Available Online at http://www.journalajst.com

ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ISSN: 0976-3376

Asian Journal of Science and Technology
Vol. 10, Issue, 09, pp.10092-10095, September, 2019

RESEARCH ARTICLE

IMAGE STEGANOGRAPHY REVOLUTION

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

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

ARTICLE INFO

Article History:
Received 08th June, 2019
Received in revised form
12th July, 2019
Accepted 17th August, 2019
Published online 30st September, 2019

Key words:
Image Steganography, Information Hiding, Embedding Capacity, Embedding Efficiency, Security, Peak Signal to Noise Rate (PSNR).

ABSTRACT

This paper investigates current state-of-the-art image steganography methods and tools. Following todays growth in Internet computing and its interference in our life, the necessity for confidentiality and personal communication has raised. Its mandatory in digital communication to have privacy when secret data is being shared among two structure via the computer communication. Current technologies like cryptography propose a solution by scrambling the confidential information such that it cannot be read by anyone else except the intended recipient. On the other hand, the problem of encryption is that cryptographic is poor of logical sense and easy to realized as the significance of the communication is highlighted. Several hidden data can pull undue awareness from eavesdropper, which is a threat for private and confidential communication. Also, the nature of cryptographic causes lost of privacy and confidentiality. All of those facts caused worry for those people who wish to have private and confidential communication.

***Citation: Abdalla A. Ramah Al Enzi and Prof. Dr. Putra Sumari.* 2019.** "Image Steganography Revolution", *Asian Journal of Science and Technology*, 10, (09), 10092-10095

INTRODUCTION

Nowadays, information on the internet is became available online and could be simply accessed from everywhere, anytime. Along with that there is the rapid advance in digital network, information technology, Web services, and using computers and data communications become a part of our daily life. Thus, the security and issue has become one of the most significant problems for distributing information. The need for sending hidden messages has become the matter of knowledge of managing how to send something to someone right in front of the eyes of others without others knowing about the communication and protect this information while passing over insecure channels (Popa, 1998). This opens a complete new perspective of the world called Steganography which is become a hot topic on the Internet in the context of electronic privacy, information security and data protection.
Steganography presents important research contributions in three essential areas: survey of data hiding and labeling techniques (steganography and watermarking), attacks against steganography information, and countermeasures to such attacks. With the propagation of multimedia and concerns of privacy on the Internet, such research has become even more imperative. Modern technology has afforded profuse amount of information available to the public and the nature of digital media allows for the exact duplication of material with no notification that the material has been copied. The availability of information to the public's reach on the Internet provokes owners of such information to protect themselves from undesired supervision, theft, and fake representation and reproduction. Such circumstances induced many concerned establishments, e.g., law enforcement authorities in computer forensics and digital traffic analysis to pay attention to systems that analyze techniques for uncovering hidden information and recovering seemingly destroyed information (Johnson, et al., 2001). In an attempt to address the security issue, information hiding techniques like steganography have shown some promising solutions. Steganographic communication is difficult to trace and hence it makes the job of the attacker difficult because the attacker now has to track all network communication rather than just encrypted communication. This steganographic feature increases the level of privacy and security by making the confidential communication invisible (Hayati, et al., 2007).

Image Steganography Revolution: 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 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

***Corresponding author:* Abdalla A. Ramah Al Enzi,**
School of Computer Sciences, Universiti Sains Malaysia, Pulau Pinang, Malaysia.

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: Pixel Value Difference Method is one more method proposed by Wu and Tsai (Wu & Tsai, 2003). In this method, two consecutive pixels are placed inside each block in the cover image which is divided into two forks without overlapping. The difference of the consecutive pixels of each block is found to be small in smooth area of the image while it is large in the edge area. The edge area would be good for high capacity storage of data and the amount of the secret message bits always depends on the difference range which is calculated in power of 2 as the message must be inserted in binary form. However, if the difference in pixels is more than the image can be more contorted.

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 & Curran (Curran, 2006). In the advanced method, 3 colors were used, Red, Green & 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

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. 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. Samidha & Agrawal (Samidha & Agrawal, 2013) presented a LSB based image steganography technique utilizing random least significant bit selection to embedding secret information within the cover image. Samidha & 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.

