http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (12): 1977-1984, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.1977.1984

Cover G for 3 and 4 G-A Stego Product

[1]Rengarajan Amirtharajan, [2]Imaculate Rosaline, [2]Rengaraja Swamy,
[1]Sai Pavan, [3]R. Sridevi and [1]J.B.B. Rayappan
[1]Department of ECE, School of Electrical and Electronics Engineering SASTRA University, India
[2]Department of ECE, Oxford Engineering College, Tamil Nadu, India
[3]Department of Physics, A.V.V.M Sri Pushpam College, Poondi, Thanjavur, 613-503, India

Abstract: The use of information over internet and our dependence on the computing machines has drastically increased with the advancements in technology. As a result, the storage and transmission of the ever increasing volumes of data in an effective way has become a high priority issue. The very systems which are boon to us are also being misused by many to cause harm. Thus, security is a major issue as far as the information is concerned. Thus, it becomes the responsibility of the parties involved in secret communication to arrange for the necessary security, preventing the sniffing by rogue entities. Advancement in digital communication technology along with internet makes data transfer easy and vulnerable to interception and modification by sneakers. Cryptography and steganography are ways of encrypting and hiding data. While Cryptography hides the essence of the data under a cover, like an encrypted text or periodic noises in a digital signal, steganography hides the fact of data itself. The information is more secure when both these techniques are used together. That is, even if the hidden information is found out, it will be encrypted. In this paper, it is proposed to explore the cover generation method. It uses information as data on covers like Image-cover, Circuit-cover Graph-cover, Chess-cover and Questionnaire etc and does not produce noise. Thus, noiseless steganography (noistega) is a fruitful option for data transmission in secured manner.

Key words: Information hiding, steganography and novel cover generation methods

INTRODUCTION

Ever since the advent of life on earth, there has been the need for communication among the living beings for their own existence. When communication evolved, evolved the need to secure it. This need to secure information became more with the evolution of the internet, which shrunk the world into a global village. There are two types of information security. They are cryptography (Schneier, 2007) and steganography (Amirtharajan and Balaguru, 2009; Amirtharajan *et al*., 2010, 2011, 2012). Cryptography aims at hiding the information in a data, while steganography aims at hiding the data itself. The integrity of the information is higher when both these techniques are used together. Steganography is implemented in any digital media like audio, video, text and images of which image steganography has good reputation in the recent past (Hmood *et al*., 2010a, b; Amirtharajan and Rayappan, 2012a; b). In image steganography, the confidential information in a cover object i.e., image with immense skill resulting in the stego object (Amirtharajan *et al*., 2012). The confidential data that is embedded should possess good quality in order to make it imperceptible (Zanganeh and Ibrahim, 2011). Furthermore, the technique employed should offer high payload by the diligent embedding of more data in a given cover image.

Three main protection techniques include the cryptography, Steganography and watermark technology (Stefan and Fabin, 2000; Cheddad *et al*., 2010). The first one aims at providing copyright protection by embedding information which would authenticate the owner. While cryptography scrambles the data beyond immediate understanding, Steganography hides the data in images and text which cannot be detected (Rajagopalan *et al*., 2012). These two when combined provide higher security compared when each is used separately (Zaidan *et al*., 2010). This is because the detection of hidden information is itself a tedious task. Even if its detected, decrypting the message will pose another time consuming problem. Cryptography and Steganography when put together will enhance further security (Janakiraman *et al*., 2012a, b). The former involves the process of encryption and decryption and the latter involves embedding of

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

information. Steganography is an ancient art to hide information in ways that prevent the detection of the hidden message. The media employed here are video, image, text, audio, binary etc. The digital signal processing is gaining more importance as they are easy to transmit. But the security involved is very poor resulting in hacking of useful information thereby creating noise in transmission. The steganography is the solution for this as it employs hiding of data through several ways. The three main elements of a Steganography system are Cover image, stego image and embedded image (Zanganeh and Ibrahim, 2011). To explain with an analogy, we used to post letters to an intended destination. Here, the content what we write is the information to be hidden (message), the packet into which the secret information is put into is termed as the cover and the final sealed information is called the Embedded message. This notion is presented in Fig. 1 in which the secret message is buried in the cover object to produce the final output called stego object.

