FreeHand Sketch based Authenticated Security System based using Damerau-Levenshtein Distance

N. Kesava Rao[1,*], G. Srinivas[2], P. V. G. D. Prasad Reddy[3]

[1]Department of CS&SE, AU College of Engineering, Andhra University, Visakhapatnam, Department of CSE, NBKRIST, Vidyanagar, Tirupati (Dist), India

[2]Department of C.S.E., GITAM Deemed to be University, Visakhapatnam, India

[3]Department of CS&SE, AU College of Engineering, Andhra University, Visakhapatnam, India

Email: kesavarn@gmail.com; srinivas.gitam@gmail.com; PrasadReddy.vizag@gmail.com

Abstract

Introducing a ground breaking approach for validation purposes, this document unveils the FreeHand Sketch-based Authentication Security System. The biggest problem right now is how we protect our information in internet digital environment, which still has certain security flaws. On-going security methods related to smartphone applications are mostly built with these security features like dotted patterns, biometrics, and iris and face recognition are the trendy methods. However, they are constrained in their own ways. Free-Hand Sketch Model enhances the basic and comparable security in digital accounts. The present research study made an attempt to make it easier in creating Free-Hand sketch passwords for easy remembrance. A simple Free-Hand sketch is an authorized model for the end users to create their own passwords against security attacks. The main methods suggested in this research study is Damerau-Levenshtein Distance (DLD) used to design Free-Hand sketch image processing model.

Keywords: Free-Hand Sketch; Image Sketch Password; Image processing; DLD Methods

1. Introduction

At present online security E-Services related to online examinations, banking services, and passport authorized services, etc., are lagging behind some of the security services. Many duplication detections are identified in online services such as password hacking, morphing, and mismatching due to drawback in the password protection services and SIM swapping[1][2]. In online accounts, the majority of web applications are providing fundamental authentication methods by creating their own username and password authentication. In some circumstances, re-authentication is available with various sets of actions. The primary goal of the designers should provide end users with simple security measures that will safeguard their security protection. In this concern, most of the online account processes related to security for mobile devices and software applications are taken into the consideration.

In order to enhance the system an approved method is required for end users to create their own Free-Hand sketch passwords to protect themselves from security threats. One of the main objectives is to offer authentication services to end users, who are permitted to establish passwords using a Free-Hand sketch during the administration of digital account services. Users have the option of creating their own sketch passwords utilizing a Free-Hand sketch technique. In order to register a Free-Hand sketch password, the user first needs to generate an image sketch password. Image type password is saved in database of the system if all conditions are satisfied. In accordance with the suggested model sketch password images are authorized.

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024

Figure 1. Password Hacking**.**

Finally, login is possible only if the user's input image password matches the registered image password in the database. Users will now have a new option to create image password sketches as part of their registration process. Users can initially make fresh password sketches there along with a user name and other required authentication details, which offers security in a modern way. The Free-Hand Sketch Model a new extraction model is used in this research. A model that is more effective at creating sketch passwords for security protection is being developed using DLD methods.

2. Problem Statement

In the current digital world, there are many safety measures taken by the companies to secure there digital data in multiple ways like text based password, OTP, finger biometric, Card Scanner, IRIS Scanner, etc. These safety measures have some limitations like text passwords [3] [13] should not be small or should contain their names, therefore it is very hard to the users to remember lengthy text passwords and also it might get typing mistakes while entering the passwords. Coming to the OTP, by using some SIM swapping techniques via social engineering [4], cloning of mobile phones [9] hackers might hack their login credentials; similarly using artificial finger prints [5] they can login into the biometric to steal their private data. Using IRIS scanner, our eyes might get problem in future like eye sight and so on.

