Comparison Of Graphical and Video Password Authentication System

N.Ramya[1*], N.Neelima[2], P.Mahitha[3], B.Pranathi[4]

Abstract

With the increase in the number of online services, there is a rapid growth in online information sharing and storing. This information can be very sensitive, hence requires strong security to overcome those security challenges. To ensure security of this online information, passwords were introduced. Text based password is a popular form of authentication method used since the ancient times. However, text-based passwords are prone to various attacks and security breaches. Strong text-based passwords could provide a certain amount of security. However, the fact that strong passwords are difficult to memorize often leads their users to write them down on papers or even save them in a computer file. Human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as the weakest link in the authentication chain. Graphical password is one of the alternative solutions to alphanumeric password. One of the major reasons behind this implementation is that, according to psychological studies, the human mind can more easily remember images than alphabets or digits. Even though graphical passwords have such advantages they are highly prone to shoulder surfing attacks. In order to provide much better safety systems, video authentication can be implemented.

Key Words: Graphical password, video password, security, frames, passwords, electronic health records

DOI Number: 10.14704/nq.2022.20.8.NQ44236 **NeuroQuantology 2022; 20(8):2154-2160**

Introduction

There are numerous security challenges that are being faced by humans who store their data online[1]. Passwords play a vital role these days. There are various types of passwords currently existing. Some of them are alphanumeric passwords, graphical passwords, OTP generated passwords, captcha based passwords and video passwords etc. Alphanumeric passwords are widely used authentication schemes till date. But, they have their own set of problems like picking up the short passwords can be a risk, storing them at vulnerable places degrades the security[2]. Whereas long passwords are not easy to remember. There are studies that prove that human minds tend to remember images or videos more easily than texts. The proposed work in this paper is to develop a web application which acts as an electronic health record system that can store all the medical reports of a user. To identify the efficient one between graphical password and video password, both the types are developed and integrated with the e-healthcare application separately. A graphical password is a type of password that excludes numbers, alphabets, special characters and is based on images. Whereas a video authentication system uses a video as a password[3].

The both passwords are compared in terms of their security. We choose an efficient and secure approach by comparing both sorts of passwords.. The graphical password is implemented using the image segmentation technique whereas video password is implemented using the region of interest (ROI). The application is deployed in the cloud to provide easy and secured access to the user[4].

Corresponding author: N.Ramya
Address: [1,2,3,4] Information Technology Velagapudi RamaKrishna Siddhartha Engeering College, Vijayawada, India
E-mail: ramyanekkalupu777@gmail.com[1], gandhaneelu@gmail.com[2], mahi.patchava123@gmail.com[3], Pranathipriya776@gmail.com[4]

Background

The proposed work has been done by taking references of some studies and existing works. There are different ways in which graphical password and video password can be implemented in order to provide authentication to the applications.

One such method is improving the memorability of system-assigned recognition-based passwords[5]. This work examines the technique to increase password memorability that includes a scientific concept of long-term memory. This paper mainly focused on the system- assigned keywords and images related to those keywords. This is somewhat a sort of complex technique. The other technique of graphical password authentication is the method 'HOPE'[6]. The method 'Hope' works on the idea of combining several images in one picture, in order to confuse the attackers. Another technique to implement a graphical password is by using Video Captcha [7]. Video Captcha was primarily used as a graphical password to differentiate computers and humans apart. It indirectly saves applications from DDOS attacks which are computer based attacks. A survey on different types of recognition-based graphical password algorithms and the common security threats of those systems were analyzed using these algorithms[8]. The idea of image segmentation technique is taken from the research articles referred to in [9,10,11]. The graphical password in this proposed work is implemented in an easy and simple form of image segmentation technique.

There are very few research articles on video authentication systems. Hence the selection of video password as a security measure for the application is done. The analysis of modern methods for video authentication is done in the work referred to in [12]. The primary requirements for a video authentication system are inferred from this work.

Methodology

The proposed work highlights the images rather than alphabets and numerical. Image segmentation, which is based on the coordinates of an image, is used to implement graphical password authentication. The coordinates of the selected image allow the system to fragment the image into segments.