The encoding is done in such a way that it is known only to the sender and receiver without being known to the third party. There exist several mechanisms to offer steganography. The simple classification is based on the type of covers. In Image-Binary, gray, color are the options.

In Audio, Video (Al-Frajat *et al.,* 2010) and text (Shirali-Shahreza and Shirali-Shahreza, 2008) According to the cover modifications it could be further classified into 6 categories. Substitution based, Transform domain based, Spread Spectrum based, Statistical Methods based, Distortion based techniques and Cover generation based methods (Desoky 2008, 2010, 2011; Desoky and Younis. 2008, 2009). This study focuses more on cover generation methods.

Review on literature: Noistega can be of textual, image, audio in nature (Desoky, 2008).

In textual, comparison is made between original texts with the modified text to reveal the hidden information. The changes can be in font size, colour, spaces and misspellings and thus the data is embedded (Desoky, 2008).

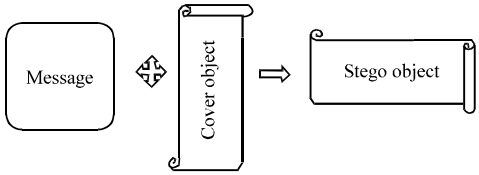

Fig. 1: General approach of a stego system

In image type (Janakiraman *et al.*, 2012a, b; Thanikaiselvan *et al.,* 2011a, b and Padmaa *et al.,* 2011), the messages can be embedded in image depending upon the image size. But in this, the counterpart is subjected to distortion and destruction thereby limiting its usage for long distances. In audio type (Zhu *et al.*, 2011), the text to speech software's are employed thereby hiding is possible through spread spectrum coding (Thenmozhi *et al.*, 2012), phase coding and echo hiding. Thus, steganography is an ocean which can be utilised depending on the user's need. The following describes this steganography as:

- Image stega
- Circuit stega
- Graphstega
- Edustega
- Chestega

The architecture and the working process for every type are explained in detail.

MATERIALS AND METHODS

Image stega: Cover based Steganography techniques are very useful in hiding the information in deceivingly innocent covers. For instance consider the example presented in Fig. 2. The image seems to consist of only some random images of flowers and by seeing it for the first time, one cannot predict that secret information is hidden in it. It need not be of same pattern.

Like one presented here. This is so because it may cause suspicion for the invaders. The more the random and ergodic the choice of cover(s), greater preserved the secrecy. Moreover, such choice does not give even a clue about what is hidden in there.

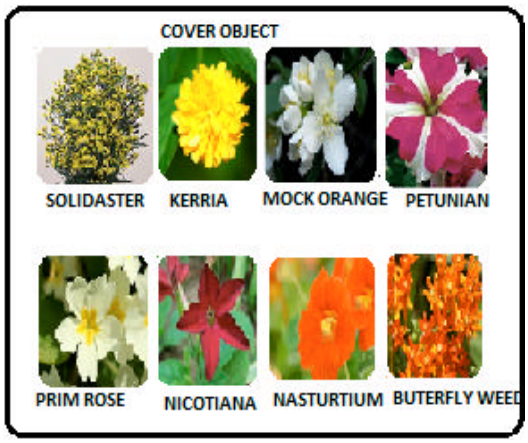

Fig. 2: Example for image stega

Methodology:

- **Selection of particular domain:** Suitable cover object here is image
- **Selection of parameters:** Identification of parameters (numeric and non-numeric) to conceal a data without generating noise. The parameters here include the suitable images to conceal the data
- **Encoding:** The message is encoded which does not constrain the generation of image cover
- **Selection of tools:** It uses non-Steganographic tools such as, images and pictures
- **Protocols:** It deals with a communication between sender and user

Explanation: The secret word is hidden in the cover in the form of the consecutive alphabets of all the names, for example, the first letter 's' from Solidaster, second letter 'e' from Kerria and so on. Thus by decoding in this way, the secret hidden is decoded as SECURITY. This is a very effective cover generation method.

The cover object is shown in Fig. 3 carries hidden information. When the picture is shown as such, the hackers other than the intended recipients will never get an idea of what the picture reveals. The corresponding Stego object is obtained by taking every second letter from each word and combining them, which reveals the word, "Security". It proves to be a good method of hiding secret information. It improves the security and the visibility to decrypt the information.

