Journal of Applied Computer Science & Artificial Intelligence

Research Paper Vol.-3, Issue- 1, June 2022 ISSN: 2582-8673

FILE ENCRYPTION AND DECRYPTION SOFTWARE USING JAVA

Ira Nath[1], Anupam Dutta[2], Subhranil Mazumder[3], Birottam Biswas[4] , Ritesh Saha[5]

[1,2,3,4,5] JIS College of Engineering, Kalyani, Nadia

Available online at: http://jacsai.org/

Received: ……../2021, Revised: ……..2021, Accepted: ……2021, Published: 30/June/2021

Abstract— We are living in a digital era and the majority of things we are doing digitally by using various digital mediums and devices. Nowadays, it is very common to have important data as a digital copy like .pdf and .jpeg or.png format. We usually sent digital media through email for doing different works but, sometimes we have to provide confidential documents or data in photo or pdf format to someone, in this process the main problem is data security. If highly sensitive digital data get into the hands of someone who shouldn't have it, it can be a nightmare for any company. That's why the company can lose a lot of money. This research paper represents a very useful and secure concept for enhancing the security of digital files. The proposed concept will work on top of the traditional encryption and decryption technology and it provides an extra layer of security.

Keyword— Security, Encryption, Decryption, Data, Pdf, Png, Confidential documents

I. INTRODUCTION

Security is the main concern in today's digital world. Most of the things done by us and our organizations are in the form of digital format. Nowadays it is very common to use digital photographs and documents for many official and legal purposes and most of the time these documents are very critical and classified for the owner of that documents. Nowadays digital photographs are playing a very important role as evidence of any occurrences which can be used as major proof in our judiciary system. Even some digital information like blueprints of any project, and account log/transaction files are very important for both persons and enterprises. It will be very harmful for the organization and the persons if those classified documents get into the hands of any other unwanted person. Let's assume a situation where a photograph is playing a vital role in giving a judgment on any judicial case. If that photograph is accidentally accessed by any accused and then tempered, in that case, the actual accused who actually may be associated with any illegal activities would be released due to insufficient proof. For preventing that tamper with that photograph, the handler should encrypt that photograph and only decrypt it when in front of the judge. So, for the security of the digital files, we need a system that can be able to encrypt that file and decrypt that file when the actual owner of that file needs to access that information. For that stated purpose, in our research paper, we have developed software using java that can encrypt files by using a key provided by the owner of the file. This system will filly change the internal bytes of the digital file provided by the owner and make that file unreadable in any traditional digital document reading software. Only those who have the key and the appropriate software developed can able to decrypt that encrypted file and read the content of the file.

II. RELATED WORK

Earlier in the year of 2015 A. Manimaran, V. M. Chandrasekaran, Arnav Bhutani, and Vansh Badkul published a paper named "A New Approach for Encryption and Decryption" in the "Research J. Pharm. and Tech" [1], they proposed the method to encrypt the message by using ASCII table and decimal to quaternary conversion. In the year 2017 Ekta Agrawal, and Dr. Parashu Ram Pal published a paper named "A Secure and Fast Approach for Encryption and Decryption of Message Communication" in IJESC [2], they proposed the method is based on the number of characters in the message and simple calculation and operation performed to minimize the execution time. After that, in 2020 Devavrat Agnihotri, Saad Ahmed, Dhanashree Darekar, Chinmay Gadkari, Sagar Jaikar, and Mohandas Pawar published a paper named "A Secure Document Archive Implemented using Multiple Encryption" [3] in "International Conference on Smart Electronics and Communication" in their research work they proposed the methodology for securing the digital document files. In 2010, Gang Hu published a research paper named "Study of file encryption and decryption system using security key" [4] in "2nd International Conference on Computer Engineering and Technology". The proposed method is based on the file encryption technique using the USB security key. In 2013 V.

