Research Journal of Applied Sciences, Engineering and Technology 7(19): 3957-3963, 2014
DOI:10.19026/rjaset.7.754
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: April 01, 2013 Accepted: May 03, 2013 Published: May 15, 2014

**Research Article**

# A Novel Approach to Enhance the Security of the LSB Image Steganography

[1]Morteza Bashardoost, [1]Mohd Shafry Mohd Rahim, [2]Ayman Altameem and [3]Amjad Rehman
[1]Faculty of Computing, Universiti Teknologi Malaysia, Skudai, 81310 Johor, Malaysia
[2]College of Applied Studies and Community Services, King Saud University, Riyadh, KSA
[3]College of Business Administration, Salman Bin Abdul Aziz University, Riyadh, KSA

**Abstract:** Forming a logical balance between the quality of the file and the scope of data that can be conveyed is the test of steganographic techniques to form such a balance. On top of that, the facts that cannot be covered up are the robustness of the method and security of the vague data. An insertion method which delivers a high level of visual quality and a huge amount of volume for the obscured data is called the Least Significant Bit (LSB), but the concealed message is poorly secured through this technique. In the recommended approach, the Vigenere encryption techniques initially used to encode the secret data to assure the safety of the concealed message. Later, the data is contracted through the Huffman coding method in order to decrease the occupational volume of the classified data. Then, each bit stream of the data is dispersed out onto the image to enhance the robustness of the technique by using the expanded knight tour algorithm. The outcomes show that apart from enhancing the visual quality of the stego image, the recommended technique enhances the safety and payload capacity issues of the simple LSB technique.

**Keywords:** Huffman coding compression, image steganography, knight tour embedding algorithm, LSB insertion technique, vigenere encryption

## INTRODUCTION

Critical concerns in the digital world today are data security and safety of personal information. Hence, there has been a drastic surge in the demand for possessing a safety technique to convey the classified data. Steganography is a division of cryptography and is the art and science of communicating in a manner which conceals the presence of communication. Hence, its term which literally means "covered writing" (Cheddad *et al*., 2010). Steganography stresses on concealing the presence of message inside another data in such a manner that nobody can identify it. On the other hand, cryptography makes data illegible for a third party by denoting certain encryption techniques (Shouchao *et al*., 2011; Du-Shiau *et al*., 2007).

The visual requirements of image for instance colour and smoothness are changed when an enormous volume of data is embedded into an image (Anderson and Petitcolas, 1998). It is essential to stipulate how the secret is embedded in the image based on the fact that steganography is the method of concealing vital information inside a cover data without causing any reservations.

There are several parameters, which can be examined, to evaluate the steganographic methods:

The capacity refers to the highest volume of bits that can be embedded in a specific cover file with a small chance of disclosure by an adversary is referred by the capacity parameter in steganographic techniques (Esra and Hakan, 2012).

As far as the quality of the image is concerned, the imperceptibility value determines the level of alterations in the look of the cover data whenever the message is embedded is demarcated by imperceptibility. The look or format of cover files must stay unharmed after concealing the secret data in case the steganographic system founders if an attacker is capable of verifying the presence of a secret message.

Robustness, which is another parameter of the steganographic methods evaluation, specifies the misrepresented amount that the digital cover can bear to retain the security of the secret message (Tariq *et al*., 2003). In an easier term, the technique must ascertain the unity of the message for the receiver albeit the stego file being impaired by the executed assaults within the transmission stage.

The security metric specifies the confidence of storing the secret data for the antagonist when it is retrieved by attacks signifies the security measure (Xinpeng and Shuozhong, 2004).