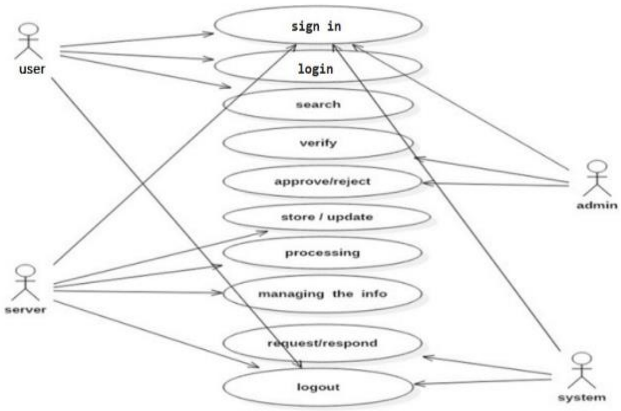

Fig.1 Use case diagram

The use case diagram of the problem solution is shown in Fig.1. The activities of the user includes signup, login and browsing the application. The responsibilities of the admin include verification and approval/rejection. The server or database stores, updates, processes and manages the data of the user along with their graphical passwords i.e., the sequential segments of the selected images. The system or the application requests/responds to the user action. The data is encrypted using certain encryption algorithms like RSA and AES. Encryption provides an extra added amount of security[13] along with the security provided by both the authentication methods. The whole application is to be placed in the cloud for the users to access it wherever they are and whenever required.

Methodology for Graphical password

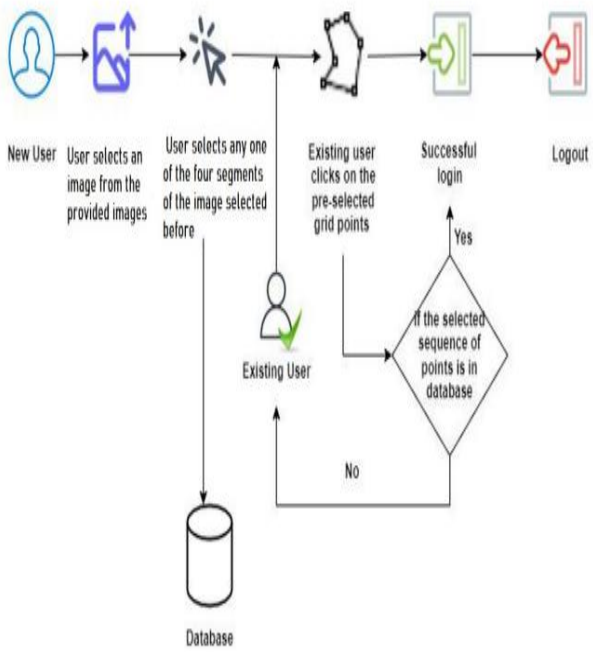

Fig.2 Graphical password methodology

Fig.2 depicts the Project Flow diagram. The figure shows how the entire project is i.e. Graphical Password Authentication System is useful for providing robust and lightweight security for the e-healthcare application developed. If the user is a new user, then he/she must sign up to the application and must create a graphical password. The segment of images selected by the user for their graphical password are stored in the database for later verification.

If the user is an existing one, he/she can directly login to the application using his username and graphical password. The graphical password is a set of three images and their respective segments. When these all are given, the system verifies them with the database and if the password is accepted, the user experiences a successful login or else the login fails. Once the user is finished with login, he/she can logout from the application whenever required.

Methodology for Video password

The proposed work highlights the video rather than alphabets and numerical. The video password authentication is provided by taking a particular number of frames out of the video and calculating their region of interest (ROI). A region of interest, is a subset of an image or dataset identified for a particular purpose.

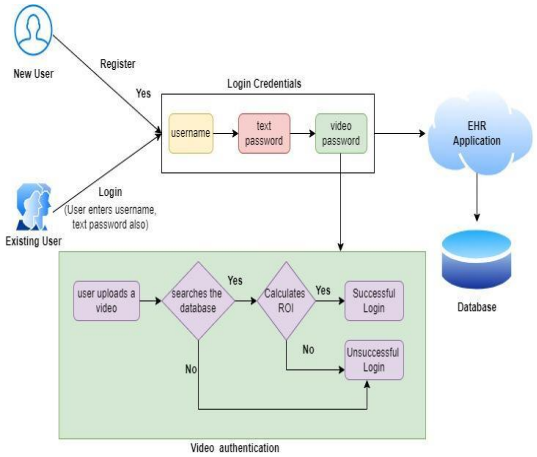

Fig.3 Video password methodology

The figure shows how the video password works and how it improves security of the e-healthcare application. If the user is a new user, then he/she must sign up to the application and must create an account along with the video password. The video password is a video of user choice. The video uploaded by the user is divided into frames and ROI is calculated from those frames. The ROI for each and every user video is stored in the database for later use.

