

# Data Security in Cloud Computing using Steganography and Biometrics

Vipul Sharma , Sandhya Tarar

Post Graduate Student, Assistant Professor

School of ICT

Gautam Buddha University, Greater Noida , Indi

**Abstract**— In today's world cloud computing is very commonly used method for accessing dynamically configurable and shared resources through the computer network when required, so there is constant threat to data. Security can be provided using Cryptography but the drawback of cryptography is that it confirms the presence of some important file which is encrypted using an algorithm. This research focuses on a methodology called Steganography is used. Basically steganography is an approach to hide a confidential message/file into a unconfidential(cover) image/file in a particular way in which the cover should stay as it was in the older version. So to the attacker it would seem like a normal file rather than an important one. Along with Steganography the fingerprint Biometric technology has been used to secure the data. As in fingerprint authentication system the accuracy is very high along with some other factors such as ease of use, small storage requirement, most economical etc. The Hackers had the capability to crack the older simple passwords as they can be easily hacked, so the data was not much secured. Hence to protect the data on cloud and prevent them from attacks we are using the concept of Steganography along with Fingerprint authentication technique.

**Keywords**—Steganography, Biometric Authentication, Data Security, Discrete Cosine Transform, Cloud Computing

## I. INTRODUCTION

Cloud computing generates a platform based on network to the users, through which the users can share information/data and resources without any worrying about their location. And the cloud computing can also be defined as, "A platform that allows user to have a storage space over the internet, so that any users approach the files or information stored on the cloud from any places disregarding of any condition just by accessing the internet". The capability to store boundless data with no stress over the capacity confinements available at our service and the privilege to utilize it as and when needed from anywhere in this world makes cloud computing the most favored technology & platform to store and transfer data. Cloud computing allows the individuals to use the shared set of system resources whenever and from wherever they require. These are the data centres that are available over the internet and the user can get access to it by giving some amount as fee to CSP (cloud service provider). There are also types of clouds such as Private cloud, which are handled and owned by some private organizations, Public clouds are like the internet, these can be accessed by the common people, Hybrid clouds in which organization makes use of the private cloud and on the other hand sometimes may access the public cloud as needed.

### A. Biometric Authentication

Individuals use passwords consistently, so as to login to various online platforms each and every day. What's more, similarly as the quantity of online administrations, the individual subscribes in to Increases, the measure of passwords that an individual needs to perceive is more. A research says that a normal individual needs to remember around 19 passwords, from online administrations to neighborhood machines. Moreover, the specialist co-ops online underline the people to utilize an alphanumeric blends of passwords so as to improve security, in some cases they likewise command clients to reexamine/change passwords on time to time premise. As this thing ends up disappointing and confused for the people to verify clients productively and safely remembering every one of the perspectives is basic to all businesses.

This is the place the interest of biometrics comes into the image by offering quicker, smooth and progressively vigorous verification in a consistent way. As biometrics will be utilized for online confirmation, henceforth the measure of biometric information that will be created will increment at a brisk pace. Hence we'll use the fingerprint Biometric which is effectively fast and the most efficient user verification technique and it requires small storage space for Biometric template.

### B. Steganography(Art of hiding) in Cloud Computing

Computer application are increasing everyday in real life. Hence, the need for data security has to be maintained and became a very crucial part of message or data transfer. So, Data security has become an fundamental aspect of our life. Among the various techniques, obscured sharing of information/data requires a concerns in the area of information security. Some of the methods used are steganography, cryptography etc. which can used for this objective. However, in past years, steganography has engaged more attention .

Steganography techniques can be act a superb tool for data extraction, to allow attacks in a network or hidden communication among unknown parties. These techniques aims is to hide a mystery message/file using a cover(unimportant) file and appending the source file along with cover file.

The word Steganography means "masked writing". From the gre-ek words "Steg-anos" meaning to "shielded or preserved" and "grap-hein" meaning to "write".