**The coneventional LSB:** The most prevalent spatial domain method (Daneshkhah *et al*., 2011) is the Least Significant Bit (LSB) insertion (Dey *et al*., 2007) which sequentially substitutes the least significant bit of cover

**Corresponding Author:** Morteza Bashardoost, Faculty of Computing, Universiti Teknologi Malaysia, Skudai, 81310 Johor, Malaysia

image with the message bits. In identifying the small difference of colors, this technique capitalizes the natural drawbacks of the Human Visual System (HVS) (Yi-Zhen *et al*., 2010). The image's change is not distinguishable to any human eye because the LSB technique alters some or the entire $8^{th}$ bit of the image's data. In the same manner, when utilizing a color image, the LSB of each of the red, green and blue constituents can be used. So, the probability for concealing secret data in a grayscale model is one third that of an identical image size in colored image.

On top of that, it would be quite simple to identify and retrieve the message when the data is embedded consequently to all bytes of the cover image. To have a secret key between the sender and receiver to identify which bytes of image have been used for concealing data is a reasonably more secured technique (Anand and Dharaneetharan, 2011). As a result, if an antagonist obtains the image, the secret data cannot be retrieved unless with the stego-key.

As mentioned above, LSB algorithm is not extremely safe against statistical assaults and the security of concealed data is not definite regardless of having the biggest payload and also high levels of quality and imperceptibility. To put it in another way, it would be quite simple to locate the original message by retrieving the data from the cover image (Chan and Cheng, 2004). Taking into account all of the above, other than having substantial quality and imperceptibility, is there any approach to increase the safety of the LSB technique?

## LITERATURE REVIEW

The LSB method or any of its derivatives are used by numerous algorithms that work in the spatial field as the algorithm for information concealment. But some kinds of statistical examination for instance RS (Xiangyang, 2005) or Sample Pairs (Dumitrescu *et al*., 2003) make it irresistible for these techniques, even if partly obscured in the volume of information concealed. The issue comes from the reality that embedding the secret data in the cover image led to a misrepresentation that is not distinguishable to the human eye, but is identifiable by statistical examinations.

The Optimal LSB insertion which executes an alteration process to locate the optimal pixels to enhance the stego-image quality is an enhanced LSB method. Indeed, to identify which one has the nearest value to the source pixel value when the secret data is embedded, three candidates are chosen to compare their values to the source pixel's value. Subsequently, the chosen or best candidate is known as the optimal pixel and used for concealing the secret data (Chan and Cheng, 2004).

Besides the high level of imperceptibility, the Pixel Value Differencing (PVD) technique (Wu *et al*., 2005) uses the features of Human Visual System to lengthen the volume of the image for concealing data. The edge area is able to embed additional secret data inside since smooth areas and edge areas have diverse payload capacities (Liping *et al*., 2010). In reality, the misrepresentation tolerance level of a smooth area is normally lower than an edge area. In addition, the features of image blocks in the PVD method stay unchanged because this technique does not alter any smooth area to the edge area as well as in reverse.

A novel method has been proposed to improve the capacity of image for hiding information. They suggested that the compression must be performed two times. Traditionally, JPEG standards reduce duplicate data by using energy compaction property and using steganography by introducing bits blocks in the resultant compressed image. The new image do not cause any increase in the size of the compressed image (Jafari *et al*., 2011).

In another study (Raja *et al*., 2005) some algorithms have been used to improve security and robustness as well as enhancement in capacity of stego-objects. First of all, they have applied the DCT to transfer images from the spatial domain into frequency domain and the LSB has been used to provide maximum payload and then the stego-object is further compressed using quantization and run length coding to derive a secure stego-object. In the receiver also the reverse of this method must be done to retrieve the payload.

## PROPOSED METHODOLOGY

The general architecture of the recommended steganography technique is created and executed. The entire process is comprised of two chief stages, which are the embedding stage and receiving stages demonstrated in Fig. 1.

**Embedding process:** All the undertakings that must be executed to conceal and safeguard the secret data inside the cover image are incorporated in this phase. The sender embeds the bit stream into the image after using some algorithms to encode and compress the data. Furthermore, the initial position of the bit stream within the image is demarcated by the secret key. This key is recognized only for the sender and receiver.

The sending process is made up of the subsequent procedures.

