ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 09, Issue, 09, pp. 29910-29914, September, 2019

REVIEW ARTICLE OPEN ACCESS

LSB BASED IMAGE STEGANOGRAPHY TECHNIQUES RENOVATION

***Abdalla A. Ramah Al Enzi and Dr. Putra Sumari**

School of Computer Sciences, Universiti Sains Malaysia, Pulau Pinang, Malaysia

ARTICLE INFO

Article History:
Received 20th June, 2019
Received in revised form
03rd July, 2019
Accepted 01st August, 2019
Published online 30th September, 2019

Key Words:
Image Steganography, Least Significant Bit (LSB), Information Hiding, Embedding Capacity.

ABSTRACT

This paper investigates current state-of-the-art LSB based image steganography techniques and tools. The LSB substitution of the image pixels selected sequentially or randomly is the most commonly used spatial domain technique and provides high embedding payload (Li, *et al*., 2011). It is substitutes secret data bits into least significant bits of cover object to generate the stego image. LSB is one of the most frequently used method because of fine concealment, high capability of hidden information and easy implementation. Changes in the value of the LSB are difficult to discern by human visual system (HVS) because the amplitude of the change is small and the stego image will look identical to the cover image. Even though it is most popular and simplest image steganographic method but susceptible to lossy compression and image manipulations such as scaling, rotation, cropping etc. Therefore, the resulting stego-image will destroy the embedded secret message. Therefore, LSB Steganography contains two techniques: Sequential Embedding and Scattered Embedding.

Citation: Abdalla A. Ramah Al Enzi and Dr. Putra Sumari. 2019. "LSB based image steganography techniques renovation", *International Journal of Development Research*, 09, (09), 29910-29914.

INTRODUCTION

The concept of "What You See Is What You Get (WYSIWYG)" in digital multimedia files is no longer precise and would not trick a Steganographer as it does not always hold true. Nowadays, digital multimedia files can be more than what the Human Visual System (HVS) sees; therefore, they can contain other data which is hidden somewhere (Cheddad, *et al*., 2010). Steganography is the process of hiding secret data within public information and considered broken when the existence of the secret information is detected (Fridrich, *et al*., 2007). The majority of steganography is to design the algorithms used in embedding secret information with the maximum amount of bits allowed to be embedded in a certain multimedia cover object in such a way undetectable concealment (Cox, *et al*., 2008). Nevertheless, steganographic systems are not required to obtain high robustness, high imperceptibility as well as steganographic capacity in all cases. Therefore, steganographic systems should obtain a high capacity and high imperceptibility, but they are not necessarily robust (Marvel, *et al*., 1998; Venkatraman, *et al*., 2004). Thus, steganographic systems are either not robust against changes or have limited robustness against data processing such as compression, format conversion, or digital-to-analogue transformation (Wang and Wang, 2004). The most widely used method of image steganography is Least Significant Bit (LSB) embedding, which is provides the basic idea of image steganography in a simple way. It is states that the least significant bits of the pixels of the cover image can be replaced by the secret message bits. This technique is reliably detectable by current steganalysis methods; the intruder can access the embedded secret data by only picking LSBs. Also it can easily be destroyed and lose the data by noise and compression techniques. Thus, the developed improvements of LSB embedding became the field of interest by researchers in the last years (Xiaopi, *et al*., 2005; Xiaoyi and Babaguchi, 2008; Yang, *et al*., 2008; Luo, *et al*., 2012). Also, there was a growth of interest of using the extensions of LSB based image steganography techniques, such as improved LSB replacement, LSB mapping, and LSB matching to overcome the limitations of simple LSB based image steganography technique.

