BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Web Application Authentication Using Visual Cryptography and Cued Clicked Point Recall-based Graphical Password

Mary Ogbuka Kenneth[1*] Stephen Michael Olujuwon[2]

1. Department of Computer Science, Federal University of Technology, Minna, Nigeria
2. Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria

ARTICLE INFO

Article history
Received: 10 August 2021
Accepted: 24 August 2021
Published Online: 26 August 2021

Keywords:
Password authentication
Graphical password
Text password
Visual cryptography
Shoulder surfing
Key-logging

ABSTRACT

Alphanumerical usernames and passwords are the most used computer authentication technique. This approach has been found to have a number of disadvantages. Users, for example, frequently choose passwords that are simple to guess. On the other side, if a password is difficult to guess, it is also difficult to remember. Graphical passwords have been proposed in the literature as a potential alternative to alphanumerical passwords, based on the fact that people remember pictures better than text. Existing graphical passwords, on the other hand, are vulnerable to a shoulder surfing assault. To address this shoulder surfing vulnerability, this study proposes an authentication system for web-applications based on visual cryptography and cued click point recall-based graphical password. The efficiency of the proposed system was validated using unit, system and usability testing measures. The results of the system and unit testing showed that the proposed system accomplished its objectives and requirements. The results of the usability test showed that the proposed system is easy to use, friendly and highly secured.

1. Introduction

Passwords, which are the most important aspect of the authentication process, are crucial to information and computer security. Authentication is the act of a system verifying a user's identity. It's a method of determining if a specific person or device should have access to a system, an application, or just an object operating on a device [1]. Authentication refers to the act of only showing the valuables to their rightful owner. Authentication is also the first line of defense in safeguarding any resource. A password is a type of secret authentication data utilized to control resource access. Those who are not given access are kept in the dark about the password, while those who seek to get access are tested to see if they know it and then granted or denied access appropriately. Passwords are required for a variety of tasks by a normal computer user, including login into accounts, getting email from servers, databases, networks, accessing data, and web sites, and even reading the morning newspaper online [2]. Nowadays, a variety of user authentication mechanisms are accessible. The most prevalent way of computer authentication is to utilize an alphanumeric username and password, which has a number of disadvantages. Since the system's developer sees alphanumeric passwords as a string of characters, they are simple to implement [3]. A properly safe password, on the other hand, should be both random and easy to remember. Randomness prevents an attacker

**Corresponding Author:*
Mary Ogbuka Kenneth,
Department of Computer Science, Federal University of Technology, Minna, Nigeria;
Email: kenneth.pg918157@st.futminna.edu.ng

 DOI: https://doi.org/10.30564/jcsr.v3i3.3535

from guessing the password, while a memorable password makes it easier for the owner to get access. However, this is difficult to achieve using alphanumeric passwords, because a random string of characters that cannot be quickly guessed is more difficult for the owner to remember. A basic password, on the other hand, will be easily remembered by the owner but will be easy to determine by an attacker, rendering it usable but vulnerable [4]. To alleviate the problem with alphanumeric authentication, a large variety of graphical password schemes have been created and tested [5]. One explanation for the surge in popularity of graphical passwords is because visuals, as opposed to strings of characters, are thought to be more remembered. Using graphics or drawings as passwords is referred to as graphical passwords. Graphical passwords should be easier to remember in theory because humans recall pictures better than words [2]. In addition, because the search space is nearly endless, they should be more resistant to brute-force attacks. In general, there are two types of graphical password techniques: recognition-based and recall-based graphical passwords techniques. A user gets authenticated using recognition-based techniques by asking him or her to identify one or more photos at the registration phase. During Login, a user is asked to reproduce anything that he or she developed or selected earlier during the registration step in recall-based procedures [6].

The vulnerability of traditional password schemes to shoulder surfing and key-logging attacks is one of their drawbacks. Shoulder surfing happens when someone looks over your shoulder as you enter sensitive information into an electronic device, such as your ATM PIN, password, or credit card number [7]. Key-logging is a type of malicious software that records keystrokes on a keyboard without the user's awareness [8] . Key-loggers are difficult to detect because they operate in stealth mode or masquerade as genuine program on the computer [9]. There are numerous methods for combating the threat of key-loggers, but none of them is adequate on its own. To effectively solve the problem, a mix of techniques is required [10]. Using a combination of visual cryptography and graphical password, this study seeks to overcome the problem of shoulder-surfing and key-logging attacks. The followings are the study's main contributions:

(1) Development of a secure cryptographic system.
(2) Development of a secure graphical password authentication system.

The following is how the rest of the paper is structured: A summary of related researches on graphical authentication is included in section two. The techniques used to accomplish the goal of authentication are presented in section three. In section four results from the experimentation are presented and discussed. The study's conclusion is presented in section five and lastly future works are presented in section six.

2. Related Works

The limits of graphical and alphanumeric passwords were identified by Chuen [11]. One of the drawbacks of using a graphical password technique is the possibility of shoulder surfing. A graphical password could be physically witnessed, especially in public locations, and if the attacker has a clearer vision of the password being entered several times, they could easily decipher the password, which is a serious weakness. Another disadvantage of a graphical password technique is that it is vulnerable to guessing. If the user only registered a brief and predictable password, the odds of it being guessable would rise, just like with an alphanumeric password. To conquer these potential drawbacks, a shoulder surfing-resistant method could be enacted, such as including multiple mouse cursors when users log in to their accounts, which would make it difficult for the attacker to determine which mouse cursors are valid and which click points the user has clicked. Next, a prerequisite of at least 10 click points to make the graphical password harder, similar to an alphanumeric password, could be enforced to the system to ensure that the user does not simply enter a sloppy password, reducing the chances of an attacker guessing the user's password significantly.

Vaddeti [12] suggested a graphical password authentication scheme based on the best existing features like hash index, distorted images, and loci metrics, as well as visual cryptographic techniques and additional naive features, to defend against well-known attacks like brute-force, educated guessing, sniffing, hidden camera, shoulder surfing, and phishing. The paper's flaw is that no assessment metric was utilised to assess the system's performance.

Shnain and Shaheed [13] employed pictorial passwords to improve E-commerce authentication problems. A modified Inkblot authentication method was presented in this paper. Images are used as a trigger for text password entry in the Inkblot authentication method. Users are given the option of selecting a series of inkblots and typing in the first and last letter of the word/phrase that best describes the inkblot during password creation. The user's password is made up of these pairs of letters. The inkblot is a useful tool for users to create their login. The problem with this inkblot authentication method is that users are only given a limited number of password options.

