Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 137-148, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.137.148

Mind Game for Cover Steganography: A Refuge

[1]Rengarajan Amirtharajan, [1]S. Deepak Roy, [1]Noel Nesakumar, [1]M. Chandrasekar, [2]R. Sridevi and [1]J.B.B. Rayappan
[1]School of Electrical and Electronics Engineering, SASTRA University, India
[2]Department of Physics, A.V.V.M Sri Pushpam College, Poondi, Thanjavur, 613 503, India

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

ABSTRACT

Living in the world of advanced and supercharged technology, habituation of internet information and computing contraptions has become inexplicably greater than before. Accordingly, communication and depot of facts, that too of confidence, has turned out to be an eminent antecedence. Thus the greater the furtherance, the greater is the need of defense. It is so because one can notice that every avant-garde digital felony has something to do with the security. Also technological progression has made a lot easier in communicating data however is assailable to snap and snatch by gatecrashers. Of all the other criteria, security tops the list for the reason that the information to be communicated may be of authoritative, high precision and insightful. To prevail over this issue come the solution in disguise, Cryptography and Steganography. Their ultimate endeavor is to have secure communication in its own right. While the former deals with text mostly, the other one deals with digital files in this modern epoch. Their intermingling is now a widely practiced platform of secret sharing. Like the rest, Image Steganography too has some basic jargons. The main of such is Cover image that is the image chosen to hide the surreptitious information. Faultless steganographic schemes lie upon the choice of building block and for sure cover images. This article takes this outlook and suggests a new way of cover generation. Thought provoking ideas are the magnificence of this script which will definitely be picked up by the researchers in the near future.

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

INTRODUCTION

From the time of discovery of communication through information, various modes to do so have also been unearthed. Be it written texts, wax tablets, tattoos, invisible inks etc. were in practice to communicate from one end to another. If one has a magnifying look in this thing, he or she can be well aware of the fact that secrecy is the underlying principle here. Thus confidentiality was the prime concern in sharing resourceful information between parties (Salem *et al*., 2011; Schneier, 2007). The terms given to this fashion are Cryptography and Steganography (Stefan and Fabin, 2000; Cheddad *et al*., 2010). Both being primordial, continue to rule the world of information security even today. The appealing reckons, though contrary, of these two schemes are simplicity (in use and implementation) and complexity (for the third party to attack). Though each of the above two is unique in their way, they do have the main motto; if formulated both in a single mechanism, no doubt that, it will show no mercy to attackers.

Though information' veracity is high in both the techniques, Steganography provides much more explorable domain. It has spread its wings to all types of digital files of which image steganography has caught immediate attention (Amirtharajan and Balaguru, 2009; Amirtharajan *et al*., 2010-2012). Its three basic attributes are cover image, steganographic algorithm and stego image. In these, cover images cloak crucial messages in them with colossal dexterousness leading to stego images. Indispensable traits of such technique is ability to bury high payload in a particular cover (embedding capacity), knack of making the resultant image indiscernible (imperceptibility), the level of secrecy maintenance (security), the cryptic effect (complexity) (Janakiraman *et al*., 2012a, b; Thanikaiselvan *et al*., 2011a, b; Padmaa *et al*., 2011) saving the best for last the toughness to withstand threats (robustness) (Hmood *et al*., 2010a, b; Amirtharajan and Rayappan, 2012a-d; Zanganeh and Ibrahim, 2011).

Nothing like Cryptography, Steganography has different mediums to achieve secret sharing which indeed has developed different covers. Popular examples are mimic functions and automatically generated English texts (Stefan and Fabin, 2000; Xiang *et al*., 2011). Reason behind cover generation is to circumvent the repeated usage of already existing covers. Newly developed covers definitely possess distinct properties as per their nature which will give an innovative horizon in developing the algorithm further. Moreover, the statistical features of the cover should also be taken into account whose dynamicity can bring a new color to the scheme. To quote it generally, steganography can take anything as cover (Janakiraman *et al*., 2012a, b; Rajagopalan *et al*., 2012; Thenmozhi *et al*., 2012; Zaidan *et al*., 2010); be it images (gray, color, binary), audio (Zhu *et al*., 2011), video (Al-Frajat *et al*., 2010), graphs, maps, time, circuits, histograms, chess, education centered testimonials and so on (Desoky 2008, 2010, 2011; Desoky and Younis, 2008, 2009).