Steganography is also used by those who want to convey a private kind of message to any other individual without anyone having a clue about it. Here we are performing at the time of storing files to the cloud, which means files will be uploaded in a manipulated form.

Such that even if that secret file is revealed nobody can guess the presence of message inside it.

For the other person to crack, the individual has to use the exact same algorithm to unhide file/message through it was hide.

### C. Safekeeping of Cloud Computing

In Cloud computing there are some new security threats due to:

- I. Earlier encryption elements for retaining data Security cannot be directly adhered because the control of data is lost by users under Cloud Computing. By examining various data of users which is saved in the cloud and the prerequisites of ceaseless information security, due this validation of the data storage becomes difficult.
- II. Data saved on the cloud is to be regularly modified by the users, which include insertion, deletion, reordering, adjoining, modifying, etc. To assure legitimacy of storehouse for renewal of live data is of much importance .
- III. The cloud computing is expanding by running the data centre's parallely at different places.

## II. TOOLS USED

### A. Fingerprint Biometric Scanner

The Fingerprint biometric scanner is a device which is used for scanning the fingerprint templates of an individual. It can be used to restrict the access to a certain amount of confidential data. The accuracy of fingerprint is very high and it is very cost-effective way of authentication too.

### B. Glassfish server

It is basically a website server that handles the HTTP requests which are usually from the browsers along with a servlet Container (eg. Tomcat) which handles all the servlets & Java Server Pages.

It has an application server (eg Glassfish). In this paper we have use the glassfish server and it is open source.

In this project we have used the glassfish server to create a local cloud on the system.

And the host system act as the server to the cloud and the devices which are connected through a network and main PC acts as host system and others are clients.

## III SYSTEM ARCHITECTURE

Amid the time spent keeping up the security of cloud, one can utilize different methods. Mostly passwords are utilized to verify clients. Be that as it may, passwords are inclined to assaults also. This is least expensive just as most straightforward innovation. Subsequently we can utilize unique finger impression biometric verification to get security for cloud computing. Different procedures that are utilized for Biometric Authentication for security of distributed computing are as per the following:-

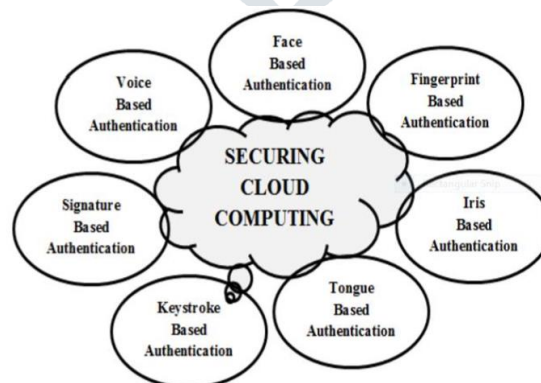


Figure 1 Biometric Security Techniques

### A. Authentication Mechanism

Authentication to a cloud computing service or any other kind of service plays a really important role. It generally means that only the users that authorized to access the system can access it.

Along with that other part there is a verifying part where the person is to be verified who is claiming to be the one who is authorized for the access to the system or set of information.

In the system developed the user will be authenticated by providing the fingerprint template which will be verified with the template present in the database.

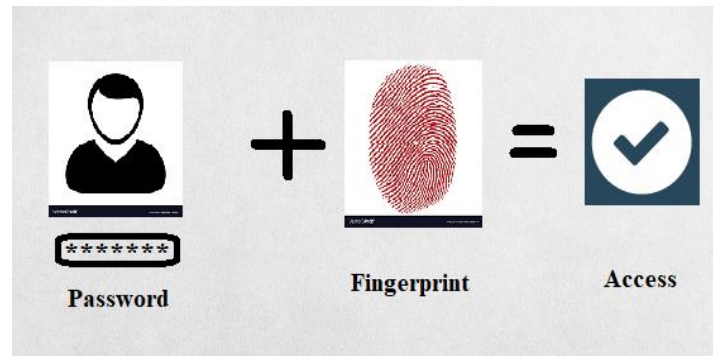


Figure 2 Multi-Factor Authentication

### B. Performing Steganography

To perform steganography, the Discrete Transform Technique is being used. There is certain sequence of steps that are being followed to do so.

