

# A New Steganography Method for Scalable Vector Graphics (SVG) Images Based On An Improved LSB Algorithm

Dr. Badr Almutairi<sup>1†</sup>

[b.algoian@mu.edu.sa](mailto:b.algoian@mu.edu.sa)

Majmaah University Kingdom of Saudi Arabia,  
College of Computer Sciences and Information Technology, KSA

## Summary

Steganography is the art of hiding secret data, which is used to hide a secret message in various types of files, including text files, digital images files, audio files, and video files. Although there are several methods designed for image steganography, they still need to be further improved to overcome their shortcomings. Therefore, this research will design A New Steganography Method for Scalable Vector Graphics (SVG) Images based on an Improved LSB Algorithm. The method embeds and extracts a secret message based on two layers; Hardening Layer and Embed/Extract Layer. Besides, this research will develop a new software tool based on our designed method. The tool should be more comprehensive utility to provide desired functions with an interactive graphical user interface and to integrate navigation capabilities. The significant of this developed tool will help users to perform data hiding more efficiently and quickly with a high-quality degree. Finally, the method is evaluated based on experiments and analysis of corresponding experimental results. The research calculated the Peak Signal-to-Noise Ratio (PSNR) in the decibel (dB) unit. The obtained results are compared to the previous related works to prove the significance of our research.

### Key words:

*Steganography; Vector Graphics; LSB Algorithm; Scalable Vector Graphics Signal-to-Noise.*

## 1. Introduction

This research aims to design A New Steganography Method for Scalable Vector Graphics (SVG) Images based on an Improved LSB Algorithm and to develop a new tool based on our new design. This aim needs to undertake several challenges, as explained in the following section

To study and analyze current available methods and techniques to explore and understand the current situations of image steganography domain [1], [2]. To design a new steganography method for scalable vector graphics (SVG) images based on an improved LSB algorithm, which handles the gaps of the previous related methods and techniques [3]. To develop a new tool based on our method, which provides a safe and robust implementation for image steganography [4], [5]. To evaluate our method by Peak Signal-to-Noise Ratio

(PSNR) measure, and to compare the obtained results with the previous related researches to prove the significance of our designed method

As the number of attacks is increasing on the data which is available online, it's important to hide the data to protect it against attacks and malware. The steganography is more advanced technology as compared to the cryptography in this method of steganography the data hidden behind the image and the information is not visible to the user without decrypting the image with the private key which is available to both the users who would like to hide his data and the also with the person who would like to receive the data in a secured format. Data will not be lost during the hiding process, but its rather more secure and can be accessible to the end-user without anyone tampering the information which is hidden behind the image. In this research project, I will be implementing the more secure method of encryption and will be optimizing the LSB algorithm so that the data which is hidden behind the image is more secure and no one can tamper the data without providing the secret key which will be available only with the authorized persons [6].

As we know that data is stored using the cryptographic method, but still, we find that many attacks are taking place and many algorithms can be decrypted, and the key data can get leaked. It's important to protect this data. I will be implementing secured method to store the data behind the image files which will be in 1080P format too large files which will be used to hide the data and to store the data on the servers these files will be stenographer with the relevant data and will be stored in the database [7], [8].

Hiding the information behind the images will require a huge amount of encryption algorithms to run to decrypt the information; thus, this method will provide more security to the content sharing with others with hidden text or any information behind the images [9]. Optimizing the LSB algorithm is also an important task as this algorithm will be the key factor in encrypting the information and also creating image vectors. As security is enhancing using the steganography usage, it's important to cater to the algorithms and functional aspects of implementing new

methods for optimizing algorithms which enhance the steganography in the upcoming days of security.

## 2. Literature Review

As many of the literature which I have seen involve hiding text information behind the image which includes such as:

### 2.1 Advances in digital image steganography

In this research paper, the author would like to hide information, which is textual information behind the image so that the attackers cannot get access to the information easily, and the contents can be saved easily on the server without user interventions.