Not only the above mentioned entities, but also, things one come across in daily life can also be exposed to steganography (Shirali-Shahreza and Shirali-Shahreza, 2008). The reason for this is one cannot even think of the actuality that such things embrace some covert information. So rather than sticking to accustomed procedures, a little different thinking will give out of the blue upshots. Moreover this initiative can minimize the threat of analysis to a great extent reducing a lumber. Many editorials have come up in relation to the cover generation throwing the light on fresh and unexampled means promising unimaginable and explicable purviews with possible-to-implement lineaments. Analyzing the aforementioned methods, this paper suggests a numerous methods for cover generation based steganography and its feasibility for real time applications.

PROPOSED METHODOLOGIES

This study paints yet another picture in generating covers for image steganography. It discusses about the custom of Trigonometry, Attendance slip, Thirukkural, Multiple choice Questions (MCQ), Sudoku, Tennis Score and Graphs. The description and methodology are also exemplified here for understanding. This paper also lists about the advantages behind using every suggestion as covers in steganography.

Cover generation through trigonometry function: Trigonometry is one of the oldest branches of Mathematics. It literally means 'triangle' measurement; it was used as a tool in astronomy. It possesses various functions and identities used in various fields like science; for instance, engineering, navigation, surveying etc. Steganography and Trigonometry is indeed a vast domain to travel around. Using Trigonometric functions to achieve steganography is really a novel

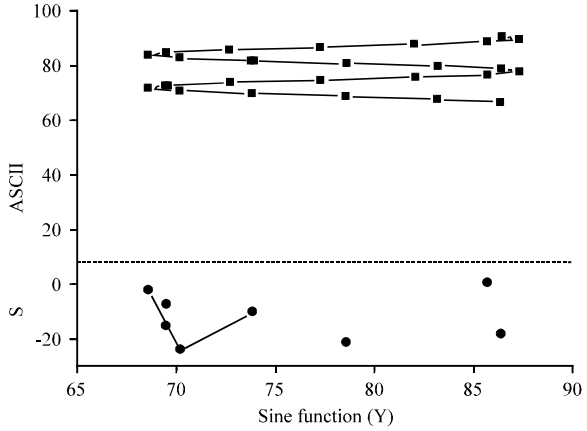

Fig. 1: Trigonometric functions to achieve steganography

technique which awe-inspires many scholars. Apart from theoretical analysis and numerical calculations, trigonometric identities can be made use for graphical plots leading to an image that can be used as a cover. One such example is given here; this pitch makes use of sine function as the base and includes statistical distribution, ASCII values, LVM algorithm and Chi-square calculation. This example is simulated in OriginPro 8. The procedure is explained in detail below and the result is presented in Fig. 1.

Algorithm

- 1,2,3,4,5,6,7,8 are assigned to S,E,C,U,R,I,T,Y. If any of the word is repeated then grand median will be considered. For e.g., 1,2.5,2.5,4,5,6,7,8 will be assigned to S,E,E,C,U,R,I,T,Y. The values are kept in X-axis
- The ASCII value of S, E, C, U, R, I, T, Y are 83, 69, 67, 85, 82, 73, 84 and 89, respectively. These numbers are kept in Y-axis
- Given data is fitted to the following sine function using Levenberg-Marquardt algorithm. Levenberg-Marquardt algorithm (LVM) tries to adjust the parameter values through iterative procedures. During each iteration, a chi square value is calculated in order to adjust the parameter values by reducing the chi square value:

$$\text{Sine function: } Y = Y_0 + A\sin\left(\pi\frac{X - X_c}{W}\right)$$

Where:

A = Amplitude (-0.13081±0.30404)
W = Period (1.75134±0.10335)
X_c = Phase shift (9.38727±1.77564)
Y_0 = Offset (77.94894±1.30319)

$$\text{LVM minimizes: } \sum\left[\frac{\text{Measured data} - \text{calculated data}}{\text{Weight}}\right]^2$$

where, weight is 1.

$$\text{Chi square minimizes: } \sum\left[\text{Weight}\left(\text{Measured data} - \text{calculated data}\right)^2\right]$$

where, weight is 1.