LSB Renovation

Most of the existing methods and tools of steganography focus on the embedding strategy and give no consideration to the post-processing stages, such as decryption, or revealing the hidden message. The existing methods or tools pay little attention to the security issue to the extent that some of them

***Corresponding author:* Abdullah Al Enzi,**
School of Computer Sciences, Universiti Sains Malaysia, Pulau Pinang, Malaysia

accept providing one key only and others go further than this by making the provision of the key an option. Thus if an attacker 'catches' one key, the hidden message is read. Another shortcoming concerns the stego object size. In some tools, the stegnography process result (i.e. the stego image) is 'larger' due to injecting it with the secret data and this can be easily detected. How? Though it is easier to hide a secret message in the area of brighter color in an image, this method is apt to be visually suspected, or even detected, due to the large number of duplicate colors, where identical colors appear twice in the image and differ only in the LSB. Other methods or tools resorted to SLSB method. The SLSB stands for 'Selected Least Significant Bit', a method in which data is hidden in only one of the three colors at each pixel of the cover image. Since this method uses only one of the three colors at each pixel, then it follows that the amount of hidden data will be less. Even in such 'sophisticated' method, the hidden data are prone to be detected (Kessler, 2002; Hayati, *et al*., 2007). With the Steganography, various methods have been proposed. These methods are briefed and compared below:

Another method was proposed by Singh *et al*. (P. Singh, 2005). In this method, the message was hidden in a combination of the 1st and 2nd bit plane. The challenge in this method was the probability of message insertion at a pseudorandom location as this percentage was 50% and dropped to 12.5% when a change in the pixel value was required. The LSB method was modified and introduced advance version of the method by Bailey and Curran (Curran, 2006). In the advanced method, 3 colors were used, Red, Green and Blue where the LSB of the Red channel was used for the 1st pixel, Green for the 2nd pixel and Blue for the 3rd pixel. This to be repeated in same cyclic order. The beauty of this method is the 100% insertion for the RGB image but the back point was the ease of decoding the insertion by the intruder. Yang *et al*. (Yang, *et al*., 2009) proposed an adaptive LSB based technique for image steganography. This technique has high payload due to using the pixel modification technique for better stego image quality. Channalli and Jadhav (Channalli and Jadhav, 2009) presented a LSB based image steganography technique. It is utilized the common bit pattern to embedding secret message. Nevertheless, this technique results in low payload because the secret message and the pattern bits LSB's of pixels are modified. One more method was proposed by (Batra and Rishi, 2010), which hide the message in the 6th, 7th and 8th bits of a pixel in a grayscale image. This method improved the probability of message insertion in Singh method to 85.93% and 43.18% when the message was not changed. Hence, this method still does not give the desired 100% message insertion rate. Pixel indicator method is another method presented by Gutub (Gutub, 2010). Gutub applied his method on the RGB image method using 2 channels of the image to store the data based on the value of the 3rd channel which is playing the indicator channel role. This method provides high capacity of decoding by the intruder in addition to high capacity data insertion as it uses sequential order to choose the indicator channel (RGB, RBG, GBR, GRB, BRG, and BGR). In this method, 2 bits and 4 bits of secret message can be hidden inside a single pixel. Despite all this, still it doesn't provide 100% insertion rate as one channel is used as indicator. Based on enhancing security to secret information Karim *et al*. (Karim, *et al*., 2011) proposed a new technique in which secret information is embedded by using LSB approach with secret key. This proposed technique is utilizing RGB true color images for embedding process. The secret information is embedded within particular LSB bits of cover image, whereas the secret key is utilized to decode the secret information in order to avoid detection. Secret information is embedded on various location of LSBs of cover image in random way based on used secret key. Therefore, improving the steganographic system robustness and imperceptibility. Experimental results represent that this technique recorded higher level of security to hidden information than traditional LSB technique. This steganography system also has good PSNR value. Al-Shatnawi (Al-Shatnawi, 2012), proposed method that depends on covering the hidden message based on searching for the similar bits between the hidden message and image pixels' values. Proposed technique was compared with the LSB benchmarking method for concealment the secret data which hides the secret message directly in the least two significant bits of the image pixels. By the end of the day, it's found off that the proposed method is more efficient, simple, appropriate and accurate than LSB method, it seeking for the correspondent bits then starts hiding, also the change in the image resolution is quite low which gives more, secure on the secret message.

