Symbiosis

www.symbiosisonline.org
www.symbiosisonlinepublishing.com

Mini Review | Journal of Computer Science Applications and Information Technology | Open Access

# Application and Implementation of Secure Hybrid Steganography Algorithm in Private Cloud Platform

**Ihssan Alkadi[1]*, Sarah Robert[2]**

[1]*College of Graduate School, ISAT Graduate Program, Southeastern Louisiana University, Hammond, USA.*
[2]*Integrated Science & Technology (ISAT), Southeastern Louisiana University, Hammond, USA.*

**Received: October 12, 2016; Accepted: October 16, 2016; Published: January 20, 2017**

***Corresponding author:** Ihssan Alkadi, College Of Graduate School, ISAT Graduate Program, Southeastern Louisiana University, SLU 10687, Hammond, LA, USA, 70402, Tel: + 985-549-2037;Fax: 985–549-5532;E-mail: ialkadi@selu.edu*

## Abstract

Steganography has been considered to be a standard way of sending secret data to the receiver without others being able to identify its immediate presence. Cloud computing has been competitive in fields like cost reduction, flexibility and optimal resource utilization. In the proposed algorithm, there is an effort taken to embed Steganography and Cloud Computing, so that, the security level of both can hold together and create a greater safety standard. The pixels are inverted and sent to Five Modulus Method (FMM) [7] or Genetic Algorithm based Steganography using Discrete Cosine Transformation (GASDCT) [11] algorithm based on its size and complexity; the steganography image is then transmitted to the receiver using the SaaS infrastructure. Using the Software as a Service (SaaS) Document Management, the image is stored, and shared to the receiver, which reduces the extra steps of upload and download, sending via email or any other meaning of communication. SaaS is Cost-efficient, secure, and scalable. Hence an efficient usage of its security and resources to create a system that can handle them in Cloud without any necessity to download an application to the network.

**Keywords:** Genetic Algorithm; SaaS; Steganography; Cloud Security;

## Introduction

Steganography is the process of hiding a secret message within a source data and the extracting them, at its destination. A steganography message might be a picture or audio/video file. Embed secret data in cover images, without creating visually noticeable changes to keep an invader unaware of the existence of the secret. Genetic Algorithms (GA) can be used with Steganography. Genetic algorithms are search algorithms that use the best out of random researching, arriving at the best possible solution. When they are used together; it increases security for more sensitive information. Genetic Algorithm has a different approach compared to other typical algorithms. They get the places where data could be easily embedded and harder to understand their location.

Cloud computing enables convenient, on-demand network access to a shared pool of computing resources available with minimal management effort or service provider interaction. Cloud Computing is best because of its Infrastructure as a service (IaaS) and platform as a service (PaaS). The comfort of cloud applications draws users to it. Cloud Computing takes enterprises search to a new level. It also allows them to reduce costs through improved utilization, infrastructure cost, and faster deployment cycles. Cloud Computing takes businesses search to a new level. It also allows them to reduce costs through improved utilization, infrastructure cost, and more rapid deployment

## Related Work

In this chapter, a review is done, that could relate to our representation - matching solution. We will discuss the algorithms that handle steganography in the cloud-based environment and a few cloud security algorithms.

### Data Security In The Cloud Using Serpent Encryption And Distributed Steganography By Izevbizua, Peter Odion(2015)

The paper discusses securing data in the cloud. They did a hybrid concept by combining two techniques: Serpent encryption algorithm and distributed steganography. This method serves a significant advantage on the cloud security, but the steganography was not well handled, i.e. distributed Steganography has its disadvantages compared to Genetic Algorithm.

### Data Security in Cloud Computing Using Encryption and Steganography By Karun Handa, Uma Singh (2015)

The paper deals with storing & retrieving data in the cloud server, encrypted then steganography algorithm applied. It stores the algorithm and data in the cloud, but there is no information about the technology used, and no traces of security handling.

### Enhancing Data Storage Security In Cloud Computing Through Steganography By Mrinal Kanti Sarkar And Trijit Chatterjee

The algorithm uses 3 Cloud Service Providers (CSP), CSP -1 has the resources for the grayscale image.CSP-2 has the algorithm for hiding and retrieving data from images. CSP-1 and CSP - 2 are

connected to CSP-3, this carries out all the task of the user. The Algorithm handles only a limited number of security threats in a relatively small environment. Data safety and integrity being an important factor of cloud we would require a better algorithm.

