Journal of Innovative Engineering and Research (JIER)
Vol.- 6, Issue -1, April 2023, pp. 11-16 (6 pages)

Enhancement of the Security of Data by Associating Obfuscation Technique along with Steganography

SARIKA HEMANT GADEKAR[1], DR. ARPANA BHARANI[2]

[1,2]Department of Computer Science, Dr. A. P. J. Abdul Kalam University, Indore 452010, India
Correspond Author Email: sarikaghadge.sg28@gmail.com

Abstract— A Data security is paramount in cloud storage. Their data can be stored in the cloud, which provides a tremendous amount of room. Users trust their information to the cloud because of its scalability, efficiency, & inconspicuousness. When information is transferred to the cloud, it is solely the responsibility of the CSP. One of the key difficulties that slows down the widespread use of cloud computing is the concern over the security of users' data. Combining obfuscation with steganography is a novel & sophisticated approach proposed in this paper to increase data security. The proposed privacy method integrates obfuscation & steganography to increase security. In contrast to obfuscation, which merely changes the appearance of data, steganography really hides the data itself. Utilizing the Least Significant Bit (LSB) replacement technique, the encrypted text can be concealed in an image. The experimental outcomes demonstrate the high embedding capability & stego image quality of the proposed method.

Keywords - Data Obfuscation, Data Security, Steganography, Cloud Storage.

I. INTRODUCTION

Cloud computing involves using shared computing that are made available via a network in the form of either hardware or software services [Buyya R et al., 2013]. Services such as IaaS, SaaS, &PaaS are all available in the cloud (PaaS). Users can access hardware, data storage, servers, and data centers through Infrastructure as a Service. Storage as a Service is a primary cloud service [Furht B 2010]. In order to consistently serve its customers, the cloud operates a distributed network of data centers in various places worldwide. It allows for infinite service expansion with no further human involvement. Information security is a major concern in cloud computing. CSP must keep up with the upkeep & monitoring of the information it has contracted out. Data on the cloud is vulnerable to a wide variety of attacks because it is stored in a public location. [sandeepK.Sood et al., 2012]. When transferring data to the cloud for storage, outsourcing poses security risks. Data maintenance, monitoring, and control are the sole responsibilities of the CSP once it has been moved to the cloud. Businesses of all sizes have recently begun to move their data storage needs to the cloud. Due to the cloud's public nature, there are numerous avenues via which users' data could be compromised. In the cloud, security is of paramount importance. Third-party CSPs store data that have been outsourced to the cloud. In this case, threats to data can originate both inside and outside of the cloud. Security factors including data confidentiality, integrity, access availability are used to secure the data.

In this research, we propose a method of improving cloud storage security by utilizing the confidentially parameter. Cryptography, obfuscation, & steganography methods are to be used to protect the privacy of sensitive information. When data is stored in the cloud, cryptography is a useful tool for preventing illegal access. The goal of cryptography is to ensure that only the intended recipients of a message can decipher & use the information it contains. Simply put, it's the act of encrypting & decrypting data. One can divide cryptographic methods into the more commonplace Conventional & more secure Public Key ones. Symmetric key cryptography is another name for conventional cryptography. In symmetric key cryptography, both enciphering and deciphering are performed with the same key. "Asymmetric key cryptography" refers to public key cryptography. Encryption & decryption rely on a pair of keys known as a public key & private key [L. Arockiam et al., 2014]. In order to protect sensitive information, obfuscation is used [S.Balamurugan et al., 2016]. Oblivious processing of obscured data is also possible. For security purposes, data obfuscation is employed to make it extremely challenging to recover the original, plaintext data. This method has recently gained traction as a means of protecting cloud-based data. Steganography refers to the practice of creating secret messages in writing that can only be deciphered by the intended recipient. This study suggests a new method of protecting private information by combining steganography with an existing obfuscation method, Magical Rolling Alpha Digits Obfuscation (MRADO).

Steganography

Steganography refers to the practice of concealing information, pictures, or sounds within another piece of data, picture, or audio. To bury information, or steganography.

