Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

An Innovative Method of Text Steganograph

Lalitha Chinmayee
Dpt,CSE
M.S.Ramaiah Institue of Technology
Bangalore,India

Tejashwini Gadag
Dpt,CSE
M.S.Ramaiah Institue of Tech*nology*
Bangalore,India

Dr. Parkavi A
(Asst Professor in Computer Science)
Dpt,CSE
M.S.Ramaiah Institue of Tech*nology*
Bangalore,India

***Abstract*—Steganography is a technique where data is hidden within data .There are various kinds of steganography depending on what type of covering media I used to hide a secret message. They are video steganography, image steganography, audio steganography and text steganography. In this paper various techniques proposed for text steganography is studied.**

Keywords—DWT, IDWT ,Text steganography, PSNR, Stegoimage

I. INTRODUCTION

In text steganography, there are two processes involved. They are embedding process and extraction process. In embedding process a secret message is hidden inside a cover message and in extraction process a secret message is recovered from the cover message.

Various kinds of steganography are video steganography, image steganography, audio steganography and text steganography.

Video Steganography is a technique to embed a secret message in a video by altering the BCH coding, quantization scale etc. For example to hide text in a video, a lot of space and processing time is required. The input video stream is changed as per the secret message and the altered bit stream is converted into final video for transmission.

Image steganography is a technique to hide information inside an image. Most widely used application of image steganography is in copywriting an image i.e. to hide the owner's information inside an image. The image resolution and color can change when image steganography is performed.

Audio steganography is a technique to hide information inside an audio file. Most widely used application of audio steganography is in sound watermarking i.e. to hide owner's information inside an audio file. The audio resolution can change when audio steganography is performed.

Text steganography is a technique to hide a text message within a cover text message. This technique is mostly used to hide confidential messages confidential missions, bank credentials etc.

II. EASE OF USE

I Text steganography Techniques

1. AITSteg

AITSteg is a text steganography technique to transmit a hidden text by way of social media. AITSteg is a symmetric key based algorithm and the secret message is hidden based on a hash function. The algorithm has two parts, one is embedding algorithm and another is extracting algorithm. The following section describes the embedding and extracting process.

A.Embedding Process

On the letters in the secret message (SM), an encoding technique called as Gödel function is applied. In Gödel function for each letter in SM, a pair of numbers is generated based on its ASCII code. These two numbers generated are termed as α and β and are unique to the letter in SM. In η is the ASCII value of letter in SM, α and β satisfies the following equation, $< \alpha , \beta > = 2^{\alpha} (2\beta + 1) - 1$, where $2^{\alpha} (2\beta + 1) \neq 0$. α is the largest number such that $(\eta + 1) / 2^{\alpha}$ must be odd and $\beta = [((\eta + 1) / 2^{\alpha}) - 1]/2$. After producing α and β, both are converted into 6 bit binary strings and joined to produce 12 bit binary string. To generate a symmetric key, hash function is used. The Sending time (MS_SK) is obtained (for example 12:15) and 4th digit of the time is omitted a number is created (for example 121). This is converted into a 8 bit binary string and the Secret key (SK) is repeated while the length of the secret key binary string is greater than or equal to the length of the SM binary string.

Later the embedding algorithm generates a hidden message by replacing each 2 bit by one zero width character (ZWC) as shown in below table.

2-Bit Classification	Hex Code
00	200C
01	202C
10	202D
11	200E

The following figure shows the pseudo code for the embedding algorithm.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

Algorithm 1 Pseudocode of Embedding Algorithm

Input: a cover message (CM), a secret message (SM), and a symmetric key (*MS_SK*).
Output: a carrier message (CM_{HM}) which includes of *HM* and *CM*.

1. *SM* ← *Secret Message;*
2. *CM* ← *Cover Message;*
3. *MS_SK* ← *Sending Time;*
4. **for each** $l_i \in SM = \{l_1, l_2, \ldots, l_n\}$ do
5. η ← Obtain ASCII Code of SM[l_i];
6. α← Calculate $[2^{\alpha} \times k = \eta + 1]$;
7. β← Calculate $[[(\frac{\eta+1}{2^{\alpha}}) - 1]/2]$;
8. α_binary ← *Convert* (α *to 6-bit);*
9. β_binary ← *Convert* (β *to 6-bit);*
10. SM_binary ← SM_binary +(α_binary +β_binary);
11. **end for**
12. *LSK* ← *Length (MS_SK_binary);*
13. **if** (*Mod(length(SM_binary), LSK)==0*) **then** *P* ← 0;
14. else *P*←*1;*
15. **end if**
16. *NC* ← *[Length(SM_binary)/LSK]+P;*
17. *Hash_position_bits* ← *NC times copy of MS_SK_ binary*
18. *Hashed_SM_binary* ← *XOR (SM_binary string based on Hash_positions_bits);*
19. *HM_SK* ← Replace (each 2-bit of SK_binary (8-bit) by one ZWC);
20. *HM* ← *HM_SK + Replace (each 2-bit of Hashed_SM_ binary by one ZWC based on Table 3 classification pattern);*
21. **Return** CM_{HM} ← HM+CM;