### 2.2 Spread spectrum image steganography

In this research article the author explains how the physics law of spread spectrum image can be used to hide information inside the image file of the spread spectrum this method will help in information storage and retrieval from the spread spectrum and the contents of the user will not be lost and the data is protected behind the spread spectrum image file and is protected from the attackers.

### 2.3 Two new approaches for image steganography using cryptography

In this research paper, the user would like to explain the two new approaches which they have implemented for the image steganography using the cryptography algorithms. These methods will improve the security of the data protection behind the image files. These two methods will improve the efficiency of data protection and also generate good cryptographic keys which can be used to protect the data and contents of the user

## 3. Functional Aspects of Steganography

This research will be implemented using the waterfall software development methodology this research project will follow all the steps of SDLC (Software development life cycle) In this research work following the methodology of SDLC will be followed:

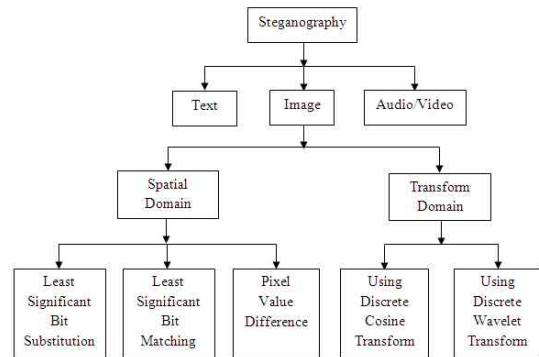


Fig. 1 Functional Aspects

### 3. 1 Requirement Engineering

In this phase it's important to collect all requirements which will help enhance and optimize the algorithms which will be used in implementing the steganography and data hiding behind the image as there is a huge demand for secure communication, and the amount of memory requirement for the secure communication should be least it's important for the members of the team responsible for hiding the text information behind the image [10], [11].

### 3. 2 Requirement Gathering

In the requirement gathering phase is important as the users will collect data from different stakeholders who are involved in the project. There are different tools available today to gather requirements in this research work. I have used the Borland Requirement gathering tool, which collects all the requirement in a pool by using different techniques such as quick survey, six hat thinking, and other methods for requirement gathering [12], [13]. As the information needs to be secured and should also consume less amount of space, the stakeholders need to gather all the requirements for this research work, and then based on the information gathered, the progress of the project would be completed. The requirement is gathered based on the feasibility of resources that are available in the market today that is hardware and software feasibility as the user can pertain to what is executable in the current hardware and using the available software.

Requirement gathering is a tedious task as all the stakeholders involved in the project have a different perspective about the project under execution and need to think about the common goal, which is securing communication and also enhancing the LSB algorithm by optimizing the steps of execution of the algorithm. The optimization of the LSB algorithm will enhance the efficiency of execution of secure communication using

steganography and image vectorization and communication of image data transmission from one communication system to the other with secure text transmitted at the other end encrypted.

### 3.3 Requirement Analysis

In requirement analysis, I have analyzed all the information which is collected from the first two phases for the requirements. The analysis of the requirement is important so that one can predict the behavior of the execution of the program and the feasibility and availability of the resources for this research work to be carried out [14]. The text information is embedded into the LSB algorithm which encrypts the data and then this encrypted data is further categorized based on the efficiency of data transmission over the network finally the information which is collected from the LSB algorithm which is running on an intel machine is wrapped with an image for that the information is not visible to the attackers and that they see only the image which is a wrapper for the hidden information which is to be sent to the other required recipient this way we can analyze the information. As the LSB algorithm is optimized, it will take less time and effort to execute the encryption of the information, and binding it to the image will also reduce the time required for the entire process [15].

Analyzing this requirement and the execution parameters is important process and also requires a huge amount of tests to be run so that the requirement gathered and captured can be easily put across execution steps this way we can understand the functional requirement of the project which needs to collect and collaborate the required information and collection of data which will be used for this research work to be successful.

