Stegtorrent using De-Clustering of Data

Murkute Reshma Balasaheb
Student, Department of Information Technology, MMIT, Lohgaon, Pune

Pattiwar Nikita Sanjayrao
Student, Department of Information Technology, MMIT, Lohgaon, Pune

Shere Shalaka Suryakant
Student, Department of Information Technology, MMIT, Lohgaon, Pune

Thombare Nalini Tukaram
Student, Department of Information Technology, MMIT, Lohgaon, Pune

G.V.Mane
Professor, Department of Computer Engineering, MMIT, Lohgoan, Pune

ABSTRACT
Nowadays, For uploading and downloading of data using torrent people widely use internet. Existing system was less secure and time consuming. To avoid this problem stegtorrent using de-clustering of data is implemented. For file transfer service, StegTorrent is a new network steganographic method. To achieve availability and scalability of storage systems are important for existing information systems.One approach to achieving high availability of parallel disk systems is to replicate the data items on separate disk drives. Many applications require considerable space, which is increasing rapidly, and essential data kept in storage must be retained. Parallel storage configurations with multiple disk drives are used to satisfy these requirements. Because of the disk failure, when one copy is damaged then other can continue to be used. In the replication-based approach, it is also important to lower the cost of update operations. To ensure that the data mapping and requests are evenly divided among disks. In replication-based approach, it takes the advantages of low cost data modification and data recovery.

Keywords
Network steganography, Bittorrent , StegTorrent, information hiding, Disk Failures, Clustering and De-clustering, Partitioning.

1. INTRODUCTION
Many application require considerable space, which is increasing rapidly, and essential data kept in storage must be retained. To satisfy these requirements, parallel storage configurations with multiple disk drives are commonly adopted. For achieving high availability and scalability data placement methods are very important. Parallel disk systems is to replicate the data items on separate disk drives. Because of the a disk failure, when one copy is damaged then other can continue to be used. For example the chained de-clustering. The horizontal partitioning strategies fall into three types: round-robin, hash and value-range partitioning. For many applications to provide better performance, clustering effect of the partitioning, which stores continuous data into physically neighbouring disk pages is used. The round-robin partitioning produces no skew but is ineffective for queries because it requires brute-force searches. The cost of the synchronization is comparatively high. If dirty copies, which might be partially inconsistent with the latest state, are acceptable, asynchronous update with logging improves the performance update. Even if the log for the synchronous update is stored in volatile memory, no data are lost during a single fault.

1.1 Steganography
Steganography is a hidden communication that means "covered writing" (derived from the Greekwords *steganoo*r "covered" and graphos or "towrite").Steganography is used to hide an information message inside a cover medium which will be harmless so that it is not possible to detect that there is any secrete message. There are many techniques used for hiding message in images. With the help of these techniques one can not detect the message hidden inside an image file. By this techniques, we not only sending message but also hiding the message itself. Steganography is designed to encode and decode the message embedded into an image using different LSB insertion methods in which the message is spread all over the image where it should be needed. For this secrete key is used, which is the combination of random numbers.

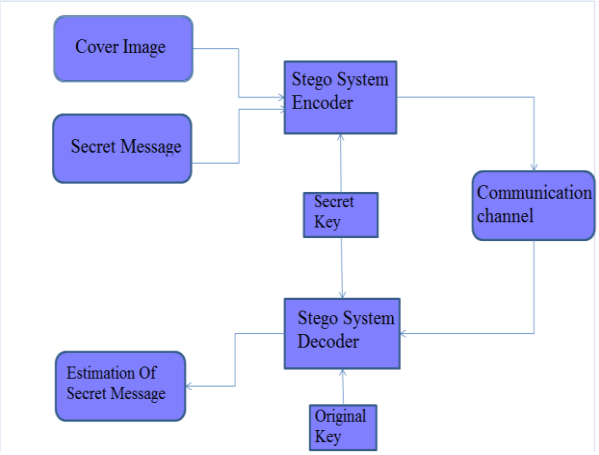

Fig.1.1 Modern Steganographic system

1.2 Torrent
There are many P2P file-sharing systems which are proposed and implemented, few of them have stood the test of intensive daily on very large number of user communities. From all of these systems the BitTorrent file-sharing system is one. That BitTorrent is evolved as one of the most popular networks .In June 2014,from all P2P traffic the BitTorrent traffic made up 53 %. BitTorrent is a file-download protocol only, it relies on

other global components like web sites for finding files. For this purpose the most popular web site that we performed our measurements was suprnova.org. Acceptance of a P2P system using a large user community is done by different important aspects. The system should have a high availability firstly. The second thing is that, the users should always receive a good version of the content. The third thing, the system have to be able to deal with flash crowds. Lastly, relatively high download speed should be obtained by users . BitTorrent and Suprnova, measurements study addresses all four mentioned aspects. In addition, from the injection of the file until its disappearance one of the most popular files we followed all 90,155 downloading peers. In a period of two weeks, it is observed that the bandwidth of newly injected files is 54,845 peers downloading over a hundred. It is one of the largest our measurement effort ever conducted. Main conclusions is that within P2P systems between availability a tension exists, when there are no global components it is improved, and data integrity, which benefits from centralization.