The stego object is shown below:

- Stego object revealed: Security

Circuit stega: Another form of cover generation method is circuit Steganography. In this method, the ASCII values of the characters of the secret message are given as the values for the resistors, capacitors and other components present in the circuit. Thus, unless it is known by a third party that the values correspond to a secret message, it will not be deciphered.

Methodology:

- **Selection of particular domain:** The selection of suitable cover object; here it is a circuit
- **Selection of parameters:** Parameters used to conceal data here include, circuit elements like resistors, capacitors, inductors
- **Encoding:** The message is encoded which does not constrain the generation of circuit cover
- **Selection of tools:** An ASCII value of the secret information is used as a tool for generating circuit cover
- **Protocols:** It deals with a communication between sender and user

Explanation: The circuit in Fig. 4 shows hidden information, 'security'. Each character of this word is converted to its equivalent ASCII value as follows:

S-115, E-101, C-99, U-117, R-114, I-105, T-116, Y-121

It is an efficient cum less-suspicion-captivating means to hide confidential information. One cannot have even an idea about veiling messages in a circuit. More information can be rooted when the circuits are employed are complex and bigger.

Graphstega: It is the form of Graph Steganography Methodology (Desoky and Younis, 2008). It does not embed message in the noise rather it does hiding of data

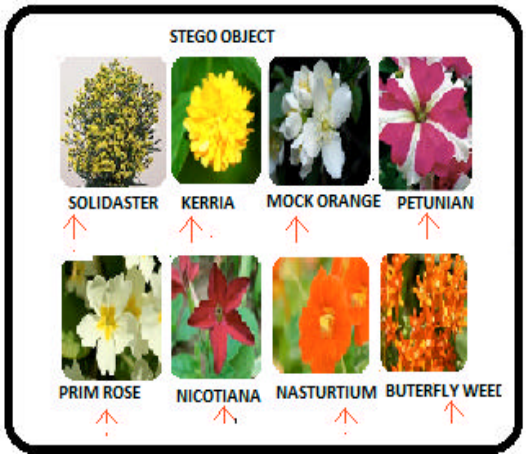

Fig. 3: Hidden message ("Security") in stego object

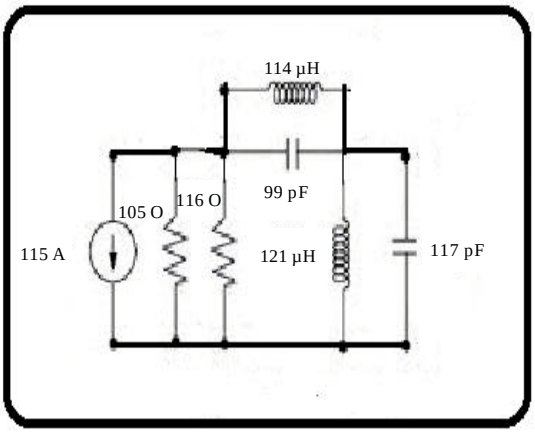

Fig. 4: Circuit stega example (hidden message-security)

as data points in the graph. Thus this graph cover uses electronic and non-electronic format which makes hacking very difficult. A variant has been proposed.

Methodology:

- **Selection of particular domain:** The selection of suitable subject for which the graph cover is to be generated. Selection of parameters: Identification of parameters (numeric and non-numeric) to conceal a data without generating noise
- **Encoding:** The message is encoded which does not constrain the generation of graph cover
- **Selection of tools:** In graphstega, the tool for generating graph cover is MS-EXCEL
- **Protocols:** It deals with a communication between sender and user

Explanation: In this graphstega, the text is converted into a group of strings. It is then partitioned into a group of bits and a decimal representation is produced for every group.

The following explains the hiding of the message: "security".

ASCII equivalent of the above word is:

115, 101, 99, 117, 114, 105, 116, 121

and these values are plotted in a graph to obtain this Steganographic method.