Earlier, various models have been developed to enhance data security through the use of sketch-based image passwords, including Sequence Matcher[6][12], Levenshtein Distance[6] & Coordinators Similarity[11], Convolutional Neural Network[10], and FuzzyWuzzy with Partial Ratio[7][14]. When evaluating these existing models, it is important to consider their individual strengths and weaknesses in relation to one another. Nevertheless, the accuracy of the existing models varies within the range of 84% to 92%. In pursuit of surpassing these percentages, a novel approach is introduced, Damerau-Levenshtein Distance [16] [17] [18] to create an improved model.

3. Proposed Methodology

The proposed system helps the user in creating a simple Free-hand sketch password in their own pattern. Most of the hackers and cyber attackers going to break the user defined passwords. In general dot patterns, text and number patterns are also not extremely securable. The sketch based image passwords are used for security measure added to the digital online system to prevent from cyber attackers.

3.1. Registration of Image Password:

In this process during the password registration, the user can use finger, mouse and digital pen in both laptop and smartphone to make their own Free-Hand sketch-based image password with any pattern with their own selected choice. Entitled Figure-2, the diagram delineates the procedure for establishing an image-centric password within the database. The user commences the online account registration by crafting five distinct sketches, each possessing noticeable resemblances. In the ensuing pre-processing phase, a technique called Gaussian Blur is employed to diminish the noise in the images, enhancing their quality. This method, functioning as a low-pass filter kernel, transforms the initial Red-Green-Blue(RGB) images to grayscale images by effectively eliminating noise from all five sketches. In addition during the registration, the user will sign up with five similar password images. This model of training the Free-Hand system will get better trained to access the authentication more accurately. The users first complete a Free-Hand password registration process in order to save the password in the database. The user will draw the five Free-Hand sketch patterns of their choices which are all similar to one another.

To achieve enhanced results, a binary inverse threshold is applied to precisely cut and confine the picture. The cropping of sketches takes into account the object boundaries, given that users have the flexibility to sketch freely across the entire canvas. Subsequently, these 5 pictures undergo resizing to conform to a standardized format of 100x100 pixels.

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024

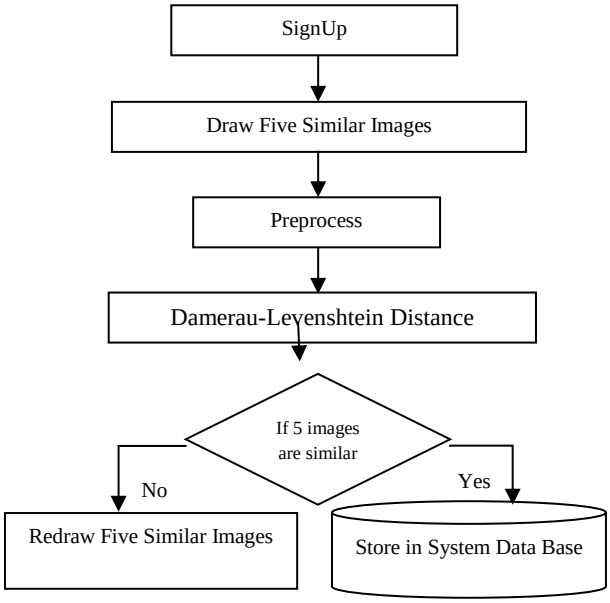

Figure 2. Architecture of Free-Hand Sketch Password Registration Procedure.

Afterward, the suggested model proceeds to analyse each image by tallying the quantity of black pixels present in every row and column. These numerical outcomes are then catalogued in an array list. Subsequently, the list undergoes a transformation into strings, which are then transmitted to the DLD. The matching process involves scrutinizing the similarity among the five images, employing ten distinct combinations (illustrated as ${}^{5}C_{2}$) as depicted in Figure-3.