Hide the file:-

1. Upload the cover image/file.
2. Upload the source image/file.
3. Hit the hide button.
4. Using DCT algorithm the source file will be appended at the end of cover file.

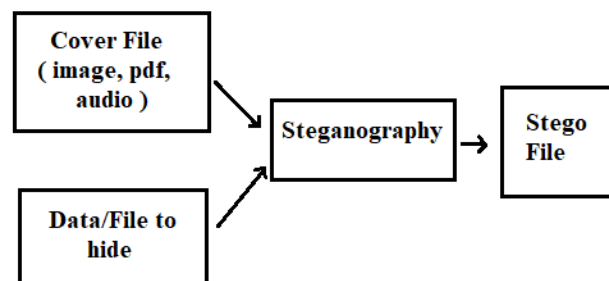


Figure 3 Flow of control in DCT

Unhide the file:-

1. Upload the image/file which contains the source file hidden in it.
2. Hit the Unhide button.
3. Using DCT algorithm, the source file be extracted from the cover file/image.

### C. Biometrics

Biometric is and technical term which means that one can use their body parts for the authentication purpose It is utilized as a verification and access control device. Biometric frameworks allows measurable proof of people taking into account behavioural or physiological attributes To accomplish more dependable confirmation or ID one need to utilize something that truly describes the individual.

A Fingerprint framework comprise of sensors, include extractor and coordinating modules which is utilized to actualize biometric acknowledgment calculations. The sensors filter the biometric property of the client and produce its computerized picture. At that point a quality check must be performed so as to make sure that the caught biometric test is solid and can be taken care of by the resulting highlight extraction and coordinating modules. The extraction highlight portion will dispose of the futile and superfluous information present in the taken example and concentrates helpful data considered highlights which can be used for further checking.

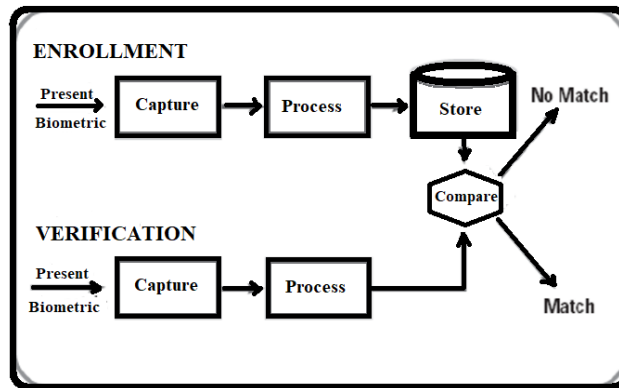


Figure 4 Working of Authentication System

Amid coordinating, the gained biometric test is coordinated with the reference data which is available in the database so as to assemble the recognizable proof related with the inquiry. This task is completed two stages, first is the Enrolment and second is the acknowledgment.

In Enrolment organize the Unique data on fingerprint of the clients is saved in the catalog. We are executing our task to coordinate unique finger impression information of client for verification in cloud. We will store the clients unique mark information in packed structure on a cloud database for the time and will utilize that for confirming the client when he endeavors to login without fail. We are utilizing fingerprint scanner to take unique mark of client. Unique finger impression information/impression will be transmitted in the packed structure for security of clients Biometric information. There is a coordinating module which coordinates the fingerprints against the layout which put away in the index. On the off chance that the unique mark matches with one present in database, at that point just , it will enable the enrolled client to login.