## Literature Review

### Steganography tools

Steganography tools help to embed the data to be hidden in a Carrier File. Using Steganography tools there is no need to conceal the original file. Steganography needs to ensure robustness against steganalysis or statistical, by balancing data whitening process, and encoding process. The carrier file can either be an image, video, or audio file.

The carrier files are considered to be the core of steganography tool; every file format has its modification ways. The processing algorithm includes injection, Generation, LSB or adaptive Substitution, Frequency space manipulation, Ancillary data & metadata, etc. Injection and Generation are considered to be suspicious because of its increase in file size and traceability aspects

### Why Image files used?

Image data have a range of numbers. The number of pixels in the picture and the granularity of the color definition is directly related to the size of the image. An image can either have 8 bits or 24 bits. A Color image with 8 bit will have a color range of 256 colors, and a gray scale image will have the range of 0 to 255 colors. An image file represents the color or the intensity of each pixel in a binary format. Gray Scale is a shade of gray color range. An excellent candid for steganography image can be graphical files because specifying small changes to the pixels in the picture does not make the steganography image look different from the original. Since the whole image data is a range of numbers it's easy to change the binary value, and it does not have a great impact in the Human Visual System, and still, it carries out the desired task.

### Genetic Algorithm (GA) [2]

The GA are search algorithms that show an intelligent use of random search to solve optimization search, helping in directing them in the direction of better performance within the search space. The individual chromosome that has been successful will produce more offspring than the others; these descendants may produce offspring's that are better than their parent.

Chromosomes determine the behavior of GA. The behavior of chromosomes is dependent on the try for resources. The successive generations deliver optimal solutions, resulting in chromosomes which may be better suitable for the solution. The GA uses set of operators like Crossover, Mutation, Selection, etc. The fitness score helps us predicts the ability of a competing individual, ones that have the closest optimal value is used.

### Preview of Successive Different Steganography Algorithms

The Comparison of different algorithms is carried out to understand different algorithms and their consideration towards the best way of providing a cost optimal and more efficient algorithms. The Optimal Pixel Adjustment Procedure(OPAP) aims in reducing the representational errors caused by the Least Significant Bit substitution method, working more in adjusting the steganography image pixels to cover the errors created in the steganography image so there could be less difference or minimal difference compared to the cover image. In Inverted Pixel (IP) Approach, pixels are inverted before the addition of secret data. Each section of the secret image is taken into consideration, undergoes a check where it's determined if the pixel inverted could be appropriate, if satisfying, they are then inverted and embedded into the image. The bits are used to record the changes, either treated as secret key or extra data that is inserted.

### SaaS Infrastructure

"Software as a service (SaaS) is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet" [4] SaaS is a software delivery model, sometimes mentioned as "on-demand software." SaaS is helpful in many business applications. Two main ways of SaaS, Vertical SaaS (answers the needs of a specific) Horizontal SaaS (focus on a software category) SaaS, does not require any software installation, and no need for maintenance and upgrading [4, 5].

## Methods

New Approach to Embed Secure Steganography in Private Cloud

The primary purpose of the study is to apply and implement steganography of secure hybrid Steganography System in Private Cloud Platform. Steganography is the process sending data between sender and receiver secretly in a public sector. Cloud computing is the best known public sector where everyone can have access to data. The Image is stored in a private cloud, with data are hidden into it and having them safe from intruders, later retrieved using the key. The base concept is to lessen the unauthorized access of private data, prohibit the access of intruder to find out the algorithm that is to be worked out for adding the secret data to the cover image. The System has the security of steganography, and the security of Cloud Computing handled in an integrated manner. The Login Procedure has the Registration, Credential Proof verification, and the Four Step Verification (FVS). The user is required to create an Id with the system and is requested to provide his identity proof credentials to ensure his identity. Once registered the user can log into his account. While logging in, the user has to undergo the FVS where, user enter the ID & password, Mobile Verification, Security code & the catch phrase (given during the id creation). Once logged in, the user could see the home screen, here the user can save data to the storage limit acquired. The user can also select the encoding/decoding procedure to encode/decode an image. The algorithm is stored in the cloud. During Encoding the image is converted to grayscale to prevent the detection of changes in Human Visual System (HVS).