1.3 De-Clustering

The technique is termed as chained de-clustering which is established to provide better performance when event failures occures at the time of maintaining data availability at very high degree. The special hardwares are not required for chain de-clustering , The existing softwares only requires minimal modifications.

It is unlike most earlier replication strategies. When solutions are prepared to increase availability and reliability of a computer system.The techniques used mostly involves mass storage and replication of precessors. Some systems uses one step further replicating, not only software modules but also hardware components so that when software or hardware failes, the application software ran using the redundant software modules.

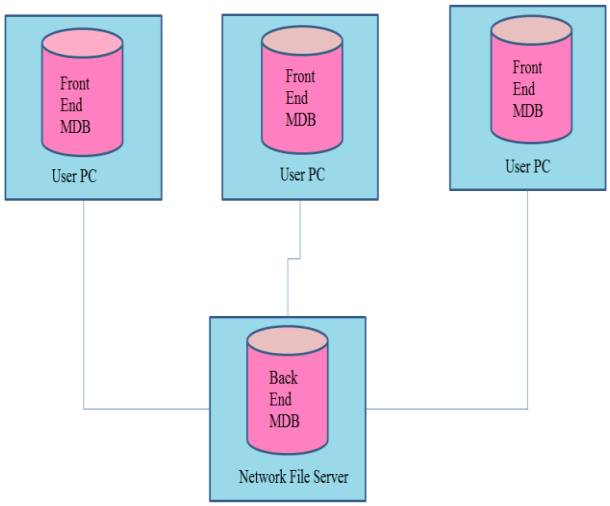

Fig.1.3 Data De-clustering

2. RELATED WORK

2.1 Steganography

2.1.1 Image based steganography using LSB insertion technique

Steganography is the science and art of hiding the communication in existence . The steganography technique make it difficult to detect a hidden message inside an image file. Using this technique we not only sending the message but also hiding message inside itself. This technique is used for encoding and decoding an image file which contains a secret file using method called LSB insertion where the data is spread out all over the image file in random manner. To achieve this secret key is used. The key generate random numbers, which helps to indentify where and in which order the hidden message is stored.

2.1.2 An overview of image steganography

The art of hiding existing communication by hiding information in other information. There are many different file formats are available, but digital images are the mostly used because of their Internet frequency. For hiding information in images secretly, there are no of steganographic techniques some are complex and having their strong and weak points respectively. The steganography technique used with different applications having different requirements. For example, absolute invisibility of the secret information may required by some applications while other require hidden secret messages.

2.2 Torrent

2.2.1 The bittorrent p2p file-sharing system: measurements and analysis

Among number of P2P file-sharing prototypes in existence, BitTorrent is one of them who has managed to attract millions of people's towards it. For file search BitTorrent relies on other global components to ensure the integrity of file data employs a moderator system, and for downloading and preventing users from free riding it uses a bartering technique. BitTorrent deals with four issues mainly flash crowd handling, and download performance, integrity, availability. In modelling P2P systems providing measurement data that may be useful.

2.3 De-Clustering

2.3.1 Reversible Palette Image Steganography Based on De-clustering and Predictive Coding

To defend information security in the network Steganographic technology plays as important role. The information could be hidden using multimedia object. The human visual system to maintain security of information which is invisible, even it will be transmitted through unsafe channel, during compression encoding the information is embedded into the image. The drawback caused by distortion of other schemes are reformed using proposed method. The original image can be recovered from stego-image by retrieving the information. For keeping transmission secure the proposed method is useful and robust.

2.3.2 Chained De-clustering: A New Availability Strategy for Multiprocessor Database machines

A new strategy in multi-processor for increasing the availability of data, shared-nothing database machines. The technique, chained de-clustering maintaining a very high degree of data availability to provide superior performance at the time of failures. Chained de-clustering requires minimal modifications in existing software and implementation of no special hardware.

3. PROPOSED WORK

3.1 Upload

Bit server is the main server and database is used to store log information. When client want to upload any file to server, first it uses steganography algorithm(LSB) then the file split

into number of parts depending on number of servers available. These parts are uploaded on there respective servers. These servers are connected to each other using Round Robbin algorithm. If any server fails, Data can be retrieve from other servers. Shown in Fig.1.