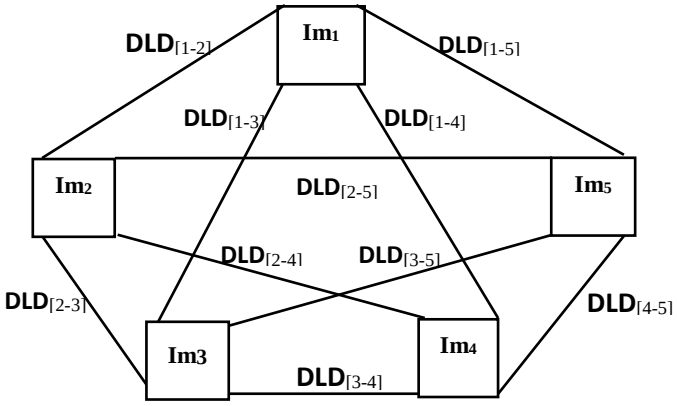

Figure 3. Images (Im_n) with Ten Combinations to Calculate Damerau-Levenshtein Distance-$DLD_{[i,j]}$

If the DLD determine a satisfactory level of similarity among the five images, then the system will proceed to store these images—changes the image size and trimmed—in its database. Conversely, if the DLD deems them dissimilar, the user will be prompted by the system to create another set of five similar sketch based images. The process is visually represented in Figure-3, where Im_1, Im_2, Im_3, Im_4, and Im_5 symbolize the user's five similar sketches. The notation $DLD_{[1-2]}$, $DLD_{[1-3]}$, $DLD_{[1-4]}$, $DLD_{[1-5]}$, ..., $DLD_{[4-5]}$ signifies the DLD percentages computed for 10 permutations of these input images.

3.2. Verification of authentication:

In Fig-4, the validation process using a sketch-based password is depicted. Process begins with the authorized user creating a password image accompanied by their account name. Subsequently, a pre-processing phase is initiated, employing a low-pass filter kernel, specifically Gaussian Blur, to reduce noise in the password image, thereby enhancing its smoothness. Following this, the original RGB (Red, Green, and Blue) image undergoes a transformation into a grayscale image after the noise has been effectively eliminated.

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024

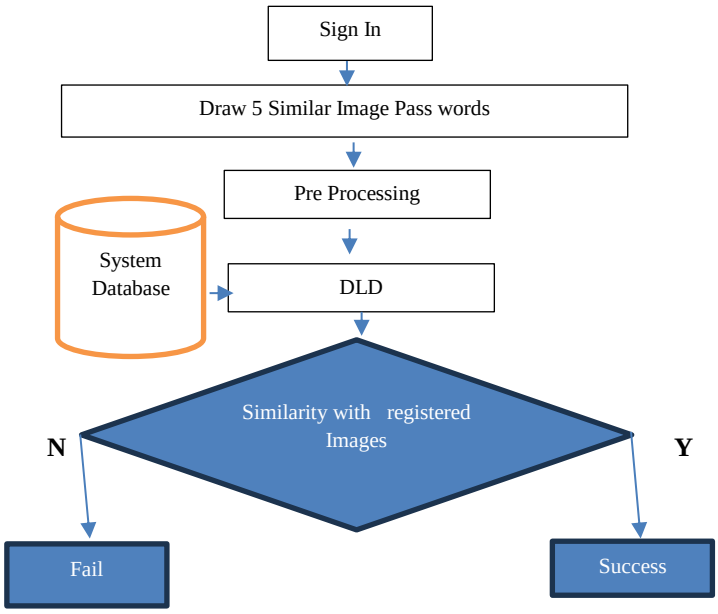

Figure 4. Architecture of Free-Hand Sketch Password Login Process

Improving the image quality involves employing an inverse thresholding using binary values to constrain and refine the image. The cropping procedure takes into account the edges of the object, accommodating the user's flexibility in sketching anyplace on the canvas. Following this, the image input undergoes resizing to a consistent dimension of 100x100 pixels. The system thoroughly manipulates and records the number of black pixels present in every row and column of the input image, recording the results in the list of an array. Then it get changed to strings and transmitted to DLD for verification, determining whether the input password picture aligns with pictures associated with sketches which are registered.