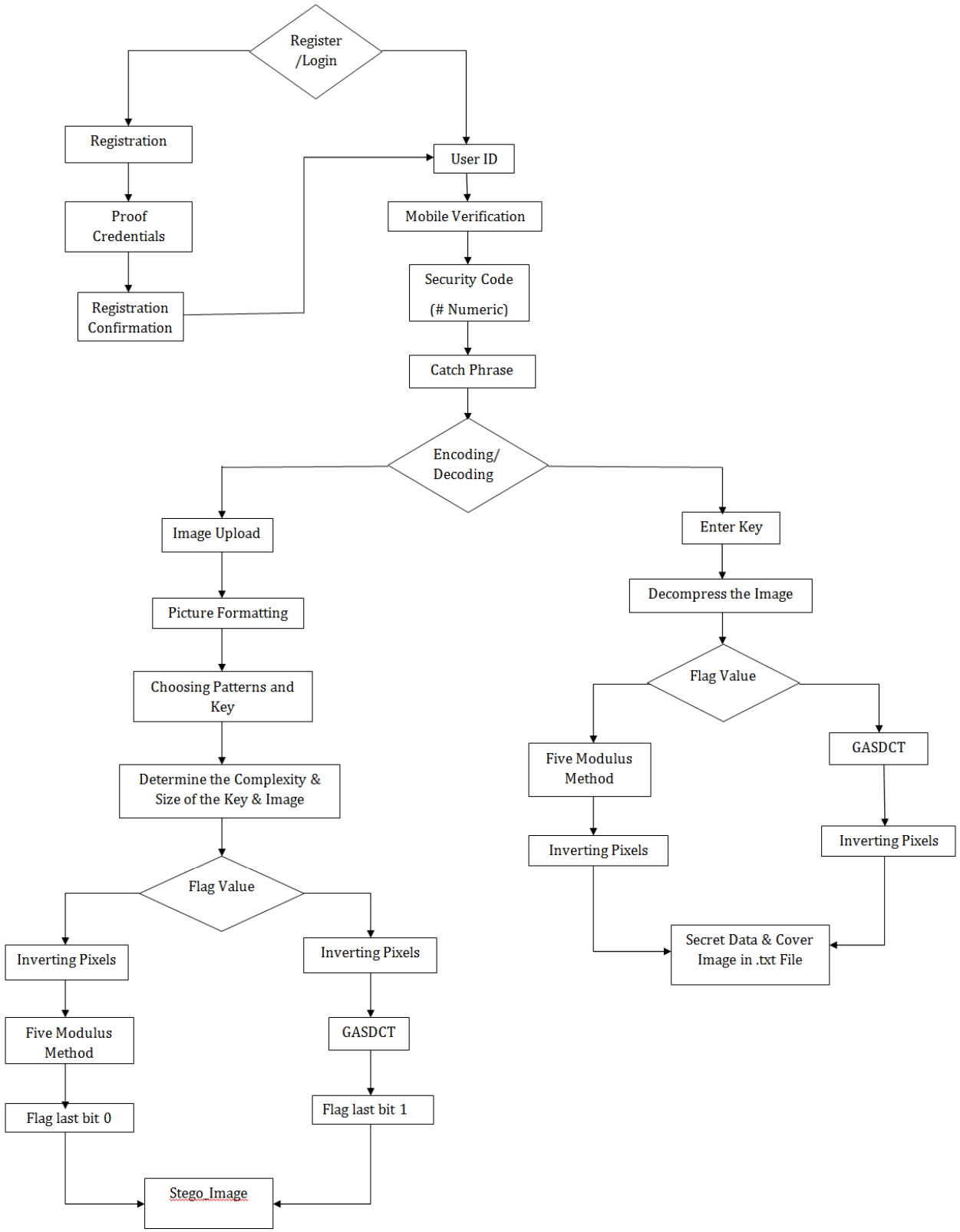


**Figure 1:**Proposed model of Secure Hybrid Steganography Algorithm in Private Cloud Platform in a simple

Once Converted the Security key, data & complexity level is obtained, and based on complexity & the size of data, the image can either be encoded using or FMM [7] or GASDCT [11] after inverting some pixels in the picture using some patterns in the picture. The inverted details are embedded in the secret key to get the cover image separately during decoding. During decoding the secret data is obtained in a .txt file. The private cloud has a proprietary architecture, which supports us to restrict the access of an intruder to a significant amount.