Algorithm: Continue

- The Fitted data Y (calculated output data) was limited to the range from 67 to 91 i.e., 25
- First 8 prime numbers (1,3,5,7,11,13,17,19) are considered in the place of 1,2 ....8 (these are the numbers which are already assigned to the letter S, E,C,U,R,I,T,Y)

Calculate:

$$S = \sum_{1=0}^{8} \text{Prime No.} - (\text{Total range} - 1)$$

- Plot both Range and S (in Y axis) against estimated Y value (X axis)
- Red spot indicates-S and black spot indicates estimated Y value

Advantages:

- Numerous entities offer countless plots
- Scope to incorporate other domains of engineering in constructing steganographic algorithm.
- Different perspective thus grabs little attention

OUTPUT

Cover generation through student attendance register: Attendance, an activity module, is to calculate the present days or hours of the participants and their course of actions. It may have different configurations and report patterns. The most common method way of posting attendance is marking a vertical line at an angle for showing ('P') the status of presence and marking ('A') for showing the status of absence which is a transparent and anybody can tamper with the data. Attendance register as a cover for hiding provides various options for embedding the secret data as it has many cells and involves both alphabetical and numerical figures in it. Ultimately, embedding capacity will be more due to the possibility of embedding high payload. An example is provided here for text steganography.

In steganography method the name of the students or some messages i.e., text image is hidden (embedded) in the cover in the form of binary value of the ASCII code. For example, the message is "CONFIDENTIAL" can be written a 10000111001111100111010001101001001100010010001 01100111010101001001001100000011001100 in the binary of the ASCII code is shown in Table 1. A present or absent mark has to be made in the corresponding columns to show his status. To show the status of presence or absence a binary value '0' is considered for marking absent and a binary value '1'is represented for marking present in this case.

Advantages:

- High capacity and imperceptibility
- Possess both numbers and alphabets thus adaptable to text and numerical secrets
- Many cells thus having large space for embedding
- Highly secure

Cover generation through SUDOKU puzzle: Sudoku is a standard 9×9 combinatorial puzzle solved by means of reasoning and logic. Sudoku in general has two patterns; one is of numbers and

Table 1: Attendance register as a cover for embedding

		Attendance status				
		15/02	18/02	19/02	20/02	21/02
Register No.	Student name	4	6	2	9	1
114004010	Ambati Veera Sheetal	P	A	A	P	P
114004014	Arjuna, G	A	P	A	A	P
114004017	Ashwin, G	A	A	P	A	A
114004029	Boyanpalli Sowmith	A	A	A	P	A
114004033	Chandawar Saichander	A	A	A	A	P
114004036	Chichhili Pratheek Reddy	P	P	A	A	P
114004039	Deepak Kumar, K	P	P	P	P	P
114004045	Ganapriya, K	P	A	A	A	P
114004050	Girija, N	A	P	P	A	P
114004054	Gowtham Raj, K	A	A	P	P	P
114004060	Hemalatha, R	P	A	A	P	P
114004061	Hirunyaa, R	P	P	A	A	P
114004067	Jataprolu Hanumath Sai Karthikesh	P	A	P	A	P
114004073	Jeyasnganthi, M S	P	A	P	A	P
114004075	Kakarlamudi Ramakrishna	P	P	P	A	P
114004085	Karthika, M R	A	P	A	A	P
114004090	Kodukula Srikanth	A	A	P	P	P
114004098	Madduri Nirup Reddy	P	A	A	P	P
114004101	Madhubala, S	P	A	P	A	P
114004103	Mahadevan, V	P	P	A	A	P

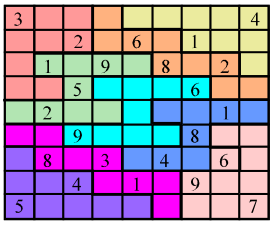

Fig. 2: Sudoku grid as a cover to embed secret data

other is of alphabets. The advantage of Sudoku is that its size and pattern can be varied in numerous ways which indeed provide countless fashion to embed the secret. An example is given here for showing how Sudoku can be used as a cover image shown in Fig. 2.

First the secret data is converted into binary. The first 4 bits are taken and its decimal value is compared with that of 9. If the value is smaller than 9 then it is embedded else first 3 bits are taken and then compared. For instance, the text message 'CONFIDENTIAL' in binary form is 100001110011111001110100011010010011000100100010110011101010100100100110000011001100. First 4 bits 1000 represent 8 which is smaller than 9. So it is embedded. For the fourth set of 4 bits it is not so. So instead 3 bits are taken for this set i.e., 111 is taken and its decimal is compared. Since it is 7, it is embedded. The process continues till all the bits are embedded. The basic principle of Sudoku is that no number should be repeated in same row, same column and in each 3×3 matrix. So, if we want to hide a phone number, say, 992564473, unlike digits should be