Ahsan and Li [14] presented a graphical password authentication employing an image sequence. In this manner, the user uploads photographs from his or her own

DOI: https://doi.org/10.30564/jcsr.v3i3.3535

directory for password selection, and the images supplied by one user are not visible to the other. The planned system is divided into four phases. The legitimate email address stage is the first step. The user will submit a genuine email address during registration, which will be used throughout the login phase. The system will redirect the visitor to the next page after inputting a valid email address, which will provide photographs for selection. The second stage is the picture selection phase, in which a user can choose between a maximum of six and a minimum of four photographs to finish the registration process. A user will be asked to pick the amount of photographs that were uploaded during the registration step after logging in. Users upload their desired photographs based on the prior number of images picked in the third phase. In the last phase, the picked photos are stored in order. When logging in, the user selects uploaded photographs in the same order as they were picked during the registration step. The user will not be able to login if the sequence of selected photos is incorrect. The suggested technique is vulnerable to shoulder surfing, because an assault can readily capture the image sequence during registration or login.

Dana [15] developed on a visual cryptography system that allows visual information to be encoded in such a way that it can be decrypted solely by sight. The encoding of the original image is split into two images in this method of cryptography by changing every pixel into a pattern that looks like grey or noise. The User ID was extracted from the server share using an optical character recognition method. As a result, a user's identity is verified by matching the retrieved and preserved IDs. Using optical character recognition raises the computational complexity of the procedures, which is a disadvantage.

Togookhuu [16] suggested a three-layer verification recall graphical password technique. The suggested recall-based authentication technique was an upgrade to the Pass-Go scheme, which included secret questions, answers, and backdrop imagery. The suggested system, dubbed CRS, is made up of three pieces that work together to ensure password security. The initial portion of the verification process is concerned with the secret question and the text-based answer. The second section is about selecting a picture based on recognition, and the third section is about constructing a password using a drawing that is easy to remember. The disadvantage of this method is that it is easy for people to forget their stroke order while using drawing to create a password.

3. Methodology

The proposed technique implements a two level graphical password schemes to provide more security to avoid should surfing attack and key-logging attack. The first level of authentication is the visual cryptography authentication and the second level of authentication is the cued click point recall-based authentication. The two level graphical passwords are embedded in two phases namely: Registration phase and the login phase. These phases and level are discussed in detail below. The proposed system was implemented using PHP, HTML, CSS, MYSQL, JavaScript and Python.

3.1 System Design

3.1.1 Architectural Design

Architectural design is all about understanding how a system should be organized and constructing the overall structure of that system. The architectural design is the first step of the software development process. It is the crucial link between design and requirements engineering since it defines the system's primary structural components and their relationships. Figure 1 depicts the suggested system design.

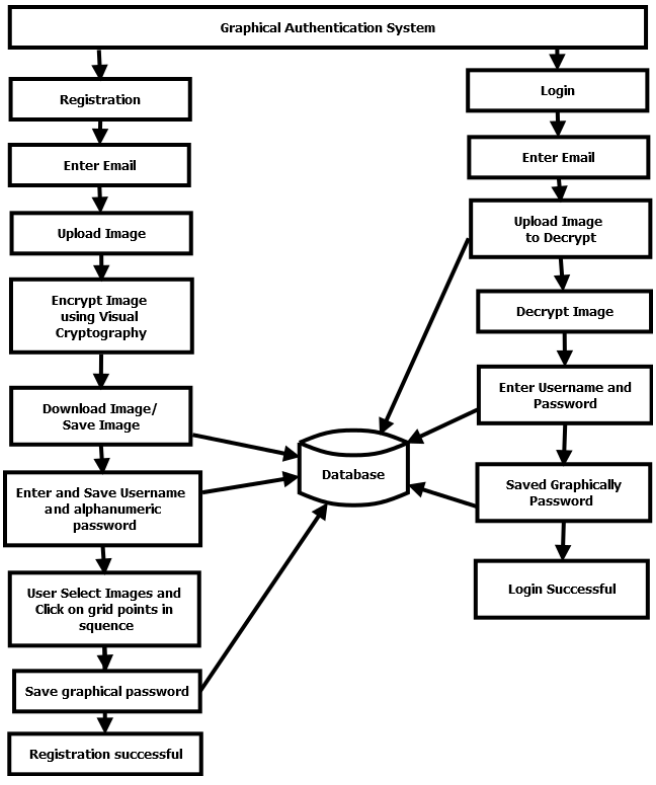

Figure 1. Proposed System Architecture

In Figure 1, the architectural design involves the process function, system database, and the external entities that will interact with the system. The authentication system in Figure 1 consists of two phases: registration and login phase. The registration phase involves the image

 DOI: https://doi.org/10.30564/jcsr.v3i3.3535

encryption using visual cryptography, alphanumeric password registration and the graphical password registration. The login phase involves shared image authentication, password verification and graphical password validation.

3.1.2 Flowchart of the Proposed System

A flowchart is a graphical depiction of a series of steps. It is commonly used to show the flow of algorithms, workflows, or processes in a sequential order [17]. Figure 2 depicts the suggested system flowchart.

The flowchart in Figure 2 shows the flow of events from the beginning to the end of the registration and login phase. In each stage of the login activity a validation process takes place. For example the shared image is validated, the username and password is validated and also the graphical password is validated. The registration or sign up activity is straightforward as it deals with just receiving the user's choice of images, username, and password as inputs for verification purpose.

3.2 Proposed Techniques

The proposed system consists of mainly of two techniques in sequential order: visual cryptography and graphical password. Each of these techniques is explained in detail in this section.

3.2.1 Visual Cryptography (VC) Authentication

The graphical password authentication scheme's initial stage is Visual Cryptography (VC). VC is a sophisticated approach that blends the concepts of cryptography's perfect cyphers and secret sharing with raster graphics [18]. Visual cryptography is a cryptography method that allows visual information (pictures and text) to be encoded and decoded in such a way that the decoded data appear as