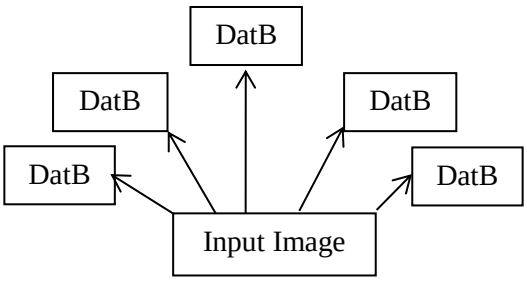

Figure 5. Analysing the Input Image and Database Pictures (DatB_i) for the computation of Damerau-Levenshtein Distance-$DLD_{(in,i)}$

When the sketch based images which are registered are matched with input sketch image, then the system takes the login as successful; otherwise, it is deemed unsuccessful and marked as a failure. The registered sketches are archived in the database to be accessed for validation.

In Fig-5, DatB_1, DatB_2, DatB_3, DatB_4, and DatB_5 represent the sketch based images which are saved in data base. Image input refers to the user's picture (sketch-based) password during the login process. The terms $DLD_{(in,1)}$, $DLD_{(in,2)}$, $DLD_{(in,3)}$, $DLD_{(in,4)}$, and $DLD_{(in,5)}$ indicate the DLD percentages computed for the 5different permutations.

3.3. Damerau-Levenshtein Distance:

The Damerau-Levenshtein Distance (DLD) algorithm [19], named after Frederick Damerau and Vladimir Levenshtein, includes an additional operation like inversion of adjacent characters and compatibility is measure with similarity between two strings. It is characterized by the least number of operations needed to convert one string into another. The actions allowed are insertions, deletions, substitutions, and transpositions of adjacent characters. The DLD is similar to the more well-known Levenshtein distance, but it also includes the transposition

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024

operation. This makes it more suitable for use in natural language processing tasks where transposition errors are common, such as in spelling correction or OCR (optical character recognition). The DLD algorithm is a modification of the Levenshtein distance algorithm, which is employed for determining the minimal number of actions needed to convert one string to another. This means that it allows for the swapping of two adjacent characters in a string as one of the possible actions that can be applied to transform the string. The algorithm creates a matrix wherein each cell signifies the minimum operations needed to convert the initial i characters of one string into the initial j characters of another string.

Damerau-Levenshtein Distance Algorithm Steps:

Step 1: Create a matrix `d` with dimensions `(len_str1) x (len_str2)`, where `len_str1` is the first string length plus 1, and `len_str2` is the second string length plus 1.

Step 2: Set the initial row with values ranging from 0 to the length of `len_str1` and Set the initial column with values ranging from 0 to the length of `len_str2`.

Step 3: Iterate through each cell `(i, j)` in the matrix, starting from `(1, 1)`.

Step 4: Calculate the cost of the current operation (insertion, deletion, substitution) based on the characters at positions `i-1` and `j-1`.

Step 5: Update the current cell `(i, j)` with the minimum cost of three probable actions (substitution, insertion, deletion).

Step 6: If a transposition is possible (characters match with the ones two positions back), consider it as a possible operation and update the current cell accordingly.

Step 7: The bottom-right cell of the matrix (`d[len_str1 - 1][len_str2 - 1]`) contains the Damerau-Levenshtein Distance between the two strings.

Let's apply these steps to the example "kitten" and "sitting":

Initialization:

Matrix d:

[[0, 1, 2, 3, 4, 5, 6],

[1, 0, 0, 0, 0, 0, 0],

[2, 0, 0, 0, 0, 0, 0],

[3, 0, 0, 0, 0, 0, 0],

[4, 0, 0, 0, 0, 0, 0],

[5, 0, 0, 0, 0, 0, 0],

[6, 0, 0, 0, 0, 0, 0]]

```

- **Filling in the Matrix:**

```

Matrix d:

[[0, 1, 2, 3, 4, 5, 6],

[1, 1, 2, 3, 4, 5, 6],

[2, 2, 1, 2, 3, 4, 5],

[3, 3, 2, 1, 2, 3, 4],

[4, 4, 3, 2, 1, 2, 3],

[5, 4, 4, 3, 2, 2, 3],

[6, 5, 5, 4, 3, 3, 3]]

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024

Damerau-Levenshtein Distance: 3

So, the smallest quantity of operations needed to accomplish the transformation "kitten" into "sitting" is 3 (insert 's', substitute 'i' for 'e', and insert 'g').

