Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 113-124, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.113.124

Short Message (Service) as Key for Steganography

[1]Rengarajan Amirtharajan, [1]Prasad Muralidharan, [1]R. Rajesh, [2]R. Sridevi and [1]J.B.B. Rayappan

[1]School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, India
[2]Department of Physics, A.V.V.M Sri Pushpam College, Poondi, 613 503, Thanjavur, India

Corresponding Author: Rengarajan Amirtharajan, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, India

ABSTRACT

In this paper, an unequaled itinerary to effectuate orphic information divvying is proposed wherein habituated steganographic rationale of text. Stand out features of texting like nonintrusive, cost effective, spontaneity; quilt etc. makes it eligible for an efficacious covert communication. The chronic progression of technology is without doubt a boon for us and at the same time is a ban when it comes with uninvited kith and kin of security aftermath. A newly blooming form of steganography is this SMS based routine whose prime concern is solely increased-cum-guaranteed privacy. This study discovers one such style through introduction of time delay betwixt continuous SMS. This work comes under noiseless communication employing cover generation; also it does not neglect the description about previous forerunners to this concept and thus discusses about line and word shifting, open spaces, semantic method etc. Here presented seven methods for a successful text steganography by assigning time delays for every character in a word, by allocating the same according the usage percentile of a letter in an increasing order, for the SMS pattern message, using frequency order of letters, by altering the same by shuffling, with the help of java, by transmitting to different SIMs.

Key words: Information security, SMS-texting, mobile phone, text steganography, time delay, noiseless communication, cover generation method

INTRODUCTION

With the boom in communication and technology and with the widespread use of Internet, free flow of information is possible. And with this increase in technologies for transfer of information, there is a considerable increase in need for protection of this information too. This need gave birth to information security and techniques like cryptography, water marking and steganography (Amirtharajan *et al*., 2012; Cheddad *et al*., 2010) were developed.

Cryptography (Schneier, 2007) is the art of scrambling of data in an unintended format so that no one other than the authorized receiver can decode it. It would look gibberish to any third person viewing it. But it has a disadvantage in that a person looking at it would find out that it is some encoded secret message. And if he gets hold of the secret code then any third person can extract it.

Eventually steganography gained its importance because it keeps the very existence of the message as a secret. Steganography has gained much appreciation in the recent past because of this. It involves a cover image, a secret data and a key. It is implemented in various media (Cheddad *et al*., 2010; Petitcolas *et al*., 1999; Karzenbeisser and Petitcolas, 2000) for example

digital audio (Zhu *et al*., 2011), images (Bender *et al.,* 1996; Amirtharajan and Balaguru, 2009; Chan and Chen, 2004; Janakiraman *et al.,* 2012; Padmaa *et al.,* 2011; Thanikaiselvan *et al*., 2011a, b), text (Xiang *et al*., 2011; Yang *et al*., 2011; Liu *et al.,* 2008; Shirali-Shahreza and Shirah-Shahreza, 2006, 2007; 2008; Al-Azawi and Fadhil, 2010; Low *et al.,* 1995; Kim *et al.,* 2003; Niimi *et al.,* 2003; Rabah, 2004; Huang and Yan, 2001; Beare, 2007; Shahreza, 2005; Al-Frajat *et al*., 2010).

Of these three, image steganography has got much commendation. Here the vital information is dissembled in a cover image and a stego-image is created. This embedded secret message is invisible to naked eye, thus making our secret data safe from intruder's eyes.

The three main characteristics of steganography areimperceptibility, capacity and its robustness (Amirtharajan *et al*., 2011; Amirtharajan and Rayappan, 2012a-d). The total amount of secret information that can be hidden in a Stego-image defines its capacity. Robustness is the limit of modifications an adversary would have to do before he can break the secret code and get the hidden message.

Methods in spatial domain and methods in frequency domain are the two main classifications of Information hiding (Amirtharajan *et al*., 2012; Rajagopalan *et al*., 2012). When the data is directly injected in image pixels it is spatial domain approach, whereas, when the image is first transformed into frequency domain and then embedded then it is frequency domain approach (Amirtharajan and Rayappan, 2012d; Provos and Honeyman, 2003).