### 3.4 Design of the system

The design of the system is an important factor as the design may affect the usage of the LSB algorithm and the design parameters will also play a vital role in improving the efficiency of the project altogether. While designing the system as all the requirements which have been collected from the above phases and after the analysis of the requirements it's clear that the design of the system should be such that all the stakeholders of the project and the research should understand how to encrypt the required information which needs to be send to the other end node and which are the key factors which will affect the execution of the LSB algorithm and what inputs are required by the LSB algorithm so that the required output from the LSB algorithm can be generated[16],[17]. In this way, we can help the design engineer to select the

appropriate functional aspects of the project when he is designing the system for secure communication.

Once the design aspects are clear it's important that the design engineer takes necessary actions on the functional aspects so that the efficiency of the encryption and the LSB algorithm can get the data or the information easily for encryption once the information is encrypted it should be easy of the user to select the image from his computer and other courses too that he can hide the encrypted information behind the image and get the required resultant output [18]. Then he can transmit this encrypted and hidden information to the other node as and when required

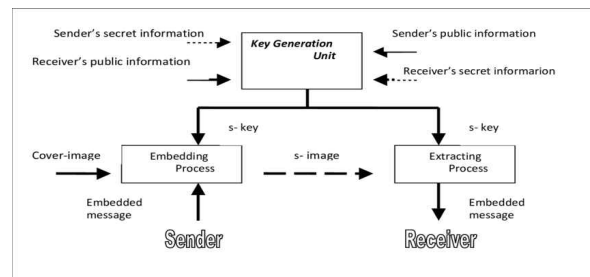


Fig 2. Design of LSB System

### 3.5 Development of the system

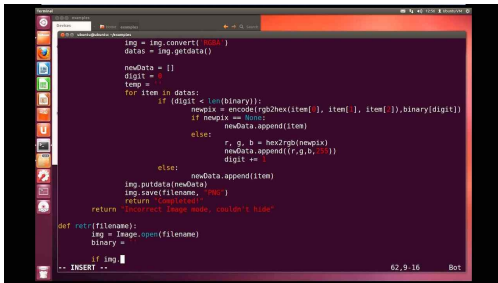
As this research work involves design and development of efficient and effective LSB algorithm so that the optimization can be performed on the algorithm execution speed and other aspects it's important to select the development environment in which the algorithm will perform efficiently as I have analyzed may programming techniques I have designed and developed the optimization on the python programming environment as it's easy to implement and modify the algorithmic aspect of the LSB algorithm using this programming environment also the testing of this can be easily performed on the windows machine on which the testbed is ready for execution and testing the development activities[19]. The code execution environment and the code design environment variables have been set for programming and running the code, and also the execution steps for the program are clearly understood by the stakeholders [20].

### 3.6 Programming of the system

This research work requires programming the LSB algorithm and then finding ways to optimize the program so that the efficiency of the encryption and the time required to run the LSB encryption can be achieved this is only possible if we select the correct programming environment [21]. All the parameters which are required

for programming the LSB algorithm using the Python Programming language are set, and the variables are defined such that they do not consume any extra memory during the execution and deployment process of the algorithm [22].

Data that is required for the program to run is given as the input to the LSB algorithm under execution and then the encrypted text is collected at the output of the system [23]. The time which is required for computation or execution and conversion of the normal text to the encrypted text which is generated by the LSB algorithm is computed and calculated based on that the optimization of code is carried out in the system.



```

img = img.convert('RGB')
data = img.getdata()
newdata = []
digit = 0
temp = 0
for item in data:
    if digit < len(binary):
        tempix = ord(hex2hex(item[0], item[1], binary[digit]))
        if tempix <= 0:
            newdata.append(item)
        else:
            r, g, b = hex2rgb(tempix)
            newdata.append((r, g, b, 255))
            digit += 1
    else:
        newdata.append(item)
img.putdata(newdata)
img.save(filename)
return "Completed"
return "Insert Image name, consider it base"
def rec(filename):
    img = Image.open(filename)
    binary =
    if img
    -- INSERT --
  
```

Fig 3. Programming LSB algorithm

### 3.7 Testing the system

As this system deals with security and secure information communication it's important to test the programming and design environments. A testbed is designed, and two different types of testing have been carried out on the LSB algorithm [24]. The First test is white box testing in which the algorithm itself without optimization and with optimization has been tested rigorously by providing different inputs at different time intervals.