Definition of "encryption" in computer science: keeping information secret within a message or file. Although it accomplishes a similar goal as cryptography, steganography merely conceals data from view.

One form of steganography that cannot be interpreted by a computer is invisible ink. Clear or "invisible" ink can be employed to write an address, which the recipient will only be able to see once the paper has been treated with another ink or liquid.

Like traditional steganography, digital steganography seeks to conceal information from anyone who isn't specifically intended to see or hear it.

Digital steganography is widely used to conceal information in media such as images, sounds, and videos from prying eyes. Hackers who deliberately bypass protections aren't the only ones who can benefit from the steganography method.

When used for steganography, it helps keep sensitive data safe. It's useful for relaying sensitive data between locations without drawing attention to the fact that a certain document—or perhaps two—have been transferred. When it comes to a company's reputation, information security is a top priority.

Obfuscation

The process of data obfuscation involves replacing sensitive information with data that appears to be genuine production data but is actually a fake, rendering the original data useless to malevolent actors. Generally speaking, it can be utilized in test or development environments where developers & testers need realistic data to build and test software without really needing to see the real data.

In highly regulated businesses, where consumers' private information must be protected at all costs, data obfuscation is a need.

Organizations can expose the data to test teams or database management as needed without risking data compromise or noncompliance by using obfuscation techniques. Obfuscating data has the major benefit of making it less vulnerable to hacking.

Obfuscation has the characteristics listed below:

- The term "masking out" refers to a method of data preparation that allows for the generation of several iterations of the same data structure. Changing the value of a data field has no effect on the field's type.
- There are a lot of ways to alter data. A few examples of data manipulation are changing numbers or letters, exchanging words, & swapping around pieces of data in different records.
- Data encryption makes the data unreadable until it is decrypted using cryptographic methods, often symmetric or private/public key systems.
- Encryption is a strong safeguard if and only if the receiving party is unable to decrypt the material for analysis or manipulation.
- As a result of data tokenization, sensitive details are replaced by random identifiers. Tokens are used to protect sensitive data, but only authorized users can access the underlying data.
- Token information can be put to use in live settings; for instance, it could be utilized to complete financial transactions without disclosing the actual credit card number.

II. LITERATURE REVIEW

K. Vandhana et al. (2022) The study's goal is to reduce the vulnerability of cloud-stored data to costly side-channel attacks through the use of new cube-based obfuscation & steganography. Secure Channel Attack & Novel Cube Based Obfuscation techniques are the two categories studied. The proposed method encodes the data in a way that is incomprehensible to attackers, rendering the image unrecognizable & rendering the extraction of steganographic images impossible; this method also reduces the amount of space needed to store the data. N=20 was used as the sample size for each group for implementing this study. Clinical sample sizes were used for the analysis. Eighty percent of the findings from the pre-test were retained. The statistical study showed that a significance level of 0.95 might be used when determining the appropriate size of an image. After analyzing the data, the authors conclude that obfuscation based on a cube appears secure & uses less space than a secure channel attack, whose image size is 2861 bytes. Experiment and statistical analysis lead to the conclusion that Novel Cube based obfuscation (CBO) is secure and uses less space than secure channel attack (SCA).

Kolawole Damilare Abel et al. (2022) Present-day society increasingly makes use of cloud computing systems. The ability to access one's data whenever it's needed has made this technology quite desirable. Access to the World Wide Web is possible from any location where one is made available. For fear of having their sensitive information compromised, some businesses have been slow to adopt this technology. Numerous studies have been conducted to solve this issue, and this study presents a fresh perspective on how to accomplish it. To improve cloud security, we suggest a paradigm that combines two cryptographic algorithms—the blowfish algorithm for data encryption & RSA algorithm for secret-key encryption—and a steganographic approach, Replace R in RGB, for the cover picture.