Kapoor published a research paper named “Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and ‘n’ prime Number” [5] in “International Journal of Scientific Research in Network Security and Communication”, the proposed method was based on RSA algorithm which eventually adds some feature over the RSA algorithm. In 2017 P. Thakkar, H.K. Mishra, Z. Shaik, and D. Sharma published a research paper named “Image Encryption and Decryption System Using AES for Secure Transmission” [6] in “The International Journal of Computer Sciences and Engineering”, in their research work they proposed an encryption methodology for images by using AES. In the year 2021 Pronika, S. S. Tyagi published a research paper named “Performance analysis of encryption and decryption algorithm” [7] in “Indonesian Journal of Electrical Engineering and Computer Science”, in their research work they analyzed the performance of different encryption and decryption methods. In 2022 Renusree Varma Mudduluri, Akhila Golla, Sushanth Raghava, Tammana Jyothi Sai Tyagi published a research paper named “Advanced Image Encryption & Decryption using Rubik’s Cube Technology” [8] in “International Journal of Engineering and Advanced Technology (IJEAT)” in their research work they proposed a new image encryption methodology by using Rubik’s Cube Technology.

III. METHODOLOGY

In the proposed research paper, we have proposed a method to encrypt any document file. In this research work, we have developed software where a technique is used to encrypt digital documents and photographs at the byte level of the files. The first step is to select the document file from the software and provide the key-value which will work as a password by the user. The software initially converts the whole file into an array of bytes. The proposed software will perform the XOR operation with each element of the byte array and the given Key value. As a result of that process now the actual bytes which are responsible for representing the whole digital file have been changed, so now, the file which is generated by the software is unreadable. When any XOR operation takes place between two variables then the output will generate and again if we perform that XOR operation with the result/output file and any operand used previously for getting the result file, then the system will provide another operand used while encrypting the data. While the process of decrypting the encrypted file is selected from the software and then the receiver has to give the key value as same as given to the user. While creating that file. If the receiver provides the same key value provided by the users, then again, the software performs the XOR operation, and due to that, we will get the actual readable document file.

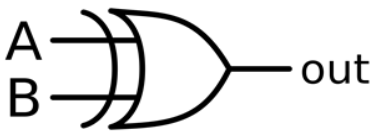

Figure 1. XOR Gate

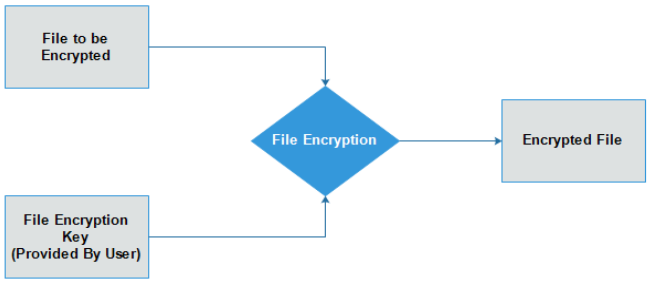

Figure 2. File Encryption Workflow Diagram

To do the encryption first you have to open the application, then enter your password after that you have to select the file or image which you want to encrypt. The application converts the file or image into an array of bytes then each element of the array index is being XOR with the given password.

XOR		
Input	Input	Output
0	0	0
0	1	1
1	0	1
1	1	0

Table 1. XOR Gate Truth Table

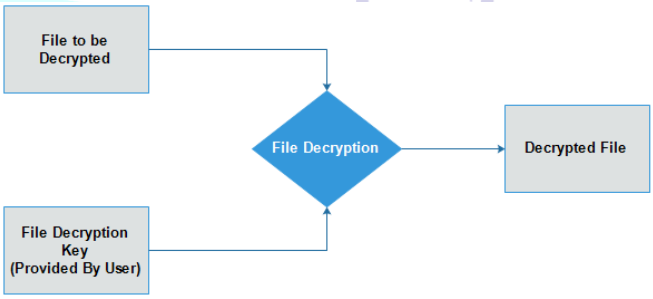

Figure 3. File Decryption Workflow Diagram

To do the decryption first open the application then enter the same password which is used to encrypt the file or image, then select the encrypted file for decryption after that the application converts the encrypted file or image into the array of bytes then each element of the array index is being XOR with the given password. The file or image will be decrypted and protected.