LSB based approach (Amirtharajan and Rayappan 2012d), PVDbased approach (Padmaa *et al.,* 2011) and mod based (Chan and Chen, 2004) approach are the approaches available in order to increase the characteristics of steganography, i.e., to make the image more robust or more imperceptible. Before transformation the cover image exists in the spatial domain later it is transformed to time or frequency domain and again it is brought back to the spatial domain. Techniques like DCT (Provos and Honeyman, 2003). DWT or IWT (Thanikaiselvan *et al*., 2011a; Amirtharajan and Rayappan, 2012d) are used for transformation. Cryptography together with steganography could be an effective solution to improve the complexity (Karzenbeisser and Petitcolas, 2000).

SMS is said to be born in 1980s for quick and discreet communication and is later developed to be exercised in accordance with globally employed technologies TDMA and GSM (Shahreza, 2005). Since it is non-voice, economical, speedy and targeting (sms are sent only to defined recipients) features makes it more eligible for use as cover for covert communication. SMS's function and service is doable which makes overhearing outrageous. Maximum of 160 characters can be sent in a message which is decided by the individual service providers and networks. Lengthier smses are divided into many short messages and then sent to the destination.

This paper will propose a new way of hiding data using time delay between the successive SMS in real time application.

LITERATURE REVIEW

Let us see the frequently used terms. Medium used for veiling confidential message, termed payload, is nothing but cover. The outcome of a steganographic technique is known as stego object and the index used for embedding and recovery is called stego key.

SMS-texting (Beare, 2007): It is a new language used throughout the world for rapid communication. SMS texting has discovered new abbreviated form of English (!) which faces callous

censure. Despite this, it has gained popularity as it consumes less time, high redemption cum open rate and its ease of use is also worth mentioning. To quote an example, in place of "Good morning", it is enough to say "Gud mrn".

Existing text steganography in SMS (Shirali-Shahreza, 2006): This method has predefined catalog of words and their corresponding ellipsis. In a text (SMS), in lieu of bits zero and one, the steganographic algorithm replaces word and acronym respectively which are part of the predefined list. Only the people knowing the routine can recover hidden information.

Persian/Arabic text steganography (Shirali-Shahreza and Shirali-Shahreza, 2006, 2008; Al-Azawi and Fadhil, 2010): This method makes use of Arabic and Persian fonts to hide data as they have special and unique characters. Their linguistic pattern contains more dots; thus, their displacement is used to screen large volume of secret data in text. This technique is applicable only for Arabic and Persian and not for English, since the latter has only two letters having dots (i, j).

LINE shifting (Low *et al.*, 1995): The technique best apt for the printed texts wherein there is a requirement for the vertical shift of the lines of the printed text to a few degrees (say up/down shift of 1/300 inch). The clandestine fact is then concealed within, through crafting a novel text shape. However, the scheme has a hitch of its own. In case, any out of the ordinary instruments used could observe the distance, then by the distance monitoring & essential changes, the hidden secret is destroyed. Moreover, if OCR or retyping of text takes place, buried message will be ruined.

WORD shifting (Low *et al.*, 1995; Kim *et al.*, 2003): Here, the shifting of the words is done horizontally or by altering the distance between them, is employed for rooting data in texts. A drawback here lies in using OCR programs or the Re-typing the text resulting in the mar of the hidden information. This method is best suited where the space between words keeps varying in texts. Filling up a line by modification of distance amidst words is pretty universal; it has comparatively less identity in terms of recognition. However, if anyone knows the distance between words, one can go for comparison of the text at hand and algorithm by using difference methodology and can extract the concealed information. Despite this routine consumes more time, high stake in knowing the hidden content is palpable.

Feature Coding (Bender *et al.*, 1996; Rabah, 2004): In Feature Coding, a few text characteristics are tainted, like, some characters' concluding parts (like b, d or h) are enhanced, say, either abbreviated or stretched out and therein, the information is buried. By this way, a voluminous amount of secret can be infixed with leaving no trace for the readers. If the characters are retained in their original preset shape, information gets lost and re-typing of text by OCR may annihilate the secrets.

Open spaces (Huang and Yan, 2001): In the method- open white spaces, information hiding in texts is implemented by the addition of more white spaces. They can be inserted at each paragraph's end or between words or at the end of each line. Therefore, this mechanism gets employed in random texts without grabbing readers' interest. Nonetheless, quantity of information

hidden by open SPACES is limited and besides, covert data may be wiped out if the additional white spaces are deleted by text editing programs.