The second test which has been carried out for this research work is black-box testing in which the functional aspects of the encryption and information hiding have been tested using black-box testing tools such as QTP and Win Runner. All the tests were successful and the execution time and efficiency of the algorithm are improved [25].

Thus it's important that the functional testing of the system will provide efficiency and performance improvements and will help the system to be implemented effectively under various environments.

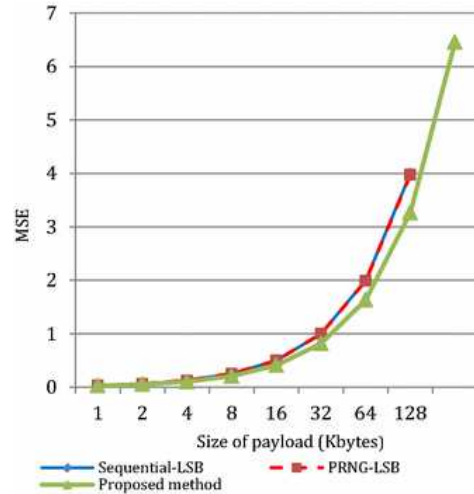


Fig 4. Functional Testing of System

### 3.8 Deployment of the system

Once the system is ready, the system must be deployed correctly so that the functionality of the system works properly. The system has been deployed on the windows machine and with all the programming environments and the variables required for the research work to execute correctly have been set so that the LSB algorithm and the graphical user interface work in coordination to each other and that they do not face any difficulty during execution [26].

The networks have been configured correctly so that the testing of the deployment process can be done and the information which is encrypted and hidden behind the image can be transmitted over this network topology

### 3.9 Maintenance of the system

After the deployment process is over and the system is functioning as required and with the efficiency required it's important to maintain the environment in which the optimal output is achieved. I have provided the maintenance strategies, and documentation using which the optimized LSB algorithm can work efficiently and effectively also these conditions need to be maintained if the throughput of the system needs to be improved or to be the same without any changes to be made further. The easiest method is to maintain the current running environment where the algorithm performs the best and without any latency in encrypting the information which can be communicated over the required network or any

other network also selected images which can be used for information hiding have been specified so that using this images the efficiency of data encryption can be improved and also less time will be required for execution and sending the information across the network and with less effort take by the algorithm and the GUI for hiding the information and binding them together[8],[9]. Data hiding could be more effective and efficient if all the parameters which are mentioned above are carried out in the same sequence so that the efficiency and effectiveness of the research work carried out can give potential outputs as desired by the stakeholders

#### 4. Implementation of Management Steganography and Signal-To-Noise Ratio Plan

The project management plan for this research project includes the following phases.  
 The requirement for the signal to noise ratio  
 Design for the signal to noise ratio  
 Development for the signal to noise ratio  
 Testing for the signal to noise ratio  
 Deployment for the signal to noise ratio  
 Maintenance for the signal to noise ratio

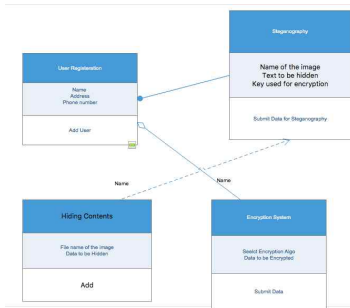


Fig 5. Class Diagram

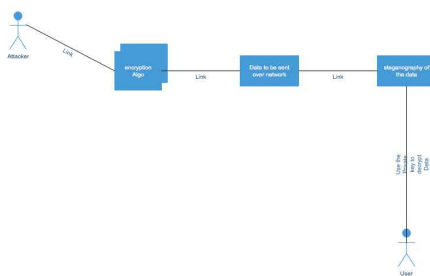


Fig 6. Use Case Diagram

#### 5. Expected results and their utilization

This research project we will be implementing the LSB algorithm optimization which will help in encrypting and hiding the information behind the image and will be used for secure transmission of the image file with the steganographic data to the end-user this method will improve the security of data transmission over the network and also spread spectrum images will be used for huge amount to data being transmitted over the network so that the data is intact and not being attacked with easy to use algorithms of data encryptions the data resides behind the image and is highly secure[10].

