelsteganographic technique that utilized Minesweeper game. The secret message was concealed by applying the position of mines available within the minesweeper grid. The recommended technique was executed to embed the secret message and the extracting algorithm was carried out for acquiring a secret message through the receiver. Humans were unable to differentiate the produced minesweeper grid visually from other minesweeper games that had commonly exploited.

In this paper the constructed covert timing channel was done to establish the Steganographic communication within the 8 ball Pool game. A time of 30 seconds was split into 4 different intervals in which two bits of information was communicated in each interval for setting up the covert timing channel.

The rest of paper is organized as: Section 2 describes regarding8 Ball Pool. In Section 3, Covert Channel Description is discussed. The Security of the channel is explained in Section 4. Section 5 discusses the Observations and efficiency of the channel is elucidated in Section 6.

3. 8 BALL POOL

The 8 Ball Pool game designed by Miniclip is one of the largest & multiplayer online games. This game is played free of cost against other players and friends in 1-on-1 matches.

3.1 How to play 8 ball pool: This game is played with 1 cue ball (white) and 15 object balls with numbered 1 through 15.An individual player tries to pocket the solid-colored balls numbered 1 through 7. While the other player attempts to hit the striped balls numbered 9 through 15. A player is not allowed to pocket the 8-ball unless he or she has pocketed every suitable ball. (stripes or solids). The player lawfully pocketing the 8-ball is declared the winner of the game.

3.2 Time Allowed: The players are allotted with a time frame of 30 second for shot playing by giving a signal of 30 seconds in this game. This involves the break shot.

3.3 How to play 8 ball pool with friends: 8 Ball pool permits user for playing against computer challengers or with friends. Steps to play against your friends are mentioned below.

Step1. Opening the App: To open the Application, click on 8 Ball Pool icon. This opens the app.

Step2.Connections with friends: Suppose you have already linked to Facebook or added friends already, Tap to "Play With Friends" button.

Step3.Finding a friend to play against: When you look at your list of friends that you have added. Choose the friend you wish to play against by tapping play next to that friend's name. Note: *The selected friend should be online to accept your challenge*.

Step4.Finding the venue: Based on coins that you have and how far you've progressed in the game, there is many choices of venue. Slide to accentuate your selected venue and tap on the venue button.

Step5. Giving it your all: Now that you have thrown challenge to your friend (assuming they are online at the same time as you) and you have chosen the venue, it's time to play the game.

Step6. Not online: If your friend is not online, you will get a notification when they come online and you can play with them.

4. COVERT CHANNEL DESCRIPTION

In order to relay messages, a covert timing channel modulates some feature of system behavior over time. This is done to enable program receiving the information for observing system behavior and inferring secure information. This means that operations carried out by timing channels make changes in the original response time noticed by the receiver.

According to the rules of "8 Ball Pool" game, every player is allotted a time of 30 seconds for playing shot. This research work manipulates the time allotted to the player for playing shot so that the information can be relayed covertly. This work creates a covert timing channel by separating the allotted 30 seconds into four differ intervals. In every interval, two-bit information is transferred as presented in the following table:

Time Interval (secs)	Bits Communicated
1-7	00
8-15	01
16-22	10
23-30	11

The broadcasted messages contain just small-case letters, numbers, dots(.) and white spaces. The use of a randomly selected upper-case latter is carried out to indicate the beginning and ending of the covert information sharing. Moreover, the preference is given to a 6-bitbinary code over the 8-bit ascii code for increasing the capacity as shown in the table below:

Letter	ASCII Code	Binary code	Letter	ASCII Code	Binary code
A	0	000000	g	32	100000
B	1	000001	h	33	100001
C	2	000010	i	34	100010
D	3	000011	j	35	100011
E	4	000100	k	36	100100
F	5	000101	l	37	100101
G	6	000110	m	38	100110
H	7	000111	n	39	100111
I	8	001000	o	40	101000
J	9	001001	p	41	101001
K	10	001010	q	42	101010
L	11	001011	r	43	101011
M	12	001100	s	44	101100
N	13	001101	t	45	101101
O	14	001110	u	46	101110
P	15	001111	v	47	101111
Q	16	010000	w	48	110000
R	17	010001	x	49	110001
S	18	010010	y	50	110010
T	19	010011	z	51	110011
U	20	010100	0	52	110100
V	21	010101	1	53	110101
W	22	010110	2	54	110110
X	23	010111	3	55	110111
Y	24	011000	4	56	111000
Z	25	011001	5	57	111001
a	26	011010	6	58	111010
b	27	011011	7	59	111011
c	28	011100	8	60	111100
d	29	011101	9	61	111101
e	30	011110	Space	62	111110
f	31	011111	.(Dot)	63	111111