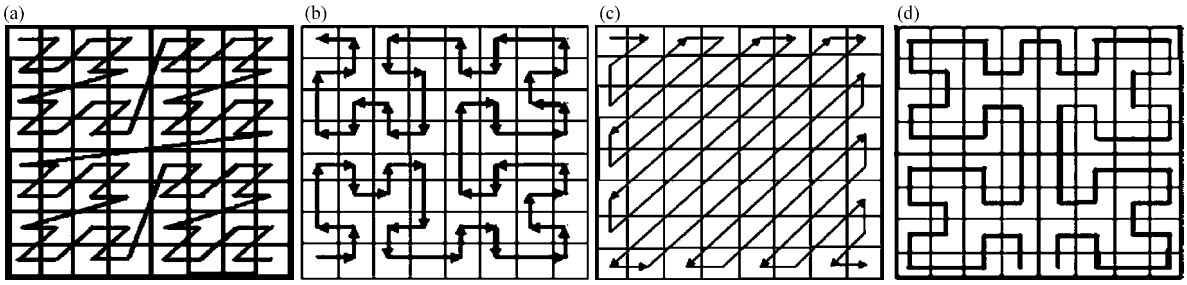

Fig. 3(a-d): Different traversing methods for data embedding, (a) Z scan SFC, (b) Hillbert SFC, (c) Zigzag SFC and (d) Moore SFC

engaged as above said. In this case if the first 9 in the phone number is embedded in 3rd row, the second 9 should have a place anywhere but that cell, row and column. Like this, confidential information can be hidden without violating the laws of the puzzle.

To increase the complexity, embedding can be done randomly rather than sequentially. For this, space filling curves like z scan, Hilbert, Zig-zag, Moore can play a good role shown in Fig. 3. This would rather make the process more secure and does not entertain human suspicion. This is a suggestion; taking this idea as initiative one can embed the secret without going against the standards of SFC. But the snag in this choice of cover is limited embedding capacity due to limited space constraints. Not only texts, other details can also be taken into account. For example, important information like phone numbers, account numbers can also be embedded in this manner.

Advantages:

- No restricted pattern; User can change the format as per his wish
- Both printable and digital versions
- Ease of use as it goes hand in hand with SFC
- Security is high

THIRUKKURAL

Thirukkural is a world famous Tamil couplet conveying most consummate human thought and is indubitably the best work in Tamil language. It holds 1330 couplets totally in 133 chapters. Each one apprizes an explicit theme maintaining unfussiness and legitimacy throughout its doggerels. Its permanence and universality are incontestable and is germane to all irrespective of religion, country and time. It is also a much unequaled choice of cover to achieve perfect steganography. As it does not constrain itself to Tamil alone, it can be used in various languages to which it is translated.

In this example, four such Kurals are shown to convey the secret message. Moreover, one cannot understand it without the particular linguistic knowledge. It is so because the meaning of 4 separate words in a particular language need not be exactly the same as that of others. So linguistic knowledge is what needed. Also, there is no limitation in number of couplets. It is completely as per the choice of the sender. The specialty here is that since each Kural ends with an understandable word than its rest, it is easy to convey a message to the destination. The numbering of Kurals also plays a vital role, in case of selection of set of Kurals belonging to a same chapter or

different chapters. Below given are two such examples comprising four couplets conveying the message 'Drinking is hazardous for life' in example 1 and 'Friendship does not come from face index' in example 2 in Tamil.

Example 1: Chosen couplets:

அரம்பொருத பொன்போலத் தேயும் உரம்பொரு(து) 888
உட்பகை உற்ற குடி.

நகைஈகை இன்சொல் இகழாமை நான்கும் 953
வகைஎன்ப வாய்மைக் குடிக்கு.

எட்பக(வு) அன்ன சிறுமைத்தே ஆயினும் 889
உட்பகை உள்ளதாம் கேடு.

மனம்மாணா உட்பகை தோன்றின் இனம்மாணா 884
ஏதம் பலவும் தரும்.

Secret message:

குடிகுடிக்குகேடுதரும்.