### III. ALGORITHM USED

#### A. Discrete Cosine Transform

The DCT which is short for Discrete Cosine Transform could be utilized to rebuild the image data(Digital) from a dimensional to the frequency domain. After converting to freq. domain the data/file is ingrained in LSB of medium freq. components and is stated for lossy compression whereas in DWT which is short for Discrete Wavelet Transform, the hidden messages are ingrained in the large freq. coefficients which are the results for DWT and have highest durability.

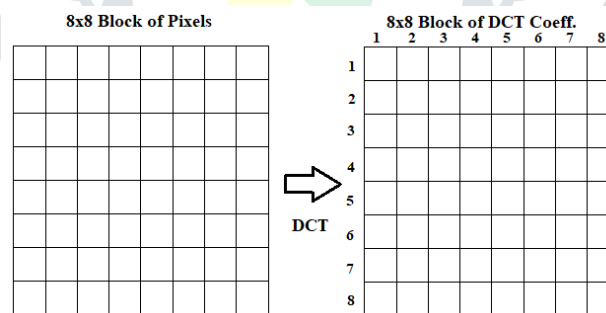


Figure 5 Hiding message inside DCT Coefficients

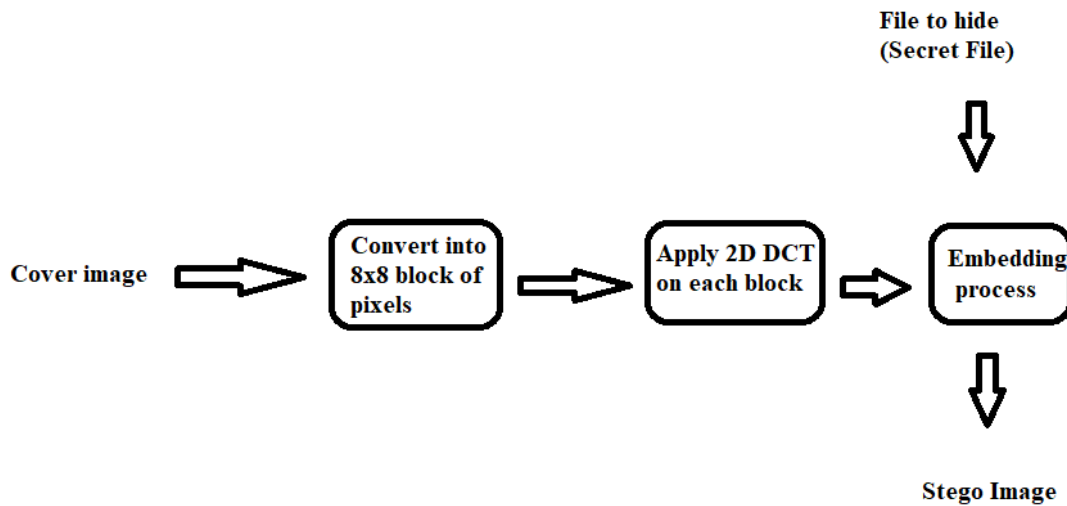
#### B. DCT Technique

In DCT there are some coefficients which are used JPEG compression, which separates the picture into different important parts. It breaks down the image into different freq. components medium, high, low.

In DCT most of the crucial information of the image is fixed on the few coeff. of DCT.

Due to the above reason this algorithm is used in the image compression applications.

The obscure message is hidden inside the cover by manipulating coefficients.



**Figure 6 Control flow diagram of DCT**

The Figure 6, describes the flow of DCT algorithm which is used to perform Steganography. The initial step is to input the cover image and the data file which is to be hide.

After that the cover image is separated into 8x8 block of pixels and the DCT algorithm for 2D is applied. The square blocks are then converted to 8x8 blocks of DCT coeff. . These coefficients have a crucial role. The separation of the image into the various freq. band regions is done as to create it, which will be more likely to hold some secret message or information by manipulating the DCT coefficients.

The embedding of the secret file into the cover image is done with very much precision due to which the cover image remains intact and looks pretty similar like it was before and its quite difficult to judge the difference between the cover image and the stego image just by looking at them.