3.4. Gaussian Filtering Method:

Gaussian filtering [15] techniques is a popular image processing method used to blur or smooth images by reducing noise and preserving edges. It works by convolving an image with a Gaussian kernel, which is a 2D bell-shaped function that represents the probability distribution of a Gaussian random variable. The Gaussian filter is defined by its standard deviation (sigma) and kernel size (width and height). The larger the sigma, the wider the Gaussian distribution, and the more smoothing affect the filter will have on the image. The kernel size determines the extent of the Gaussian filter, and larger kernel sizes will result in stronger smoothing effects.

The process of Gaussian filtering involves the following steps:

a. Create a Gaussian kernel with a given sigma and kernel size.
b. Convolve the kernel with the image using a convolution operation. This involves sliding the kernel over the image and multiplying each kernel value by the corresponding pixel value in the image.
c. Normalize the resulting values by dividing them by the sum of the kernel values to maintain the image brightness.
d. Gaussian filtering has a wide range of applications in image processing, such as image enhancement, noise reduction, feature extraction, and edge detection. It is commonly used as a preprocessing step before performing more complex image analysis tasks, such as object recognition or segmentation.
e. Normalize the kernel by dividing all values by the sum of the kernel values to ensure that the resulting image has the same brightness as the original image.
f. Convolve the Gaussian kernel with the image using a convolution operation. This involves sliding the kernel over the image and computing the weighted average of the pixel values in the kernel neighbourhood.
g. Repeat the convolution process for each pixel in the image to generate the final smoothed image.
h. The new image (G (x, y)) on the right is produced by moving the sample filter (H (u, v)) around the original image (F (x, y)).

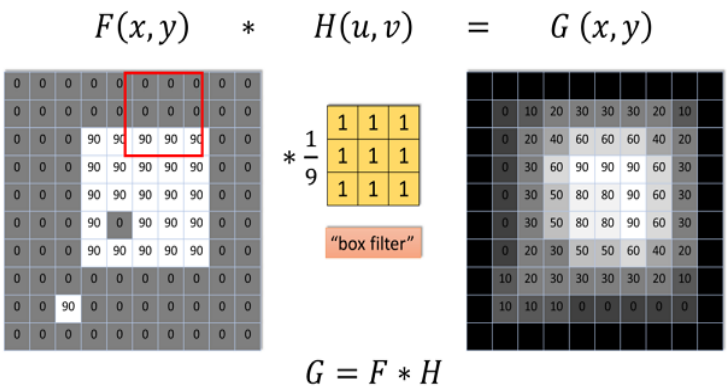

Figure 6. Pre-processing technique in Gaussian filtering

4. Experimental Results

The model classification analysis is evaluated in three step process for accurate image identification from the given Free-Hand Sketches with features like similar and dissimilar methods. Similar images have common features, characteristics or attributes that make them alike or comparable to each other. On the other hand, dissimilar images have unique features, characteristics or attributes that make them different from each other. When creating Free-hand sketches, you can vary the features and characteristics of your images to make them similar or dissimilar. This can include changing the size, shape, texture, or orientation of your drawings. Experimenting with these different elements can help you create images that are both unique.

4.1 Registration Process with experimental results:

The registration process evaluations are classified with three different cases findings such as all similar images, one single dissimilar image, and five dissimilar images.