Sematic method (Niimi *et al.*, 2003): In this methodology, text hiding is done through utilizing the words' synonyms. This feature is more secure in spite of re-typing and OCR. However, the meaning of the text may succumb to variations by this method.

Stealth steganography in SMS (Shirali-Shahreza, 2006): In this work, steganography is done on picture SMS messages. Here, after converting the picture into black and white and apt layout for mobiles, it is segmented into 3×3 dimensioned blocks. Password is used to encode the covert data and for each block if steganography is possible and if tested positive, 1 bit of secret data is embedded by changing that particular block. Recovery is just the opposite of embedding. After morphological recovery of secret, picture message can be hoarded in the mobile of the receiver with no secret data.

PROPOSED METHOD

In this method, imperceptibility and robustness is very high, capacity is moderate and security lies in the algorithm. The proposed schematic diagram is given in Fig. 1.

Method 1: Steps to follow to encrypt:

- Write the message you want to send in a paper
- Time delay allocated for characters and numbers
- Allocate time for each character according to the below table. Number of ways in which time is allocated for characters, numbers and symbols are nPr = (26+10+11)P(26+10+11) = 47P47 =2.586232415*10^59 Ways Take any one way from the above number of ways. For example: Let the message to be delivered be-"charge" time allocated are "4, 9, 2, 19, 8 and 6 min" Schedule the messages using your cell phone SMS, such that the delay between them is as follows:

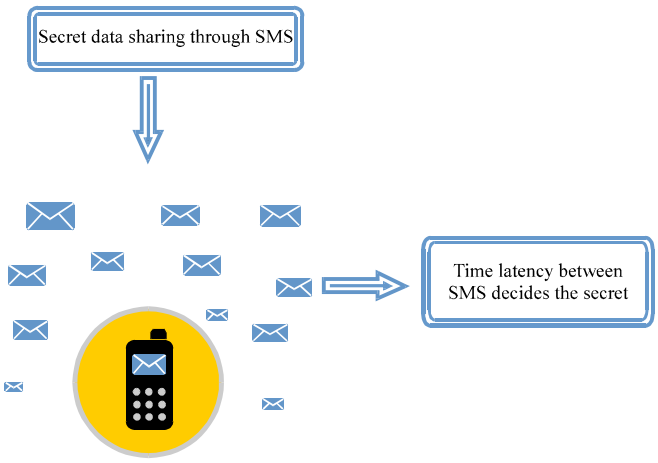

Fig. 1: Schematic diagram of the proposed methods

  - 1st and the 2nd message is 4 min
  - 2nd and the 3rd message is 9 min
  - 3rd and the 4th message is 2 min
  - 4th and the 5th message is 19 min
  - 5th and the 6th message is 8 min
  - 6th and the 7th message is 6 min
- Now send the messages to the desired person. He will receive the message in which the send time is specified.

Extraction method: Once the desired person knows in which way you have assigned the time, he or she can decrypt it (reverse of encryption).

Advantages:

- Countless SMS are traded daily turning steganalysis a difficult task
- Simple implementation in mobiles
- Third party is diverted with the text message present inside the message
- Time taken to decrypt by brute force attack is (If 1 way takes 1 second, then 47p47 takes 20088919*10^51 years

Disadvantage: When delay is used in minutes, the characters sent is very less (time-depends on the message content).Time taken to send 27 characters at a stretch from(a to z and space) is 6.3 h. Example:

- Feel good when somebody Miss you Feel better when somebody Loves you But feel best when somebody never forgets you Good Friday
- Total number of letters including space:123
- Time taken is 23.75 hours

Method 2: Steps to be followed while embedding:

- Write the message you want to send.
- In English, the usage of letters are as follows
  (more to less usage):

  "etaon rishd lfcmu gypwb vkxjq z"

Allocate time for each character according to the above. But it makes the job easy for the hackers. So, change the time allocated to each character every time you send message or keep a particular sequence fixed but give less time allocation for the most frequently used words.

Schedule the messages using your cell phone. 4. Now send the messages to the desired person. He will receive the message in which the send time is specified. Table 1-3 provide the time allocated to symbols, characters and numbers.