S. Prabu et al. (2020) Steganography has become famous for its ability to conceal the transmission of messages by concealing data within other data. Picture encryption, a rapidly developing innovation in the field of picture preparation, can be defined as the method of encoding messages and data uniquely to the point where they can be retrieved from secure components in essence. The paper provides a synopsis of the literature on the delineation puzzle, covering both its practical and theoretical aspects. It also makes an effort to learn the basics of good cipher figuring and to quickly weigh which steganography techniques are best for a given task. Due to the exponential growth of the internet & technological advancements in the fields of sight & sound, information transmission between systems is now commonplace. This study demonstrated the most often used least significant bit (LSB) method for secretly conveying a message within an image. Here, the goal of steganography was to achieve safe applications by subtly embedding sensitive information within visually and aurally unobtrusive media such as images, sounds, & videos.

Wid Akeel Awadh et al. (2019) Cloud computing is a modern development in the IT industry. Capabilities can be grown organically, with no need to hire additional staff, buy expensive software, or upgrade hardware. Currently, users store and exchange a great deal of data in the cloud, making it crucial that cloud computing be as safe as possible. Steganography is rapidly replacing other methods as the go-to defense for both cloud consumers and cloud service providers against prying eyes. The term "steganography" is used to describe the practice of secretly communicating information between a sender & recipient without compromising the integrity of the message. Through a comparison of studies based on technique selection, carrier formats, payload capacity, & embedding algorithm, this work aims to shed light on the state of the art in cloud computing steganography and point the way toward promising new avenues of study.

A. H. Mohsin et al. (2018) Biometric technology plays an important part in identification systems in real-time medical systems by allowing for the verification of individual identities via the use of biometric traits. Biometrics technology gives essential qualities for biometric features that can aid in the identifying procedure. The security of a biometric template can be compromised both during storage & transmission if it is sent to a centralized database. Since this is the case, it is crucial to create a new safeguard. This study therefore aims to provide a comprehensive analysis of the existing literature (from 2013-2018) in order to determine the taxonomy & research dispersion. This research aims to better understand the barriers and drivers of biometric steganography in real-time medical systems in order to make suggestions that will improve the efficacy of these systems when used to this field of study. Following a rigorous review procedure, we examine the literature on human biometric steganography in real-time medical systems from the three most prominent databases (IEEE Xplore, ScienceDirect, & Web of Science). From there, 41 articles are chosen based on their relevance to the initial topic utilizing exclusion & inclusion criteria. The examined research mostly concerned data concealing (especially steganography) techniques. This article examines the use of steganographic techniques in a range of human biometrics. Following a taxonomic classification, the outcomes are given in accordance with criteria such as human steganography biometric real-time medical systems, testing & assessment strategies, the relevance of use, and applications & approaches. We conclude with some suggestions for overcoming the difficulties of data concealment in order to make better use of biometric data processed by any authenticating real-time medical system. The development community, business users, and academic researchers should all benefit greatly from these suggestions.

Harpreet Kaur et al. (2016) Steganography is significant because of the astronomical growth of the internet & need for secure, private communication among its potential users. Secret information can be concealed within other data using a process called steganography. The purpose of Steganalysis is to foil Steganography by uncovering & removing any hidden data. The term "steganography" refers to the practice of hiding information in various media such as photographs, written documents, audio recordings, & video clips. The report also features several examples of how video steganography can be used to increase security.

Anita Pradhan et al. (2016) Several metrics for gauging an image steganography method's efficacy are laid out here. There are three metrics that can be used to evaluate a steganographic method's efficacy: I its ability to conceal information, (ii) its degree of distortion, and (iii) its level of security. What we mean by "hiding capacity" here is the maximum amount of information that could be cloaked from view within a given image. It is also expressed in terms of bits per pixel. Multiple metrics, including MSE, RMSE, PSNR, quality index, correlation, structural similarity index, or others, are used to assess the level of distortion. Mathematical representations of all of these measures are available. Tests using steganalysis systems, such as pixel difference histogram analysis, RS analysis, etc., can provide insight into the steganography method's security. There are mathematical equations to show how each of these measures is calculated. At the paper's conclusion, some potential next steps are also noted.