Another method called FMM, Five Modulus Method. This method has a cover image that is divided into N number of blocks and each block has the size k*k pixels and the size of the window is represented by the k. The modification in this method is dividing the pixel of the block by 5 and having the message scattered over the image. However, the concern in this method is the low hiding capacity which is below 1 bit per pixel (Jassim, 2013). Dagar and Dagar (Dagar & 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 X-Boxes. 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 & 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.
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 & 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 & 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. Thenmozhi and Menakadeviin (Thenmozhi & Menakadevi, 2016), they hide the secret image into cover image with having equal sizes for both images. the mechanism works by press the secret information using Set Partitioning in Hierarchical Trees (SPIHT) algorithm, thereafter the result of compression embeds into the cover image using default LSB technique. this press is made by wavelet convert and then by using the SPIHT coding. Image quality is retained with high PSNR values. Shabnam and Hemachandranin (Shabnam & Hemachandran, 2016), they hide the secret information data into cover image by transforming the image into 3 colored matrices (R, G, B) the data switch into binary, depending on the hidden data bit using OR or AND logic gates operation, sequentially (RGB, BGR, RGB, BGR…). The effect of their technique showed better performance in terms of quality of the stego image obtained. Emam et al. (Emam, et al., 2016), used methodology works by hiding the byte of the secret message in three pixels randomly in the cover image using Pseudo Random Number Generator (PRNG) of each pixel value. In the embedding method (2-1-2) layer applied (two layers Blue and green) and the byte of the hidden data being embedded in three pixels only in this form (3-2-3). The proposed method obtained a high hiding capacity without degrading the stego image quality, which is leads to gain high PSNR value.

Conclusion

In this paper, we have presented various methodologies for image steganography. A series of method enhancements, performance improvements, and also analyzing these strength and weaknesses of these methodologies. Understanding the limitations of these methods will allow the construction of more vigorous methods that can better survive manipulations and attacks. It is worth to mention that the battle between the evil and the good never comes to an end. Attempts to devise new methods for concealing messages and attempts to devise methods for revealing them go proportionally. To overcome shortcomings in the aforementioned methods of hiding messages and to ensure a better level of security, a new method needs to be developed. Therefore, the performance enhancement cycle life in image steganography is continues.

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

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

Dagar, E. & 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. & 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.

Emam, M. M., Aly, A. A. & Omara, F. A., 2016. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. *International Journal of Advanced Computer Science & Applications,* 1(7), pp. 361-366.

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

Goel, S., Gupta, S. & 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. & Aggarwal, N., 2012. Enhanced Least Significant Bit Algorithm for Image Steganography. *International Journal of Computational Engineering & 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. & 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. & Jajodia, S. G., 2001. *Information Hiding Steganography and Watermarking-Attacks and Countermeasures (1st Ed.).* Boston: Kluwer Academic.

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

Joshi, K., Gill, S. & 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.*

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

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

Karim, S. M. M., Rahman, M. S. & 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 & >NET Magazine.

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

Lee, C. & 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. & Shi, Y. Q., 2011. A survey on image steganography and steganalysis. *Journal of Information Hiding and Mltimedia Signal Processing,* 2(2), pp. 142-172.

Mandal, J. K. & Das, D., 2012. Colour image steganography based on pixel value differencing in spatial domain. *International journal of information sciences and techniques,* 2(4).

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

Akhtar, N.,N., Khan, S. & Johri, P., 2014. An Improved Inverted LSB Image Steganography. *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT),* pp. 749-755.

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

Nusrati, M., Hanani, A. & Karimi, R., 2015. Steganography in Image Segments Using Genetic Algorithm. *5th IEEE International Conference on Advanced Computing & Communication Technologies (ACCT),* pp. 102-107.

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

Samidha, D. & 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.

Shabnam, S. & Hemachandran, K., 2016. LSB based Steganography using Bit masking method on RGB planes. *International Journal of Computer Science and Information Technologies (IJCSIT),* 7(3), pp. 1169-1173.

Thenmozhi, M. J. & Menakadevi, T., 2016. A New Secure Image Steganography Using Lsb And Spiht Based Compression Method. *International Journal of Engineering,* 16(17).

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

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

****