Gupta *et al*. (Gupta, *et al*., 2012) proposed an improved LSB image steganography technique in which secret information is embedded in blue component only of the RGB color image. The size is determined by M×N of particular image which is used as a cover image. Only blue components are used for embedding secret information. Depending upon the best regions determined to embed secret information in cover image, pixel filters used to obtain best possible rate. Experimental results represent that this technique decreases the distortion level of cover image, enhancing the stego image quality, and modifications in cover image are difficult to discern by Human Visual System (HVS). Samidha and Agrawal (Samidha and Agrawal, 2013) presented a LSB based image steganography technique utilizing random least significant bit selection to embedding secret information within the cover image. Samidha and Agrawal also developed other methods based on random selection bits of random pixels used in cover image to embedding secret information. This random selection approach based on some parametersw such as intensity values, pixels location etc. A new novel steganography technique based on LSB method got created by providing new concept to secure data which is proposed by Modi *et al*. (Modi, *et al*., 2013). It is used least two significant bits of edges to embed secret information. The edge regions are considered as suitable areas to hide the secret information compared to other smooth regions of cover image. The detection of edge regions depends upon the amount of embedded information within cover image, which means it does adaptive edge detection. Experimental results analysis represents that these techniques enhances performing compared to the traditional LSB based image steganographic systems. These techniques are also providing better security to hidden information versus visual attacks.

Dagar and Dagar (Dagar and Dagar, 2014) proposed a steganography technique for color RGB images for embedding secret information with enhanced security level of data transferred online. The cover image utilized to embed secret data in 24 bit RGB pixels by using X-Box mapping. Whereas, some boxes consist of 16 various values, were "X" represented by any integer number from 0 to 9 to stored theses values in XBoxes. Subsequently, X-Boxes values are mapped with

LSBs of cover image. Experimental results analysis shows that this method provides a better level of security of hidden information due to the attacker must use of mapping to extract the embedded secret information. Furthermore, this mapping generates high PSNR value which leads to higher stego image quality. Based on LSB substitution, Deshmuk and Pattewar (Deshmukh and Pattewar, 2014) also proposed an adaptive edge steganography technique. Edges regions of the cover image utilized to embed secret information using adaptive scheme and variation among two adjacent pixels of cover image. Experimental results analysis shows that their method performs better than other LSB image steganographic methods and Pixel difference based techniques, while maintaining a certain level of stego image quality that is acceptable. N. Akhtar *et al*. (N. Akhtar, *et al*., 2014) also proposed the enhanced version of traditional LSB image steganography technique. They concerned with implementing two approaches of bit inversion techniques, with an enhancement in both security and image quality. In these techniques, certain least significant bits of cover image are inverted only and only if they arise with particular pattern of pixel's bits. Thus, reduces the number of least significant bits of cover image is altered compared to traditional LSB method. Embedded secret information can be obtained correctly by embedding the bit patterns for which LSBs are inverted somewhere within the stego image. Therefore, LSB indices utilized in such a way to embedding the secret information and thus, making it very difficult for attacker to extract the secret information. xperimental results represent that this method generates good PSNR value and shows good enhancement to stago image quality.