If an existing user tries to login to the application, he/she must provide all three user credentials i.e., username, text password and the video password, which is nothing but a video that the user has chosen while registering. Whenever a video is uploaded, it is divided into frames and ROI is calculated for the respective video. If the calculated ROI and the one that is stored in the database of that particular user matches, successful login happens otherwise the user cannot login to the application. The application can be accessed by four types of people. They are Data Owner, Data User, Key Issuer and Cloud Server Admin.

a. Data Owner

Data Owner is the one who can use the application for storing their medical reports. The activities of the Data Owner include Upload, Update, Delete and View patient reports.

b. Data User

Data User is the one who can access other people's medical reports only with permission. Data Users can access the data and use it for research purposes etc. The activities of the Data User include Search, View, Download(only if permission is granted) reports and Request Key, View Key Response, Req

Decrypt Permission(to decrypt the encrypted report data), Decrypt Permission Response.

c. Key Issuer

The permission for accessing data to Data User is given by the Key Issuer. Key Issuer has certain admin rights of the application. The activities of the Key Issuer include Transactions, View File Private Keys, Private Key Permission, Give Decrypt Permission, Files with Decrypt Permission, Files without Decrypt Permission.

d. Cloud Server Admin

Cloud Server Admin is the one who manages the application and its users. All the data related to end users is stored in this. The Cloud Server Admin can see all the end users, their reports etc.

The reports stored in the application are encrypted using Advanced Encryption Standard(AES) Algorithm[14].WhereasRivest-Shamir Adleman(RSA) Algorithm[15] is used for the key generation. Key is generated when a data user requests for permission to access some data out of the application.

Algorithm: Advanced Encryption standard(AES)

Input: Plaintext
Output: Ciphertext
Procure the set of round keys from the cipher text.
The state array is initialised with the block data.
Attach the initial round key to the starting state array.
Execute nine rounds of state manipulation.
Execute the tenth and final round of state manipulation.
Derive the final state array out as the encrypted data i.e., ciphertext.

Algorithm: Rivest-Shamir-Adleman(RSA)

Input: Request for a key
Output: Key Generation
Select two large primes p and q.
Compute: n=pxq, where n is called modulus for encryption and decryption.
Calculate totient function; φ (n)=(p-1)(q-1).
Choose an integer e, 1<e<φ, such that gcd(e,φ)=1.
Compute the secret exponent d, 1<d<φ, such that ed=1 mod φ.
To get the cipher text from the plain text the following formula is used

$C = Me \bmod n$

To calculate plain text D from the cipher text C the following formula is used.

$M = Cd \bmod n$

Components

Java

Java is one of the most widely used programming languages and platforms . Java is an object-oriented programming language. This language is most widely used for developing large mobile applications and web applications. Using the tools given by the Java Enterprise Edition, we can create any application. It is also said to be a portable language and we can develop an optimised code. It provides a large set of packages with an Integrated Development Environment such as IntelliJ IDEA, NetBeans, Eclipse.

NetBeans

It is an open-source software used for developing C++, Java and other programming languages. NetBeans has the capability to dynamically install the modules. Modules are nothing but a software modular component. It is the most used IDE to reduce the code complexity and to increase the coding comfort for the developers while developing large applications. And it works on various platforms like Mac OS, Linux, Windows etc. It also allows you to write bug free code using smart code editing.

HTML

HTML stands for Hypertext Markup Language. It doesn't support any logic to develop any webpage, this language is all about tags. HTML is used to format web pages that consist of a series of elements. Hypertext refers to the manner in which web pages (HTML documents) are linked together. HTML turned into advanced with the motive of defining the structure of documents like headings, paragraphs, lists. HTML is being widely used to layout web pages with the assistance of different tags available in HTML language.

D. JSP

Java Server Pages (JSP) is a technology for developing net pages that helps dynamic content. This facilitates to insert java code in HTML pages by means of Making use of unique JSP tags, maximum of which start with <% and end with %>. Developers write JSPs as matter content

documents that integrate hypertext markup language or XHTML code, elements of XML are embedded JSP actions and instructions. JSP tags may be used for an expansion of purposes, which includes retrieving records from a database or registering person preferences, getting access to JavaBeans components, passing manipulate among pages, and sharing facts between requests, pages etc. It is an extension of servlet technology.