The SaaS infrastructure helps in sharing the steganography image with the receiver instead of using a standard means of transmission which could result in some leakage. The proposed algorithm would be implemented in a private Cloud. There are different techniques available, but the proposed system has a better way of overcoming the security alerts of cloud and a better way of creating a steganography image and transmitting it to the receiver. It's hard for any user who is not the profile owner himself will have a very hard time logging into the system. This level itself has its advantage of not letting an intruder. The System makes security be the key element. A clear diagrammatic representation of model is given in the tables section Figure 1.

## Results

From the survey we conducted we conclude that steganography is an important in securing the data when transmitted over a public cloud. The survey was conducted on campus, with a population of 25. The general condenses is that most individuals who answered the survey had agreed with the point that associating an image with data element in the cloud would guarantee secure and hidden management of data.

## Acknowledgment

However, I would like to thank Professor Ihssan Alkadi for his relentless supervision and constant leadership and mentorship in leading the way to get this paper publication ready as a Mini Review to be able to have an opportunity to submit this as a potential accepted mini review paper in your highly esteemed journal. I do appreciate the time he has given me to help me accomplish this special milestone.

## Discussion

The proposed algorithm has the steganography implemented in the private cloud, and the transfer of data is carried out by the SaaS infrastructure, this clearly proves that there is no way for the intruder to get access to data even when he gets in contact with any of his profile. The system makes the best use of the modern technologies available in a safer way, minimizing the security alerts in the cloud.

## References

1. Grayscale. Wikipedia. Wikimedia Foundation; Available from: https://en.wikipedia.org/wiki/grayscale
2. Genetic Algorithms. Introduction to. Availablefrom: https://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol1v/hmw/article1.html
3. Intralinks. Available from: https://www.intralinks.com/sites/default/files/intralinks_multi-tenant_saas_platform_security.pdf
4. Whatisdotcom. What is SPI model (SaaS, PaaS, IaaS)? - Definition from WhatIs.com. Search Cloud Computing. Available from: http://searchcloudcomputing.techtarget.com/definition/SPI-model
5. Software as a service. Wikipedia. Wikimedia Foundation. Available from: https://en.wikipedia.org/wiki/software_as_a_service
6. Akhtar N, Khan S, Johri P. An improved inverted LSB image steganography. 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT). 2014. doi: 10.1109/ICICICT.2014.6781374
7. Jassim FA, Hind EQ. Five Modulus Method for Image Compression. Signal & Image Processing: An International Journal SIPIJ. 2012;3(5):19–28.
8. Yang CH. Inverted pattern approach to improve image quality of information hiding by LSB substitution. Pattern Recognition. 2008;41(8):2674–2683.
9. Mazurczyk W, Szczypiorski K. Is Cloud Computing Steganography-proof? 2011 Third International Conference on Multimedia Information Networking and Security. 2011.
10. Akinola SO, A.olatidoye A. On the Image Quality and Encoding Times of LSB, MSB and Combined LSB-MSB Steganography Algorithms Using Digital Images. International Journal of Computer Science and Information Technology IJCSIT. 2015;7(4):79–91.
11. Khamrui A, Mandal Jk. A Genetic Algorithm based Steganography Using Discrete Cosine Transformation (GASDCT). Procedia Technology. 2013;10:105–111.
12. Rengarajan M, Aishwarya G, Rameshbabu M, Rayappan JBB. Optimum Pixel and Bit location for Colour Image Stego- A Distortion Resistant Approach. International Journal of Computer Applications. 2010;10(7):17–24.
13. Genetic Algorithm. MATLAB. Available from: https://www.mathworks.com/discovery/genetic-algorithm.html?s_tid=gn_loc_drop
14. Intro to Genetic Algorithms. Intro to Genetic Algorithms. Available from: http://lancet.mit.edu/mbwall/presentations/IntroToGAs/
15. Cloud computing [Internet]. Wikipedia. Wikimedia Foundation; Available from: https://en.wikipedia.org/wiki/cloud_computing
16. Mandal S, Bhattacharyya S. Secret data sharing in cloud environment using steganography and encryption using GA. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). 2015. DOI: 10.1109/ICGCIoT.2015.7380699.