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): 2005-2010, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.2005.2010

Gyratory Assisted Info Hide-A Nibble Differencing for Message Embedding

Sundararaman Rajagopalan, Har Narayan Upadhyay, Swetha Varadarajan,
J.B.B. Rayappan and Rengarajan Amirtharajan
School of Electrical and Electronics Engineering, SASTRA University, India

Abstract: The growing demand to protect the confidential messages and documents paved way for the invent of information security techniques. Whatever, be the strength of security algorithms and standards, an equal amount or greater than that attempt is made to crack the information which employs an algorithm to make it invisible to anonymous. New techniques and algorithms will help a lot for strengthening the security of our information systems. Steganography is basically a science turned art to hide the payload with the help of a carrier. We propose a spatial domain image steganography technique which uses two aspects for information hiding-one being the pixel nibble difference and the other in the form of block rotation decided by a variable P'. This technique adds a technique to the group of information hiding techniques where block rotation can be decided by various parameters concerned with the carrier which may be audio, video or text.

Key words: Image steganography nibble differencing, block rotation, LabVIEW based steganography, NI IMAQ vision

INTRODUCTION

The radical change in information handling has been enhanced by the kind of information security methodologies (Al-Azawi and Fadhil, 2010; Al-Frajat *et al*., 2010; Amirtharajan and Balaguru, 2009; Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al*., 2011) which have been developed over the years. The present internet world works with enormous payload but protection of the payload till it reaches out the concerned is a big challenge (Cheddad *et al*., 2010; Amirtharajan *et al*., 2012). We have come across security approaches broadly classified into three. Cryptography (Schneier, 2007), a technique which scrambles the payload with the help of a key to make the payload or data, known to be cipher text. Public Key, Private Key, Block Ciphers, Stream Ciphers and Encryption standards proposed by Forensic agencies are a part of cryptography family. On the other hand, Information copy right protection is achieved through watermarking (Karzenbeisser and Perircolas, 2000; Zeki *et al*., 2011). Robust and Fragile are the predominantly used categories of watermarking.

Steganography, the third approach is a methodology to hide the secret message in a carrier which is also called cover (Cheddad *et al*., 2010; Hmood *et al*., 2010a, b; Amirtharajan and Balaguru, 2009; Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al*., 2011). The cover for carrying or hiding the information may be an image, audio file (Zhu *et al*., 2011) or a video file (Al-Frajat *et al*., 2010). Steganography on image has been reported in various earlier works (Janakiraman *et al*., 2012a, b; Thanikaiselvan *et al*., 2011a, b). Various parameters have been considered in the past such as methods to decide the amount of information to be hidden (ie) capacity, Increasing the robustness of hiding process, Encryption hiding on image, Image processing based hiding techniques, Adaptive embedding, Integrity check mechanism added stegano approach (Amirtharajan *et al*., 2011), Random pixel embedding, Block based emedding etc., Also FPGA based steganography approaches (Rajagopalan *et al*., 2012a, b) have been reported in literature.

Simple LSB substitution with optimal pixel adjustment process, fondly called as OPAP has been proposed by Chan and Cheng (2004). Pixel value differencing is proposed by Wu and Tsai (2003) where number of bits embedded is decided by the proposed algorithm. Hiding information on RGB images have been presented by Amirtharajan and Balaguru (2009) and Amirtharajan *et al*. (2011) and many other works (Padmaa *et al*., 2011; Mohammad *et al*., 2011; Thenmozhi *et al*., 2012; Qi *et al*., 2010; Zaidan *et al*., 2010; Zanganeh and Ibrahim, 2011).

We propose a grayscale image steganographic algorithm which uses nibble differencing technique where minimum absolute difference between the Upper nibble of the pixels of a selected 2×2 message embedded image block guides the block bits rotation angle to make the final stego image.

Corresponding Author: Sundararaman Rajagopalan, School of Electrical and Electronics Engineering, SASTRA University, India

PROPOSED METHODOLOGY

Let I be the grayscale image with A_x and B_y as its row and column dimensions, where $1 \leq x \leq N$ and $1 \leq y \leq N$. Here, I_{xy} is an element of the image I.