The efficiency and security of the proposed covert channel is analyzed by playing the game many times within one-month period. The record of game statistics for the normal games and the steganography driven games is maintained.

5. Security of the channel

The game statistics of normal games and steganography driven games were analyzed by comparison for determining the security. Three different sets consisting 500 games per set were used for recording the statistics of game. Merely general games were included in the first set while the second set (stego) contained just steganographydriven games. The third set contained a mixture of both sorts of games in equal share.

	Normal	Stego	Mix
Mean	12.19	14.77	13.15
Std. Dev.	7.36	8.40	8.09
Median	10	15	12
Skewness	4.65	0.03	3.38
Kurtosis	113.54	1.21	75.50

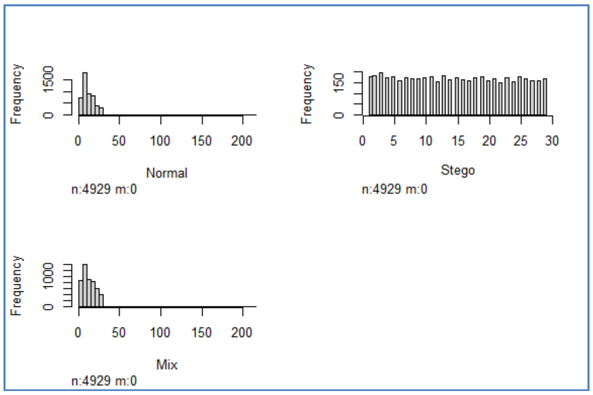

Fig.: Histogram comparison

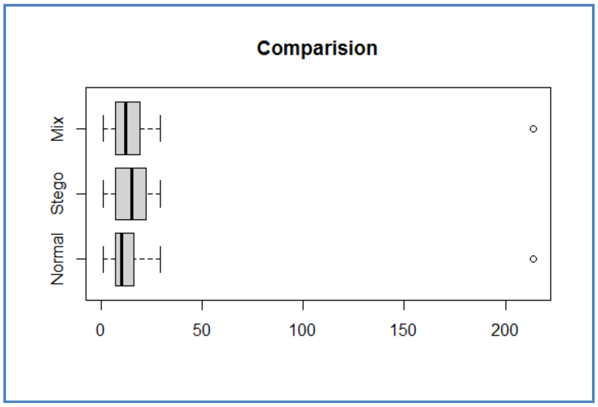

Fig.: Box Plot Comparison

Game statistics of four dissimilar sets, each including 150 normal games, for deciding the changes in normal situation.

Descriptive Statistics:

	Normal 1	Normal2	Normal3	Normal 4
Mean	12.27	11.71	12.27	12.89
Std. Dev.	6.64	6.81	6.92	6.65
Median	11	9	10	12
Skewnes s	0.56	0.67	0.64	0.50
Kurtosis	0.40	0.38	0.46	0.54