Nag *et al*. (Nag, *et al*., 2014) proposed a novel steganographic technique of LSB substitution based on Huffman Coding. It aims to improve security and the payload; hence acceptable level of stego image quality. Using Huffman tree is by encoding every 8 bits of the hidden image. Subsequently, the encoded bits partitioned into four parts were represented by decimal values from 0 to 3. These decimal values are determining the embedded information location in cover image. Experimental results analysis demonstrates that PSNR value of stego image is acceptable and it is very hard to detection and secret message extraction by the attacker due to Huffman table utilized, which reduces the cover image size.
An enhanced version of LSB++ technique is presented by Qazanfari and Safabakhsh (Qazanfari and Safabakhsh, 2014) based on the distinction among sensitive pixels. This process is allow preserving sensitive pixels from embedding of extra bits, which reduces distortion level in co-occurrence matrices. This proposed method has lower traces or signatures in the co-occurrence matrices than previous LSB++ technique. Moreover, experimental results analysis shows that it has greater security versus histogram based attacks because this technique does not make any modifications in the histogram, thus histograms of both cover and stego image are identical. This improved technique also has high quality of stego image due to abstraction of extra bit embedding. Nusrati *et al*. (Nusrati, *et al*., 2015) also present steganographic technique for embedding secret information in a cover image based on heuristic genetic algorithm. It determines the convenient locations in cover image to embed secret information in order to reduce the amount of possible modifications of image histogram. The heuristic genetic algorithm working on partitioning the secret information and LSBs into set of block called secret blocks. Hence, this algorithm determines the convenient locations embedding process, then, the secret blocks are embedded. Whereas, embedding process, it generates the secret key which is used to retrieve the hidden information from the stego image during extraction process. An improved version of LSB image steganography technique using different progressions proposed by Goel *et al*. (Goel, *et al*., 2014-2015) Stego image quality parameters such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), histograms and CPU time, Structure Similarity (SSIM) index and Feature Similarity Index Measure (FSIM) are used as performance analysis parameters and experimental results are compared with original cover image. Practical results show that proposed steganographic technique has higher efficiency than traditional LSB techniques. Prashantiand Sandhyarani in (Prashanti and Sandhyarani, 2015) presented a survey on neoteric accomplishments of LSB based image steganography. Their analysis enhancements obtain on experimenting steganographic systems results such as high security, high imperceptibility, high payload and acceptable level of robustness for embedded secret information.

There are two techniques are also presented along with this survey, first technique utilized to embed secret information into cover image. Were second technique is used gray scale image as a secret information which is embedded into another gray scale image. Hence, four state table utilized to generate produce pseudo random numbers, which that used for embedding the secret information. These techniques have higher security due to hidden secret information on LSBs locations of cover image that selected randomly based on pseudo random numbers generated by the four state table. Khalind and Aziz in (Khalind and Aziz, 2015) proposed a new method of non-adaptive LSB steganography . Their technique aims to improve the embedding efficiency from 2 to 8/3 random bits per one embedding change even for the embedding rate of 1 bit per pixel. After it takes 2 bits of the secret information per one embedding change, compare these 2 bits to the LSBs of the two selected pixel values for embedding process. This technique always assumes a single mismatch existed between the two values and utilized the second LSB of the first pixel value to store the index of the mismatch. Authors have found that their experimental results are provides greater security than existing approaches such as LSB replacement, LSB matching, and LSB matching by decreasing the probability of detection. Moreover, the proposed technique is also reduces the overall bit-level modifications to the cover image for the same amount of secret information and avoiding complex calculations. On the other hand, experimental results represent that this technique traces additional distortion to the stego image behind embedding information.

LBS-S method provides two layers of security as first layer provides cryptographic security whereas the second layer uses steganoraphic security (Yadav, 2015). Another two methods where proposed by Joshi (Joshi, *et al*., 2015; Joshi and Yadav, 2016) based on XOR operation. The first method used two bits of the cover media while the second one used three bits with claim of 100% message insertion. Joshi *et al*. (Joshi, *et al*., 2018) came with another method that works on gray images. This method used the 7th bits of selected pixel after applying mathematical calculation. The value of the 7th bits of the selected pixel and the pixel + 1 are extracted and 2 bits of the message can be extracted from each pixel based on certain combination of these values. In this method, 4 possible combinations can be utilized (00,01, 10 and 11). This method gives several features such as two bits of secret message are embedded in each pixel, it is independent of the 8th bit, and +2 or -2 are the maximum change that can happen in this method.

Conclusion

In this paper, we have presented various methodologies for LSB based image steganography. Each of those methodologies enhancements, performance improvements, and also analyzing are described in their strength and weaknesses. Thus, the performance enhancement cycle of LSB based image steganography will never end.

REFERENCES

Al-Shatnawi, A. M., 2012. A new method in image steganography with improved image quality. *Applied Mathematical Sciences,* 6(79), pp. 3907-3915.

Baby, D. *et al*., 2015. A Novel DWT based Image Securing method using Steganography. *International Conference on Information and Communication Technologies (ICICT), Procedia Computer Science,* pp. 612-618.