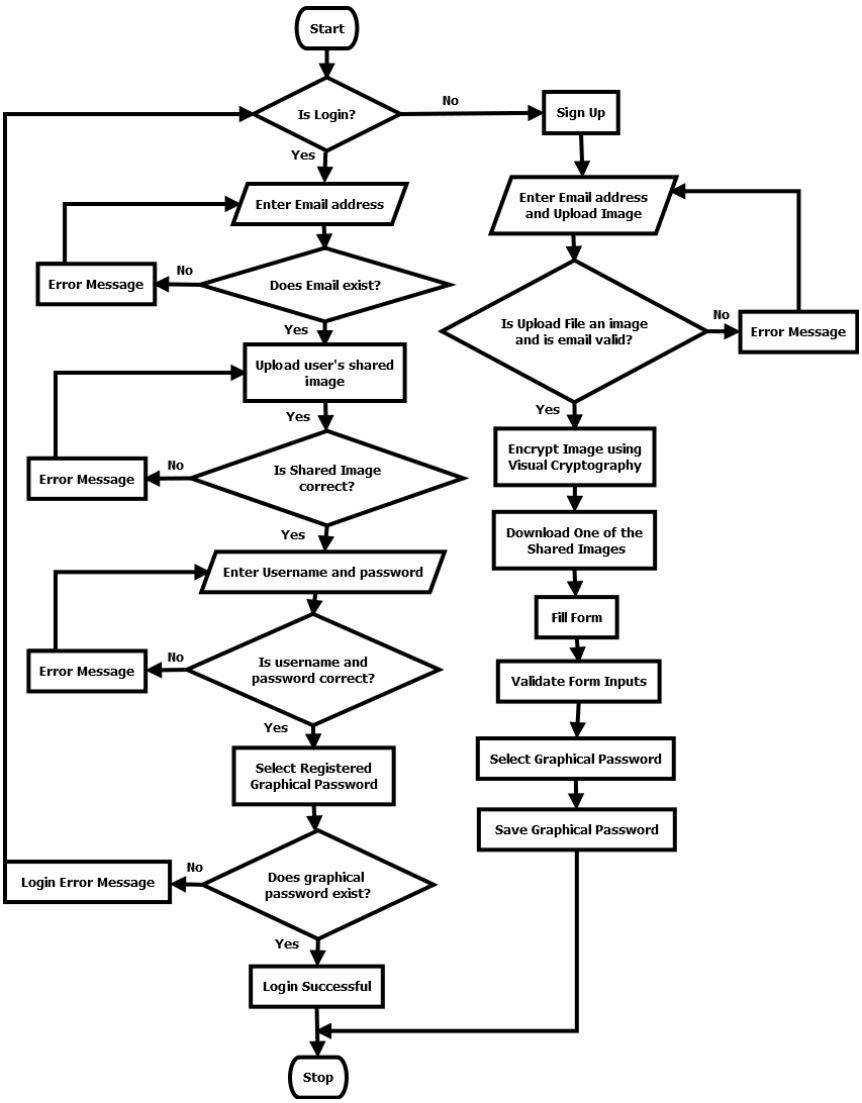

Figure 2. Flowchart for the Proposed Authentication System

DOI: https://doi.org/10.30564/jcsr.v3i3.3535

a visual image. A binary image can be split into shares, which can then be stacked to resemble the original image. A secret sharing technique allows a secret to be distributed among n parties, with only predefined approved sets being able to reconstruct it [19]. In terms of VC, the secret can be visually reconstructed by superimposing shares. VC enables the transfer of visual data, and many facets of this field are discussed, from its inception to current approaches that are being used and actively researched today. This assessment looks at the progress of VC, as well as contemporary trends and applications [18]. It is quite desirable to be able to conceal information such as personal information. The data are completely unrecognizable when it is concealed within distinct images (known as shares). The data are entirely incomprehensible, despite the fact that the shares are separate. Each image contains distinct pieces of data, and when they are combined, the secret may be easily discovered. In order to access the decrypted information, they each depend on one another. Anyone should be unable to read the information stored within any of the shares. When the shares are brought together and stacked on top of one another, decoding is possible. The information becomes instantaneously available at this point. The information can be decrypted with no computational resources at all [20].

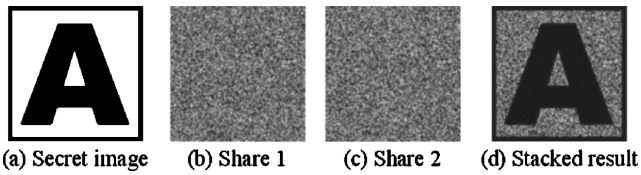

Figure 3. Results of a Visual Cryptography Scheme

Figure 3 shows the implementation and results of basic visual cryptography. It displays the secret image, the two shares that are generated and the recovery of the secret after superimposing share one and share two.

3.2.2 Cued Click Point Recall-Based Authentication

In this strategy, the system provides certain tips that assist users in accurately reproducing their passwords. Hot spots (regions) inside an image will be used to provide these hints [1]. To register as a password, the user must select one of these regions, and to log into the system, they must select the same region in the same order. Cued Click Points (CCP), a recall-based approach, was employed for user authentication in this study. A potential replacement to Pass-Points is Cued Click Points (CCP) [4]. In CCP, users click one point on each image rather than several points on a single image. It has cued-recall and visual cues that immediately notify valid users if they make a mistake when entering their most recent click-point. It also makes hotspot analysis-based attacks more difficult [21].

A wrong click progresses down the wrong path, with verification failure being explicitly indicated only after the final click. Users can only choose their images to the extent that the next image is dictated by their click-point. If they don't like the images that come up, they can make a new password with different click-points to achieve other results. CCP works in the same way as Pass-Points when it comes to implementation. A discretization approach is utilized to identify a click-tolerance point's square and associated grid during password formation. This grid is obtained and used to determine if each click-point on a subsequent login attempt falls within the tolerance of the originating point [21]. Being cued to recall one point on each of the three photos appears to be easier than recalling an ordered sequence of three points on one image, which is a usability benefit of CCP. Figures 4 and 5 illustrate