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024

Case- 1: All Similar Images:

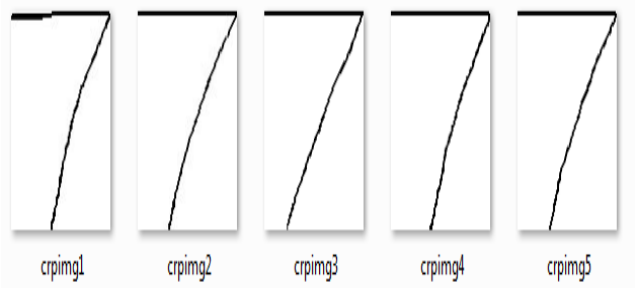

Figure 7. All Similar Images

In the initial registration stage, if a user opts to use 5similar image passwords, as illustrated in Fig-7, Table-1 showcases the outcomes of DLD's matches for both successful and unsuccessful attempts among the 10 potential combinations ($^5C_2$) derived from these 5 sketch-based password images. Within this collection of ten combinations, table-2 presents the variations between adjacent images for the 45 conceivable pairings ($^{10}C_2$).

Table-1 is categorized into 3differentkinds: (a) Uniformity in all provided image passwords, (b) Presence of a single image password that differs from the others, and (c) Complete dissimilarity among all user-input image passwords. These categories are further subdivided into 2categories: (i) Column-wise Percentage and (ii) Row-wise Percentage, derived from DLD ratios. The initial column in Table-1 is labelled from C1 through C10, where C1 signifies the coupling of Pictures one and two, C2 denotes the blending of pictures one and three, and so forth for the rest of the permutations. The presented model analyses image pairs both row-wise and column-wise, providing percentages for both rows and columns. If DLD specifies a likeness range of 30% to 100% for 2 pictures, and both column and row percentages are at minimum 30%, the success (S) count increments by 1; otherwise, the failure (F) count increments by 1. Similar to table-1 and tabkle-2 is structured around 3 major types: (a) Uniformity in all provided picture passwords, (b) Existence of a single picture password that differs from others, and (c) Complete dissimilarity among all user-input image passwords. These primary categories are further subdivided into: i) Differences adjacent to columns, and (ii) Differences adjacent to rows. The first column of Table-2 enumerates combinations such as (C_3-C_1), (C_2-C_1),(C_4-C_1), extending up to (C_{10}-C_9). These combinations represent the adjacent differences in column% and row% values from Table-1. The adjacent differences, both column-wise and row-wise, are computed from the percentages provided by DLD. If the disparity between adjacent rows is a minimum of 30%, the tally increments by one. Likewise, when the difference between adjacent columns reaches or exceeds 30%, the count also undergoes an increase.

Table 1: The number of unsuccessful registrations in the Sketch-based Image Password Registration process.

Comparison of Images with Combinations	**5 Similar Images**		**1 Dissimilar Image**		**All Dissimilar Images**	
	Row Per	**Col Per**	**Row Per**	**Col Per**	**Row Per**	**Col Per**
C1: Img[1,2]	59	30	1	31	53	24
C2: Img[1,3]	64	31	4	25	5	17
C3: Img[1,4]	65	35	0	31	22	22
C4: Img[1,5]	63	32	1	31	2	9
C5: Img[2,3]	74	58	74	58	9	29
C6: Img[2,4]	66	55	66	55	24	29
C7: Img[2,5]	70	67	70	67	7	10
C8: Img[3,4]	61	66	61	66	26	9
C9: Img[3,5]	63	58	63	58	61	13
C10: Img[4,5]	75	57	75	57	21	37
Failure Count<30	F= 0		F= 4		F= 10	
	Registration Success		Registration Failed		Registration Failed	

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024

Case2- One Single Dissimilar Image:

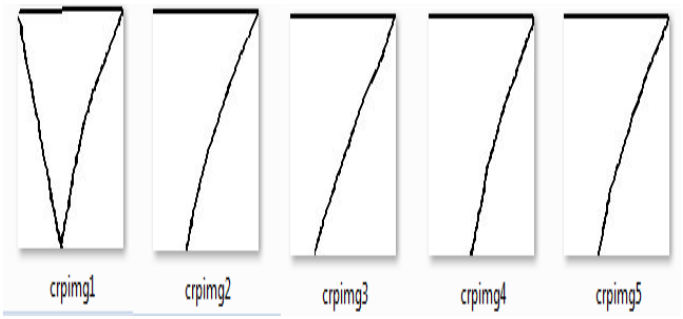

Figure 8. One Single Dissimilar Image

When a unique picture password input is provided by the person, as illustrated in Fig-8, the suggested method generates diverse outcomes, as outlined in tables 1 and 2. In the table-1, 4th and 5th columns encompassing image combinations from C_1 to C_4, both column and row percentages are below 30%, specified in the colour yellow. Conversely, for combinations spanning from C_5 to C_{10}, both percentages exceed 30%. In adherence to the conditions specified in case-1, there are 4 instances of failure. Turning to table-2, the fourth and fifth columns reveal that the count of adjacent differences in rows & columns reaching or surpassing 30% is 0 and 15, respectively. If the number of failures equal or exceed four, or if the count of adjacent differences in either rows or columns reaches nine or more, the prescribed approach signals an unfavourable outcome. In such cases, users are advised to generate five similar sketch-based image passwords anew.

Table 2: Counting the adjacent differences in rows and columns for DLD during the Sketch-Based Image Password Registration process.

Adjacent Differences (AD)	5 Similar Images		1Dissimilar Image		All Dissimilar Images	
	RowAD	Column AD	RowAD	Column AD	RowAD	ColumnAD
(C1-C2)	6	1	3	5	48	7
(C1-C3)	7	5	1	1	31	2
(C1-C4)	4	2	0	1	51	14
(C1-C5)	15	28	73	28	44	5
(C1-C6)	8	26	65	25	29	5
(C1-C7)	12	37	69	37	47	14
(C1-C8)	2	37	60	36	27	15
(C1-C9)	4	28	62	28	8	11
(C1-C10)	16	28	74	27	33	13
(C2-C3)	1	4	4	6	17	5
(C2-C4)	2	1	3	6	3	8
(C2-C5)	9	27	70	33	4	12
(C2-C6)	2	25	63	30	19	12
(C2-C7)	6	36	66	42	1	7
(C2-C8)	4	36	57	41	21	8
(C2-C9)	2	27	59	33	56	4
(C2-C10)	10	27	71	32	15	20
(C3-C4)	3	3	1	0	20	12
(C3-C5)	8	23	74	27	13	7
(C3-C6)	1	21	66	24	2	7
(C3-C7)	5	32	70	36	16	12

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024

(C3-C8)	5	32	61	35	4	13
(C3-C9)	3	23	63	27	39	9
(C3-C10)	9	23	75	26	2	15
(C4-C5)	11	26	73	27	7	19
(C4-C6)	4	24	65	24	22	19
(C4-C7)	8	35	69	36	5	0
(C4-C8)	2	35	60	35	24	1
(C4-C9)	0	26	62	27	59	3

Case 3-Five Dissimilar Images:

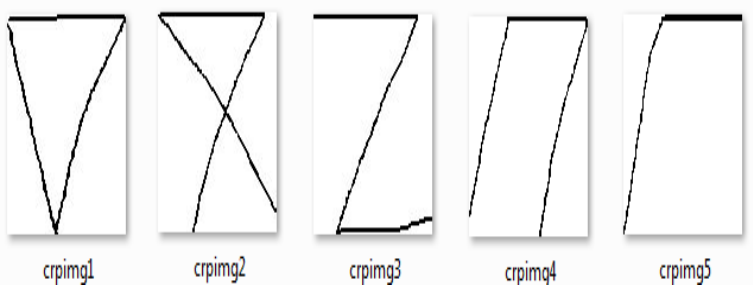

Figure 9. Five Dissimilar Images

When user-supplied input passwords(sketch-based) exhibit distinctiveness, as illustrated in figure-9, the method produces varied outcomes, as emphasized in Tables-1 and Table-2. Significantly, within Table-1, in both column-6 and column-7, the respective row percentages and column percentages for image combinations spanning from C_1 to C_{10} consistently register values below the 30% threshold. Adhering to the stipulations set forth in Case-1, there are 10 occurrences of failure. Similarly, within columns 7 and 6 of Table-2, there are 0 instances of column-wise counts and 14 instance of row-wise count where differences between adjacent values surpass the 30% threshold. When the total number of failures reaches 4 or more, or if the total counts of column or row adjacent differences are 9 or more, the system suggests the user to generate 5 new sketch-based picture passwords.