In the above, the plain text is encoded without affecting the correctness of it. Now MS-EXCEL is used to generate graph cover as follows:

This Steganographic method shows the secret message 'security' written in its ASCII form is plotted in a graph shown in Fig. 5 to remain concealed. This means promises elevated security as there is countless pattern of graphs which are put to use nowadays. As per the information to be hidden, the pattern of graphs can be chosen.

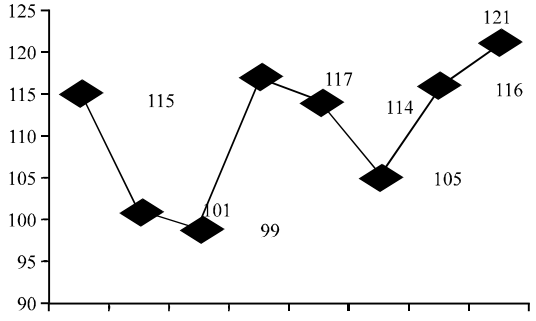

Fig. 5: Secret message "security" hidden in graph cover

Graphstega is capable of handling both the short and long messages. For short messages the encoded values are the data plotted in the graph. Inspection of the graph is very easy. For long messages, values cannot be read from the graph so easily because of the scale constraints. For that, data are considered as the part of objects in the graph cover for retrieving the data. Example is that attaching an excel file in an email message.

Thus, graphstega is effective to camouflage every sort of data as mentioned by Desoky and Younis (2008).

Conversion techniques

Presenting data in image cover: The graph is converted into image formats like .jpg, .bmp. Here also the message is concealed as data values rather than pixels in image steganography, thereby reducing noise. It is unfit for large messages because the data should not exceed the prescribed size of the image.

Presenting data in text cover: Here, the encoded message is mixed up with some other texts and it is transmitted. It is explained in the following table.

In this graph cover, the encoded message is given as the prices of the books.

In the same way, we can produce graph cover as Tracking Number:

5790-152-21-1-53-861-055729-44-3867-1

Presenting data in audio cover: The data is encoded and then converted into audio using "text to speech" software. But the data is exposed to distortion and destruction.

The Graphstega could be implemented using MS-Excel and it is merely a tedious job to extract or hack data from the graph thereby enabling a graphstega, a successful technique in steganographic process.

Edustega: Education-centric steganography methodology.

It is a novel linguistic steganography methodology, which camouflages the data by manipulation. It includes the method of "question and answers" (Desoky, 2008; Xiang *et al*., 2011). Edu cover may be a pdf file, MS-word, even an image enabling the recipient to extract the hidden data. A variant has been proposed.

Methodology:

- Selection of a particular field: For edustega, it is concerned about the selection of suitable cover object and here is a graph cover

- Selection of parameters: Identification of parameters to conceal data without noise. In this, puzzles, matching, fill ups are the parameters
- Encoding: Encoding is done without affecting graph cover generation. The advantage of edustega is that it will make available questions for this process
- Selection of tools: The text cover can be generated by using non-steganographical tools such as 'exam generators'
- Protocols: It is a covert channel for transmitting a steganographic cover

Table 1 illustrates the hiding of word 'security'. The ASCII equivalent of this word is 115, 101, 99, 117, 114, 105, 116, 121 which is listed the price of various books. Figure 6 explains the Edustega modules and their interfacing. The Edustega is explained as shown:

(1) Frog is an amphibian		
(a) True	(b) False	
(2) Sachin Tendulkar belongs to		
(a) India	(b) Pakistan	(c) Australia
(3) Which one of the following refers to the family of horse?		
(a) Zebra	(b) Giraffe	(c) Camel
4) HAL headquarter is located at		
(a) Delhi	(b) Bangalore	(c) Calcutta
(5)"Sister " in other word can be referred as		
(a) Nun	(b) Mother	(c) Bishop
(6) Which of the following is the famous place of Pakistan?		
(a) Lahore	(b) Swatch	(c) Sindh
(7) "Pink City" of India is		
(a) Jaipur	(b) Raipur	(c) Kanpur
(8) Switzerland is famous for		
(a) Currency	(b) Jewels	(c) Swiz bank
(9) Victory is similar to		
(a) Failure	(b) Triumph	(c) Equal
(10) '=' is symbolic of		
(a) Equal to	(b) Greater	(c) Lesser
(11) Paisa tower is located in		
(a) Assam	(b) USA	(c) Italy
(12) 0,1s are the data for		
(a) Hex	(b) Binary	(c) Decimal

In these, we have to take the first letter of the correct answer. Then we need to take the previous letter of the correct one. The first letter of the correct values will be "tizbnljsteib". Now the letter previous to each will be "shyamkirubha".