**Encryption:** The plain text will be encrypted by means of the Vigenere table in the initial step of the embedding stage (Dennie, 2007). In this situation, we require a technique that does not generate a cipher text

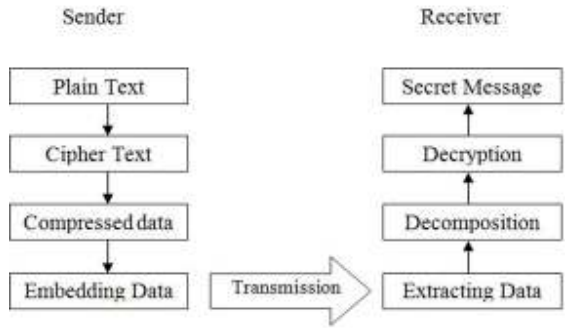



Fig. 1: The proposed framework

lengthier than the plain text even though there are some encryption techniques that can be employed to encrypt the data. In addition, compared to other preferred encryption techniques, the Vigenere table is safer because it is a symmetric encryption (Aruljothi and Venkatesulu, 2010) method and maps each input character into precisely one character for output. The Vigenere table has the most advantage compared to other symmetric encryption techniques is that based on the indicated secret key, it generates diverse outputs for a specific input character.

**Compression:** An appropriate answer for the restricted payload space of the host image can be compressing the message. Limiting the message size not only lessens the possibility of finding the message inside the host image, but also enhances the capacity of the cover image. To efficiently reduce the size of the message, the Huffman coding compression method (Das and Tuithung, 2012) is applied. To substitute the recurrent subsequent characters with a binary code, Huffman coding creates a table which will be forwarded to the recipient at the completion of the compression process to be used for retrieving original secret messages.

**Embedding:** The most significant part of the steganographic techniques is the embedding algorithm. In reality, it demarcates in which order the pixels be altered with the secret data as well as which pixels of the image should be changed.

An appropriate method to formulate the series of the secret bit stream within the image pixels is called the "Knight Tour" algorithm. As knight tour is a self-created algorithm based on the Knight Tour mathematical problem (Parberry, 1997) and it is virtually unknown for the inadvertent receivers, it poses an advantage over the PRNG technique (Sobol and Levitan, 1999). By taking into account the image as stretched chessboard, we are able to determine the path of the knight within the image by having an algorithm.

The answer to the "Knight Tour" problem is by dividing the chess board into blocks with the size of 4×4 squares. Moreover, in each block it considers four groups of four squares that are: "Right Diamond", "Left Diamond", "Right Square" and "Left Square". The chief rule of the surfing is to finish the squares within the chessboard on each group and then proceed to the following group of squares.

The "Knight Tour" algorithm forms the basis of the embedding algorithm of the recommended steganographic technique. Nevertheless, it has the bigger board and furthermore it is not required to constantly pass all the squares. The algorithm will include all the pixels if the size of the image can be divided by four. Or else, the additional columns or rows (which are below 4) will be useless. The recommended embedding method follows the subsequent steps.

First of all, consider the images width and height divisible by four (Disregard the extra pixels). Then, divide the image into 4×4-pixel blocks. After that, proceed to the first pixel which has been indicated by the stego-key and commence with a single group (color) and go across all the blocks. Next, to proceed from one block to the following one, all the 4 squares must be gone across. After that, commence with the following group if the movement for one group (color) has completed. Finally, duplicate the steps to go across the entire pixels.

**Replacement:** When the series of the target pixels is demarcated in the earlier step, now it is the time for the bit stream of the secret message to substitute the least significant bits of the image pixels.

**Extraction stage:** The receiver should be able to grasp the secret data within the Stego-imageon the other end of the communication line. Thus, to recover the matter of the message and reorganize it, an additional procedure is needed.

Firstly, bits of the secret message are acquired to create a compressed database on the stego-key and the removing algorithm (similar to the sender's side). At that juncture, the encrypted data will be generated by the unzipping algorithm and lastly, by utilizing the Vigenere table, the plain message will be exposed.