Table 1: Time delay allocated for characters and symbols

Character/Symbol	Time delay (min)	Character/Symbol	Time delay (min)	Character/Symbol	Time delay (min)
‘ ‘	1	‘0’-	28	‘@’	38
‘-‘	43	‘?’	49	‘ e’	2
‘1’	29	‘$’	39	‘ ‘ ’	44
t’	3	‘2’	30	‘%’	40
‘/’	45	……	upto	……	upto
‘&’	41	‘\’	46	‘z’	27
‘9’	37	‘+’	42	‘,’	48

Table 2: Time delay allocated for characters and numbers

Character/Symbol	Time delay (min)	Character/Symbol	Time delay (min)
‘ ‘	1	‘0’	28
‘@’	38	‘-‘	43
‘ a’-	2	‘1’	29
‘$’	39	‘ ‘ ’	44
‘b’	3	‘2’	30
‘%’	40	‘/’	45
……	upto	……	upto
‘&’	41	‘\’	46
‘z’	27	‘9’	37
‘+’	42	‘,’	48
‘?’	49		

Table 3: Time delay allocated for alphabets, characters and symbols

Character/Symbol	Time delay (min)	Character/Symbol	Time delay (min)	Character/Symbol	Time delay (min)
‘ ‘	1	‘0’	28	‘@’	38
‘-‘	43	‘?’	49	‘ a’	2
‘1’	29	‘$	39	‘ ‘ ’	44
‘b’	3	‘2’	30	‘%’	40
‘/’	45	……	upto	……	upto
‘&’	41	‘\’	46	‘z’	27
‘9’	37	‘+’	42	‘,’	48

Extraction method: Once the desired person knows in which way you have assigned the time, he or she can decrypt it (reverse of encryption).

Advantages:

- Numerous SMSs are communicated between people; hence it is really tough for intruders to attack
- In mobiles it can be realized effortlessly
- Third party is diverted with the text message present inside the message
- Time taken to decrypt by brute force attack is more.

Disadvantage: When delay is used in minutes, the time taken to deliver all the messages is high. On comparing it with the above method the time taken to send a passage or message is reduced.

Example: Feel good when somebody Miss you Feel better when somebody Loves you But feel best when somebody never forgets you Good Friday Time taken is 17.16 h.

Method 3: Steps to be followed while embedding:

- Write the message you want to send
- Convert that into sms language
- Time delay allocated for characters and numbers

Allocate time for each character according to the above. Number of ways in which time is allocated for characters, numbers and symbols are:

$$nPr = (26+10+11)P(26+10+11) = 47P47 = 2.586232415*10^{59} \text{ Ways}$$

Take any one way from the above number of ways.
For example: Let the message to be delivered be –"charge" In SMS language-"chrg"
Time allocated are "4, 9, 19 and 8 min" Total time = 40 min:

- Schedule the messages using your phone
- Now send the messages to the desired person. He will receive the message in which the send time is specified

Extraction method: Once the desired person knows in which way you have assigned the time, he or she can decrypt it(reverse of encryption).

Advantages:

- Stego attack is a nightmare since innumerable SMSs are exchanged per day
- Can be easily implemented on any mobile phone
- Third party is diverted with the text message present inside the message
- Time taken to decrypt by brute force attack is (If 1way takes 1 second, then 47p47 takes 20088919*10^51 years
- Time taken by the information is less when compared to the above methods
- To hack or trying to decrypt (by third party) is very difficult since SMS language is used

Disadvantage: When delay is used in minutes, the characters sent is very less.

Example: Feel good when somebody Miss you Feel better when somebody Loves you But feel best when somebody never forgets you Good Friday.

SMS language:

- Feel gud wen sumbdy ms u:
- Feel btrwen sumbdy luvs u
- bt feel bst wen sumbdy nvr 4gets u
- gud fri

Time taken is 17.61 h

Method 4: Steps to be followed while embedding:

- Write the message you want to send
- Convert that into SMS language
- Use C++ or any language to find frequency order of the letters used in your information. Allocate time for each character accordingly
- Schedule the messages using your cell phone
- Now send the messages to the desired person. He will receive the message in which the send time is specified

Decryption method: Once the desired person knows in which way you have assigned the time, he or she can decrypt it (reverse of encryption).

Advantage:

- Cell phones can by far implement this method and can highly resist security attacks because infinite texts (SMS) are traded in one day
- Third party is diverted with the text message present inside the message
- Time taken to decrypt by brute force attack is: (If 1way takes 1 second, then 47p47 takes 20088919*10^51 years)
- Time taken by the information is less when compared to the above methods
- To hack or trying to decrypt (by third party) is very difficult since SMS language is used

Disadvantage: When delay is used in minutes, the characters sent are very less.