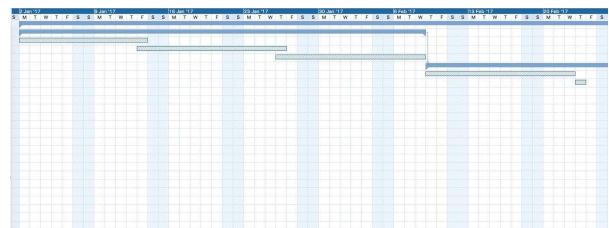


Fig 7. Gantt Chart

#### 6. Methodology for Results Implementation

The methodology for the implementation will follow the SDLC (Software development life cycle) we will be implementing the project using the waterfall model this method will fix different issues starting from

- i. Requirement analysis of the project
- ii. Design Phase of the project
- iii. Development of the project
- iv. Coding the project outcomes
- v. Testing the System for stability
- vi. Deployment of the project
- vii. Maintenance of the project

These are some of the limited operations which will be performed during the project implementation [2], [3]

#### Acknowledgments

This research article would not have been completed without the support of many stakeholders involved in this project. Dr. Badr Almutairi would like to thank Deanship of Scientific Research at Majmaah University for supporting this work under the Project No. R-1441-32.

Constant motivation and departmental support have allowed me to work hard on the research project and to complete this research work within the stipulated time successfully.

