

**MIT SCHOOL OF ENGINEERING Department of Computer Science and Engineering**

MINI PROJECT

**Project Title:** **CONFIDENTIAL IMAGE**

1. Abstract of the Project…………………………………………………………… 1
2. Introduction of the Project……………………………………………………….. 2
3. Problem Statement………………………………………………………………. 3
4. Feasibility Analysis of the Project………………………………………………. 4
   1. Technical Feasibility………………………………………………………… 4
   2. Operational Feasibility………………………………………………………. 4
   3. Economic Feasibility………………………………………………………… 5
   4. Schedule Feasibility…………………………………………………………. 5
5. Requirements of Project…………………………………………………………. 6
6. Block Diagram of the Project……………………………………………………. 7
7. Literature Survey of the Project…………………………………………………. 8
8. Code of the project………………………………………………………………. 9
9. Result of the Project…………………………………………………………….. 10
10. Future Scope, Limitations and Conclusion of the Project……………………….. 11
11. Bibliography……………………………………………………………………... 12

Gantt Chart……………………………………………………………………….

**ABSTRACT**

Data security is a major issue which we are facing in this digital world of communication. As we know that today hackers are almost at every corner in search of our useful data which can be hacked by them for their different purposes. Even the risk gets doubled when come to the data of any country’s government. So, a system or terminology is must required to make that data safe forever by any means during communication.

Data protection can be accomplished by changing the original image by any means to some other un useful data so that if someone gets that image then also it must remain in un useful bits. This process can be achieved by Encrypting that data by some means of algorithms which are known to the sender and the similar Decryption algorithms to be known to only the desired receiver so that it can convert that encrypted data back to the user understandable form. Today as it is a need to develop such kind of applications which performs the specified task but along with it should be very much user friendly so that no special skills need to be required to learn in order to use that application or project.

In this application the user has to select the image to send something by encrypting or wants to receive by decrypting. If it wants to send then it have to select the image which is to Encrypt and then transfer. Whereas on the receiver side again the receiver have to select the image which is to be received from the sender along with a decryption key which is embedded within the code to decrypt the image thus, the receiver will need the same code to decrypt the image this will make the process of image decryption much faster and convenient for the user.

# INTRODUCTION

The Project is based on – “Confidential Image”

Security of data/images is one of the most crucial aspects in the gigantic and still expanding domain of digital transfer. Our product satisfies a large customer base and has therefore cleared the market acceptability test.Image Encryption enables businesses to securely share confidential and sensitive data with their clients.

This project will be helpful to the companies who have some confidential information in the form of image. So, that their information can be protected by hackers. It will be helpful in reducing the frauds and crimes such as blackmailing.

The image encryption can save one’s confidential data from getting hacked. Also, some important images or blueprints related to the top secret projects of the companies are also been protected from getting exposed or been hacked.Unauthorized access can be prevented by encrypting images and converting them into a secret code.

FEASIBILITY STUDY

A feasibility study is a preliminary study which investigates the information of prospective users and determines the resources requirements, costs, benefits and feasibility of proposed system. A feasibility study takes into account various constraints within which the system should be implemented and operated. In this stage, the resource needed for the implementation such as computing equipment, manpower and costs are estimated. The estimated are compared with available resources and a cost benefit analysis of the system is made. The feasibility analysis activity involves the analysis of the problem and collection of all relevant information relating to the project. The main objectives of the feasibility study are to determine whether the project would be feasible in terms of economic feasibility, technical feasibility and operational feasibility and schedule feasibility or not. It is to make sure that the input data which are required for the project are available. Thus we evaluated the feasibility of the system in terms of the following categories:

* Technical Feasibility
* Operational Feasibility
* Economic Feasibility
* Schedule Feasibility

## 3.1 Technical Feasibility

Evaluating the technical feasibility is the trickiest part of a feasibility study. This is because, at the point in time there is no any detailed designed of the system, making it difficult to access issues like performance, costs (on account of the kind of technology to be deployed) etc. A number of issues have to be considered while doing a technical analysis; understand the different technologies involved in the proposed system. Before commencing the project, we have to be very clear about what are the technologies that are to be required for the development of the new system. Is the required technology available? Our system is technically feasible since all the required tools are easily available. Java can be easily handled. Although all tools seem to be easily available there are challenges too.

## 3.2 Operational Feasibility

Proposed project is beneficial only if it can be turned into information systems that will meet the operating requirements. Simply stated, this test of feasibility asks if the system will work when it is developed and installed. Are there major barriers to Implementation?

The proposed was to make a simplified web application. It is simpler to operate and can be used in any webpages. It is free and not costly to operate.

## 3.3 Economic Feasibility

Economic feasibility attempts to weigh the costs of developing and implementing a new system, against the benefits that would accrue from having the new system in place. This feasibility study gives the top management the economic justification for the new system. A simple economic analysis which gives the actual comparison of costs and benefits are much more meaningful in this case. In addition, this proves to be useful point of reference to compare actual costs as the project progresses. There could be various types of intangible benefits on account of automation. These could increase improvement in product quality, better decision making, and timeliness of information, expediting activities, improved accuracy of operations, better documentation and record keeping, faster retrieval of information.