## EXPERIMENTAL RESULTS

To evaluate the proposed method, we used MATLAB tools. Furthermore, we employed the standard images of Photographer and Peppers, which are depicted in the Fig. 2, as the grayscale samples to prove the performance of our method. We performed the testing operation for different sizes of host images and verity sizes of hidden data to meticulously examine the results.

To have a precise observation of the fulfillment of our method, we examined the results in terms of

(a) (b)

Fig. 2: Standard photos of (a) photographer, (b) peppers

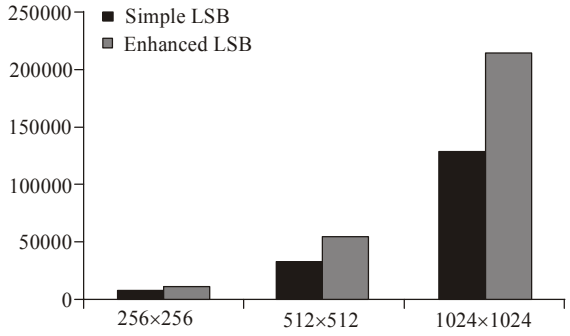



Fig. 3: Maximum payload capacity of simple and enhanced LSB methods

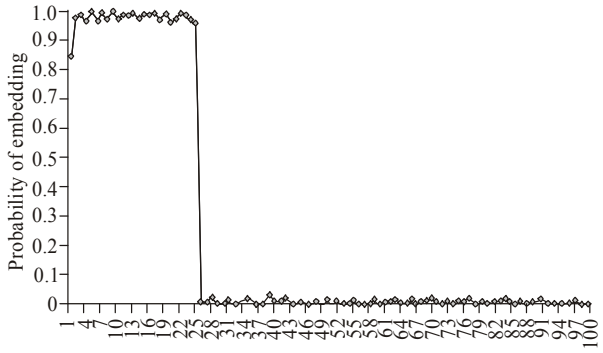



Fig. 4: Chi-square attack result of simple LSB method for embedding 2 KB data

capacity, quality, robustness and security. As we expected, our Enhanced LSB method shows a satisfactory performance especially when the capacity of the host image is the metric of the evaluation.

**Capacity:** The maximum payload capacity for the Simple LSB approach is the situation that the least significant bit of all the image pixels are used for the embedding. Therefore, the maximum bits of the capacity would be the multiplication of the image's width and height. Since the size of the secret data is reduced by using Huffman coding in our proposed method, the payload amount elaborated significantly. Figure 3, depicts the clear comparison between the

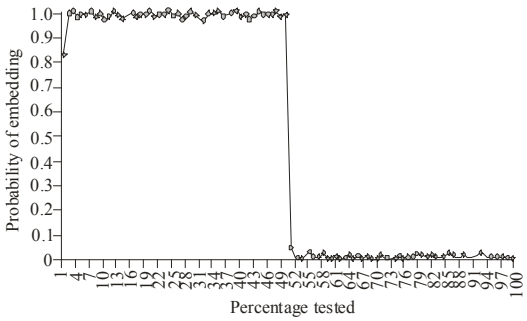



Fig. 5: Chi-square attack result of simple LSB method for embedding 4 KB data

enhanced and conventional LSB methods in terms of payload capacity.

**Quality:** In this phase, we have investigated the quality of the result image to understand how much the outputs are similar to the host images. In the other words, we want to make sure that the stego-images do not arouse the suspicion when they are probed by the unintended person. To inspect the imperceptibility of the image, we utilized the PSNR (Peak Signal-to-Noise Ratio) standard quality metric, which is defined as the Formula 1. To interpret the result of the PSNR equation, we must know that the higher amount of PSNR shows the better quality of the result image and vice versa:

$$\mathrm{PSNR(dB)} = 10 * \log\left(\frac{255^2}{\mathrm{MSE}}\right) \quad (1)$$

$$\mathrm{MSE} = \sum_{i=1}^{x}\sum_{j=1}^{y}\frac{(|A_{ij}-B_{ij}|)^2}{x*y}$$

As it presented in the Table 1, the PSNR values for the Simple LSB method and our Enhanced LSB method has been calculated for the different input images. The outcome figures show a dramatic increase in the PSNR value for all the tested instances, when we used our Enhanced LSB method. In addition, comparing the outcome results indicates that the PSNR values are varied for the different images even with the same dimensions. Last but not the least, the figures of the Table 1, proves that increasing the size of the secret data leads to moderate drop in the PSNR value.