When a message m_j from the {M} has to be embedded into a pixel $I_{xy,}$ the pixel undergoes the following change:

$$I'_{xy} = I_{xy} - I_{xy} \bmod 2^k + m_j$$

where, k is the No. of bits to be embedded in a pixel I_{xy}. Grayscale Image of size N×N I is divided into blocks such that:

$$Ib_{mn} \in I \mid Ib \subset I$$

where $1 \leq m \leq 2$ and $1 \leq n \leq 2$. Figure 1 shows the Ib subset.

Now Ib is a subset of I (ie) a 2×2 pixel group which belongs to the grayscale image I. Let us assume the Ib with the following elements:

$Ib_{i,j-1}$	$Ib_{i,j}$
$Ib_{i-1,j-1}$	$Ib'_{i-1,j}$

where, i and j are row and column respectively. After embedding encrypted k-bits in the Ib block, the block becomes:

$Ib'_{i,j-1}$	$Ib'_{i,j}$
$Ib'_{i-1,j-1}$	$Ib_{i-1,j}$

Let this embedded block be an intermediate block Intb. Calculating the absolute differences between Upper nibble of the Intb block pixels:

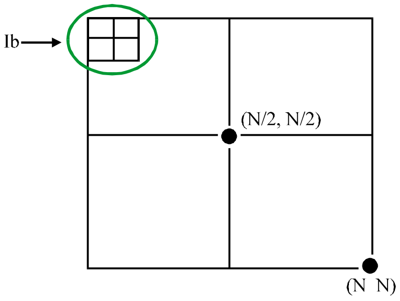

Fig 1: Subblock Ib from the Image I

- **D1** = abs $((Ib'_{i,j-1}>>4)-(Ib'_{i,j}>>4))$
- **D2** = abs $((Ib'_{i,j-1}>>4)-(Ib'_{i-1,j-1}>>4))$
- **D3** = abs $((Ib'_{i,j-1}>>4)-(Ib'_{i-1,j}>>4))$
- **D4** = abs $((Ib'_{i,j}>>4)-(Ib'_{i-1,j-1}>>4))$
- **D5** = abs $((Ib'_{i,j}>>4)-(Ib'_{i-1,j}>>4))$
- **D6** = abs $((Ib'_{i-1,j-1}>>4)-(Ib'_{i-1,j}>>4))$

where, $\{D1,D2,D3,D4,D5,D6\} \in \{D\}$. Finding minimum ({D}) which is the minimum difference between a pair of pixels of the block and {el(minimum({D})}, which is the pair of nibbles producing minimum difference to decide the number of times the embedded k-bits of all the pixels of the block has to be rotated. By concatenating upper nibbles of {el} by doing the following operation we get:

$$P' = ((el_1 \in \{el\})\ \&\ 240)\ \text{OR}\ (el_2 \in \{el\}) >> 4$$

where, P' gives a number of times the lower nibbles of the block has to be rotated. The 6th bit b_6 of P' decides the direction in which the rotation should happen:

- If b_6 is 1_Clockwise Embedded k-bits rotation P' times
- If $b_6$is 0_Anti-clockwise Embedded k-bits rotation P' times

P' can also be expressed as:

$$P' = (((el_1 \in \{el\})\ \&\ 240)\ \text{OR}\ (el_2 \in \{el\}) >> 4) \bmod 4$$

Because if block is rotated 4 times, the resultant block will be equal to the Intermediate block and also one time rotation of the block clockwise or anticlockwise results in change in orientation of the block by 90°. This holds good for even 1 bit rotation among the pixels of the block.

Therefore P' times rotation = (P' mod 4) times rotation. Figure 2 shows the orientation of the Intermediate block Intb after various rotation angles.

