International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Implementation of Encryption and Decryption Technique

Dayanand G Savakar[1], Anand S Ghuli[2]

[1]Rani Chennamma University, Belagavi

[2]BLDEA's Vachana Pitamaha Dr. P.G.Halaktti College of Engg. & Tech, Bijapur

Abstract: ***An application is to secure the all files from different users. It is concerned with encrypting the information in most secure and robust manner. It also includes the algorithm that convert the given text data into different form. This project also includes the good key generation that secure the given file from malicious users. This project allows the users to encrypt there important files from various other users. It gives immense security from the harmful users. File Encryption includes Audio Encryption, Video Encryption, Image Encryption and Text File Encryption. Information Hiding of this project includes Watermarking And Steganography to hide the information in the image. Watermarking include key generation to secure the text from other users. Steganography includes the mechanism to convert the data into another based on some Algorithm.***

Keywords: Network, Encryption, Security, Decryption, classification

1. Introduction

Protective piece of the action are the great start for protecting the computer, but providing a mechanism when a gainful offence hits is also equally significant. The major aim of this web application is to provide a solution from the attacks of other users to the files. It provides a security from various users to the computer. It protects your file from being harmed by the other people. Today Encryption techniques are used by various businessman and also the common computer users to hide the data from various evil users. However this technique could be burden to the user if he forgot his generated private key. The prime advantage of file encryption is that even if you are about to loose your computer or laptop, or get attacked by noxious malware or if your laptop is hacked, the content inside your laptop is still safe. Encryption of files help the one last saving grace, the data may be not be present in your computer but it will not allow the other one also to use it. Encryption gives an extra additional layer of security to make you feel secure even if your laptop is stolen. Information hiding is the mechanism for protecting the given content of data from modification. It reduces software development risk by depending on the key generation technique. File Encryption is the better easy and efficient style for accomplishing data security. To glance an encrypted file, you must approach the secret key to decrypt it. It is the process of hiding the text file details. The hiding of these details results in abstraction, it helps to lower the external complexity and make the function easy to use.

2. Review of Literature

Presently some forms of offers only temporary protection to the files. These could be easily ruptured with correct and appropriate program e.g former ZIP extract file or word evidence file. Part of the encryption applications are very complicated for routine users and it may allow to terminate them clumsily. Previously the existence of encryption programs and encypted files attracted SUSPICION to protect the file whereas the non-encrypted system did not attract that level of interest. The Existing System did not provide key generation techniques for securing data.

Before developing any software it is significant to consider time constraint, budget and stamina of a company. These activities are analyzed in this stage. At start, we need to find out the defects of the current setup and analyze how well they are solved to meet the requirements of organizations. Once we get clear idea on the basic needs of resulting framework, it is necessary to evaluate the means that best suits it. Finally, the last step is to check whether the system is feasible w.r.t various perspectives.

The method [1], witness's huge notice and a wealth of assure in content-based image recovery as a rising technology. It also a horizontal way for a huge number of new techniques and systems, get various new citizens include. In this piece, we survey almost 300 new hypothetical and experimental charity in the existing decade related to image recovery and regular image clarification. We also discuss significant challenges involved in the difference of existing image recovery techniques to build systems that can be useful in the genuine world. In retrospect of what has been achieved so far, we also work out what the prospect may hold for image recovery study.

Predictable methods [2] of image revival require that metadata is connected with the image, usually known as keywords. Though some content based image retrieval systems utilize together semantic and prehistoric attributes to relation search principle, history has proven that it is tricky to remove linguistic in sequence from a 2D picture. In this observe, activity theory is used as a foundation to express how semantic in sequence can be retrieved from objects recognized in a picture. Via an picture segmentation method.
By The Berkeley Digital Library Project, and merge it with, a high-level accepting of he picture can be established Content-Based Image Retrieval [3] has become one of the popular most research areas. Many diagram attribute representations contain been explored and many systems build. While, these

research information found the foundation of satisfied based image recovery, the kindness of the future approaches is incomplete. Specially, these efforts have comparatively overlooked two different characteristics of systems the space between towering level concepts and low level skin texture bias of human compassion of visual content. Which electively takes into account the above two uniqueness in CBIR. During the recovery process, the user's high level query and insight partisanship are captured by dynamically updated weights based on the user's advice. The provisional results over more than 70,000 images show that the future approach greatly reduces the user's effort of composing a doubt and capture the user's in sequence.

Application feedback [4] scheme based on support vector equipment have been generally used in content-based image retrieval. However, the arrangement of based application criticism is frequently abridged when the figure of labeled positive advice sample is little. This is mostly due to three reasons a classifier is disturbed on a little sized teaching locate, and over suitable happens since the number of characteristic dimensions is much senior than the size of the preparation set. In this document, we expand a device to overcome these troubles. To speak to the first two troubles, we propose an asymmetric container based. For the third problem, we combine the random subspace method and SVM for application feedback, which is named random subspace SVM (RS-SVM). Finally, by AB-SVM and RSSVM, an asymmetric bag and accidental subspace SVM (ABRS-SVM) is build to solve these three problems and further improve the application feedback performance. Some researchers used Image processing techniques for security[5][6] and for agriculture and horticulture produce[7][8].