**Security:** To challenge the security aspect of the Enhanced LSB method, we exploited the Chi-square attack on the stego-images. In fact, the Chi-square attack examines the pixels of suspected image for existence of concealed data.

When the Chi-square attack applied on the stego-image of Simple LSB method, the result revealed the presence of the hidden data. Figure 4 and 5 depict the

Table 1: Payload size-simple LSB method and enhanced LSB method

| | Simple LSB | | | | Enhanced LSB | | | |
|---|---|---|---|---|---|---|---|---|
| | Photographer | | Peppers | | Photographer | | Peppers | |
| Message size (bits) | 32768 | 65536 | 32768 | 65536 | 32768 | 65536 | 32768 | 65536 |
| Embedding rate | 0.0625 | 0.1250 | 0.0625 | 0.1250 | 0.0625 | 0.1250 | 0.0625 | 0.1250 |
| PSNR (dB) | 57.4995 | 54.5289 | 57.6139 | 54.5678 | 58.7321 | 56.0103 | 59.1103 | 55.7043 |

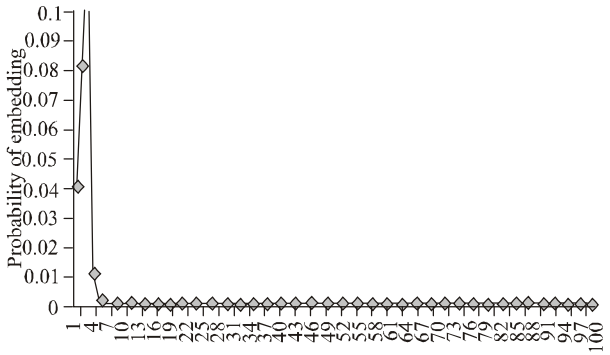



Fig. 6: Chi-square attack result-enhanced LSB method (embedding 2 KB data)

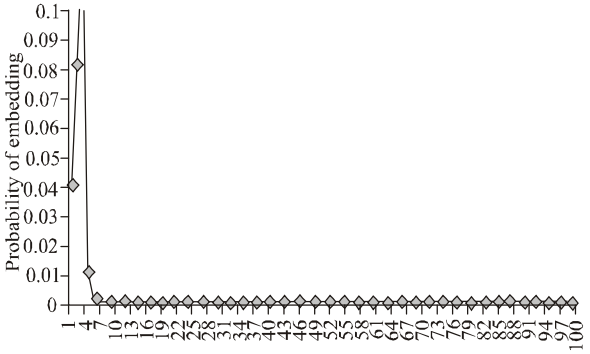
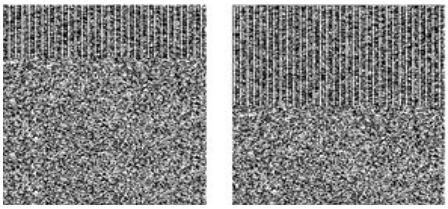



Fig. 7: Chi-square attack result-enhanced LSB method (embedding 4 KB data)

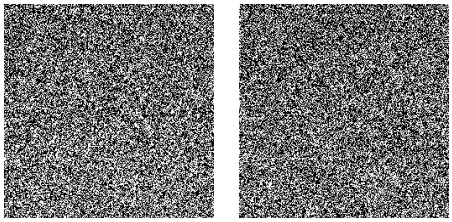
(a) (b)

Fig. 8: Photographer test image (a) and (b) its least significant bit layer



(a) (b)

Fig. 9: The result of simple LSB method, (a) layer zero with 50%, (b) 100% of hidden data



(a) (b)

Fig. 10: The result of enhanced LSB method, (a) layer zero with 50%, (b) 100% of hidden data

detection probability of the confidential message when the size of the secret data is 2 and 4 kilobytes. By having a detailed view on the diagram, we can see that the probability value notably falls down from one to the zero after investigating 25% of the pixels in Fig. 4 and 50% of the pixels in the Fig. 5.