B.Embedding Process

The extraction algorithm divides the secret message binary string into 12 bit groups and obtains α and β and then generates the ASCII character from α and β. The following figure shows the pseudo code of extraction algorithm.

Algorithm 2 Pseudocode of Extraction Algorithm

Input: a carrier message (CM_{HM}), and a symmetric key (*MR_SK*).
Output: a secret message (SM).

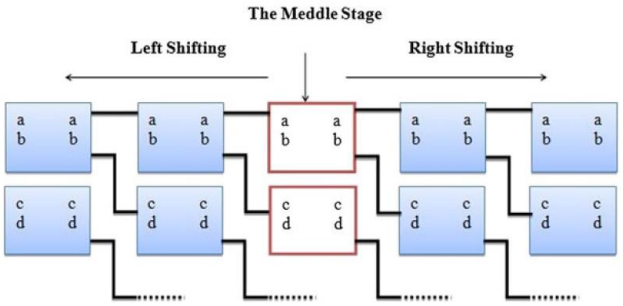
1. CM_{HM} ← *Carrier Message;*
2. *MR_SK* ← *Receiving Time;*
3. **foreach** $l_i \in CM_{HM} = \{l_1, l_2, \ldots, l_n\}$ **do**
4. switch ($CM_{HM}[l_i]$) {
5. case 'u200C':
6. *Hashed_SM_binary*← *Hashed_SM_binary* +"00"; break;
7. case 'u202C':
8. *Hashed_SM_binary* ← *Hashed_SM_binary* +"01"; break;
9. case 'u202D':
10. *Hashed_SM_binary* ← *Hashed_SM_binary* +"10"; break;
11. case 'u200E':
12. *Hashed_SM_binary* ← *Hashed_SM_binary* +"11"; break; }
13. **end for**
14. *MS_SK* ← *Hashed_SM_binary*.Substring(0,8);
15. **if** (*MR_SK==MS_SK*) **then**
16. *Hashed_SM_binary* ← *Hashed_SM_binary.* Substring(8);
17. *LSK* ← *Length (MR_SK_binary);*
18. **if** (*Mod(length(Hashed_SM_binary), LSK)==0*) then *P*← *0;*
19. **else** *P*← *1;*
20. **end if**
21. *NC* ← *[Length(Hashed_SM_binary)/LT]+P;*
22. *Hash_position_bits* ← *NC times copy of MR_SK_binary;*
23. *SM_binary* ← *XOR (Hashed_SM_binary based on Hash_position_bits);*
24. **While** (*Length(SM_binary) >=12*)
25. *AlfaBeta* ← *SM_binary.Substring(0,12);*
26. *SM_binary* ← *SM_binary.Substring(12);*
27. *Alfa* ← *AlfaBeta.Substring(0,6);*
28. *Beta* ← *AlfaBeta.Substring(6,6);*
29. α← *Calculate the decimal number of (Alfa);*
30. α← *Calculate the decimal number of (Beta);*
31. η← *Compute* $[2^{\alpha}(2\beta + 1) - 1]$;
32. *SM* ← *SM + (Convertηto its ASCII letter);*
33. **end while**
34. **end if**
35. **Return** *SM*

2. AH4S

AH4S is an algorithm for text steganography based on omega networks..

a. Embedding process

The structure of omega network is used to generate the cover message for a secret message. The following figure shows the structure of omega network.



All the character in the secret message is read sequentially and is passed through the omega network to generate two cover characters. The omega network has two possibilities for the secret message so a random character is chosen amongst the two. The dictionary is searched to find a suitable word containing these two cover characters. A 12 digit key is generated for every word before transmitting by the embedding process. The structure of the generated key is as described below.