#### IV. PROPOSED SYSTEM

In previously system developed the data security was provided using the traditional methods only and it was not much secure. Simple passwords are easy to crack, that's why there was a need for a change and an advanced system for security.

Hence the Fingerprint Biometric Authentication was implemented in this research paper. Which will act as a fast and efficient way to authorize users.

When any new user wants to get access to the Cloud and the data files. Firstly, he has to do is, to register by using his fingerprints. The Biometric fingerprint template is then stored for verification.

After authentication is done one can upload any data file along with the cover image/file which will be used in order to perform Steganography and hide the original file under the cover image/file.

This mean is the confirmed with the methods for the information that is as of now spared in the catalogue while enrolment. It finds the connection between the two pictures and gives the outcome whether he/she is a substantial client or not.

If some user wants to decode a data file then the individual has upload the file to the cloud, and has to provide the biometric Authentication in order to Extract the original file from the cover image/file. This makes sure that only the authenticated users are able to login and decode the original files.

#### V. IMPLEMENTATION

##### A. Authentication

This is the point from when the user will enter into the system. The individual will have to validate himself by providing some information in order to use the cloud services.

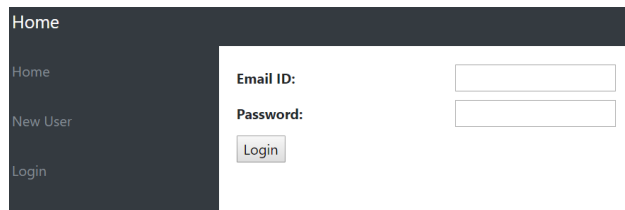
##### 1. Using credentials

This is the normal way to login where individual has to input the e-mail and the password which was saved into the database at the time of registration. The process will match the credentials with the one in the system's database and allow the user if it matches.



**2. Fingerprint Biometric scan**

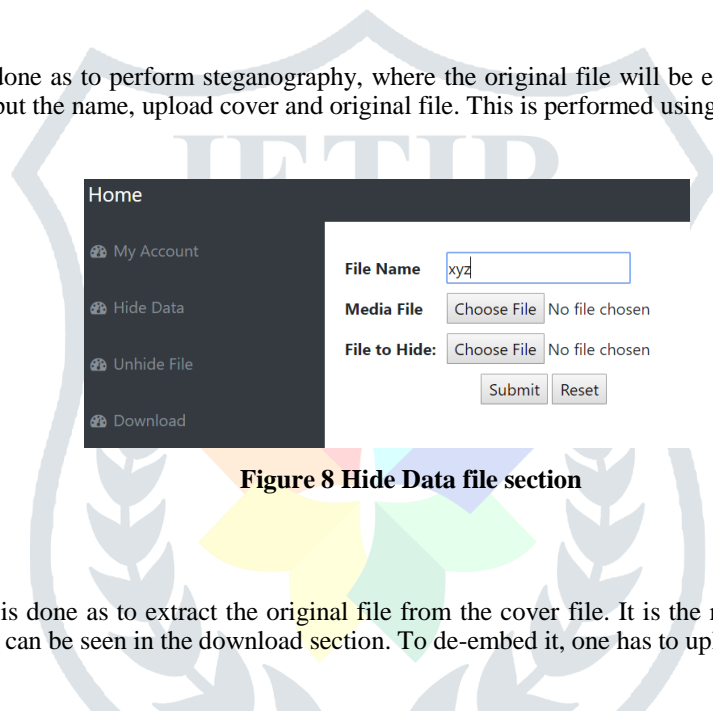
This is the additional security that is added to the system to make it more secure and less prone to threats. The individual will then give the fingerprint impression which will also be verified with the template present in the database.