(a) $Ib'_{i,j-1}$	$Ib'_{i,j}$
$Ib'_{i-1,j-1}$	$Ib_{i-1,j-1}$

(b) $Ib''_{i-1,j-1}$	$Ib''_{i,j-1}$
$Ib''_{i-1,j}$	$Ib''_{i,j}$

(c) $Ib''_{i-1,j}$	$Ib''_{i-1,j-1}$
$Ib'_{i,j}$	$Ib''_{i,j-1}$

(d) $Ib''_{i,j}$	$Ib''_{i-1,j}$
$Ib''_{i,j}$	$Ib''_{i-1,j-1}$

Fig. 2(a-d): (a) Intermediate block, (b) 90° clockwise lower nibble rotation (c) 180° clockwise lower nibble rotation and (d) 270° clockwise lower nibble rotation

Here, $Ib''_{i-1,j-1}$ = ($Ib'_{i,j-1}$ & 240) OR ($Ib'_{i-1,j-1}$ & 15), if k = 4. Similarly other elements of Ib” can be computed for different k values.

After rotation, the procedure has to be repeated for other Ib blocks by selecting the blocks in a random manner or by a specific order defined by the user.

Let us consider an example. Let Ib be:

150	155
161	170

A total number of 16 bits have to be embedded in this block. The encrypted message to be embedded is 0000111100001111. It is evident that each pixel should carry 4 bits of secret information making k = 4. After embedding the secret message the Ib becomes:

Intb =

144	159
160	175

When finding the {D}, the elements of {D} are D1 = 0, D2 = 1, D3 = 1, D4 = 1, D 5 = 1 and D6 = 0. As the minimum of {D} are D1 and D6 and considering the difference pair based on the order of precedence which is D1, {el} elements are 144 and 159. Concatenating the upper nibbles of 144 and 159 we get P’ as 10011001_2 which is equivalent to 153 in decimal. As b6 of P’ is 0, 153 times Anticlockwise rotation or P’ = 153 mod 4 (ie) 90° anticlockwise rotation (or) one time block rotation by left. Now the resulting block will be:

Final stego subblock =

159	159
160	160

The decryption of message from the stego image can be done as per the following pseudo code:

```
For I = 1: Total blocks
{
    Select a single 2×2 block;
    Calculate minimum absolute Upper nibble difference;
    Find the lowest difference pair {eld} ;
    Form P” through concatenation of the elements ∈{eld};
    If $b_6$ (P”) = ‘0’
    {
        Rotate 2x2 block by 4-(P” mod 4) times anticlockwise;
    }
    Else
    {
        Rotate 2x2 block by 4-(P” mod 4)
        times clockwise;
    }
    Collect the embedded k-bits from each pixel of 2x2 block;
}
repeat till the last stego block;
}
```

RESULTS AND DISCUSSION

The algorithm has been tested on various grayscale images of size 256×256 using LabVIEW software with IMAQ tool box. Four images namely Cameraman, Vegetables, Mahathma Gandhiji and Sailboat were used for testing our hiding method. Figure 3(a-d) show the cover images considered and Fig. 4(a-d) display the stego images for k = 1, 2,3 and 4.

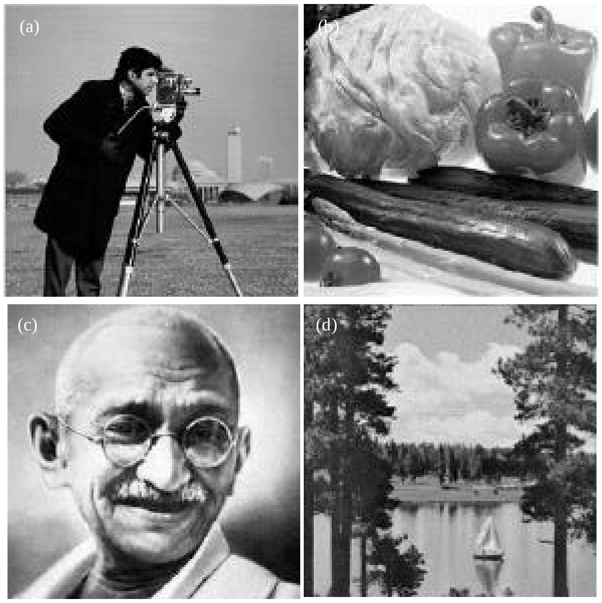

Fig. 3(a-d): Cover images (a) Cameraman, (b) Vegetables, (c) Mahathma Gandhiji and (d) Sail Boat