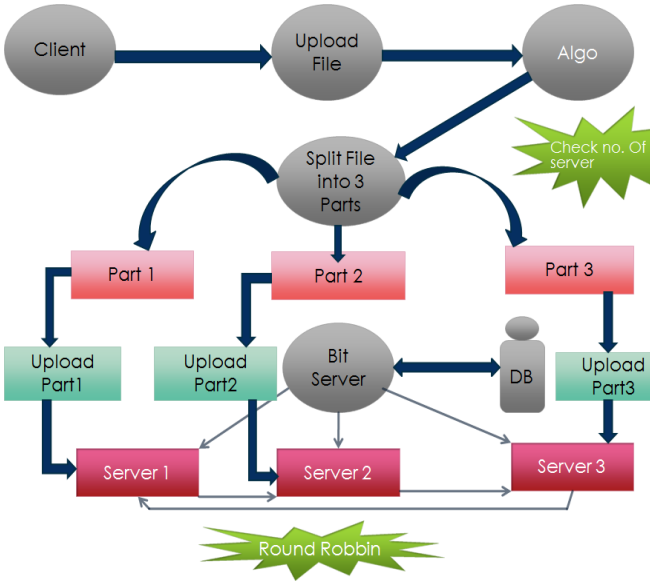

Fig.3.1.Architecture for Uploading

3.1.1 LSB(Least Significant Bit)

A simple approach to embed information in an image file.
Algorithm:-
1. Select a cover image of size M*N as an input.

2. The message to be hidden is embedded in RGB component only of an image.

3. Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).

4. After that Message is hidden using Bit Replacement method.

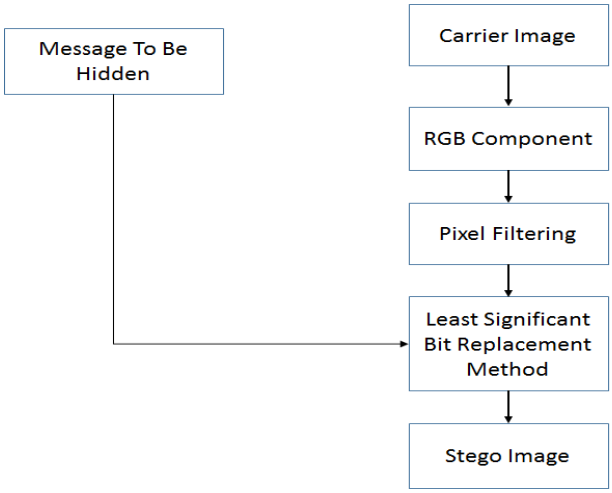

Fig.3.1.1 Least significant bit

3.1.2 Round Robin

Round robin is used for time sharing system. It is similar to first come first serves scheduling algorithm, but the pre-emption is the added functionality to switch between the processes.
The measure features of round robin algorithm is:
1. Throughput is low as the large process is holding up the central processing unit for execution.

2. The main advantages of round robin is to remove starvation. As long as all processes completes the execution but the problem starts when any of the process fails to complete. The incomplete execution of any process leads to starvation.

Queuing is done without using any prioritization of the processes. Round robin is an arrangement of choosing all elements in a group equally in some rational order, usually from the top to the bottom of a list and then starting again at the top of the list and so on.

3.2 Download

When client want to download any file from server,all parts are downloaded from available servers.After downloading all parts merge together on client side.Later,file is decrypted(AES) and available to client.

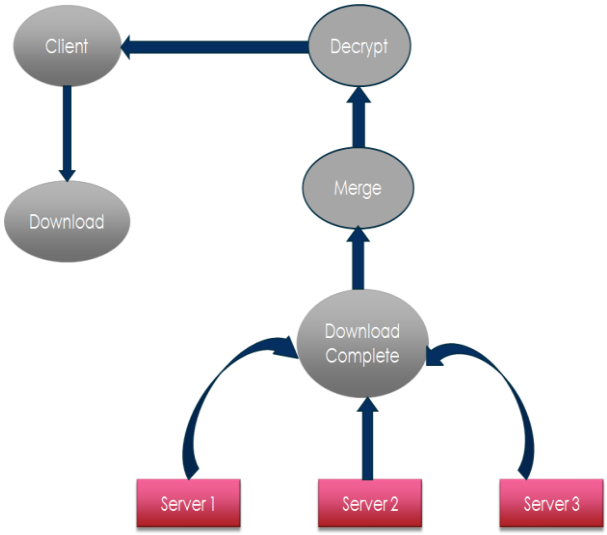

Fig.3.2 Download architecture

4. ALGORITHMS

a)AES(Advanced Encryption Standard)

AES defined a cipher in which the block length and the key length can be independently specified to be 128,192,or 256 bits. The AES specification uses the same three key size alternatives but limits the block length to 128 bits.It is an iterative cipher (operates on entire data block in every round) rather than feistel (operate on halves at a time), and was designed to have characteristics of: Resistance against all known attacks, Speed and code compactness on a wide range of platforms, Design simplicity.