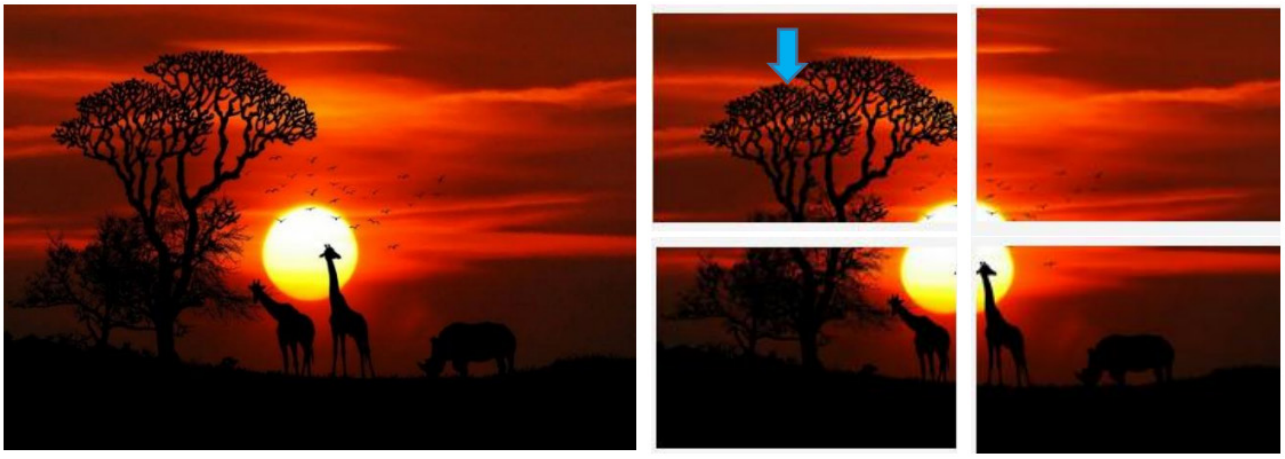

Figure 4. first selected image in the Cue Clicked Point process

 DOI: https://doi.org/10.30564/jcsr.v3i3.3535

Figure 5. Second selected image in the Cue Clicked Point process

an example of a 2 × 2 grid of two selected photos for the CCP procedure.

In Figure 4, a user selects the first image at the left, the selected image is then divided into four images shown in the right. A user now clicks to select one from this sub-images. After clicking one of the sub-images another image is loaded as shown in Figure 5 for another selection. The second selected image is also divided into four sub-images, in which the user also clicks and selects from the sub-images. After the second sub-image is selected another third image is loaded and the process continues.

Registration phase

The registration phase consists of three main processes: visual cryptography, input data and CCP implementation. The registration phase is presented in Figure 6 and the steps involved in the registration phase are discussed below.

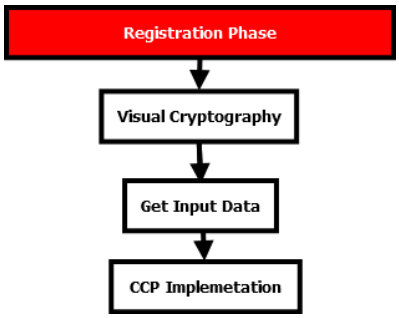

Figure 6. Registration Phase

- **Step 1: Visual cryptography**

In this phase the user is asked to upload an image of their choice. This uploaded image is then encrypted and converted into two shared images using visual cryptography technique. The user is then prompted to download and save one among these two images. This generated images are stored in the database for further use.

- **Step 2: Get Data**

The get data phase obtains the details of users such as user-id, email-id, password, full name and phone number.

- **Step 3: CCP implementation**

A 2 × 2-image grid is now displayed to the user from which the user clicks on one point of the image. After which, the user is to select another image and click on the generated 2 × 2-image grid.

Login and authentication phase

The login and authentication phase is depicted in Figure 7. The steps involve in also in the login phase is discussed below.

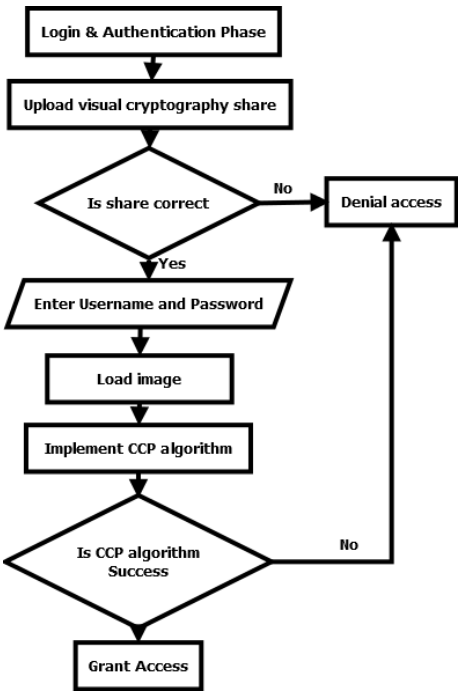

Figure 7. Login and Authentication Phase

DOI: https://doi.org/10.30564/jcsr.v3i3.3535

- **Step 1: Share Submission (Visual Cryptography)**

During the login phase, the user shared image must be submitted which is compared with the shares stored in the database. If shared images match then the user is allowed to move to the next step.

- **Step 2: Username and Password Authentication**

In this step the user is asked to supply their registered username and password. If a wrong username and password is supplied the access is denied. However if the username and password is correct the user is given access to the next authentication process.

- **Step 3: Graphical password (Cued Clicked point)**

After authenticating the username and password, five images are displayed. The user is prompted to select one of the displayed images. On click of an image a 2 x 2 grid containing parts of the selected image is displayed user is expected to click on the grid in image for successful authentication. If the first attempt fails, the user is asked to login from the beginning.

Another significant point to be noticed in the proposed scheme is no image is highlighted when user clicks the images during login phase in order to prevent shoulder surfing and hidden camera based attacks. The Proposed system was implemented using PHP, HTML, CSS, and Python.

3.3 Evaluation Metrics

Software evaluation refers to the examination of the program itself to see if it works or has any errors or bugs. Evaluation of the web-based application was carried out on the system thoroughly from start to finish of the program. Individual units and components were tested before bringing them together into the whole system which was also tested thoroughly. The different evaluation metric or testing carried out on the prototype is discussed in the subsections below.

3.3.1 Unit Testing

In unit testing each unit of the program were tested to ensure that the program performs its functions as defined in the program specification [22]. A unit is a single testable part of a software system. The aim of unit testing is to validate unit components with its performance [23].

3.3.2 System Testing

System testing is a testing conducted on a complete integrated system to evaluate the system's compliance with its specified requirements [23].

3.3.3 Usability Testing

Usability testing refers to evaluate a software by testing it with representative users. This was done by the users to check that the system meets its supposed requirements [24].

4 Results and Discussion

This chapter provides the proposed system implementation with screenshots for the registration and login process. The system provides easy to use graphics user interface. It also presents all the experiments conducted to evaluate the proposed system and results of the evaluation obtained from the research.

4.1 Registration Interfaces

The registration interfaces which includes upload page, visual cryptography page, data input page and graphical password page are presented in this section.

4.1.1 Upload Page

The sign up interface is the page where the passwords registration takes place. The first page shown for the sign up process is the upload page. The upload interface is shown in Figure 8.