Example: Feel good when somebody Miss you Feel better when somebody Loves you But feel best when somebody never forgets you Good Friday

SMS language:

- Feel gud wen sumbdy ms u
- Feel btrwen sumbdy luvs u
- bt feel bst wen sumbdy nvr 4gets u
- gud fri

Time taken is less than the previous method

Method 5: Steps to be followed while embedding:

- Write the message you want to send.
- Convert that into SMS language.
- Use C++ or any language to find frequency order of use of letters in your information. Allocate time for each character accordingly.
- Shuffle the letters in the SMS language information using any good algorithm

- Schedule the messages using your cell phone
- Now send the messages to the desired person. He will receive the message in which the send time is specified

Extraction method: Once the desired person knows in which way you have assigned the time, he or she can decrypt it (reverse of encryption).

Advantage:

- Higher the no. of SMS exchange, harder the stego attack
- Ease in implementing in every mobile phone
- Third party is diverted with the text message present inside the message
- Time taken to decrypt by brute force attack is (If 1way takes 1 second, then 47p47 takes 20088919*10^51 years)
- Time taken by the information is less when compared to the above methods
- To hack or trying to decrypt (by third party) is very difficult since SMS language is used
- Decryption is made complex when compared to the above. Hence, hackers will suffer

Disadvantage: When delay is used in minutes, the characters sent is very less.

Example: Feel good when somebody Miss you Feel better when somebody Loves you But feel best when somebody never forgets you Good Friday.

SMS language:

- Feel gud wen sumbdy ms u
- Feel btrwen sumbdy luvs u
- bt feel bst wen sumbdy nvr 4gets u
- gud fri

  Shuffle the message information.

  Time taken is less than the previous method.

Method 6: Once java program is made in a way that messages can be scheduled in seconds, time duration is reduced considerably.

Example: Feel good when somebody Miss you Feel better when somebody Loves you But feel best when somebody never forgets you Good Friday
Total number of words is 105

SMS language:

- Feel gud wen sumbdy ms u
- Feel btrwen sumbdy luvs u
- bt feel bst wen sumbdy nvr 4gets u
- gud fri

Total number of letters including space is 91
Time taken is very less.

Method 7: Way to reduce time consumption: Since, scheduling messages with respect to minutes takes more time, follow the below to reduce the time consumption:

- Split the SMS language message into five parts
- Send 1st part to 1st sim, 2nd part to 2nd SIM;... ... ... 5 h part to 5th SIM

Take the example of the
1st method: actual time 23.75 h
Reduced to: 5.53 h
2nd method: actual time: 17.16 h
Reduced to: 3.86 h

CONCLUSION AND FUTURE IMPROVEMENTS

This method is first of its kind in using time as a cover to hide the secret. When compared to other methods, this steganography form is very simple and secure since one cannot imagine of hiding in texts traded between millions per day. The added advantage here is that it is felicitous to all languages and platforms and its ease in implementing is also a remarkable trait. Even if one senses the mystery, he or she cannot recover the data unless and until he or she knows the index and platform of embedding and especially the key. Hence SMS based steganographic technique is a remarkable path to private communication and this method copes up to the crucial panorama of a perfect, lossless and nonintrusive communication.

REFERENCES

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

Amirtharajan, R. and R.J.B. Balaguru, 2009. Tri-layer stego for enhanced security-a keyless random approach. Proceedings of the IEEE International Conference on Internet Multimedia Services Architecture and Applications, December 9-11, 2009, Bangalore, India, pp: 1-6.

Amirtharajan, R. and R.J.B. Balaguru, 2011. Covered CDMA multi-user writing on spatially divided image. Proceedings of the Wireless ViTAE Conference, February 28-March 3, 2011, IEEE, Chennai, India, pp: 1-5.

Amirtharajan, R. and J.B.B. Rayappan, 2012a. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., 193: 115-124.

Amirtharajan, R. and J.B.B. Rayappan, 2012b. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

Amirtharajan, R. and J.B.B. Rayappan, 2012c. Inverted pattern in inverted time domain for icon steganography. Inform. Technol. J., 11: 587-595.

Amirtharajan, R. and J.B.B. Rayappan, 2012d. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: A comparative study on PI stego. Res. J. Inform. Technol., 4: 124-139.

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.