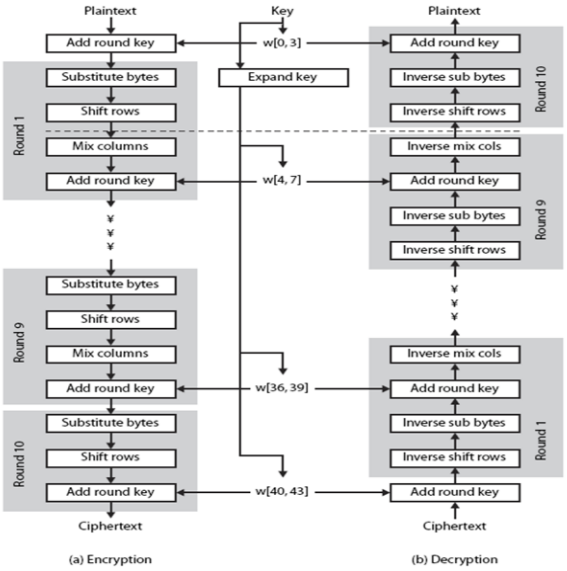

Fig.4. Advanced Encryption Standard

5. EXPERIMENTAL RESULTS

To experimentally evaluate the proposed steganographic method, the StegTorrent prototype implementation was Developed**.** StegTorrent cost is less because it requires less time for downloading .This is completely different from Bittorrent .If the size of file is 10MB then time require to upload and download any file as shown in graph. On Y-axis time is in millisecond and on X-axis is file size in MB.

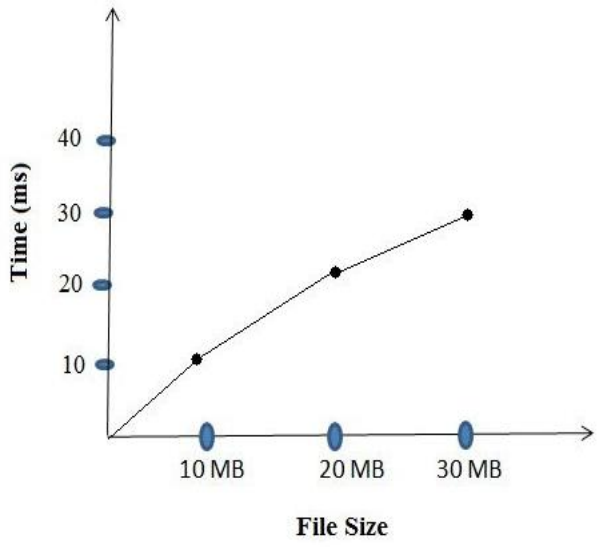

Fig.5 Comparitive graph for file size and time

Fig.6 shows comparative study of bittorrent. Here, Here, X-axis represents size of file in kilobytes and y-axis represents time is in seconds. In bittorrent one-to-one transmission. Therefore, while uploading it takes 4.30min.

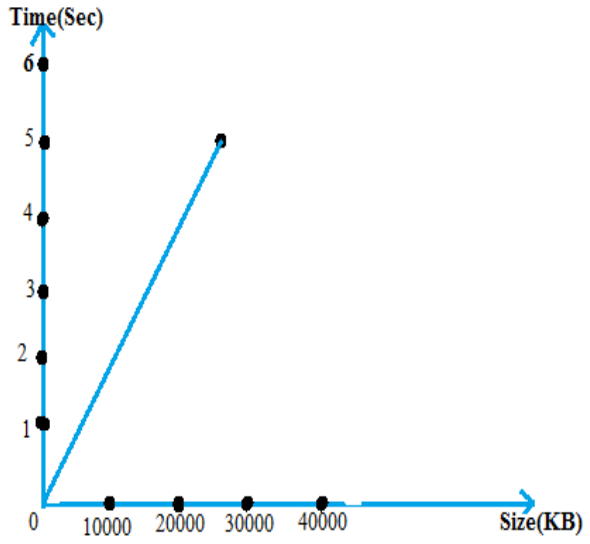

Fig.6.Comparative study of Bittorrent

Fig.7 shows the comparative study of stegtorrent. Here,X-axis represents size of file in kilobytes and y-zxis represents time is in seconds.For uploading file on 3 servers it takes 1.30min and on 2 servers it takes 3 min.