Example 2: Chosen couplets:

அடுத்தது காட்டும் பளிங்குபோல் நெஞ்சம்
கடுத்தது காட்டும் முகம். 706

தாள்ஆற்றித் தந்த பொருளெல்லாம் தக்கார்க்கு
வேளாண்மை செய்தற் பொருட்டு. 212

நுண்ணிய நூல்பல கற்பினும் மற்றும்தன்
உண்மை அறிவே மிகும். 373

முகம்நக நட்பது நட்பன்று; நெஞ்சத்(து)
அகம்நக நட்பது நட்பு. 786

நீங்கீன் தொறூஉம்; குறுகுங்கால் தண்ணென்னும்:
தீயாண்டுப் பெற்றாள் இவள்? 1104

நட்பிற்கு வீற்றிருக்கை யாதெனின் கொட்பின்றி
ஒல்லும்வாய் ஊன்றும் நிலை. 789

வருகமன் கொண்கன் ஒருநாள்; பருகுவென்
பைதல்நோய் எல்லாம் கெட. 1266

நுனிக்கொம்பர் ஏறினார் அ்.திறந்(து) ஊக்கின்
உயிர்க்கிறுதி யாகி விடும். 476

Secret message:

முகம்பொருட்டுமிகும்நட்புஇவள்நிலைகெடவிடும்

Advantages:

- Bandwidth consumption
- Availability
- No complex pre and post processing
- Intricacy increases with number and linguistics

Cover generation through multiple choice questions (MCQ): Multiple choice questions as a cover? Yes it is! It is a kind of education centric steganographic line of attack. It is a fresh linguistic approach that disguises the data through manipulation. With the correct answers for the questionnaire, one can form a hint about the secret to be conveyed or directly convey the secret itself. Furthermore, it can be a word document, a pdf that facilitate the receiver to haul out the secret data. Another variants include match the following, synonymous, antonyms, fill up the blanks, jumbled words, comprehension, finding errors, omission, telegraph writing, notice writing etc. Though sounds undemanding, they can be modified up to the convenience of the user or sender. Thus it can very well accommodate more information and different types of it (like symbols, numerical etc.). Scholars are exploring it deeply to give it a new color of steganography.

Here, presented three such examples. Example 1 is the disguised version of decoding 'AMIR'. It is hidden after converting the word into double. One can decode the secret by extracting two bits from each correct answer. Thus by having 2 bits from 14 answers 28 bits are obtained. By having 7×4 amalgamations, the secret can be decoded. In example 2, the first letter of the correct answer for first question is read, second letter of the correct answer for second question like this for the 4 questions 4 characters are read to form SEEE which is the covert data to be communicated. In example 3, in all the correct answers, first letter should be taken and for each letter in the obtained word, the previous letter is read to get the secret information.

Multiple choice questions:
Example 1:

- ----------is the capital of Tamilnadu a] Thanjavur b]Madurai c] Chennai d] Trichy
- ----------is the capital of karnataka a] Bangalore b]Bombay c] Madras d] delhi
- USA flag has----------stars. a] 50 b] 88 c] 55 d] 100
- A+B is the representation of----------gate a] NOR b] AND c] NAND d] OR
- A.B is the representation of----------gate a] AND b] NAND c] OR d] XOR
- AB'+A'B is for----------gate a] OR b] AND c] NAND d] XOR
- ----------is the capital of Maharashtra a] Chennai b] Mumbai c] Calcutta d] Delhi.
- ----------is the capital of Bengal a] Mumbai b] Chennai c] Calcutta. D] Delhi
- Saniamirza related to----------event. a] Cricket b] Tennis c] Table tennis d] Hockey
- Present USA president is----------a] Obama b] Hillary c] Clinton d] Osama
- Microsoft founder is----------a] Naraya moorthy b] Bill Clinton c] Bin laden d] Bill gates
- Frequency of the pulse varied in----------a] FM b] ASK c] AM d] FSK
- Big temple constructed by----- a] Rajaraja Cholan b] Sophy raja Cholan c] Amirtharaja Cholan d] Rajandra cholan
- Who is the father of the nation a] Indra Gandhi b] Rajiv Gandhi c] Mahatma Gandhi d] Sonia Gandhi.

Example 2:

- Colombo is the capital of
- India b) Srilanka c) China d) Pakistan
- According to the Newton's third law, Every action has a equal and opposite----------
- When some one deposits money in an account, the money is (a) Spent b) lost c) credited d) created
- Which color is considered to be the symbol of prosperity (a) white b) red c) green d) black

Example 3:

- Jaipur is the capital of (a) Tamilnadu b) Andra c) Rajastan d) kerala
- A diode with reduced break down voltage is (a) Zener diode b) photo diode c) LED d) Gunn diode
- Who wrote the Indian National Anthem? (a) Amirtharajan b) sophy c) Kevin d) Rabindranath Tagore
- What is the name of this association----------
- The process of mapping cont voltage value to finite discrete levels is called (a) Breaking b) mapping c) Quantization d) decomposition
- ---------- is the name of a country Thanjavur b) Tamilnadu c) SASTRA d) Zimbabwe