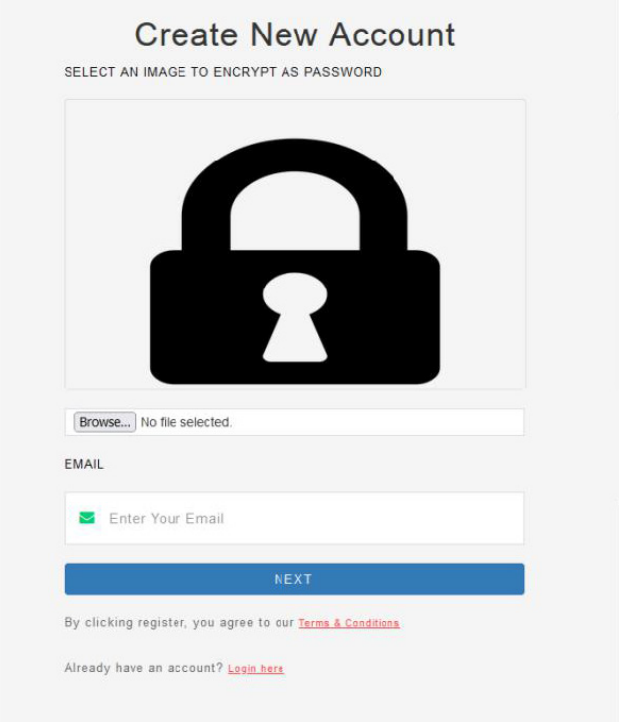

Figure 8. Upload Page

The upload page provides an interface for a user to

select an image of their choice and upload for visual encryption. The browser button in Figure 8 is used to browse the user PC for images. Figure 9 shows the upload page interface after an image has been uploaded by the user.

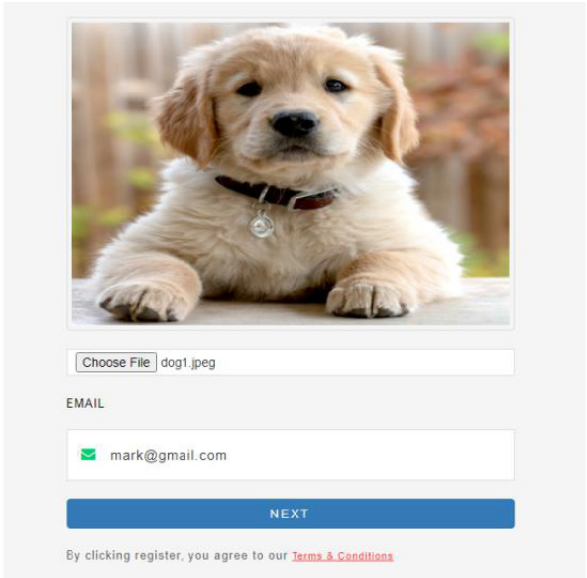

Figure 9. Upload page after user selects and uploads their desired image

4.1.2 Visual Cryptography Page

After uploading the image as shown in Figure 9 the user clicks the next button which leads to the visual cryptography page. The visual cryptography page is shown in Figure 10.

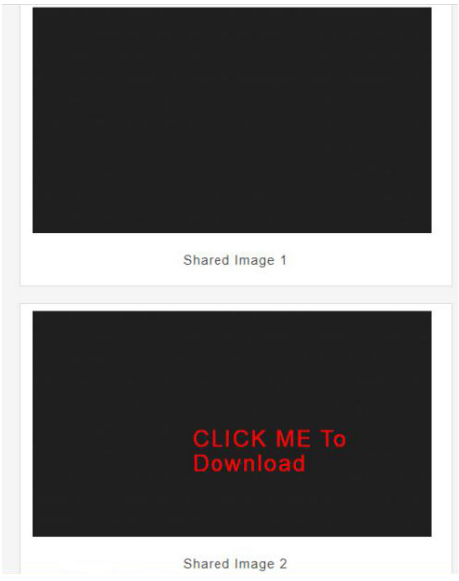

Figure 10. Generated encrypted shared images after performing visual cryptography

The visual cryptography page performance visual encryption on the image and then generates two shared images. The user is prompted to download the second shared image as shown in red on the second shared image in Figure 10. After downloading the second shared image the user clicks the next button which takes the user to the data input page. The required input data are: username, password, full name, email and phone number. The email address is automatically field based on the email address provided at the upload page. After the user fills the form as all fields are required the user clicks the register button and the user is taken to the graphical password page.

4.1.3 Graphical password registration page

In the graphical password registration page, the user is allowed to registers their graphical password by clicking on their desired images and image grids. The graphical password registration page is illustrated in Figure 11, 12 and 13.

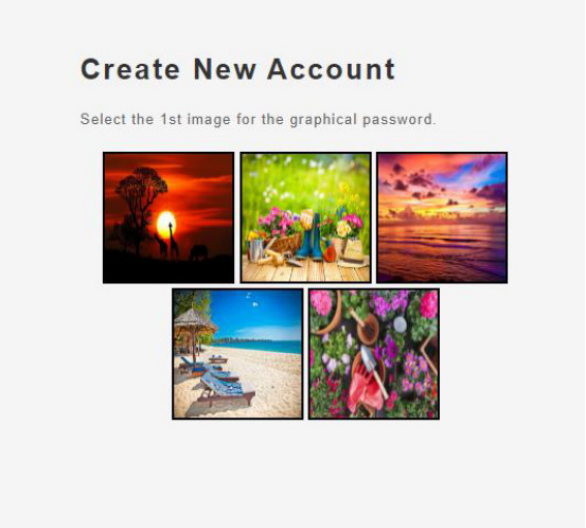

Figure 11. Graphical Password Registration Page

Figure 11 shows the graphical password registration interface with five images displayed. The user is required to click and select one out of this five images. On selecting any of the images, another interface is loaded with four sub-images showing different parts of the selected image. An example of this four sub-images are shown in Figure 12 and Figure 13.

Figure 12 shows four sub-images of the first selected image. The user is required to select one of these four sub-images. After clicking on one of the sub-images, the user is asked to select another image from the five initial images. The second selected image is then divided into four sub-images and the user is prompted to select from this sub-images. The second selected image interface is shown in Figure 13.