This is the correct value what we wish to transmit. But before this transmission, sender and receiver has to agree on the fact that they should take the previous value of the correct one. Thus, Edustega is one of the commonly used steganography methods for camouflaging datas by manipulating in terms of questions and answers. As this educational field draws people attention, many researches are being developed in this area (Desoky, 2011).

Chestega:

- Selection of tools: It includes the selection of tools like chessmaster 8000 to produce the graph cover. The Chestega Cover can be in a form of a graph
- Protocols: For transmission between two parties

The following illustrates Chestega having chessboard as a criteria.

Assume that now the intension is to hide the content "shyamkirubha". The 8 bit representation of this:

Table 1: Secret information is hidden in "Price" column

Books	Prices in (s)
Introduction to C	115
Angles and demons	101
Horticulture magazine	99
The jazz piano book	117
The well cat book	114
4 blondes	105
The lab view style book	116
Introduction to nanotechnology	121

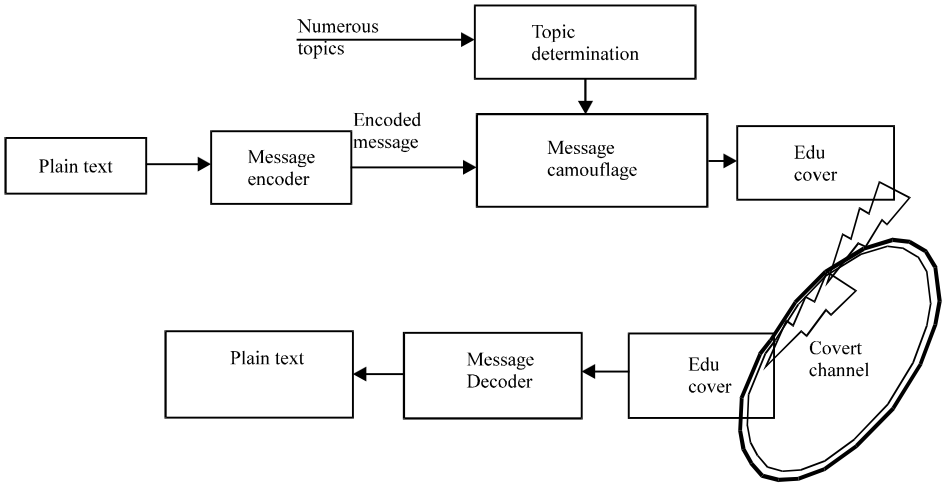

Fig. 6: Interfacing of Edu stega modules

01110011011010000111100101100001011011010110101101101001011100100111010101011000100110100001100001

It is then grouped as 7 digits and the corresponding decimal values are:

57, 90, 15, 22, 11, 53, 86, 105, 57, 29, 44, 38, 67, 1

The squares are encoded from 0 (in binary 0000000) to 127 (in binary 1111111). Employing an index that starts at 1 referring to 0 in decimal (in binary 0000000) up to 128 referring to 127 in decimal (in binary 1111111).

Figure 7 illustrates the white side and black side blocks after the secret message is buried. Table 2 explains how the bits are allotted in particular position.

While playing, the players will notice the moves and the corresponding decoding part is done and thus the data "shyamkirubha" is reached at the receiver side. In this way, Chestega can be employed for camouflaging the important information. The below example is for Chestega using players name as parameters: The data are taken from the chess master database. In this, binary values are assigned for the every first letter of the player name. The corresponding decimal values are calculated.

By using this, we can hide the data as we know the corresponding binary and decimal values for every first letter of the player name.

It legitimizes the interactions between the sender and recipient based on their interest in chess games. Therefore, the hacking will be difficult as the deal is made between the users, as they know how to hide the information. Thus, this Chestega can be used to convey long messages also as mentioned in Desoky and Younis (2009). Table 3 gives the performance evaluation of all the proposed stego methods. All the metrics of performance are convincingly satisfied and thus justify their creation.