Advantages:

- Most common and widely used element that draws no attention
- Highly impregnable
- Different formats of questionnaire are accessible to be covers
- Enhanced imperceptibility

Cover generation through GRAPH: Graphs are clear choice of cover as they are the effective measure of performance of a particular scheme and also give the relationship between two or more entities. It has diverse forms like directed, undirected, quiver, multi-, mixed, weighted, line, pie, bar, area, polar, waterfall etc. Each graph has one of its kind structure, outline and prototype giving rise to countless uses. Therefore, graphs can be used as cover images for steganography and can be modified as the algorithm requires. Since it is very commonly used in the academics as well as in researches, they tend to be a good choice for covers. Since pictorial representations employ multicolor they form the indispensable metrics for steganography.

In this example, the secret message hidden is 'welcome to covert communication' shown in Fig. 4. This is converted to corresponding ASCII values and by maneuvering it numerical values are obtained and finally the graph is plotted with the register number of the students along x axis and their marks in the subject Computer Networks along y axis. This proposal does not leave a clue about the covert information and hence interest no mistrust. Altering the entities in the axes, adopting multiple entries and espousing complex formats one can go achieve superior hiding capacity.

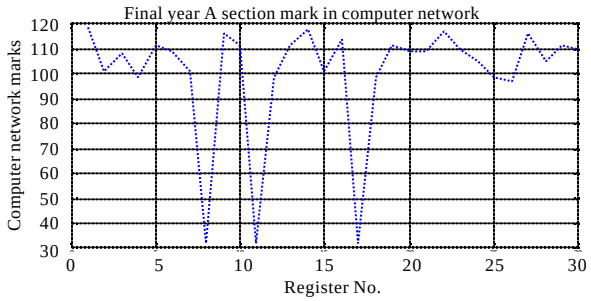

Fig. 4: Graphical method example of hidden communication

Table 2: Sample tennis score sheet-COURT NUMBER 16

Previous sets				Players	Sets	Games	Points
6	6	6	5	Mr. A. Agassi	2	1	40
7	3	4	7	Mr. T. Henman	2	2	40

Advantages:

- Plentiful formats as coves
- Ease to extend and decrease the axis
- Peculiar choice giving rise to distinct covers

Cover generation through TENNIS scores: It has now become a new perspective to include score sheet of sports as covers in steganographic techniques for instance cricket. As it has many entities, it suffices its application as cover image. Taking this as initiative, this proposed method takes the cover as Tennis score sheet. It is composed of sets, points and games. A set is composed of number of Games and in turn gives points to the players. Number of games is restricted from six to twelve. Tennis score sheet includes previous sets, players name, current set, Games and Points. Mostly all are of one digit value from 0 to 9.The secret data is first converted into binary. For embedding 3 bits are considered and then changed into decimal and place this in first place of score sheet. This process continues till all the secret bits are used. The sample score sheet is shown in Fig. 1. Except the players name and sets columns, this method can embed the data in all other columns, since names are not numerical and sets value depends on previous sets.

All columns are of single digit value except games and points column, consider that as a two single digit value to entrench. For games columns, consider only first bit to embed and the next is kept blank always and point column values should be restricted up to the values of 40, if the secret bits exceeds this value, embed the exceeded value only. Apart from typical score card, additional entries like match time, time of the day, court number can also be made use of to achieve data hiding. This is so because, tennis game score have only limited number of numerical figures as shown in Table 2 unlike cricket which can have many. Therefore, high margin of capacity is assured.

Advantages:

- Fair margin of capacity
- Security is emphasized
- Steganography goes unnoticed
- Robustness is guaranteed

CONCLUSION

Important attribute of steganography is Cover irrespective of the format. It plays a crucial role in constructing a steganographic routine. As various operations are done on covers to make the plot strong, their need of indestructibility is inevitable. This paper discusses about the importance of covers used in steganographic techniques and proposes different covers to be used as so. Each proposal is explained with an example providing justification to this paper. Benefits of each method

are highlighted. Thus, these methods are one of its kinds and have the highest possibilities to be exercised commercially. This paper gives a clear view about covers and their uses without compromising other horizons of 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. 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.

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

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

Desoky, A., 2010. Comprehensive linguistic steganography survey. Int. J. Inform. Comput. 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 2^n: 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.

Salem, Y., M. Abomhara, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2011. A review on multimedia communications cryptography. Res. J. Inform. Technol., 3: 146-152.

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.