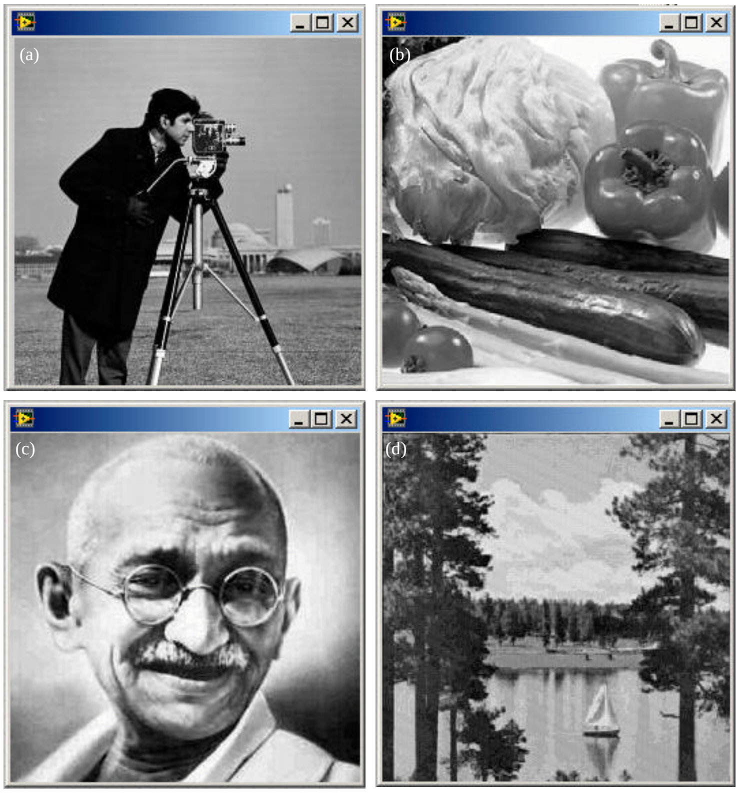

Fig 4(a-d): Stego images (a) Cameraman (k = 1), (b) Vegetables (k = 2), (c) Mahathma Gandhiji (k = 3) and (d) Sailboat (k = 4)

Table 1: MSE results for various K values

	MSE			
Cover Image	K = 1	K = 2	K = 3	K = 4
Cameraman	0.5005	2.2644	10.9991	34.1708
Mahathma Gandhiji	0.4976	2.2546	11.1793	33.7893
Vegetables	0.4959	2.2415	10.7852	33.4857
Sailboat	0.497	2.2588	11.0889	34.0121

Table 2: PSNR results for various K values

	MSE			
Cover Image	K = 1	K = 2	K = 3	K = 4
Cameraman	51.1363	44.5813	37.7172	32.7942
Mahathma Gandhiji	51.1616	44.6000	37.6467	32.8430
Vegetables	51.1761	44.6253	37.8025	32.8822
Sailboat	51.1672	44.5920	37.6819	32.8145

The quality of the stego images after embedding secret data in the cover images has been computed with parameters like Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). Table 1 presents the MSE and Table 2 presents the PSNR for the test images with different k-bit embedding.

The Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) of a received stego image can be calculated as follows:

$$\text{MSE} = \frac{1}{\text{MN}}\sum_{X=1}^{M}\sum_{Y=1}^{N}(S_{XY} - C_{XY})^2$$

$$\text{PSNR} = 10\log_{10}\left(\frac{C_{\max}^2}{\text{MSE}}\right)$$

where, X and Y are image coordinates, M and N are the dimensions of the image. S_{XY} is the message containing stego-image and C_{XY} is the cover image. Also $S^2_{\max}$ has the maximum intensity value in the image which is 255 for the grayscale images.