Batra, S. and Rishi, R., 2010. Insertion of message in 6th, 7th and 8thbit of pixel values and its retrieval in case intruder changes theleast significant bit of image pixels. *International Journal of Security and Its Applications,* 4(3), pp. 1-10.

Channalli, S. and Jadhav, A., 2009. Steganography an Art of Hiding Data. *International Journal on Computer Science and Engineering (IJCSE),* pp. 137-141.

Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P., 2010. Digital image steganography: Survey and analysis of current methods.. *Signal Processing,* 3(90), pp. 727-752.

Cox, I. *et al*., 2008. *Digital Watermarking and Steganography.* s.l.:Morgan Kaufmann Publishers Inc..

Curran, K. B. a. K., 2006. An evaluation of image basedsteganography methods. *Multimedia Tools and Applications,* 30(1), pp. 55-88.

Dagar, E. and Dagar, S., 2014. LSB based Image Steganography using X-Box Mapping. *IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI),* pp. 351-355.

Deshmukh, P. U. and Pattewar, T. M., 2014. A Novel Approach for Edge Adaptive Steganography on LSB Insertion Technique. *IEEE International Conference on Information Communication and Embedded Systems (ICICES),* pp. 1-5.

Feng, B., Lu, W. and and Sun, W., 2015. Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture. *IEEE transactions on Information Forensics and Security.*

Fridrich, J., Lisonek, P. and Soukal, D., 2007. On steganographic embedding efficiency. *Proceedings of the 8th Information Hiding Workshop,* Issue 4437, pp. 282-296.

Goel, S., Gupta, S. and Kaushik, N., 2014-2015. Image Steganography – Least Significant Bit with Multiple Progressions. *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA),* pp. 105-11.

Gupta, S., Gujral, G. and Aggarwal, N., 2012. Enhanced Least Significant Bit Algorithm for Image Steganography. *International Journal of Computational Engineering and Management,* pp. 40-42.

Gutub, A. A.-A., 2010. Pixel indicator technique for RGB imagesteganography. *Journal of Emerging Technologies in WebIntelligence,* 2(1).

Hayati, P., Potdar, V. and Chang, E., 2007. *A Survey of Steganographic and Steganalytic Tools for the Digital Forensic Investigator,* s.l.: In Workshop of Information Hiding and Digital Watermarking .

Jassim, F. A., 2013. *A novel steganography algorithm for hiding textin image using five modulus method.* [Online] Available at: https://arxiv.org/abs/1307.0642.

Johnson, N. F., Duric, Z. and Jajodia, S. G., 2001. *Information Hiding Steganography and Watermarking- Attacks and Countermeasures (1st Ed.).* Boston: Kluwer Academic.

Joshi, K. and Yadav, R., 2016. *New approach toward data hidingusing XOR for image steganography.*

Joshi, K., Dhankhar, P. and Yadav, R., 2015. *A new image steg-anography method in spatial domain using XOR.* New Delhi, India, Annual IEEE India Conference (INDICON).

Joshi, K., Gill, S. and Yadav, R., 2018. A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image. *Journal of Computer Networks and Communications.*

Karim, S. M. M., Rahman, M. S. and Hossain, M. I., 2011. A New Approach for LSB Based Image Steganography using Secret Key. *Proceedings of 14th IEEE International Conference on Computer and Information Technology,* pp. 286-29.

Kessler, G. C., 2002. *Hiding Data in Data,* s.l.: Windows and>NET Magazine.

Khalind, O. and Aziz, B., 2015. LSB Steganography with Improved Embedding Efficiency and Undetectability. *4th International Conference on Signal and Image Processing,* 5(1), pp. 89-105.

Lee, C. and Tsai, W., 2010. A New Steganographic Method Based on Information Sharing via PNG Images. *IEEE 2nd International Conference on Computer and Automation Engineering (ICCAE),* pp. 807-811.

Li, B., He, J., Huang, J. and Shi, Y. Q., 2011. A survey on image steganography and steganalysis. *Journal of Information Hiding and Mltimedia Signal Processing,* 2(2), pp. 142-172.