Beare, K., 2007. SMS-texting-english as 2nd language. http://esl.about.com/

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. J. Pattern Recognit. Soc., 37: 469-474.

Cheddad, A., J. Condell, K. Curran and P.M. Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Huang, D. and H. Yan, 2001. Interword distance changes represented by sine waves for watermarking text images. IEEE. T. Circ. Syst. Video Technol., 11: 1237-1245.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012. Pixel forefinger for gray in color: A layer by layer stego. Inform. Technol. J., 11: 9-19.

Karzenbeisser, S. and F.A. Perircolas, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, UK., ISBN: 9781580530354, Pages: 220.

Kim, Y., K. Moon and I. Oh, 2003. A text watermarking algorithm based on word classification and inter-word space statistics. Proceedings of the 7th International Conference on Document Analysis and Recognition, August 3-6, 2003, IAPR, pp: 775-779.

Liu, Y., X. Sun, Y. Liu and C.T. Li, 2008. MIMIC-PPT: Mimicking-based steganography for microsoft power point document. Inform. Technol. J., 7: 654-660.

Low, S.H., N.F. Maxemchuk, J.T. Brassil and L. O'Gorman, 1995. Document marking and identification using both line and word shifting. Proceedings of the 14th Annual Joint Conference of the IEEE Computer and Communications Societies, April 2-6, 1995, IEEE Computer Society, Washington, DC. USA., pp: 853-860.

Niimi, M., S. Minewaki, H. Noda and E. Kawaguchi, 2003. A framework of text-based steganography using SD-form semantics model. Proceedings of the Pacific Rim Workshop on Digital Steganography, July 3-4, 2003, Kyushu Institute of Technology, Kitakyushu, Japan.

Padmaa, M., Y. Venkataramani and R. Amirtharajan, 2011. Stego on 2^n: 1 Platform for users and embedding. Inform. Technol. J., 10: 1896-1907.

Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078.

Provos, N. and P. Honeyman, 2003. Hide and seek: An introduction to steganography. IEEE Secur. Privacy, 1: 32-44.

Rabah, K., 2004. Steganography-the art of hiding data. Inform. Technol. J., 3: 245-269.

Rajagopalan, S., R. Amirtharajan, H.N. Upadhyay and J.B.B. Rayappan, 2012. Survey and analysis of hardware cryptographic and steganographic systems on FPGA. J. Applied Sci., 12: 201-210.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., Wiley, India.

Shahreza, M.S., 2005. An improved method for steganography on mobile phone. WSEAS Trans. Syst., 4: 955-957.

Shirali-Shahreza, M., 2006. Stealth steganography in SMS. Proceedings of the 3rd IEEE and IFIP International Conference on Wireless and Optical Communications Networks, April, 2006, IEEE, pp: 11-13.

Shirali-Shahreza, M.H. and M. Shirali-Shahreza, 2006. A new approach to persian/Arabic text steganography. Proceedings of the 5th International Conference on Computer and Information Science, July 10-12, 2006, Honolulu, HI, USA., pp: 310-315.

Shirali-Shahreza, M. and M.H. Shirali-Shahreza, 2007. Text steganography in SMS. Proceedigns of the International Conference on Convergence Information Technology, November 21-23, 2007, Gyeongju, pp: 2260-2265.

Shirali-Shahreza, M. and S. Shirali-Shahreza, 2008. High capacity persian/Arabic text steganography. J. Applied Sci., 8: 4173-4179.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2011a. Wave (let) decide choosy pixel embedding for stego. Proceedings of the International Conference on Computer, Communication and Electrical Technology, March 18-19, 2011, India, pp: 157-162.

Thanikaiselvan, V., S. Kumar, N. Neelima and R. Amirtharajan, 2011b. Data battle on the digital field between horse cavalry and interlopers. J. Theor. Applied Inform. Technol., 29: 85-91.

Xiang, L., X. Sun, Y. Liu and H. Yang, 2011. A secure steganographic method via multiple choice questions. Inform. Technol. J., 10: 992-1000.

Yang, B., X. Sun, L. Xiang, Z. Ruan and R. Wu, 2011. Steganography in Ms Excel document using text-rotation technique. Inform. Technol. J., 10: 889-893.

Zhu, J., R.D. Wang, J. Li and D.Q. Yan, 2011. A huffman coding section-based steganography for AAC audio. Inform. Technol. J., 10: 1983-1988.