3. Proposed System

Our new proposed system has the capability to overcome all the drawbacks of the existing system where all individual problems and issues are checked continuously. It has the capability to collect and store all the types of solutions to the given problems and by doing this we can further try to understand and reduce the rising regular problem. The goal of this web application is to provide the good quality of service and give better satisfaction to the customer. The aim of this new implemented web based application is to provide very quick and instant solution to the problem and provide better services to the problem.

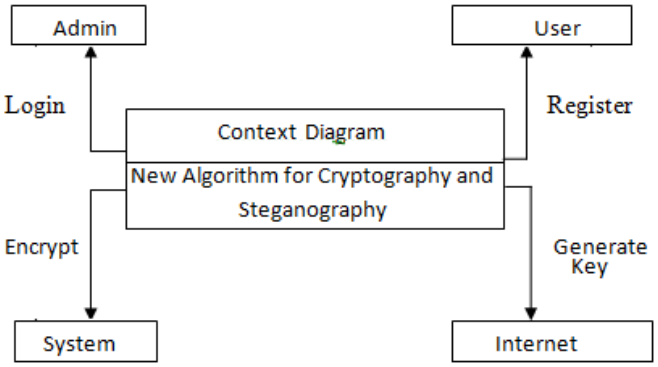
In this Feasibility study we can determine if or not a project is working correctly. This action ensue by making this indomitability is called a Feasibility Study. The chief objective of this feasibility course is to objectively and rationally uncover the strengths and weakness of existing problems or proposed problems. It is used to check whether there are any threats that can stop the running process of the system. The well designed Feasibility study should be able to provide all of its historical background of the project. Once it has been understood that project is feasible then keeping all of the advantages of the companies in mind, the user can go ahead and prepare the specification for the given , which finalizes the requirements of the project. Various different form of feasibility test are studied during the project investigation.

This is concerned to specify equipment and software for successfully satisfying the requirements of user. It determines whether or not a system can actually be constructed or upgraded to solve the problem. To regulate whether the contemplated system is mechanically feasible, we let consider the vocational matter that are muddled within the organization. Web based technology are used within this web application. Today the without the internet is incomprehensible.. This is applied to proposed system technically.

The main aim of Economic feasibility is to determine which are the positive economic benefits to the organization that will be provided by the proposed system. It must include all the benefits and advantages of identification and quantification expected. It mainly includes cost/benefit analysis.

Feasibility factors are as follows:

- Cost benefits analysis along with market analysis must be performed by product manager for the good assessment of a software and it should be fraction of the global expediency study.
- Returns can be done in long turns.
- It has low cost of subsistence.
- Proposed system is economically viable. The reason for this is, as the cost of overall functionalities is less than the usability. The proposed system can be used for longer periods.
- Full systems investigation does not require any additional extra cost.
- Basic Hardware and Software helps to run your applications smoothly with the available necessary tools.
- It provide you the benefit charging minimum cost with zero errors. It also reduces the manual work.
- If the system is used with minor changes in it, no extra costs would be added.
- Operational feasibility is used to determine how the proposed system provide solutions to the problem and take benefits from the opportunities which were diagnosed in the interim of the area definition and by what means it gladdens the essentials identifies in system development facet of requirement analysis. The users have to be convinced about the new advantages of the proposed application. The new proposed application must be user friendly and flexible to the user.
- Any new changes within the proposed application is made very easily and efficiently.
- It is one of the important aspect of software engineering which is the main part of the system design process.
- This proposed web application is operationally feasible. As this application is built with graphical user interface (GUI). Hence a user having a very less knowledge of computers can also be understand and get needed information from this application.



Implementation is the phase of carrying out the plan, execution of a method, design an plan, idea, for specifying standards and policy for doing something. It is the action that needs to prepare for main action or event thinking in order for something to really happen. In this phase the theoretical design are put into a real system. After the completion of the theoretical design the main aim of this phase is to convert the code of the system design into programming language platform. Building the system design in the best possible way is the main purpose of this phase. It may be considered as a blue print with the various defined set of rules views to get users and organization for running a precise and clear software product. The requirements of the proposed system is the main thing that needs to be successfully fulfilled by the code user during implementation phase. Both testing and maintenance are affected in this coding phase. It cost more than the hardware and software requirements affecting both testing and maintenance cost and consumes up to 1/3 an estimate of income of a software purchase. It is the responsibility of the coding phase to reduce work of testing and maintenance. Hence, during the process of coding phase the main aim should be to focus should be to systematically structure the easy understandable programs but not to develop the programs that can be easily implemented.