E. MySQL

It is a Structured Query Language that is used to access and manage records in databases. It is developed by Oracle. IT allows users to directly connect to the database. MySQL works on many working structures and with many languages which include php, PERL, C, C++, JAVA, etc. It is customizable, the open-supply GPL licence allows programmers to regulate the MySQL software program to suit their own unique environments. Massive number of developers around the sector uses MySQL.

B. Video Password

The Video Password is implemented using a novel approach by calculating the region of interest of frames within the video. This novel technique is implemented using Java Server Pages. Whenever a user wants to use this application, the user first needs to create a video password. To create a video password the user can upload a video of their choice as shown in Fig.6. Once the video is uploaded, the system divides the video into frames as in Fig.7. A particular number of frames are stored in the MySQL database as a password to recognize the user. These frames will get automatically deleted within a particular time frame.When the user wants to login to the application, the user has to upload the same video which is uploaded at the time of account creation. The system will then calculate the region of interest of the frames of the video. If it matches, the user experiences successful login like in Fig.8 or else the user experiences unsuccessful login.

C. Registration page

When the user wants to use an application the user needs to register into the application by providing the required details and setting up a password. In the case of a graphical password authentication system, the user must create a graphical password and in the other case must create a video password.

D. Login page

When the user wants to use an application, the user needs to login to the application by providing the required credentials and passwords. If the user provides the correct password the user can successfully login to the application and can access the homepage and required content in the application. If the user provides wrong credentials the user cannot login to the application.

E. Home page

The proposed work mainly focuses on providing authentication to the applications. In this an electronic health record system is incorporated to provide
security for the medical data of users. In the home page the user can access their medical records and encrypt them as well as shown in Fig.9 and Fig.10.