On the other hand, because of using Knight Tour algorithm in the Enhanced LSB approach, the results are dramatically different. When the Chi-square attack applied on the result images of the proposed method, no hidden data has been revealed. Even when the size of the secret data increased from 2 kilobytes in the Fig. 6 to 4 kilobytes in the Fig. 7, no suspicious trend appeared in the diagrams.

The result of the security test over proposed method proves the resistance of the Enhanced LSB method against Chi-square attack.

Another visual attack which can be applied to inspect the security of our method is the LSB layer visual attack. In this attack the least significant layer of the image will be investigated to detect the hidden data. The mechanism of this attack is to decompose the stego-image into its eight layers. Then, by probing the Least Significant Layer the image artifacts, which are not observable by human eyes, can be detected.

As it shown in the Fig. 8, the LSB layer of the cover image displays some random black and white pixels which do not present any clear pattern. In contrast, the LSB layer of the stego-image that is generated by Simple LSB approach obviously displays the zebra pattern. The vertical lines which are presented in the Fig. 9a and b indicate the existence of 25 and 50% of hidden data. However, the experimental results confirm the stability of our method against this visual attack in the Fig. 10.

## CONCLUSION

In this study, by offering certain augmentations, we decided to repair the short comings of the Simple LSB

system. Three essential enhancements mainly Knight Tour embedding algorithm, Vigenere encryption and Huffman coding compression are used by the Enhanced LSB method. The encoding of the classified information by utilizing the Vigenere encryption method is the commencement of the process. The sender as well as the receiver has a secret key which is used in encryption and decryption stages. After that, the size of encrypted data is reduced by the Huffman coding compression method in order to increase the payload capacity. Evidently, as much the rate of compression surges, the length of input data rises, as well. Lastly, in the positions which are demarcated by the recommended embedding algorithm, the generated bit stream is embedded into the image. The aforementioned embedding method provides the highest number of pixels to conceal the secret message and is a protracted form of the Knight Tour algorithm.

As it was anticipated theoretically, when the method was established, satisfactory results were attained. Due to exploitation of the compression technique, the Enhanced LSB technique saves up to forty percent of volumes demonstrated by results. Hence, small number of pixels of the image will be most likely altered and subsequently there is an enhancement in the quality of the stego image. On top of that, lesser volume of data will be misrepresented although active visual attacks by the third party will affect the Stego image. Lastly, when the private message becomes encrypted, the prospect of retrieving the matter of hidden data decreases substantially.

## RECOMMENDATIONS

We have attempted to enhance the security level of Simple LSB method through this study and due to the utilization of the compression stage in the proposed technique, apart from the volume of payloads had increased, the quality and robustness were also enhanced. Nevertheless, if the subsequent criteria are taken into account in future works; the recommended technique can be enhanced, which are analyses the stability of the technique as compared to other statistical assaults and also by taking other bits of the host image into consideration to enhance the robustness of the technique. And lastly, improve the technique by way of rectitude. That means the receiver must be aware that it is a false message whenever the secret data has been altered within the transmission channel.

## REFERENCES

Anand, J.V. and G.D. Dharaneetharan, 2011. New approach in steganography by integrating different LSB algorithms and applying randomization concept to enhance security. Proceedings of the 2011 International Conference on Communication, Computing. Rourkela, Odisha, India, pp: 474-476.