Encryption is all about protecting the data from the unwanted person like cybercriminals, the encryption process leads to making encrypted data so that without the valid key any other person who is not supposed to access that encrypted file will not be able to access that file. In today's digital era everything is now digitalized, all of our details and many important files are not only kept in the physical paper format,

most of that file has now digital existence also, security of that digital data is a prime concern.

There are lots of encryption processes and technology used in markets right now, but Our Main concern is to provide security to the most important files like a blueprint of any project, important files, etc. Our proposed method and software can be used as a parallel encryption process with the traditional encryption paradigm, for an example, we can consider a situation let's think that your Gmail account is being hacked by your colleague or

any unknown people and you lost your access from the very important content and files saved in the Google Drive, now as you uploaded any kind of important PDF or Picture document in its own readable format so that, who has hacked your account can access that file and read that file easily. In this case, your important information will get public.

We proposed a method through which you can first encrypt your file by using a key provided by you and then you can upload that encrypted file to Google Drive for long-term storage, now in this case if any unwanted public gets access to your Gmail account and still want to access your Google drive then that unwanted public will only get the encrypted & unreadable file without the key provided by you that public will not be able to decrypt that file easily. Our proposed concept will work underlying our current technologies used in markets globally without creating any problems.

Encryption Process Algorithm

Step 1: Open the application.
Step 2: Enter the password
Step 3: Select the file for encryption.
Step 4: Initially the application converts the image or document file into the array of bytes, then each element of the array index is being XOR with the password value given by the user.
Step 5: The output encrypted file will be generated.

Decryption Process Algorithm

Step 1: Open the application.
Step 2: Enter the same password used for encryption purposes.
Step 3: Select the encrypted file for decryption.
Step 4: Initially the application converts the encrypted image or document file into the array of bytes, then each element of the array index is being XOR with the password value given by the user.
Step 5: The output decrypted file will be generated.

IV. RESULTS AND DISCUSSION

Figure 4. welcome page

Figure 4 shows only the welcome page of the software.

Figure 5. Main Interface

In figure 5 the main interface page of the software will come first. In the “Enter The Key Value Here” textbox the user has to provide the encryption key. The “Clear” button is used to clear the text field whereas the “Open Any File” button is used to select the file to be encrypted.

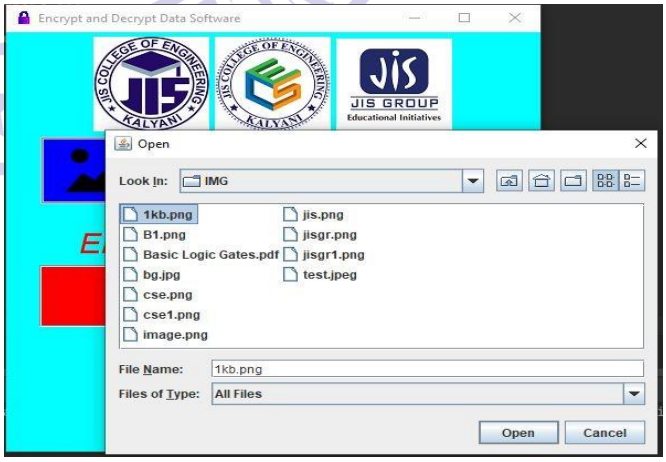

Figure 6. File Selection Window

In figure 6 The file that the user wants to encrypt must be selected from the File Selection Window.

Figure 7. Process Done page

In the figure 7, it shows the process done message which means that the intended file is being encrypted.

For Decrypting the file, the same process has to follow but at that time the user has to provide the same key used in the time of encryption and select the encrypted file.

V. Conclusion and Future Scope

In this paper, we proposed a method for encrypting digital files to maintain security and reliability. The proposed concept can be used to provide extra security to highly classified and important digital documents.
This method can be applicable underlying with the traditional encryption and decryption system.
The main objective of the work is to make our traditional encryption and decryption system more secure so that the hacking and financial threats that happen due to cyber hacking and stealing may reduce.