COMPLEXITY AND ROTATION STATISTICS OF STEGO ALGORITHM

The complexity of this algorithm can be analysed as follows:

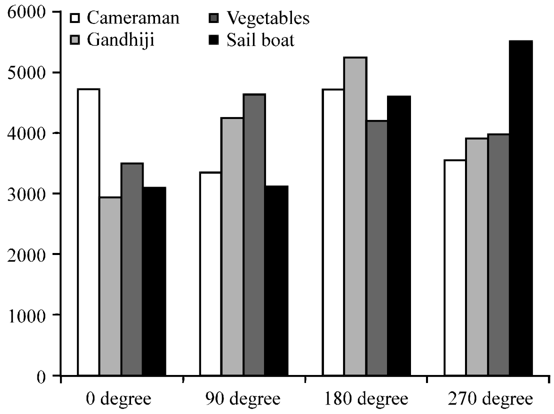

Fig. 5: Rotation statistics for various test images

We have considered 256×256 grayscale images that contain 16384 2×2 blocks. The order of choosing the 2×2 blocks can be done in 16384! ways. For full capacity embedding, as per the worst case PSNR, each pixel can carry 4 bits which means a 2×2 block needs 16 bits. This 16 bit message can be scrambled in 16! ways. The arrangement of 4bits message/pixel for a 2x2 block can be done in 4! ways. Also the block can be rotated in 4 different ways.

Therefore, the total complexity of the system is 16384! ×16!×4!×4.

The theoretical probability of rotating the block by specific angle from angle set {0, 90, 180, 270°} ∈ {A} is ¼. We have done an analysis on the probability of rotating a block by a specific angle from the {A} by computing, of the 16384 2×2 blocks of 256×256 stego image how many blocks are rotated by an angle from {A} and this analysis is shown in the graph displayed in Fig 5.

It is inferred from the Fig. 5 that comparatively lesser number of blocks were not rotated (ie) number of blocks rotated by 0 or 360° is less. As per this analysis, the average probability of rotating a block by 0° is 0.218201, 90° is 0.235138, 180° is 0.287048 and that of 270° is 0.259613. Comparing this with theoretical probability of block rotation, 0° and 90° fell short of ¼ threshold.

CONCLUSION

A gray image steganographic algorithm with block rotation has been proposed in this paper. Nibble differencing has been the key to decide block rotation and this approach has resulted in distributed angle rotation. This approach has also yielded approximately 78.17% of total 16384 blocks being rotated by non-zero angle. Also the stego images generated by our algorithm has an excellent imperceptibility being supported by the PSNR and MSE results of various test images. This technique can also be coupled with other stegano approaches like transform domain steganography.

ACKNOWLEDGMENT

The authors wish to express their sincere thanks to DRDO, New Delhi for their financial support (ERIP/ER/1003836/M/01/1230). They also wish to acknowledge SASTRA University, Thanjavur for extending infrastructural support to carry out the study.

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., 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.

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.

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.

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

Mohammad, N., X. Sun and H. Yang, 2011. An excellent Image data hiding algorithm based on BTC. Inform. Technol. J., 10: 1415-1420.

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

Qi, K., D.F. Zhang and D. Xie, 2010. A high-capacity steganographic scheme for 3D point cloud models. Inform. Technol. J., 9: 412-421.

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

Rajagopalan, S., S. Janakiraman, H.N. Upadhyay and K. Thenmozhi, 2012b. Hide and Seek in Silicon-Performance Analysis of Quad Block Equisum Hardware Steganographic Systems. Procedia Eng., 30: 806-813.

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

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.

Wu, D.C. and W.H. Tsai, 2003. A steganographic method for images by pixel-value differencing. Pattern Recogn. Lett., 24: 1613-1626.

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.

Zeki, A.M., A.A. Manaf and S.S. Mahmod, 2011. High watermarking capacity based on spatial domain technique. Inform. Technol. J., 10: 1367-1373.

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.