DOI: https://doi.org/10.30564/jcsr.v3i3.3535

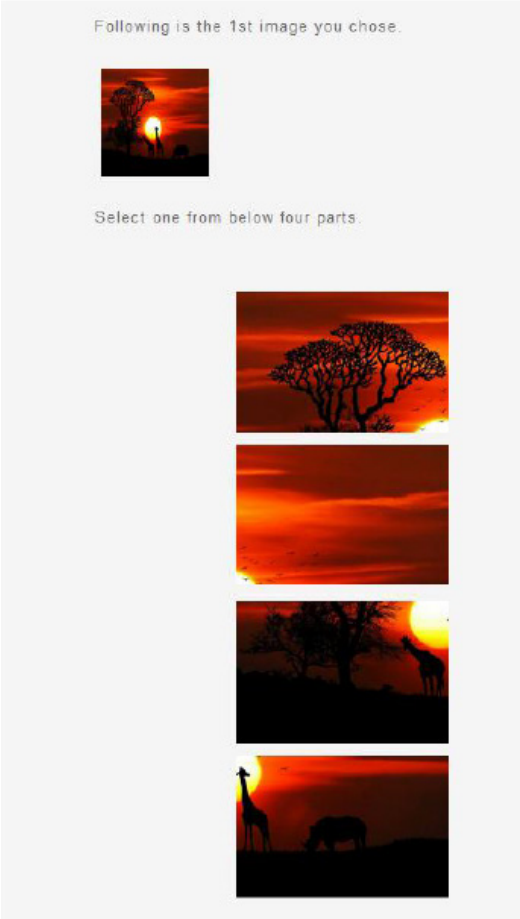

Figure 12. Selected images 4 grids

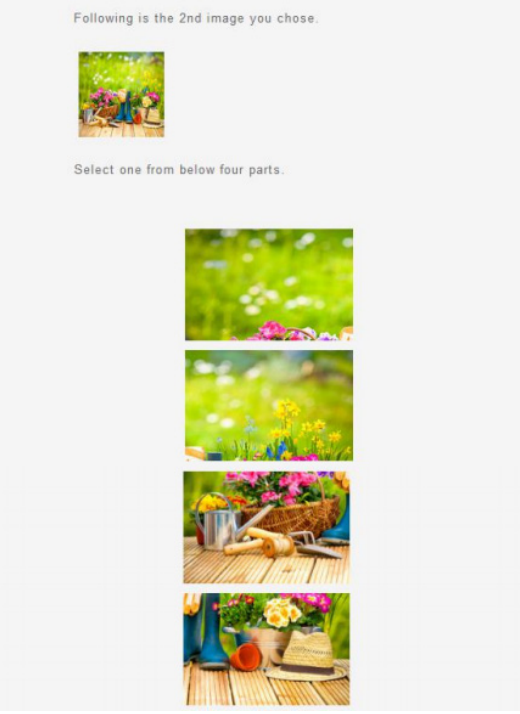

Figure 13. Second image select by user

4.2 Login Interface

After a user registers their password the user is prompted to login to have access to the web-application. The login interfaces are shown in figures in this section.

4.2.1 Email Validation Page

This is the first page in the login process. In the email validation page the user is required to fill in their registered email. The email validation interface is shown in Figure 14.

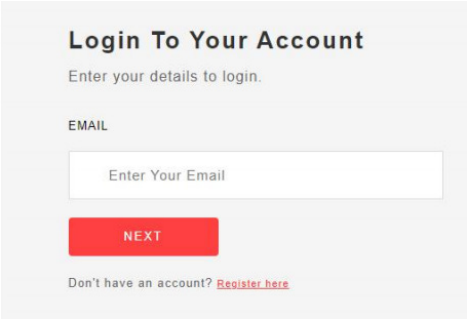

Figure 14. Email Validation Page

If the supplied email address is correct then the user is given access to the decryption page, however if the email is wrong an error message is displayed.

4.2.2 Login Upload Page

After a user's email address is verified the user gets access to the login upload page. The login upload page is a page where a user uploads their downloaded shared image for verification. A sample of the login upload page is shown in Figure 15.

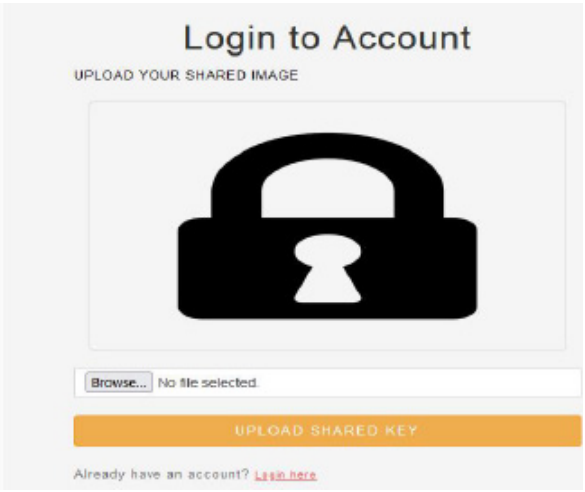

Figure 15. Login Upload Page

The browser button in Figure 15 allows the user to browse their PC and select the downloaded shared images.

 DOI: https://doi.org/10.30564/jcsr.v3i3.3535

Figure 16 shows the interface after the user has selected a shared image.

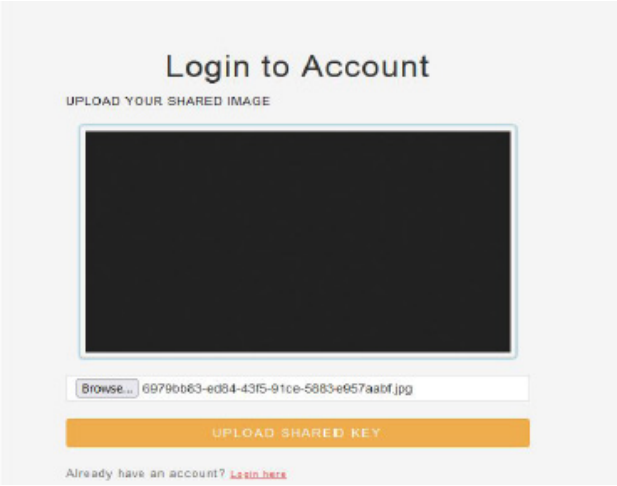

Figure 16. Login Upload Page after user uploads shared key

After loading the shared image, the user then clicks on the upload share key button which takes the user to the shared image authentication page. If a wrong shared image is uploaded then an error message is outputted and a back button to the login upload page is displayed. If the uploaded shared image is correct then a successful message is shown to the user and a continue button is shown which gives user access to the next phase of authentication.

4.2.3 Username and Password Authentication Page

On successful authentication of the uploaded shared key. The user is asked to enter their username and password on the username and password authentication page. This authentication page is shown in Figure 17.