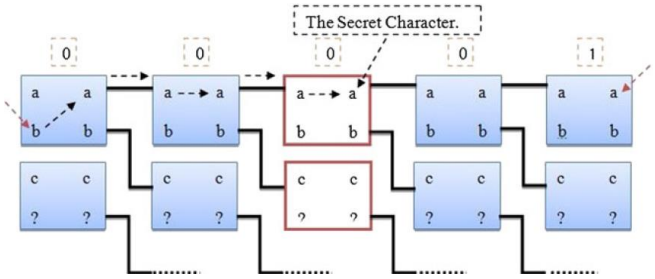
The 1st digit in the key decides if first cover character is first one or the second character inside the input stage node in the omega network and similarly the 2nd digit if second cover letter is first one or second inside the output stage node of the omega network. The 3rd digit decides if the secret letter is a capital letter or not. The 4th to 7th digit is used to memorize the position of the first cover character. Similarly the 8th to 11th digits to memorize second cover character's position. The last position is used to determine if the secret character is at the end of the secret word or not.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

To hide the key string inside the cover message, white space steganography is used. An error control value is generated to add to the final cover word.

b. Extraction process

In extraction process the key error detection is done to make sure the correctness of the key. The cover characters are extracted from cover message and the secret character is found using the structure of the omega network. The following figure shows the flow in the omega network.



3. *Text Steganography based on Discrete wavelet transform*

This algorithm is based on DWT. The embedding and extraction process is described in the following section.

a. *Embedding process*

An input image and a secret text is input to the embedding algorithm. The text is converted to a binary string and DWT is applied on the image.
The detailed coefficients of the DWT are selected and the data hiding process is applied on the detailed coefficients and on the secret message binary string. Now Inverse DWT is applied to get the stego-image.

b. *Extraction process*

The received stego-image is input to a decoder and DWT is applied on it. A message retrieval algorithm is applied on stego and cover image. On applying Inverse DWT the secret message is obtained.

4. *Text Watermarking in Social media*

In this method, the original text is encoded using confusable symbols. These symbols are called Unicode homoglyphs. The following set of Unicode homoglyphs is used in this technique.

	Bit 0	Bit 1
Symbol	Original code	Duplicate code
-	0x002d	0x2010
C	0x0043	0x216d
D	0x0044	0x216e
L	0x004c	0x216c
M	0x004d	0x216f
V	0x0056	0x2164
X	0x0058	0x2169
c	0x0063	0x217d
d	0x0064	0x217e
i	0x0069	0x2170
j	0x006a	0x0458
l	0x006c	0x217c
v	0x0076	0x2174
x	0x0078	0x2179

When a confusable letter is found, the above table is used for encoding and the final string is shared on the social media.

5. *Text Steganography using Daily Emotions Monitoring*

In this technique an emoticon is used to send a secret message.

a. *Embedding process*

A random key is selected and based on the key for each letter an emoticon is selected and final message is prefixed with “Today I Felt:” string and a random timestamp is added after the emoticons. The following table shows the keys to convert a message into an emoticon.

Key 1		
User Input	Mapped Number	Emoticons
A	0	😀
B	1	😁
C	2	😂
D	3	😃
E	4	😄
F	5	😅
G	6	😇
H	7	😈
I	8	😉
J	9	😊
K	10	😋

b. *Extraction process*

The extraction process involves generation of the secret message in exactly opposite way of embedding process. Selection of wrong key results in generation of gibberish secret messages.

REFERENCES

[1] Hedge R. “A review: data transmission techniques over the network by using steganography, SDM Institute of Technology, Ujire, P2-4
[2] Faris AJ,A novel steganography algorithm for hiding text in image using five modulus”, Faculty of Administrative Science-Irbid National University ,Jordan,17 ,jun,2013,P 39 -42.
[3] Jayaram P,Ranganatha HR,Anupama HS.”Information hiding using audio steganography – survey.”Department ofcomputer cience and Engineering V College of College, Bangalore, India, 3, August 2011.
[4] Kekre HB.”Information hiding in audio signals.”MPSTME,SVKM’s NMIMS ,Mumbai,October 2010.
[5] Prasad RSR.”A new approach to telugu text steganography”Acharya Nagarjuna Uiversity,Nagarjuna Nagar,Guntur,Andra Pradesh,India,September,2011.
[6] N.Saxena and N.S Chaudhari,”EaySMS:A protocol for end-to-end secure transmission of sms,”IEEE Trans.Inf,Forensics ,1168,Jul,2014
[7] A Das and H.U.Khan,”Security behaviors of smartphone users,”Inf. Comput,Secur,vol.24,no.1.pp.116-134,2016
[8] M.T.Ahvanooey.Q.Li.M.Rabbani and A.R.Rajput,”A Survey on smartphone security:oftware vulnerabilities,malware,and attacks,”Int.J.Adv.Comput,.Sci,Appl,vol 8,no 10,pp.30-45,2017