Luo, X. *et al*., 2012. Steganalysis of adaptive image steganography in multiple gray code bit-planes. *Multimedia Tools and Applications,* 57(3), pp. 651-667.

Marvel, M., Retter, C. and Boncelet, C., 1998. A methodology for data hiding using images. *IEEE Proceedings on Military Communications Conference, MILCOM 98,* Volume 3, p. 1044–1047.

Modi, M. R., Islam, M. R. and Gupta, P., 2013. Edge Based Steganography on Colored Images. *9th International Conference on Intelligent Computing (ICIC),* pp. 593-600.

N. Akhtar, N., Khan, S. and Johri, P., 2014. An Improved Inverted LSB Image Steganography. *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT),* pp. 749755.

Nag, A. *et al*., 2014. A Huffman Code Based Image Steganography Technique. *1st International Conference on Applied Algorithm (ICAA),* pp. 257-265.

Noida, India, Proceedings of theNinth International Conference on Contemporary Computing(IC3).

Nusrati, M., Hanani, A. and Karimi, R., 2015. Steganography in Image Segments Using Genetic Algorithm. *5th IEEE*

International Conference on Advanced Computing and Communication Technologies (ACCT), pp. 102-107.

P. Singh, S. B. a. H. R. S., 2005. Evaluating the per-formance of message hidden in first and second bit plane. *WSEAS Transaction on Information Science and Technology,* 2(8), pp. 1220-1222.

Popa, R., 1998. *An analysis of steganographic techniques,* Timisoara: The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering.

Prashanti, G. and Sandhyarani, K., 2015. A New Approach for Data Hiding with LSB Steganography. *Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI,* pp. 423-430.

Qazanfari, K. and Safabakhsh, R., 2014. A new Steganography Method which Preserves Histogram: Generalization of LSB++. *Elsevier International Journal of Information Sciences,* pp. 90-101.

Qing, X., Jianquan, X. and Yunhua, X., 2010. A High Capacity Information Hiding Algorithm in Color Image. *Proceedings of 2nd IEEE International Conference on E-Business and Information System Security,* pp. 1-4.

Sachdeva, S. and Kumar, A., 2012. Colour Image Steganography Based on Modified Quantization Table. *Proceedings of IEEE 2nd International Conference on Advanced Computing and Communication Technologies,* pp. 309-313.

Samidha, D. and Agrawal, D., 2013. Random Image Steganography in Spatial Domain. *IEEE International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT),* pp. 1-3.

Venkatraman, S., Ajith, A. and Paprzycki, M., 2004. *(2004, 5-7 April 2004). . Paper presented at the Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004..* s.l., The Information Technology: Coding and Computing, p. Significance of steganography on data security.

Wang, H. and Wang, S., 2004. *Cyber warfare: Steganography vs. Steganalysis,* s.l.: Communications of the ACM.

Wu, D. C. and Tsai, W. H., 2003. A steganographic method forimages by pixel-value differencing. *Pattern RecognitionLetters,* 24(9-10), p. 1613–1626.

Xiaopi, Y., Tan, T. and Wang, Y., 2005. Extended optimization method of LSB steganalysis. *Image Processing, ICIP IEEE International Conference,* 2(1), pp. II- 1102-5.

Xiaoyi, Y. and Babaguchi, N., 2008. Run length based steganalysis for LSB matching steganography. *Multimedia and Expo, IEEE International Conference,* 1(1), pp. 353-356.

Yadav, K. J. a. R., 2015. *A new LSB-S image steganographymethod blend with cryptography for secret communication.* India, Proceedings of the third International Conference on ImageInformation Processing (ICIIP).

Yang , C., Liu, F., Luo, X. and Liu, B., 2008. Steganalysis frameworks of embedding in multiple leastsignificant bits. *Information Forensics and Security, IEEE Transactions,* 3(4), pp. 662-672.

Yang, H., Sun, X. and Sun, G., 2009. A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution. *Journal of Radio Engineering,* 18(4), pp. 509-516.

****