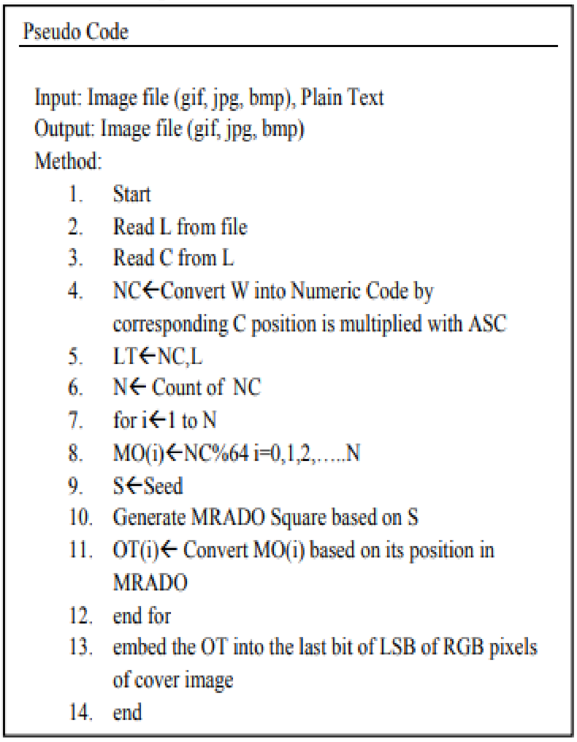
Shivani Sharma et al. (2016) By hiding information in seemingly innocuous formats, steganography facilitates the secure transfer of information between parties. Data can be concealed in a variety of electronic formats. There are several varieties of steganography, including those that hide information in images, texts, sounds, and videos. Less redundancy & easier detection of changes make text steganography more challenging than other methods. We have covered some of the techniques, traits, and operation of text steganography.

Alessio Viticchié et al. (2016) By making applications tougher to understand & alter, obfuscation techniques help avoid unauthorized modification of the code. Code obfuscation & data obfuscation are two types of obfuscation used for different purposes. While earlier empirical studies have been undertaken to identify the effects of code obfuscation, the goal of our work is to evaluate the efficacy & reliability of a particular data obfuscation technique, VarMerge, in deterring attacks. We ran an experiment in which students performed two attack tasks on versions of two C apps that were either completely transparent or heavily masked. Both the amount of time needed to complete the task & effectiveness of the assault were found to be significantly affected by the level of data obfuscation. The number of successful attacks on a VarMerge-enabled application is reduced by a factor of six. This result yields a useful hint that can be put to use in data obfuscation-based software security.

Gerardo Canfora et al. (2015) The sophistication of malware designed to harm Android devices is rapidly expanding. Malware authors are increasingly deploying variants of their programs that can alter their code as they spread to avoid detection by signature-based antimalware software. In this study, we hope to measure how well Android antimalware technologies perform against malware that employs a variety of evasion strategies to hide its dangerous payload. As part of this evaluation, we created a tool that makes several standard transformations to the source code of malware applications; we then applied this tool to the code of over 5000 malicious programs. Our findings show that most anti-malware programs are unable to detect malware following the code changes, even though the infection was accurately recognized before the transformations were applied. Those findings point to the urgent need to rethink the way malware is detected in order to ensure the safety of modern smart devices.

III. METHODOLOGY

This research suggests a method for improving the security of data stored in the cloud by concealing it within images using a combination of obfuscation & steganography. Data contained in an image can be accessed by an attacker. Therefore, the secret information must be encrypted or otherwise obscured. Using the MRADO approach, the data is first transformed into an obfuscated format, and then the LSB embedding technique is utilized to permanently attach the obfuscated data to an image. Utilizing LSB modification as a stand-alone method of data concealment is not a particularly safe practice. The embedded data will be more secure if these two techniques are combined. Afterwards, the stego-image can be safely kept in the cloud without anyone ever finding out what it actually is. If an adversary were able to decode the steganographic method & retrieve the data from the stego-image, they would still require the deobfuscation method to decipher the data.



```
Pseudo Code

Input: Image file (gif, jpg, bmp), Plain Text
Output: Image file (gif, jpg, bmp)
Method:
    Start
    Read L from file
    Read C from L
    NC←Convert W into Numeric Code by
        corresponding C position is multiplied with ASC
    LT←NC,L
    N← Count of NC
    for i←1 to N
    MO(i)←NC%64 i=0,1,2,….N
    S←Seed
    Generate MRADO Square based on S
    OT(i)← Convert MO(i) based on its position in
        MRADO
    end for
    embed the OT into the last bit of LSB of RGB pixels
        of cover image
    end
```