Results

Graphical Password Results

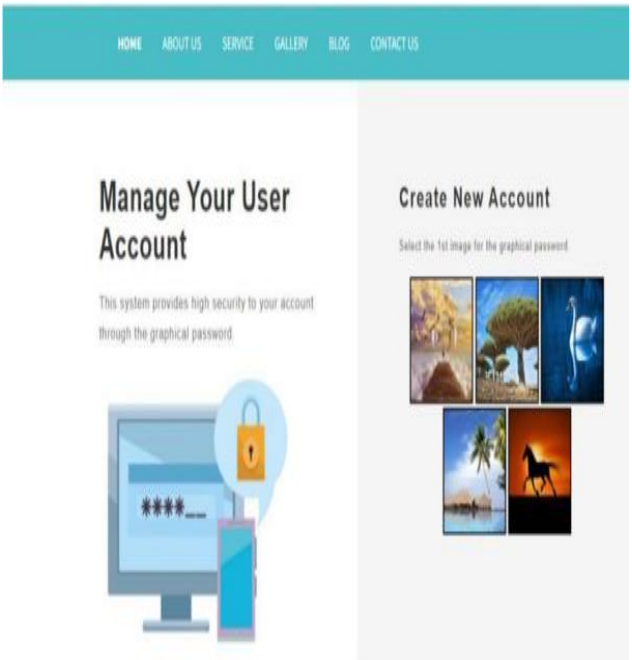

Fig.4 Selection of image

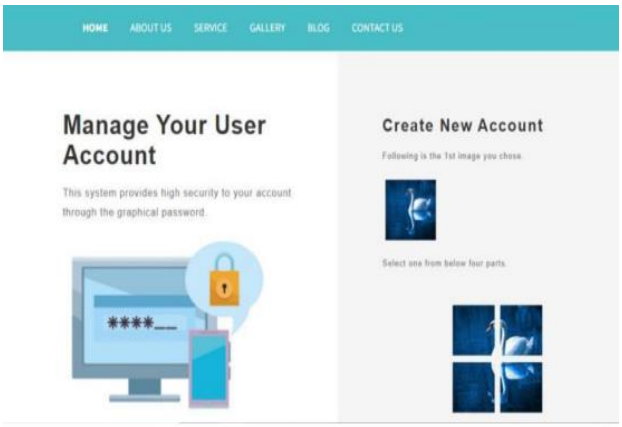

Fig.5 Selection of image's segment

B. Video Password Results

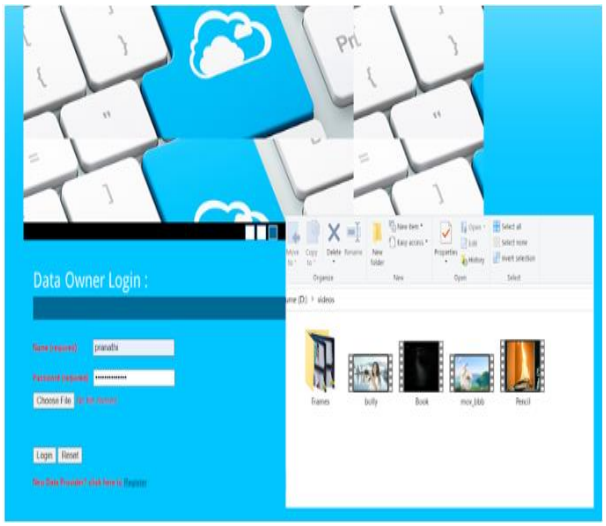

Fig.6 Selection of video

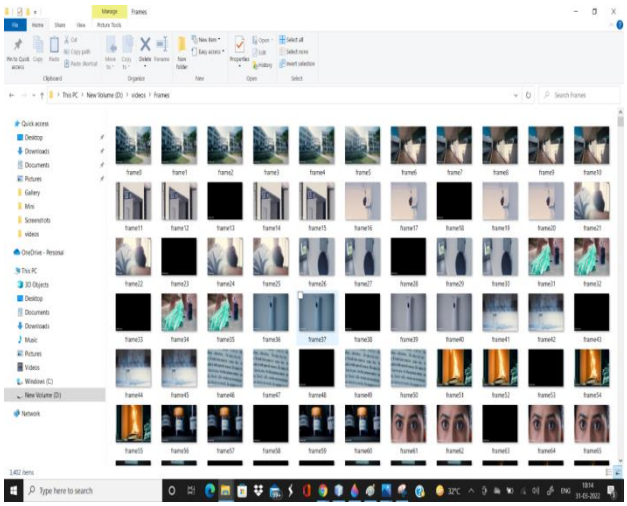

Fig.7 Division of video into frames

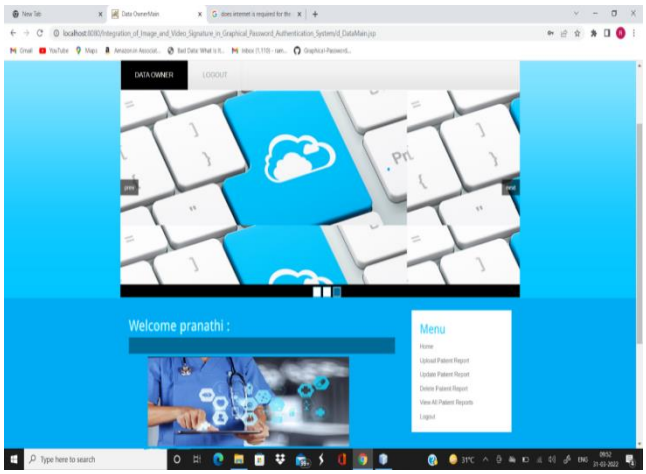

Fig.8 Web application's Home Page

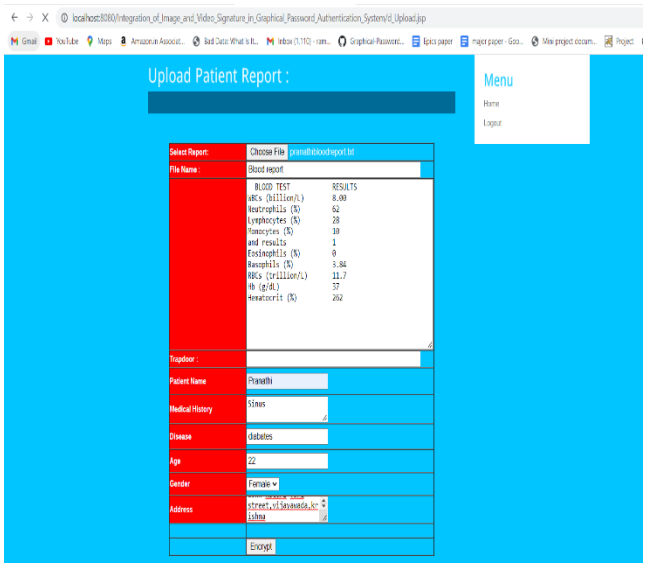

Fig.9 Uploading a report

Fig.10 Encrypted report

Conclusion

To conclude, there's a heavy need for security of online information these days due to the increase of use of online sources and hence the security breaches. General alphanumeric passwords provide meagre security. So, there's a need for new security mechanisms which can provide an ample amount of security. In this proposed work, both the graphical password and video password are implemented separately and compared for an e-healthcare application, which acts as an Electronic Health Record(EHR).