(a) White side block

8	1	2	3	4	5	6	7	8
7	9	10	11	2	13	14	15	16
6	17	18	19	20	21	22	23	24
5	25	26	27	28	29	30	31	32
4	33	34	35	36	37	38	39	40
3	41	42	43	44	45	46	47	48
2	49	50	51	52	53	54	55	56
1	57	58	59	60	61	62	63	63
	A	B	C	d	e	f	g	h

(b) Black side block

8	65	66	67	68	69	70	71	72
7	73	74	75	76	77	78	79	80
6	81	82	83	84	85	86	87	88
5	89	90	91	92	93	94	95	96
4	99	98	99	100	101	102	103	104
3	105	106	107	108	109	110	111	112
2	113	114	115	116	117	118	119	120
1	121	122	123	124	125	126	127	128
	a	b	c	d	e	f	g	h

Fig. 7(a-b): Representation of secret in (a) White and (b) Black side blocks

CONCLUSION

To summarize, this cover generation based steganography the critical data is camouflaged in any created cover object. In this study, five such cover generation based steganography has been explained with necessary illustrations. Among all, Image Stega, Circuit Stega would never raise any suspicion to the normal users. The rest Graphstega, Edustega and Chestega would offer better payload. Robustness, imperceptibility and capacity is good for all the described methods.

Table 2: Allocation methodology in chestega

Binary	Decimal	Colour	Square
111001	57	W	A1
1011010	90	B	B5
1111	15	W	G7
10110	22	W	F6
1011	11	W	C7
110101	53	W	E2
1010110	86	B	F6
1101001	105	B	A3
111001	57	W	A1
11101	29	W	E5
101100	44	W	D3
100110	38	W	F4
1000011	67	W	C8
0	1	W	A8

Table 3: Performance analysis

Stego methods	Capacity	Visibility	Detectability	Robustness
Image stega	Limited by the number of images	Invisible	Probable to detect	Fairly robust
Circuit stega	Limited by the number of circuit elements	Invisible	Less probable to detect	Highly robust
Graph stega	Better capacity	Invisible	Poor probability to detect	Highly robust
Edu stega	Good	Invisible	Poor probability to detect	Highly robust
Chess stega	Good	Invisible	Poor probability to detect	Highly robust

ACKNOWLEDGMENT

Authors wish to appreciate Shyamkirubha for her earlier work on cover generation based steganography.

REFERENCES

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., D. Adharsh, V. Vignesh and R.J.B. Balaguru, 2010. PVD blend with pixel indicator-OPAP composite for high fidelity steganography. Int. J. Comput. Appl., 7: 31-37.

Amirtharajan, R., R.R. Subrahmanyam, P.J.S. Prabhakar, R. Kavitha and J.B.B. Rayappan, 2011. MSB over hides LSB: A dark communication with integrity. Proceedings of the IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application, December 12-14, 2011, Bangalore, Karnataka, India pp: 1-6.

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

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.

Desoky, A. and M. Younis, 2008. Graphstega: Graph steganography methodology. J. Digit. Forensic Pract., 2: 27-36.

Desoky, A., 2008. Nostega: A novel noiseless steganography paradigm. J. Digit. Forensic Pract., 2: 132-139.

Desoky, A. and M. Younis, 2009. Chestega: Chess steganography methodology. Secur. Commun. Networks, 2: 555-566.

Desoky, A., 2010. Comprehensive linguistic steganography survey. Int. J. Inf. Comp. Secur., 4: 164-197.

Desoky, A., 2011. Edustega: An education-centric steganography methodology. Int. J. Secur. Networks, 6: 153-173.

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010a. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, B.B. Zaidan and A.A. Zaidan, 2010b. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Firmware for data security: A review. Res. J. Inform. Technol., 4: 61-72.

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

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

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.

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

Stefan, K. and A. Fabin, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, London, UK.

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.

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure Communication: A Review. Res. J. Inform. Technol., 4: 31-46.

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

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

Zanganeh, O. and S. Ibrahim, 2011. Adaptive image steganography based on optimal embedding and robust against chi-square attack. Inform. Technol. J., 10: 1285-1294.

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.