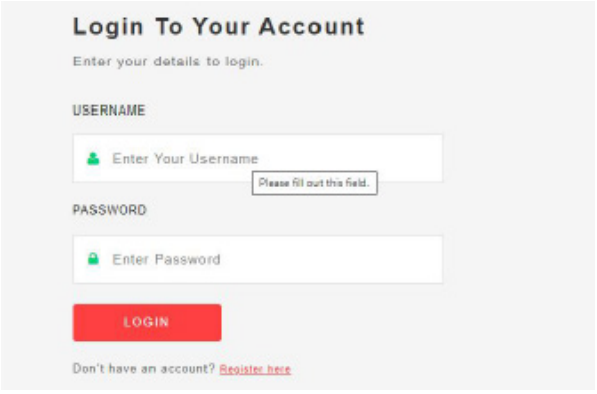

Figure 17. Username and Password Authentication Page

After the user fills in their username and password on click of the login button the inputs are authenticated. If authentication is unsuccessful and error message is displayed and the user is directed to login again. However if the authentication is successful, then the user is redirected to the graphical password page.

4.2.4 Login Graphical Password Page

On the graphical password authentication page the user is required to click on the registered images in same sequence the images were registered during registration. If the wrong graphical password is submitted then user is denied access. If the graphical password is correct then the user is granted access to your profile or the webpage they want to access. The login graphical password page is shown in Figure 18.

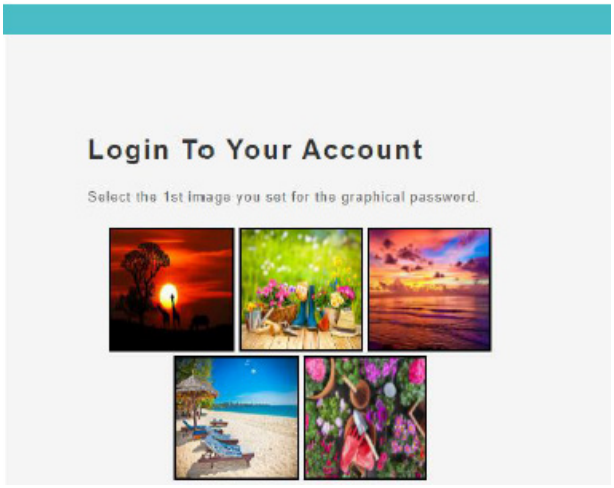

Figure 18. Login Graphical Password Page

4.3 Testing

In this study three types of software testing were conducted. These testing are unit testing, system testing and usability testing. The system was put to the test by a variety of people in terms of functionality and usability. The developer conducted unit and system testing to ensure that each feature and portion of the program and the program as a whole is completely functional. The system was tested by twenty users. Tables 1 and 2 display the results of the system's unit and system testing and usability testing, respectively, to demonstrate that the system meets its specifications.

4.3.1 Unit and System testing

Unit testing deals with testing each software unit to ensure that it performed the functions specified in the program specification. System testing is used to test the functionality of the whole system. The unit and system testing results is presented in Table 1.

DOI: https://doi.org/10.30564/jcsr.v3i3.3535

Table 1. Unit and System Testing

SECTION	INPUT	EXPECTED RESULT	ACTUAL RESULT	COMMENT
REGISTRATION	Select Image	Allows user to browse images from PC.	Correct	Passed
	Upload Image	Allows user to upload browsed image	Correct	Passed
	Encrypt Image	Allows user to encrypt image using visual cryptography	Correct	Passed
	Download Image	Allows user to download shared image	Correct	Passed
	Fill Sign up form	Allows user to input their details	Correct	Passed
	Submit form	Allows user to submit their details	Correct	Passed
	Click on image to register as password	Allows user click on image to register as password	Correct	Passed
	Save password	System sends and details and passwords to database	Correct	Passed
LOGIN	Enter email address	Allows user to input their email address	Correct	Passed
	Select Shared image	Allows user to browse for shared image from PC.	Correct	Passed
	Upload shared image	Allows user to upload browsed shared image	Correct	Passed
	Authenticate shared image	System authenticates upload shared image	Correct	Passed
	Username and password input	Allow user to input username and password	Correct	Passed
	Authenticate username and password	System verifies the username and password	Correct	Passed
	Select images in sequence	Allow users select images in sequence	Correct	Passed
	Authenticate select images	System authenticates the graphical password	Correct	Passed
USER PROFILE	Change Graphical Password	Enables user to change graphical password	Correct	Passed
	Change text Password	Enables user to change text password	Correct	Passed
	Upload and change profile picture	Allows user to upload and change profile photo	Correct	Passed
SYSTEM TESTING	Registration to user profile process	The completeness of the system from the point of registration to the point of user profile change.	Correct	Passed

4.3.2 Usability Testing

Usability is defined as the degree to which a product allows certain users to achieve their specific goals efficiently, effectively, and satisfactorily in the given context. Usability is an important factor to consider when creating a decent graphical password technique that fulfills the needs and requirements of its users. User given Images, Category of Images, Easy to Use, Easy to Create, Easy to Execute, Nice and Simple Interface, Login Time, and Memorability are some of the primary usability features used in graphical passwords. These usability aspects are described in more detail below.

- **User-assigned Images:** When users are given a password at random, they have a harder time remembering it than when they are given the option to pick their own password.
- **Category of Images:** Users can choose from a variety of image categories based on their personal preferences.
- **Easy to Use:** This refers to the system's ability to provide a good platform for password creation.
- **Easy to Create:** When the registration process is straightforward, people may quickly create their graphical passwords.
- **Easily Executed:** When the registration and login are presented in simple steps, people can easily perform the algorithm.
- **Nice and Simple Interface:** Focuses on the user's interactions rather than the aesthetics of the interface. The goal of a nice and simple interface is to make user interactions as efficient and straightforward as possible.
- **Time to Login:** How long does it take for a user to complete the login process?
- **Memorability:** How easy is it for a person to remember their password?

The system's usability testing based on the six defined features above is presented in Table 2.

Table 2. Usability testing

Usability features	Rating
User assigned Images	High
Category of Images	High
Easy to Use	Moderate
Easy to Create	High
Easily Executed	Moderate
Nice and Simple Interface	High
Login Time	Fast
Memorability	High

 DOI: https://doi.org/10.30564/jcsr.v3i3.3535

5. Conclusions - Future Works

In this study the visual cryptography and cued click point recall-based graphical password techniques were used to perform user's authentication for access to web application. The user authentication system consists of the registration and login phase. The registration phase captures the user's graphical password in sequence, textual password and encrypts the user selected image using visual cryptography. The login phase gives user access to a web application by verifying the authenticity of the user via the submitted encrypted shared image, username, textual password and the submitted sequence of the graphical password. In conclusion, a method for authentication of users for web application was proposed based on visual cryptography and cued click point recall-based graphical password techniques. In this study, authentication using this combined techniques achieved a stronger and reliably security than the existing textual and graphical password systems which are vulnerable to shoulder surfing attack.