This is a web-based application. Creation of application is not costly.

## 3.4 Schedule Feasibility

A project will fail if it takes too long to be completed before it is useful. Typically, this means estimating how long the system will take to develop, and if it can be completed in a given period of time using some methods like payback period. Schedule feasibility is a measure how reasonable the project timetable is. Given our technical expertise, are the project deadlines reasonable? Some project is initiated 10 with specific deadlines. It is necessary to determine whether the deadlines are mandatory or desirable.

A minor deviation can be encountered in the original schedule decided at the beginning of the project. The application development is feasible in terms of schedule.

## Requirement of Project

**Hardware and Software Requirements of Project:**

**Hardware Requirement:**

Here is the recommended hardware requirement for this software to run efficiently.

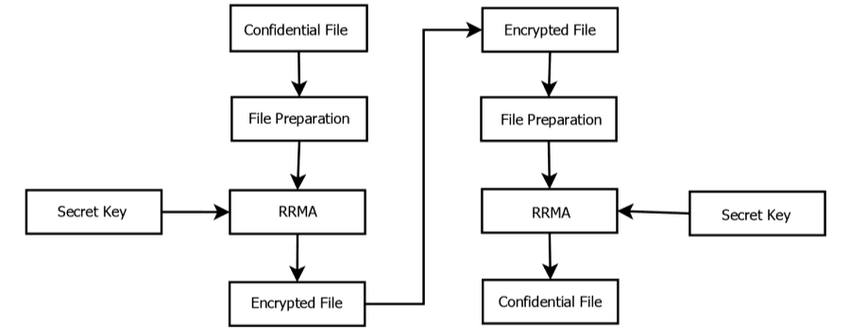
1. CPU: 2 x 64-bit 2.8 GHz 8.00 GT/s CPUs
2. RAM: 32 GB (or 16 GB of 1600 MHz DDR3 RAM)
3. Storage: 300 GB. (600 GB for air-gapped deployments.) Additional space recommended if the repository will be used to store packages built by the customer. With an empty repository, a base install requires 2 GB.
4. Internet access to download the files.

**Software Requirement:**

Here’s the necessary software requirements for the application to run –

1. 32- or 64-bit computer.
2. For Java ---Minimum 3 GB disk space to download and install.
3. Windows, macOS, or Linux.
4. For Windows: Windows 8.1 or newer for Java, or Windows Vista.

### BLOCK DIAGRAM



## LITERATURE SURVEY

**A. A New Combined Symmetric Key Cryptography CRDDBT Using – Relative Displacement (RDC) and Dynamic Base Transformation (DBTC) 2013.**

This paper [21] focused a new technique of encryption without a predefined key. The input string is fragmented into several parts, with each part encrypted using a different algorithm. On the whole, three unique algorithms have been applied to encrypt the fragmented string on the basis of its orientation. For higher security levels, the key is derived from the two differently determined keys. The salient feature of this algorithm is that, a part of string is manipulated using base conversion, second part of string is deformed by interchanging position and increasing number of repetitions. time taken for encryption time taken for encryption.

**B. New Image Encryption Technique Based On Combination of Block Displacement and Block Cipher Technique 2013.**

In this paper [20], a new image encryption algorithm is proposed. It is already known that security of the algorithm is depended on the length of the key that mean longer key length will always support to good security feature and proposed algorithm used 128 bits key length which is provided too much security for the proposed algorithm. To access original key or crypto analysis of the proposed key is required 2128 time to break the key which is almost impossible for any hacker. There is no chance to generate floating point error because no such types of mathematical formula have applied on the proposed algorithm. The correlation co-efficient as well as their entropy values for the proposed algorithm was calculated.

**C. Image Encryption based on the RGB PIXEL Transposition and Shuffling 2013.**

This paper [19] proposed a technique of transposition and reshuffling of the RGB values of the image in steps has proven to be really effective in terms of the security analysis. The extra swapping of RGB values in the image file after R G B component shifting has increased the security of the image against all possible attacks available currently.

**D. Enhanced Color Visual Cryptography 2012.**

In this paper [18] a new algorithm is proposed. For image encryption by using sorting of pixels as per their RGB values and arranging them group-wise which helped to reduce the correlation between pixels and increased entropy value. Experimental results were taken out on Matlab 6.0.1 and this is a lossless image encryption algorithm with results. Histogram of plain image and cipher image is also carried out. Further inter pixel algorithm can be used with another confusing property to result in better image encryption technique.

**E. Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a Pixel, 2011**

This paper [17] was proposed in 2011 which focused in manipulation of RGB values of pixel and its displacement as per the predefine key. Circular shift applied on the three component of pixel with different key so that R, G and B values of pixel inter mix with the R, G, B value of other pixel which is also terms as explosive inter-pixel displacement.

**F. Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices, 2011.**

This paper [16] was proposed in 2011 which was further extension of work of Inter-Pixel displacement of the RGB attributes of a Pixel by making the 4 slices and shuffling of those slices before encryption. Slices were made from the centre of image and these four slices were diagonally inter exchanged before doing actual image encryption.