## References

- [1] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding", IBM Syst. J., vol. 35, 1996. <https://doi.org/10.1147/sj.353.0313>
- [2] I. J. Cox, J. Kilian, T. Leighton, T. Shamoan, "Secure spread spectrum watermarking for images audio and video", Proc. IEEE Int. Conf. Image Processing, vol. 111, pp. 243-246, Sept. 1996.3. <https://doi.org/10.1109/ICIP.1996.560429>
- [3] D. Kahn, *The Codebreakers: The Story of Secret Writing*, Scribner, 1967.
- [4] Stallings William, *Cryptography and Network Security Principles and Practices*, Singa-pore: Pearson Education, 2003.
- [5] B. Dunba, "A detailed look at Steganographic Techniques and their use in an open sys-tem environment Sans Institute", 2002
- [6] C. Christian, "An Information Theoretic Model for Steganography", Proceedings of 2nd Workshop on Information Hiding, 1998
- [7] A. Amsaveni Department of ECE, Kumaraguru College of Technology, Coimbatore , "A comprehensive study on image steganography and steganalysis techniques", Journal International Journal of Information and Communication Technology <https://dx.doi.org/10.1504/IJICT.2015.070300>
- [8] S. Uma Maheswari Department of ECE, Karunya University, Coimbatore, India - 641 049, Tamil Nadu, India "Different methodology for image steganogra-phy-based data hiding: review paper <https://doi.org/10.1504/IJICT.2015.070330>
- [9] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital image steganog-raphy: Survey and analysis of current methods", Signal Processing Volume 90, Issue 3, March 2010, Pages 727-752 <https://doi.org/10.1016/j.sigpro.2009.08.010>
- [10] S. Hemalatha, U. Dinesh Acharya, A. Renuka "Wavelet Transform Based Steganogra-phy Technique to Hide Audio Signals in Image", Procedia Computer Science Volume 47, 2015, Pages 272-281 <https://doi.org/10.1016/j.procs.2015.03.207>
- [11] Xiang-Yang Luo a, b, Dao-Shun Wang b, Ping Wang a, Fen-Lin Liu a, "A review on blind detection for image steganography", Signal Processing Volume 88, Issue 9, September 2008, Pages 2138-2157 <https://doi.org/10.1016/j.sigpro.2008.03.016>
- [12] D. Renzel, M. Behrendt, R. Klamma, M. Jarke, "Requirements Bazaar: Social Require-ments Engineering for Community-Driven Innovation", Proceedings of the 21st IEEE International Requirements Engineering Conference, Rio de Janeiro, 2013, pp. 326-327. <https://doi.org/10.1109/RE.2013.6636738>
- [13] T. J. Lehman and A. Sharma, "Software Development as a Service: Agile Experiences", Proceedings of the 2011 Annual SRII Global Conference, 29 Mar. - 2 Apr. 2011, San Jose, USA, Publisher: IEEE, doi: 10.1109/SRII.2011.82, pp. 749-758
- [14] J. A. Livermore, "Factors that impact implementing an agile software development methodology", Proceedings of the 2007 IEEE SoutheastCon, 22-25 March 2007, Rich-mond, USA, Publisher: IEEE, doi: 10.1109/SECON.2007.342860, pp.82-86. <https://doi.org/10.1109/SECON.2007.342860>
- [15] P. Robinson, "Towards a theory of digital editions," in the Journal of the European So-cietiy for Textual Scholarship vol 10 W.Van Mierlo, A. Fachard eds., Amsterdam: Rodopi, 2013, pp.105-132.
- [16] N. Sathisha, P. R, K. S. Babu, K. B. Raja, K. R. Venugopal, and L. M. Patnaik, "Dtcwt based high capacity steganography using coefficient replacement and adaptive scaling," Sixth International Conference on Machine Vision, vol. 9067, 2013.
- [17] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography tech-niques: An overview," International Journal of Computer Science and Security, 2012.
- [18] A. S. Ratnakirti Roy, Suvamoy Changder and N. C. Debnath, "Evaluating image ste-ganography techniques: Future research challenges," IEEE, 2013. <https://doi.org/10.1109/ComManTel.2013.6482411>
- [19] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganaly-sis," Journal of Information Hiding and Multimedia Signal Processing, Ubiquitous Inter-national, 2010
- [20] S. V. Sathyanarayana and K. N. H. Bhat, "Novel scheme for storage and transmission of medical images with patient information using elliptic curve based image encryption schemes with lsb based steganographic technique," Journal of Medical Imaging and Health Informatics, vol. 2, no. 6, pp. 1-10, 2012. <https://doi.org/10.1166/jmihi.2012.1068>
- [21] Y. J. Chanu, K. M. Singh, and T. Tuithung, "Image steganography and steganalysis: A survey," International Journal of Computer Applications, 2012
- [22] L. Y. POR and B. Delina, "Information hiding: A new approach in text steganography," 7th WSEAS Int. Conf. on APPLIED COMPUTER & APPLIED COMPUTATIONAL SCIENCE, 2008.
- [23] J. Nayak, P. S. Bhat, R. A. U, and M. S. Kumar, "Efficient storage and transmission of digital fundus images with patient information using reversible watermarking technique and error control codes," Springer, 2008. <https://doi.org/10.1007/s10916-008-9176-2>
- [24] H. S. M. Reddy and K. B. Raja, "Steganography based on adaptive embedding of en-crypted payload in wavelet domain," International Journal of Scientific & Engineering Research, 2012
- [25] I. W. Selesnick, R. G. Baraniuk, and N. G., "The dual-tree complex wavelet transform," IEEE SIGNAL PROCESSING MAGAZINE, Kingsbury, 2005.
- [26] R. C. Gonzalez, R. E. Woods, and S. L. Eddins, *Digital Image Processing Using MATLAB*, second edition ed. Mc Graw Hill Education



**Dr. Badr Almutairi** is affiliated with the Department of Information Technology, University of Majmaah. He is currently providing services as Assistant Professor. He has published numerous publications in various national and international peer-reviewed journals and presented scientific papers across the world. Because of the active association with different societies and academies as well as the contributions, he is being recognized by the subject experts around the world.