In present setup, there is a lack of identity privacy for users of the crew. If there is no identity then it's meaningless to say that the system provides security. Other scheme involves partaking of data files with single owner who acts like an admin. Here the members of the gathering are not allowed to use the resources directly. If each participant of the working party wants to upload or download the material then he must send request to the authorized person. The person in charge (admin) will then check the user list; if present he will accept the request and send message to send the materials to be sent to or retrieved from the storage. The manager then transmits the data to cloud. This is time consuming task and doesn't work effectively. As new members enter into or exit from the gathering there is a change in membership, in this situation providing security and confirmation of safe data sharing is critical. So the existing schemes are not feeding the fruitful results.

The intended system is a complete description of solution to the problems raised in current plan. This new setup gives you a shielded scenario for information sharing by offering with two keys, one is group key and other is file key to decrypt the encoded form of data. At first, it prompts secure transport of key means providing protected approach to key dispersion with safer correspondence channels, so that the workers can receive their key safer way, from the administrator. Secondly, it will accomplish fine access to data files, it implies that members in crew are allowed to use the data stored in cloud, by maintaining group member list and the renounced one cannot be permitted to access the resources if they are denied. Third, it can attain data privacy i.e. data reserved in cloud must not be in readable format by unauthorized people with inclusion of cloud, so information is encrypted before transmitting it to cloud storage. Fourth, the system can provide safe sharing of data files that can be saved from collusion attacks. The denied member's aren't capable of getting the original document once those people are revoked by crew head even if they are in link with the untrusted cloud. At last, it can control dynamic sets effectively which indicates that when a new member is added to or deleted from the group, the keys of other categories need not to be upgraded. Thus the proposed scheme overcomes all the obstacles of present system.

4. Conclusion

File encryption and Information Hiding is the is complicated solution that helps to secure the many file types like audio, video, images and text files. These practices are today used by many of the companies, industries , college faculties , hospitals for securing data from the unauthorized user. This proposed system involves all those necessary that are needed to handle all the request made by the users. It includes all those capabilities from protecting the private data to hiding of information in different forms. It contains the key generation mechanism which will make your system robust. Steganography is the technique that makes of the algorithm for converting the plain text to the cipher text. Admin has the ability to add the new users and also has the power to remove those users who are vulnerable to the applications. It supports various tools and techniques that can be implied in future enhancements.

The scheme is targeted mainly for facilitating the crew users to share their documents among their network in safeguarded approach. The users can receive their key safely from an authorized person. Strong control on accessing of resources is achieved by allowing only members of crew to utilize the cloud and the denied ones are not capable of getting the materials. The end-users can freely reserve their data even though the cloud is untrustworthy because the data is stored in an unreadable format. Thus preserves data from unauthorized access. Hence the scheme guarantees the required security concerns and is well efficient.

5. Future Enhancement

Each of the designed module is independent to each other from this project. New modules can be added to the proposed system whenever necessary. Each and every attempt had been made to ensure the system functionality and performs effectively and efficiently. The system is flexible and has been tested with simple data to check if any errors occurs and all outputs are also checked. Further modification to this package can be easily applied. All the

projects that have been developed by the use of various technology must have future enhancements.

The following enhancements can be done to File encryption and Information hiding

- User can add their own data.
- Recovery of passwords.
- Recovery of file name.

All the objectives that were given by the user in the requirement analysis has been met in this developed application. Still, if there are some of the objectives that are not correctly implemented and if they have been missed out that were developed in analysis phase they can be implemented in further development.

References

[1] R. Datta, D. Joshi, and J.Z. Wang (2007), "Image Retrieval: Ideas, Influences, and Trends" ACM Computing Surveys, vol. 40, article 5

[2] A.W.M. Smeulders, M. Worring, S. Santini, A. Gupta, and R. Jain (2000),"Content-Based Image Retrieval," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 22, no. 12, pp. 1349-1380

[3] Y. Rui, T.S. Huang, M. Ortega, and S. Mehrotra(1998), "Relevance Feedback: A Power Tool for Interactive Content-Based Image Retrieval," IEEE Trans. Circuits and Systems for Video Technology, vol. 8, no. 5, pp. 644-655

[4] X.S. Zhou and T.S. Huang (2003), "Relevance Feedback in Image Retrieval: A Comprehensive Review," Multimedia Systems, vol. 8,pp. 536-544D.G.Savakar, Anand Ghuli (2015), "Digital Watermarking A Combined Approach by DWT, Chirp-Z and Fast Walsh-Hadamard Transform", IJCTA, Vol. 5 No.6, pp 2006-2010.

[5] D.G.Savakar, Anand Ghuli (2015), "Digital Watermarking as a distributed noise by Discrete Wavelet Transformation, Fast Fourier Transformation and Fast Walsh-Hadamard Transform to study the sensitivity between Robustness and Fidelity", IJCA, Issue 1, Volume 5, pp 102-107

[6] Dayanand G. Savakar (2012), Identification and Classification of Bulk Fruits Images using Artificial Neural Networks. International Journal of Engineering and Innovative Technology (IJEIT), Volume 1, Issue 3, Pages: 35-40

[7] Dayanand G. Savakar (2012), Recognition and Classification of Similar Looking Food Grain Images using ANN, Journal of Applied Computer Science and Mathematics ,Volume 13(6), Pages: 61- 65