Anderson, R.J. and F.A.P. Petitcolas, 1998. On the limits of steganography. IEEE J. Sel. Area. Comm., 16: 474-481.

Aruljothi, S. and M. Venkatesulu, 2010. Symmetric key cryptosystem based on randomized block cipher. Proceedings of the 5th International Conference on Future Information Technology (Future Tech), pp: 1-5.

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

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

Daneshkhah, A., H. Aghaeinia and S.H. Seyedi, 2011. A more secure steganography method in spatial domain. Proceeding of the 2nd International Conference on Intelligent Systems, Modelling and Simulation (ISMS), pp: 189-194.

Das, R. and T. Tuithung, 2012. A novel steganography method for image based on Huffman encoding. Proceeding of the 3rd National Conference on Emerging Trends and Applications in Computer Science (NCETACS). Shillong, pp: 14-18.

Dennie, V.T., 2007. Cryptographic techniques for computers: Substitution methods. Inform. Storage Ret., 6: 241-249.

Dey, S., A. Ajith and A. Sugata, 2007. An LSB data hiding technique using prime numbers. Proceedings of the 3rd International Symposium on Information Assurance and Security (IAS 2007), pp: 101-108.

Dumitrescu, S., W. Xiaolin and W. Zhe, 2003. Detection of LSB steganography via sample pair analysis. IEEE T. Signal Proces., 51: 355-372.

Du-Shiau, T., C. Tzung-Her and H. Gwoboa, 2007. A cheating prevention scheme for binary visual cryptography with homogeneous secret images. Pattern Recogn., 40(8): 2356-2366.

Esra, S. and I. Hakan, 2012. A compression-based text steganography method. J. Syst. Software., 85(10): 2385-2394.

Jafari, R., D. Ziou and A. Mammeri, 2011. Increasing compression of JPEG images using steganography. Proceeding of the IEEE International Symposium on Robotic and Sensors Environments (ROSE), pp: 226-230.

Liping, J., L. Xiaolong, Y. Bin and L. Zhihong, 2010. A further study on a PVD-based steganography. Proceeding of the International Conference on Multimedia Information Networking and Security (MINES), pp: 686-690.

Parberry, I., 1997. An efficient algorithm for the Knight's tour problem. Discrete Appl. Math., 73: 251-260.

Raja, K.B., C.R. Chowdary, K.R. Venugopal and L.M. Patnaik, 2005. A secure image steganography using LSB, DCT and compression techniques on raw images. Proceedings of the 3rd International Conference on Intelligent Sensing and Information Processing (ICISIP 2005), pp: 170-176.

Shouchao, S., Z. Jie, L. Xin, D. Jiao and W. Qiaoyan, 2011. A novel secure communication protocol combining steganography and cryptography. Proc. Eng., 15: 2767-2772.

Sobol, I.M. and Y.L. Levitan, 1999. A pseudo-random number generator for personal computers. Comput. Math. Appl., 37: 33-40.

Tariq, A.H., A.Q. Mahmoud and B. Hassan, 2003. A testbed for evaluating security and robustness of steganography techniques. Proceeding of the IEEE 46th Midwest Symposium on Circuits and Systems, 3: 1583-1586.

Wu, H.C., N.I. Wu, C.S. Tsai and M.S. Hwang, 2005. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. Proceedings of the IEE Vision, Image and Signal Processing, 152: 611-615.

Xiangyang, L., L. Bin and L. Fenlin, 2005. Detecting LSB steganography based on dynamic masks. Proceedings of the 5th International Conference on Intelligent Systems Design and Applications (ISDA '05), pp: 251-255.

Xinpeng, Z. and W. Shuozhong, 2004. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recogn. Lett., 25(3): 331-339.

Yi-Zhen, C., H. Zhi, L. Shu-Ping, L. Chun-Hui and Y. Xiao-Hui, 2010. An adaptive steganography algorithm based on block sensitivity vectors using HVS features. Proceedings of the 3rd International Congress on Image and Signal Processing (CISP), 3: 1151-1155.