**G. Permutation based Image Encryption Technique, 2011.**

Sesha Pallavi Indrakanti and P.S.Avadhani [15] introduced an algorithm on the basis of random pixel permutation with the motivation to maintain the quality of the image. It had three phases in the process of encryption. The phase one was the image encryption. The phase two was the key generation phase. And the phase three was the identification process. This provides confidentiality to color image with less computations.

**H. Digital image encryption algorithm based on chaos and improved DES, 2009**

Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di [14] researches on the combination of image encryption algorithm like chaotic encryption, DES encryption etc. In their algorithm, for making the pseudo-random sequence, logistic chaos sequencer was used, it carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES. This algorithm had high security and the encryption speed.

**I. Image Encryption Using Block-Based Transformation Algorithm, 2008**

Mohammad Ali Bani Younes and Aman [13] introduce a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, and using the transformation algorithm it was rearranged, and then the Blowfish algorithm is used for encrypting the transformed image their results showed that the correlation between image elements was significantly decreased. Their results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

**J. An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption, 2008.**

RijnDael was introduced by Mohammad Ali Bani Younes and Aman Jantan [12] using the combination of image permutation. The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process, and then RijnDael algorithm was applied on the generated image for encryption. Their results showed that the correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved.

**K. Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm, 2008**

Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jena [11] present image encryption technique using the Hill cipher. They are generating self-invertible matrix for Hill Cipher algorithm. Using this key matrix they encrypted gray scale as well as color images. Their algorithm works well for all types of gray scale as well as color images except for those images which have background of same gray level or of same color.

## Future Scope, Limitations and Conclusion

**Future Scope:**

This project will be helpful to the companies who have some confidential information in the form of image. So, that their information can be protected by hackers. It will be helpful in reducing the frauds and crimes such as blackmailing.

The image encryption can save one’s confidential data from getting hacked. Also, some important images or blueprints related to the top secret projects of the companies are also been protected from getting exposed or been hacked.

**Limitations:**

We will experience problems using the image import or generation facilities for our own images and sounds.

**Conclusion:**

The project: Confidential Image will be completed using Java as a language.

## Bibliography

[1] http://en.wikipedia.org/wiki/Encryption

[2] <http://en.wikipedia.org/wiki/Plaintext>

[3] <http://en.wikipedia.org/wiki/Ciphertext>

[4] <http://en.wikipedia.org/wiki/Decryption>

[5] <http://en.wikipedia.org/wiki/Cryptography>

[6] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, “Multilevel Image Encryption by Binary Phase XOR Operations “, IEEE Proceeding in the year 2003.

[7] M.-R. Zhang, G.-C. Shao and K.-C. Yi, ― T-matrix and its applications in image processing IEEE Electronics Letters 9th December 2004 Vol. 40 No. 25

[8] Wang Ying, Zheng DeLing, Ju Lei, et al., ―The Spatial-Domain Encryption of Digital Images Based on High-Dimension Chaotic System, Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172-1176, December. 2004

[9] Guosheng Gu, Guoqiang Han “An Enchanced Chaos Based Image Encryption Algorithm”, IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC’06) in 2006.

[10] N.K. Pareek, Vinod Patidar "Image encryption using chaotic logistic map", Elsevier, Image and Vision Computing 24 (2006) 926–934.

[11] Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jen, Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm 1st t International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008

[12] Mohammad Ali Bani Younes and Aman Jantan, An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption, IJCSNS International Journal of Computer Science and Network Security, VOL.8, April 2008.

[13] Mohammad Ali Bani Younes and Aman Jantan Image Encryption Using Block-Based Transformation Algorithm IAENG International Journal of Computer Science, 35,2008.

[14] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan , Dai Wei-di, Digital image encryption algorithm based on chaos and improved DES, IEEE International Conference on Systems, Man and Cybernetics, 2009.

[15] Sesha Pallavi Indrakanti, P.S.Avadhani, Permutation based Image Encryption Technique, International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011.

[16] Amnesh Goel, Reji Mathews & Nidhi Chandra, "Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices", International Journal of Computer Applications (0975 – 8887), Volume 36– No.3, December 2011.

[17] Reji Mathews, Amnesh Goel, Prachur Saxena & Ved Prakash Mishra, "Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a PIXEL", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA. ISBN: 978-988-18210-9-6.

[18] S.Bosu Babu & S.S.P Kumar “Enhanced Color Visual Cryptography” Engineering Science and Technology: An International Journl, , ISSN: 2250-3498, Vol.2, No. 5, October 2012

[19] Quist-Aphetsi Keste, “Image Encryption based on the RGB PIXEL Transposition and Shuffling” I.J.Computer Network and Information Security, 2013,7, 43-50,2013.

[20] Keerti Kushwah, Sini Shibu “New Image Encryption Technique Based on Combination of Block Displacement and Block Cipher Technique,” International Journal of Computer Science and Information Technologies, Vol. 4 (1), 2013, 61 - 65