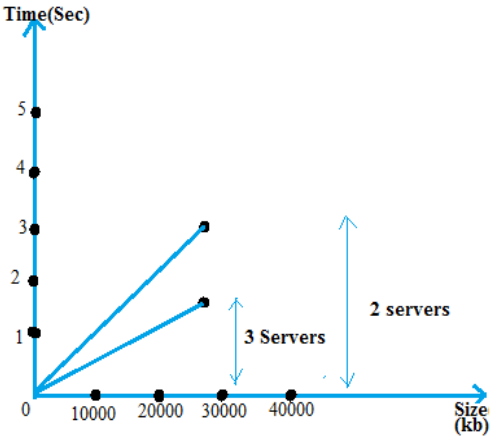

Fig.7.Comparative study of Stegtorrent

6. ADVANTAGESAND LIMITATIONS

6.1 Advantages

6.1.1 Highly secure:

System is highly secure because data is hide in image so that no one can able to access the data.

6.1.2 Less time required:

Data is splitted into number of parts so that time required to download that part is less.

6.1.3 Data recovery:

One of the server gets failed data is recoverd from other server.

6.1.4 User-Friendly:

Accessing speed is faster.

6.2 Limitations

Minimum 3 personal computers are required.

7. CONCLUSION

Due to lack of security related to data sharing in existing system, This system 'StegTorrent using de-clustering of data' with the help of Steganography is being proposed. This system helps users to upload/download files with more speed and securely. If any third party user trying to catch the data they will not get whole data from one server. The data which he get will be in the hidden form. So, it will not be easy to hack information. At the same time when any of the server gets failed, user can retrieve the data from another server.

Server failure do not causes the failure in data transfer. As the number of servers available and the data transferring is simultaneous process on all the available server the system performs its task in minimum amount of time. As tall the requirements of the users are full filled with help of this system,this system is more user friendly.

This project helps for organization, As the demands for highly secure and high speed data increasing rapidly.

8. ACKNOWLEDGMENT

We would like to thank the entire department of Information Technology Engineering for their sincere guidance and continuous motivation and support to gain superior degree of knowledge in the vast domain of Information Technology. We are very thankful to our project guide who supported us and guided us to implement this project with great success. Also thankful to all teachers who motivated us to achieve this goal.

9. REFERENCES

[1] Analysis of LSB based image steganography techniques:-Published in:Image Processing, 2001. Proceedings. 2001 International Conference on (Volume:3)Date of Conference:2001

[2] AN OVERVIEW OF IMAGE STEGANOGRAPHYT. Morkel 1, J.H.P. Eloff 2, M.S. Olivier 3Information and Computer Security Architecture (ICSA) Research GroupDepartment of Computer Science University of Pretoria, 0002, Pretoria, South Africa

[3] THE BITTORRENT P2P FILE-SHARING SYSTEM: MEASUREMENTS AND ANALYSIS *J.A. Pouwelse, P. Garbacki, D.H.J. Epema, H.J. Sips* Department of Computer Science, Delft University of Technology, the Netherlands j.a.pouwelse@ewi.tudelft.nl

[4] Reversible Palette Image Steganography Based onDe-clustering and Predictive CodingHsien-Chu Wu1, Hui-Chuan Lin2 and Chin-Chen Chang3

[5] Chained Declustering: A New Availability Strategy for Multiprocssor Database machines by Hui- I Hsiao and David J. DeWitt

[6] A Modified High Capacity Image Steganography Technique Based on Wavelet TransformAli Al-Ataby1 andFawzi Al-Naima2

[7] "Stegtorrent Using Data De-Clustering"MurkuteReshma, Pattiwar Nikita, ShereShalaka, ThombareNalini,Student,Department of Information Technology, MMIT, Lohgaon, Pune, Maharashtra, India

[8] StegTorrent: a Steganographic Method for the P2P File Sharing Service PawełKopiczko, WojciechMazurczyk, Krzysztof SzczypiorskiWarsaw University of Technology, Institute of TelecommunicationsWarsaw, Poland

[9] S. Hand, T. Roscoe, "Mnemosyne: Peer-to-Peer SteganographicStorage", Proc. of IPTPS 2002, LNCS 2429, pp. 130–140, 2002.

[10] R. Anderson, R. Needham, A. Shamir. "The Steganographic File System," Proc. of International Workshop on Information Hiding, 1998.