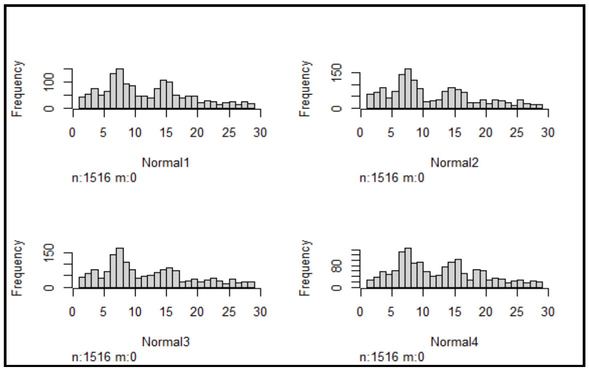

Fig.: Histogram Comparison

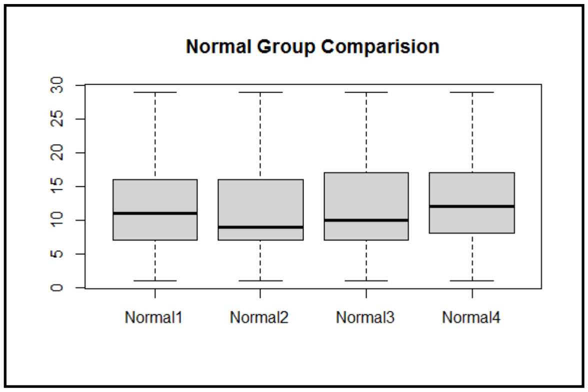

Fig.: Box Plot Comparison

6. OBSERVATIONS

As per the observation, the playing of steganography driven games amidst normal games makes detection task intricate. In such condition, the changes in game statistics is similar to what is realized generally. The continuous play of just steganography driven games for a long time, increases the susceptibility of covert channel detection.

7. EFFICIENCY OF THE CHANNEL

The game statistics of 500 different games indicates that:
Average time duration of a game = 6.084 mins
Average number of moves in a game = 9.858
Number of bits transferred in a single move = 2 bits
Efficacy of the channel = (9.858 x 2)/6.084 bits/min =3.24 bits/min

It is possible to surge the efficacy of the channel up to 4.86 bits/min by transferring covert bits using 8 rather than 4 intervals.

Efficiently, the efficacy of the presented channel will be 1.62 bits/min due to the requirement of steganography driven games for playing games cleanly.

8. Conclusion

According to the rules of "8 Ball Pool" game, every player is allotted a time of 30 seconds for playing shot. This work presents a covert timing channel by separating the allotted 30 seconds into four differ intervals. In every interval, two-bit information is transferred. The obtained outcomes reveal that the detection turns out to be difficult when steganography directed games are played amidst normal games. Also, the information relayed via this covert timing channel includes merely white spaces, dots (.), numbers, and lower-case letters. The use of a randomly selected upper-case latter is carried out to indicate the beginning and ending of the covert information sharing. Moreover, the preference is given to a 6-bitbinary code over the 8-bit ascii code for increasing the capacity.

References:

[1] Hernandez-Castro, Julio C., Ignacio Blasco-Lopez, Juan M. Estevez-Tapiador, and Arturo Ribagorda-Garnacho. "Steganography in games: A general methodology and its application to the game of Go." computers & security 25, no. 1 (2006): 64-71.

[2] Kieu, Duc, Zhi-Hui Wang, Chin-Chen Chang, and Ming-Chu Li. "A Sudoku based wet paper hiding scheme." (2011).

[3] Farn, En-Jung, and Chaur-Chin Chen. "Jigsaw puzzle images for steganography." Optical Engineering 48, no. 7 (2009): 077006.

[4] Farn, En-Jung, and Chaur-Chin Chen. "Novel steganographic method based on jig swap puzzle images." Journal of electronic imaging 18, no. 1 (2009): 013003.

[5] Desoky, Abdelrahman, and Mohamed Younis. "Chestega: chess steganography methodology." security and communication networks 2, no. 6 (2009): 555-566.

[6] Lee, Hui-Lung, Chia-Feng Lee, and Ling-Hwei Chen. "A perfect maze based steganographic method." Journal of Systems and Software 83, no. 12 (2010): 2528-2535.

[7] Ritchey, Philip C., and Vernon J. Rego. "Covert channels in combinatorial games." In Proceedings of the 5th International ICST Conference on Simulation Tools and Techniques, pp. 234-241. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012.

[8] Ou, Zhan-He, and Ling-Hwei Chen. "A steganographic method based on tetris games." Information Sciences 276 (2014): 343-353.

[9] Mahato, Susmita, Dilip Kumar Yadav, and Danish Ali Khan. "A minesweeper game-based steganography scheme." Journal of Information Security and Applications 32 (2017): 1-14.