**Figure 7 Login Screen**

**B. Embedding Process**

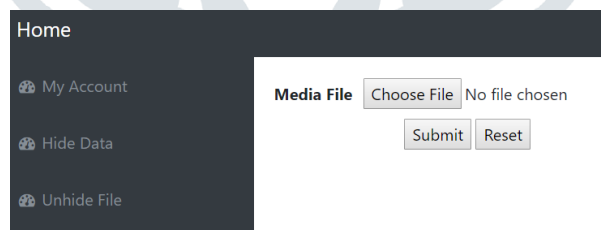
The Embedding of file is done as to perform steganography, where the original file will be embedded at the end of the cover file. To do so one has to input the name, upload cover and original file. This is performed using the DCT algorithm.



**Figure 8 Hide Data file section**

**C. De Embedding Data**

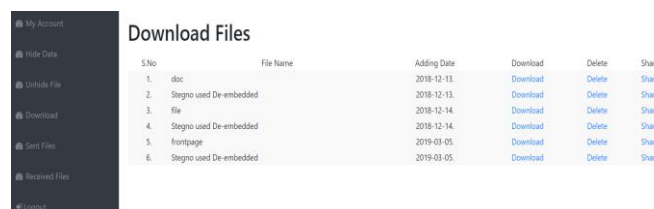
The De-embedding of file is done as to extract the original file from the cover file. It is the reverse procedure of embedding. After embedding the file, it can be seen in the download section. To de-embed it, one has to upload to stego file and hit submit.



**Figure 9 Unhide data section**

**D. Sharing Files among users**

Data files uploaded to the system can be shared too. The users have to option to share data among other fellow users also, this can be done from the download section. And can check shared history in Sent files and Received files tab.



**Figure 10 File repository and share file section**








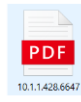


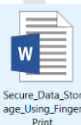




## VI. RESULT ANALYSIS

Data Security is a major issue these days. Hence steganography can help at certain extent to improve the security on cloud.

In the system developed, for safeguarding the data steganography was performed using the DCT algorithm. The main focus of interest was that whether the attacker can find out the presence of a secret image/file embedded inside another file.

Due to the ability of Steganography, it becomes quite difficult to judge the presence of a secret file that may be attached with some other file.

**Table 1 Variation in properties of file after Steganography**

Cover Image	File to Hide (Secret file)	Secret File Extension	Stego Image	Size (before)	Size (after)
		.pdf		120 KB	789 KB
		.doc		326 KB	535 KB
		.pdf		2140 KB	2590 KB
		.doc		2080 KB	2370 KB
		.pdf		1160 KB	1440 KB

In the above Table 1, the set of images which were used in order to hide/embed some secret file along with it are shown. The practice of Steganography is preferred over cryptography as do not attract any unwanted attention to itself.

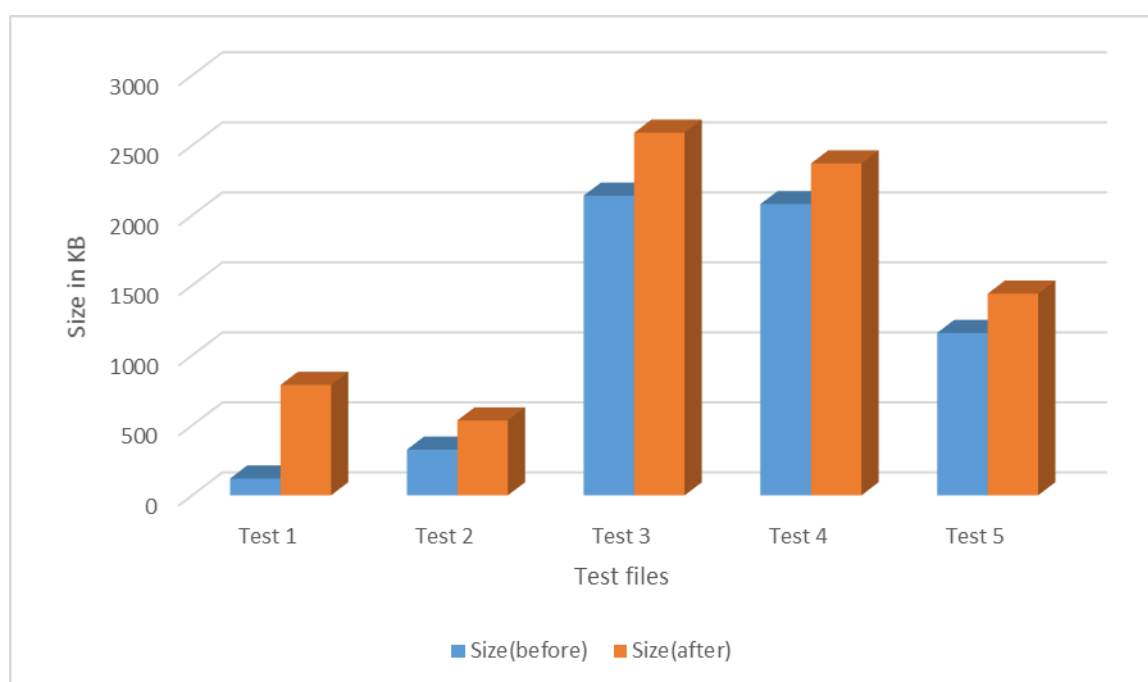
The system implemented supports most of the file types such as .jpeg, .png, .pdf, .doc, .xlsx, .mp3 etc for embedding.