A. MRADO Technique

By combining replacement, transposition, & ASCII values, the MRADO Technique [Dr.D.I.George et al. 2016] enhances conventional methods of obfuscation. Substitution, redaction, nulling, shuffling, & blurring are now used in obfuscation methods. Data's true value can be concealed using the proposed method, but the process is irreversible. Line (L) lists are first created from the raw text. Characters (C) are translated into their ASCII equivalents in the relevant lines, & resulting ASCII (ASC) values are then multiplied by the character positions at which they occur in the word. The resulting Numerical Code (NC) for the word is calculated by multiplying the value of each character by itself and then adding the result to the value of another character. Eventually, the LT will be created. It keeps the line & NC value derived from it intact. To find the quotient and remainder, divide NC by 64 using the Modulo Operation (MO). The Seed(s) are used to generate the MRADO Square, which features lowercase & uppercase letters, numbers, and symbols like @ and #. There can only be one value for S, and it must consist of either letters or numbers. Figure 1 shows how the S value organizes the alphabet & numerals inside the MRADO square.In the end, the remainder of the NC value is used to derive the Alpha-Digits values. Finally, AlphaDigits are combined to produce obfuscated text (OT).

B. LSB-Based Pixel Processing (LSB)

Once the data has been encrypted, it must be patched back into the picture. When referring to pixel-based images, "RGB" refers to the abbreviation for "red, green, & blue" that is used whenever a pixel is formed utilizing those specific colors. One byte of information represents the density of a pixel's color. According to common knowledge, the first bit of an 8-bit value is the Most Significant-Bit (MSB), whereas the eighth bit is the LSB. In this case, the least significant bit is employed to conceal secret information within the image. Thus, only the final pixel is required to be modified. The following explains why LSB is needed for data patching.

- After information has been concealed, the only two possible values for the image's intensity change are 1 & 0. e.g. 11111000 11111001
- The intensity of the image is not drastically altered, & data transfer is simplified, because the shift is only one bit.

IV. RESULTS & DISCUSSION

The research offers is a Java program. There is a combination of steganography & obfuscation. The current method of obfuscation relies on a character-by-character approach. This method will thereby enhance both the speed and safety of data transfers. The time needed to produce the magical rolling alpha-digits square is increased. The process of obfuscation and de-obfuscation does not require any additional time.

The MRADO square's unpredictability adds an extra layer of protection to the masked message. The MRADO square is built from the seed value. Every line's worth of data, both numerical or otherwise, is obscured by a process of obfuscation. The stego image is created by inserting the encrypted data into a cover image via LSB substitution. The suggested merged algorithm is measured by the PSNR. For any pair of photos, the PSNR will determine the maximum allowed difference in signal-to-noise levels. This is a common metric for comparing the quality of the original & compressed version of an image. A higher PSNR indicates a higher quality compressed or reconstructed image. Image compression quality is measured using two error metrics: MSE & PSNR. Compared to the PSNR, which measures the peak error, the MSE indicates the total squared deviation from the original image. In order to calculate the PSNR, the block must initial determine the MSE utilizing the equation.