The study made use of the cued click point graphical password technique for authentication. For future work other graphical password methods such as the recognition based authentication can be used in combination with the visual cryptography. A disadvantage of graphical password techniques is that it requires more memory space than textual. The visual cryptography also requires large memory space to store the encrypted shared images. A combination of visual cryptography and graphical password in study makes the proposed system memory/space intensive. Hence it is recommended that other encryption methods or authentication methods which requires less memory space be combined with the graphical password technique.

References

[1] P. G. Panduranga Rao, 'A Study of Various Graphical Passwords Authentication Schemes Using Ai Hans Peter Wickelgren Approach', *IOSR J. Comput. Eng.*, vol. 10, no. 6, pp. 14-20, 2013. DOI: 10.9790/0661-1061420.

[2] A. Karode, S. Mistry, and S. Chavan, 'Graphical Password Authentication System', *Int. J. Eng. Res.*, vol. 2, no. 9, p. 4, 2013.

[3] L. Y. Por, C. S. Ku, A. Islam, and T. F. Ang, 'Graphical password: prevent shoulder-surfing attack using digraph substitution rules', *Front. Comput. Sci.*, vol. 11, no. 6, pp. 1098-1108, Dec. 2017. DOI: 10.1007/s11704-016-5472-z.

[4] A. Islam, 'A review of the recognition-based graphical password', p. 11, Jul. 2021.

[5] J. Rajesh, C. Durgesh, W. Milind, and K. Santosh, 'Graphical Password Authentication system', *IJLTEMAS*, vol. 3, p. 5, 2014.

[6] S. Istyaq and M. S. Umar, 'Hybrid Authentication Scheme for Graphical Password Using QR Code and Integrated Sound Signature', vol. 12, no. 2, p. 5, 2018.

[7] Mrs. A. S. Gokhale and V. S. Waghmare, 'The Shoulder Surfing Resistant Graphical Password Authentication Technique', *Procedia Comput. Sci.*, vol. 79, pp. 490-498, 2016. DOI: 10.1016/j.procs.2016.03.063.

[8] S. Shinde and U. H. Wanaskar, 'Keylogging: A Malicious Attack', *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 6, p. 5, Jun. 2016. DOI: 10.17148/IJARCCE.2016.5661.

[9] M. K. Shah, D. Kataria, and S. B. Raj, 'Real Time Working of Keylogger Malware Analysis', *Int. J. Eng. Res.*, vol. 9, no. 10, p. 5, 2020.

[10] C. Santwana and K. S. Aditya, 'Hypervisor based Mitigation Technique for Keylogger Spyware Attacks', vol. 5, p. 4, 2014.

[11] Y. S. Chuen, M. Al-Rashdan, and Q. Al-Maatouk, 'GRAPHICAL PASSWORD STRATEGY', *J. Crit. Rev.*, vol. 7, no. 03, Jan. 2020. DOI: 10.31838/jcr.07.03.19.

[12] A. Vaddeti, D. Vidiyala, V. Puritipati, R. B. Ponnuru, J. S. Shin, and G. R. Alavalapati, 'Graphical passwords: Behind the attainment of goals', *Secur. Priv.*, vol. 3, no. 6, Nov. 2020. DOI: 10.1002/spy2.125.

[13] A. H. Shnain and S. H. Shaheed, 'The Use of Graphical Password to Improve Authentication Problems in E-Commerce', presented at the Proceeding of the 3rd International Conference on Applied Science and Technology, Sep. 2018.

[14] M. Ahsan and Y. Li, 'Graphical Password Authentication using Images Sequence', *Int. Res. J. Enigeering Technol.*, vol. 04, no. 11, p. 9, Nov. 2017.

[15] Dana Yang, I. Doh, and K. Chae, 'Enhanced password processing scheme based on visual cryptography and OCR', in *2017 International Conference on Information Networking (ICOIN)*, Da Nang, Vietnam, 2017, pp. 254-258. DOI: 10.1109/ICOIN.2017.7899514.

[16] B. Togookhuu, W. Li, Y. Sun, and J. Zhang, 'New Graphical Password Scheme Containing Questions- Background-Pattern and Implementation', in *Computer Graphics and Imaging*, IntechOpen, 2019. Accessed: Jul. 05, 2021. [Online]. Available: eativeCommonhttp://creativecommons.org/licenses/

DOI: https://doi.org/10.30564/jcsr.v3i3.3535

by/3.0.

[17] N. Tiwari and L. Prasad, 'A Comparative Study: Reverse Engineering Flowcharting Tools', vol. 07, no. 01, p. 8, 2015.

[18] V. Vaishnavi, B. Shanthi, and S. S. Rani, 'SECURE DATA SHARING USING VISUAL CRYPTOGRAPHY', vol. 12, no. 1, p. 5, 2017.

[19] P. V. Chavan, M. Atique, and L. Malik, 'Design and Implementation of Hierarchical Visual Cryptography with Expansionless Shares', *Int. J. Netw. Secur. Its Appl.*, vol. 6, no. 1, pp. 91-102, Jan. 2014. DOI: 10.5121/ijnsa.2014.6108.

[20] D. Vaya, S. Khandelwal, and T. Hadpawat, 'Visual Cryptography: A Review', *Int. J. Comput. Appl.*, vol. 174, no. 5, pp. 40-43, Sep. 2017. DOI: 10.5120/ijca2017915406.

[21] V. Moraskar, S. Jaikalyani, M. Saiyyed, J. Gurnani, and K. Pendke, 'Cued Click Point Technique for Graphical Password Authentication', *Int. J. Comput. Sci. Mob. Comput.*, vol. 3, no. 1, pp. 166-172, Jan. 2014.

[22] D. Almog, D. O. V. B. Sohacheski, M. L. Gillenson, R. Poston, and S. Mark, 'THE UNIT TEST : FACING CICD - ARE THEY ELUSIVE DEFINITIONS ?', *J. Inf. Technol. Manag. Publ. Assoc. Manag.*, vol. 29, no. 2, pp. 40-54, 2018.

[23] N. Anwar and S. Kar, 'Review Paper on Various Software Testing Techniques & Strategies', *Glob. J. Comput. Sci. Technol. C Softw. Data Eng.*, vol. 19, no. 2, 2019.

[24] A. Elsafi, D. N. A. Jawawi, A. Abdelmaboud, and A. Ali, 'A comparative evaluation of state-of-the-art integration testing techniques of component-based software', *J. Theor. Appl. Inf. Technol.*, vol. 71, no. 2, pp. 257-267, 2015.

 DOI: https://doi.org/10.30564/jcsr.v3i3.3535