As one can see that the images of the Cover and the stego images are quite the same. This shows that even after we append the data at the end of the cover image and even after that there is negligible change in the appearance of the image which is a positive point. Their histogram also does not show much variation. So the outcome we get from the following is that even the merging of data with the Cover image, it has a very negligible effect on the look of Stego file(image) as it looks just the same as it was before.

The only change in the property of the image we get is only the increase in size. The increase in size will be directly proportional to the data size of the secret file.

Therefore it will not be simple for an attacker to identify the presence of hidden file/data. And we can say that steganography can be used to enhance the security along with the Fingerprint Biometric authentication mechanism which ensures only users with permission to enter the system can login and de-embed the data.

The bar graph representation of the variation in size is shown below:-



**Figure 11 Comparison of data size before and after embedding**

The most important factor that comes into the mind regarding the implementation of the system is the change in data size.

The above Figure 11 shows the variation in the data size of the image file before and after the application of DCT on them or we should say before and after appending secret data files at the end in each of the cover images.

In the graph the above the subsequent increase in the data size of the image can be calculated which will be directly proportional to the data size of the secret file. As bigger the size of secret file, more will be the increase in size of the image.

On the X- axis, the test files are represented as Test 1, Test 2 ..... Test 5. And on the Y-Axis, the data size of the image is represented in Kilobytes(KB).

## VII. CONCLUSIONS

In this research, discussion about the term Steganography was done and it was performed on the data using Discrete Cosine Transform algorithm which is used to hide the original file in some cover file to increase the security. As an improvement with that, the fingerprint based biometric authentication system was used, by adding a layer of security we were able to enhance the Data Security in cloud computing. Every user has to be authenticated using biometric at the time of login as well as the time of Unhide the original file. This will improve security as only the users which are authorized can handle the file after the decrypting process of Steganography. The main motive of the research was to minimize any unauthorized access to the system. The approach can be in used in the organizations to safeguard their data files and improve their security. This research paper focussed on securing the data present on the cloud using a Fingerprint mechanism which is not too expensive to implement. In future wireless mechanism can be made for the fingerprint authentication and the effectiveness can be further improved.

## VIII. ACKNOWLEDGEMENT

This research was supervised by Dr. Sandhya Tarar for her guidelines, useful suggestions and for permitting me to carry out this work which helped me in completing the work on time and without whom this research would not have been possible. I would like to acknowledge Dr. Anurag Baghel, HOD of CSE Department for his encouragement that boosted my morale and confidence. I would like to express my gratitude and heartfelt thanks to Dr. Indu Uprety, Dean of ICT for her excellent supervision and support in this research. I also want to take this opportunity to thank our colleagues from Gautam Buddha University who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper.