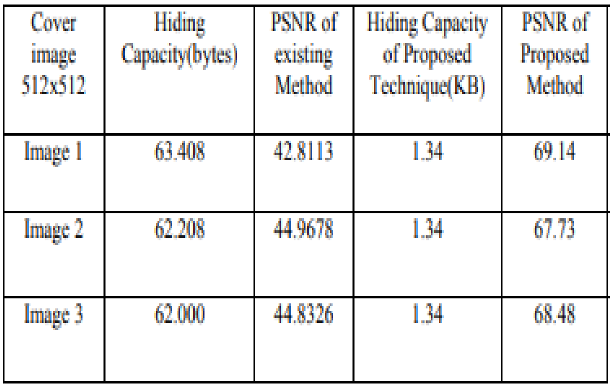
$$SE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N}$$

Thus, M and N in Equation represent the no. of rows/columns of input pictures, accordingly. This equation is then used by the block to calculate the PSNR.

$$PSNR = 10 \log 10 \left(\frac{R^2}{MSE}\right)$$

Table 1 evaluates the suggestion to [Marwa E. 2016] by hiding bytes in three 512 by 512 cover pictures (Baboon, Lena, & Peppers). The new method outperforms the existing strategy in PSNR & concealment.Table 1 demonstrates that the proposed method outperforms the status quo in terms of hiding capacity & PSNR value.

Table 1: Existing and proposed methods are compared.



Cover image 512x512	Hiding Capacity(bytes)	PSNR of existing Method	Hiding Capacity of Proposed Technique(KB)	PSNR of Proposed Method
Image 1	63.408	42.8113	1.34	69.14
Image 2	62.208	44.9678	1.34	67.73
Image 3	62.000	44.8326	1.34	68.48

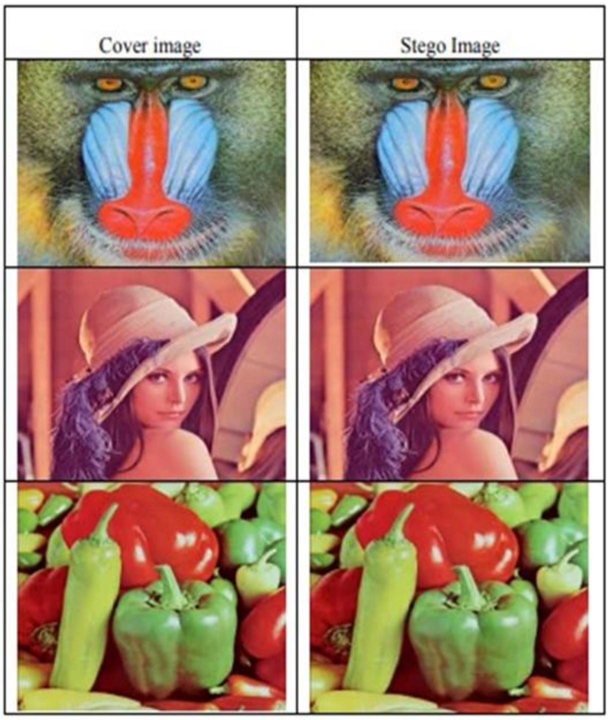


Figure.1: Compare of cover & stego image

V. CONCLUSION

Cloud storage is beneficial for businesses & consumers alike because of the low prices at which it offers its services. A large quantity of storage is available, making cloud computing an attractive option for moving data off-site. They are able to keep their data in the cloud safe and secure with the assistance of data outsourcing. Many different attacks can be launched on data both while it is at rest in the cloud and while it is being transferred to and from the cloud. Using obfuscation & steganography with the ability to maintain data secrecy in the cloud is the focus of this article. As soon as the masked information is uploaded to the cloud, hackers begin trying to access it. However, distinguishing between a cover image & stego image becomes challenging when the encrypted data is included into the image itself.

REFERENCES

[1] Abel, K. D., Misra, S., Agrawal, A., Maskeliunas, R., &Damasevicius, R., Data Security Using Cryptography and Steganography Technique on the Cloud. In Computational Intelligence in Machine Learning: Select Proceedings of ICCIML 2021 (pp. 475-481). 2022.

[2] Awadh, W. A., Hashim, A. S., &Hamoud, A., A review of various steganography techniques in cloud computing. University of Thi-Qar Journal of Science, 7(1), 113-119, 2019.

[3] Behera, C. K., &Bhaskari, D. L., Different obfuscation techniques for code protection. Procedia Computer Science, 70, 757-763, 2015.

[4] Buyya R, Vecchiola C, S. ThamaraiSelvi.," Mastering Cloud Computing Foundations and Applications Programming" Elsevier, 1-469, 2013.