Both the passwords seemed efficient in terms of working. Surprisingly, the video password consumes less time than the graphical password. As far as the security is concerned, both the passwords play well. Since time is also a crucial factor, the use of video passwords with this particular technique of calculating ROI, can be put to use for applications instead of routine text passwords. This work can be extended for other applications in sectors like banking, e-commerce, retail etc.

References

M. A. Kamoona and A. M. Altamimi, "Cloud E-health Systems: A Survay on Security Challenges and Solutions," 2018 8th International Conference on Computer Science and Information Technology (CSIT), 2018, pp. 189-194, doi: 10.1109/CSIT.2018.8486167.

A. V. D. M. Kayem, "Graphical Passwords -- A Discussion," 2016 30th International Conference on Advanced Information Networking and Applications Workshops

(WAINA), 2016, pp. 596-600, doi: 10.1109/WAINA.2016.31.

M. Harshini, P. L. Sai, S. Chennamma, Thanuja, A. G. Reddy and H. S. Kim, "Easy-Auth: Graphical Password Authentication using a Randomization Method," 2021 IEEE Latin-American Conference on Communications (LATINCOM), 2021, pp. 1-6, doi: 10.1109/LATINCOM53176.2021.9647825.

M. K. Kundalwal, A. Singh and K. Chatterjee, "A Privacy Framework in Cloud Computing for Healthcare Data," 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2018, pp. 58-63, doi: 10.1109/ICACCCN.2018.8748480.

Mahdi Nasrullah Al-Ameen , Sonali T. Marne , Kanis Fatema , Matthew Wright & Shannon Scielzo (2020): On improving the memorability of system-assigned recognition-based passwords, Behaviour & Information Technology, DOI: 10.1080/0144929X.2020.1858161

N. Zujevs, "Authentication by Graphical Passwords Method 'Hope'," 2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE), 2019, pp. 94-99,doi: 10.1109/iCCECE46942.2019.8941758.

Pooja Kute, Tejaswini Lokhande, Manasi Kanadi, Sayali Kashid, Ruchira Deshmukh, "Video Captcha as a Graphical Password", International Research Journal of Engineering and Technology(IRJET), 2018, e-ISSN: 2395-0056, p-ISSN: 2395-0072.

J. G. Kaka, O. O. Ishaq and J. O. Ojeniyi, "Recognition-Based Graphical Password Algorithms: A Survey," 2020 IEEE 2nd International Conference on Cyberspace (CYBERNIGERIA),2021,pp.44-51,doi: 10.1109/CYBERNIGERIA51635.2021.9428801.

A Balamurali, M V R Harsha,V Sai Hitesh, A Sai Chaitanya, "Graphical Password by Image Segmentation", 2019, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-6S4, April 2019

Rohitkumar Kolay, Animesh Vora, Vinaykumar Yadav, "Graphical Password Authentication Using Image Segmentation", 2017, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 03, March 2017

Eshita Agrawal, VijayKumar A, "Graphical Password by Image Segmentation", 2022, International Research Journal of Engineering and Technology (IRJET), Volume: 09 Issue: 04, April 2022

Pavel D. Gusev, Georgii I. Borzunov, The Analysis of Modern Methods for Video Authentication, Procedia Computer Science, Volume 123, 2018, Pages 161-164, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2018.01.026.

"What is encryption and how does it protect your data?". (2022). [Online]. Available at: https://us.norton.com/internetsecurity-privacy-what-is-encryption.html

Abdullah, Ako. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.

Hengki Tamando Sihotang, Syahril Efendi, Elvyawati M Zamzami and Herman

Mawengkang, Journal of Physics: Conference Series, Volume 1641, International Conference on Advanced Information Scientific Development (ICAISD) 2020 6-7 August 2020

eISSN 1303-5150