There are lots of future expansion and up-gradation is possible for the proposed concept. This system can be incorporated with blockchain technology and SHA256 cryptographic encryption and decryption process in the future which can create a new era for securing digital files.

References

[1] A. Manimaran, V. M. Chandrasekaran, Arnav Bhutani, Vansh Badkul, paper on "*A New Approach for Encryption and Decryption*" published in "Research J. Pharm. and Tech" Volume - 9, Issue - 12, Year – 2016

[2] Ekta Agrawal, Dr. Parashu Ram Pal published a paper named *"A Secure and Fast Approach for Encryption and Decryption of Message Communication"* Published in IJESC, Volume 7 Issue No.5

[3] Devavrat Agnihotri, Saad Ahmed, Dhanashree Darekar, Chinmay Gadkari, Sagar Jaikar, Mohandas Pawar, paper on *"A Secure Document Archive Implemented using Multiple Encryption"* in the "International Conference on Smart Electronics and Communication", 2020

[4] Gang Hu paper published named *"Study of file encryption and decryption system using security key"* in "2010 2nd International Conference on Computer Engineering and Technology"

[5] V. Kapoor, publish a paper named *"Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and 'n' prime Number"* in "International Journal of Scientific Research in Network Security and Communication", 2013

[6] P. Thakkar, H.K. Mishra, Z. Shaik, D. Sharma, published a research paper named *"Image Encryption and Decryption System Using AES for Secure Transmission"* in the program of "International Journal of Computer Sciences and Engineering", 2017

[7] Pronika, S. S. Tyagi paper on *"Performance analysis of encryption and decryption algorithm"* published in "Indonesian Journal of Electrical Engineering and Computer Science", year - 2021

[8] Renusree Varma Mudduluri, Akhila Golla, Sushanth Raghava, Tammana Jyothi Sai Tyagi paper on *"Advanced Image Encryption & Decryption using Rubik's Cube Technology"* was published in "International Journal of Engineering and Advanced Technology (IJEAT)" , year - 2022

Authors Profile

Ira Nath received the Ph.D degree in computer science and technology from the Indian Institute of Engineering Science and Technology (IIEST), Shibpur, India in 2020. She received the B.Tech. degree in computer science and engineering and the M.Tech. degree in software engineering from the Maulana Abul Kalam Azad University of Technology (formerly West Bengal University of Technology), India, in 2005 and 2008, respectively. She is currently an Assistant Professor in the Department of Computer Science and Engineering, JIS College of Engineering, India. Her research interests include regenerator placement, survivability, and routing, and wavelength assignment in translucent WDM optical networks, cybersecurity, and blockchain.

Anupam Dutta is pursuing Batchelor of Technology (BTECH) in Computer Science and Engineering from JIS College of Engineering. Kalyani, Nadia. He has completed his Diploma in Computer Science and Technology from JIS School of Polytechnic, Kalyani in 2017 & 2020. His Technical Skills are Computer Networking, Computer Hardware Maintenance, C, Java.

Subhranil Mazumder is pursuing Batchelor of Technology (BTECH) in Computer Science and Engineering from JIS College of Engineering. Kalyani, Nadia. He has completed his Diploma in Computer Science and Technology from Technique Polytechnic Institute in 2017 & 2020. His Technical Skills are HTML, C, C++ Java.

Ritesh Saha is pursuing Batchelor of Technology (BTECH) in Computer Science and Engineering from JIS College of Engineering. Kalyani, Nadia. He has completed his Diploma in Computer Science and Technology from Saroj Mohan Institute of Technology (Diploma Division) in 2017 & 2020. His Technical Skills are HTML, C, C++.

Birottam Biswas is pursuing Batchelor of Technology (BTECH) in Computer Science and Engineering from JIS College of Engineering. Kalyani, Nadia. He has completed his Diploma in Computer Science and Technology from Raja Ranjit Kishore Government Polytechnic in 2017 & 2020. His Technical Skills are HTML, C, C++, Java, SQL.