[5] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I., "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility" Elsevier Science Publishers, 25, 599–616, 2009.

[6] Canfora, G., Di Sorbo, A., Mercaldo, F., &Visaggio, C. A., Obfuscation techniques against signature-based detection: a case study. In 2015 Mobile systems technologies workshop (MST) (pp. 21-26), 2015.

[7] Data Obfuscation 2013.Available from: http://www.techopedia.com/definition/25015/ data obfuscation-do.

[8] Dr. D. I. George Amalarethinam, B. Fathima Mary., "Data Security Enhancement in Public Cloud Storage using Data Obfuscation" Perspective in Science, Elsevier, 2016. (communicated).

[9] Furht B., "Cloud computing fundamentals. Handbook of Cloud Computing" Springer Science, 1–17, 2010.

[10] https://www.lia.deis.unibo.it/Courses/RetiDiCalcolatori/ Progetti98/Forti ni/lsb.html.

[11] Joseph Raphael, Dr. V Sundaram, "Cryptography and Steganography - A Survey", International Journal of Computer Technology and Applications, Volume 2 ,Issue 3, May 2011

[12] Kaur, H., & Rani, J. (2016). A Survey on different techniques of steganography. In MATEC Web of Conferences (Vol. 57, p. 02003). EDP Sciences, 2016.

[13] L. Arockiam, S. Monikandan, P. D. Sheba K Malarchelvi., "Obfuscrypt: A Novel Confidentiality Technique for Cloud Storage" International Journal of Computer Applications,88,17-21, 2014.

[14] Marwa E. Saleh, Abdelmgeid A. Aly, Fatma A. Omara,"Data Security using Cryptography and Steganography techniques", International Journal of Advanced Computer Science and Applications,vol.7, 2016

[15] Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Ariffin, S. A. B., Albahri, O. S., Albahri, A. S., ... &Hashim, M., Real-time medical systems based on human biometric steganography: A systematic review. Journal of medical systems, 42, 1-20, 2018.

[16] Prabu, S., &Ganapathy, G., Steganographic approach to enhance the data security in public cloud. International Journal of Computer Aided Engineering and Technology, 13(3), 388-408, 2020.

[17] Pradhan, A., Sahu, A. K., Swain, G., &Sekhar, K. R., Performance evaluation parameters of image steganography techniques. In 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS) (pp. 1-8), 2016

[18] Robertson C. PDF obfuscation - A primer., Available from: https://www.sans.org/reading-room/whitepapers/engineering/pdfobfuscation-primer-34005, 2012.

[19] S. Balamurugan, S. Sathyanarayana.,"ESSAO: Enhanced Security Service Algorithm using Data Obfuscation Technique to Protect Data in Public Cloud Storage" Indian Journal of Science and Technology,9,1-6,2016.

[20] Sandeep K. Sood," A combined approach to ensure data security in cloud computing", Journal of Network and Computer Application,Vol.35,pp.1831-1832, 2012.

[21] Seyed Rahman Soleimani, Masood NiaziTorshiz, "A New High Quality Vision Non-Adaptive Steganographic Method, Using Module and Combined Functions", International Journal of Emerging Trends in Signal Processing, Volume 1 ,Issue 2, January 2013.

[22] Sharma, S., Gupta, A., Trivedi, M. C., & Yadav, V. K., Analysis of different text steganography techniques: a survey. In 2016 Second International Conference on Computational Intelligence & Communication Technology (CICT) (pp. 130-133), 2016.

[23] Vandhana, K., &Sriramya, P., Security Enhancement and Efficient Storage Enhancement in Public Cloud using Novel Cube Based Obfuscation and Steganography Comparing with SCA with Minimal Cost. In 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS) (pp. 96-101), 2022.

[24] Viticchié, A., Regano, L., Torchiano, M., Basile, C., Ceccato, M., Tonella, P., &Tiella, R., Assessment of source code obfuscation techniques. In 2016 IEEE 16th international working conference on source code analysis and manipulation (SCAM) (pp. 11-20) 2016.