## REFERENCES

- [1] Chandra Shekhar Vorugunti , “A Secure and efficient Biometric Authentication as a service for cloud computing,” IEEE, October 09-11 2014 .
- [2] Kiran Kumar K, K.B Raja, “Hy-brid Finger-print Match-ing using Blo-ck filter and strength factor,” Second International Conf-erence on Computer Eng-ineering and Applications,2010
- [3] Robert Gellm-an and World Privacy Forum , “Privacy in the Clouds: Risks to Pr-ivacy and Conf-identiality from Cloud Computing”, February 23, 2009.
- [4] Amazon.com, “Amazon Web Services (AWS),” Online at <http://aws.amazon.com>, Version 2019
- [5] <https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/>
- [6] K. Zhao, H. Jin, D. Zou, G. Chen and W. Dai, "Feasibi-lity of deploying bio-metric encrypt-tion in mobile cloud computing," in 8th IEEE ChinaGrid Annual Conference, 2013.
- [7] J. Yuan and S. Yu, " Efficient privacy-preserving biometric identification in cloud compu-ting," in 2013 IEEE Infocom Proce-edings, 2013
- [8] P. Peer, J. Bule, J. Z. Gros and V. Struc, "Building cloud-based bio-metric services," Infor-matica, vol. 37, no. 2, p. 115, 2013.
- [9] SU Khurana & AN Verma. (2013). Comp-arison of Cloud Computing Service Models: SaaS, PaaS, Iaas, IJECT Vol. 4, Issue Spl-3. ISSN: 2230-7109 (Online) | ISSN: 2230- 9543(Print)
- [10] UD Kamred (2014). A Steganography Technique for Hiding Inform-ation in Image. International Journal of Emerging Techn-nologies in Computa-tional and Applied Sciences (IJETCAS). ISSN (Print): 2279-0047 ISSN (Online): 2279-0055.
- [11] Vaishali & AN Goyal. (2014). An Implementa-tion of 4 Bit Image Stegano-graphy for Data Security in Clouds. Inter-national Journal of Advanced Re-search in Computer Science and Soft-ware Engineering. Volume 4, Issue 11.
- [12] Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Sec-urity and privacy for storage and compu-tation in cloud computing. Inf Sci 2014;258:371–86www.elsevier.com/locate/ins.
- [13][https://www.researchgate.net/publication/317401791\\_Secure\\_Image\\_Steganography\\_Algorithm\\_Based\\_on\\_DCT\\_with\\_OTP\\_Encryption](https://www.researchgate.net/publication/317401791_Secure_Image_Steganography_Algorithm_Based_on_DCT_with_OTP_Encryption)
- [14] Achmad Solichi, Erwin Wahyu Ramadhan.  
“Enhancing data security using DES-based cryptography and DCT-based steganography” IEEE,15 January 2019.
- [15] Gurmeet Kaur, Aarti Kochhar,“A Stegano-graphy Implementation based on LSB & DCT”, International Journal for Science and Emerging, Technologies with Latest Trends 4(1), pp. 35-41, 2012.
- [16] Xiu Nan ; Zhou Pei ; Zhi-Tang Li, “A Steganography Algorithm Based on  $\pm 1$  DCT Coefficients for H.264/AVC” , November 2, 2015
- [16] Achmad Solichin ; Erwin Wahyu Ramadhan, “ Enhancing data security using DES-based cryptography and DCT-based steganography “ January 15, 2018
- [17] C. Manikopoulos ; Yun-Qing Shi ; Sui Song ; Zheng Zhang ; Zhicheng Ni ; Dekun Zou, “Detection of block DCT-based steganography in gray-scale images” , June 11,2003
- [18] Kun Huang ; Jiangyong Shi ; Ming Xian ; Jian Liu, IEEE “Achieving robust biometric based access control mechanism for cloud computing” June 5 2017