4.2 Results from the experiments alongside the login procedure:

The methodology under consideration discerns 2 cases within the login process of user:

Case 1: Image password for a valid login

Case 2: Image password for a Invalid login

Case 1: Image password for a valid login:

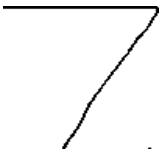

Figure 10. Login valid Image Password

Upon generating a valid image password login, which is mentioned in Fig-10, the process involves employing the Damerau-Levenshtein Distance (DLD) algorithm. The algorithm computes the percentages for both columns and rows comparing the sketch password login with the saved image passwords, found in the columns 2 & 3 of table-3. DLD examines the image login password (INP) against the 5 images stored in the database ($DB_1$to DB_5), recording the corresponding row and column percentage values in the table-3. If both the row and column percentage surpass 30%, the tally of the success will be increased by one; else, the tally of the failure does. As per table-3, under these circumstances, columns two and three percentage values show 5 as successes count and 0 as failures count. With the success count of 5 exceeding the failure count of 0, the model confirms the user's authorization, facilitating a successful login.

Case 2: Image password for an Invalid login:

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024

Figure 11. Invalid Login Image Password

In the event of a user generating login image password that is not valid, as depicted in Fig-11, the process involves utilizing the Damerau-Levenshtein Distance (DLD) algorithm to derive row and column percentages. This algorithm compares the login sketch password with the saved ones located in columns 4 and 5 of Table-3. The Matcher assesses the login sketch (IMP) against the five images stored in the database (DB_1 to DB_5), presenting details on row and column percentage in Table-3. If both the row and column percentage exceed 30%, the tally of success increases by 1; otherwise, the count of failure increases by 1. As per the specified criteria, columns 4 and 5 in Table-3 indicate zero successes (0) and 5 failures. Since the success tally of 0 is surpassed by the 5 failures, the system concludes that the user is not real and suggests them to re-enter the sketch-based password

Table 3: DLD Correct and Wrong Input Image Sketch Passwords

Image Combinations	**Correct Login Sketch Password**		**Wrong Login Sketch Password**	
	Row%	**Col%**	**Row%**	**Col%**
[INP-DB1]	60	37.62	8.57	6.86
[INP-DB2]	73.08	59	4.81	5.88
[INP-DB3]	66.36	62	8.41	6.86
[INP-DB4]	65.05	60	5.83	8.82
[INP-DB5]	50.49	51	7.77	8.82
Outcome	**S=5**	**F=0**	**S=0**	**F=5**
	Login Successfully		**Login Unsuccessful**	

4.3 Performance Evaluation on DLD:

The DLD model's outcomes underwent assessment using performance metrics. In gauging accuracy, we employed recall and precision as key benchmarks. Precision, recall, and overall accuracy metrics were determined based on TrueNegative, True Positive and False Negative, False Positive values. The formulas for these metrics [8], as outlined in Table-4, were utilized to calculate the model's accuracy. The summarized results are shown in Table-5.

Table 4: Precision, Recall and Accuracy Metric Formulas

Metrics	**Formulas**
Precision	N(TPv) / (N(TPv)+ N(FPv))
Recall	N(TPv) / (N(TPv)+ N(FNv))
Accuracy	(N(TPv) + N(TNv)) / (N(TPv)+ N(TNv)+ N(FPv)+N(FNv))

Note:

1. During the registration process, providing more than 5 input images leads to heightened memory utilization and processing time, imposing a computational load. Equally, a decrease in the number of input images below 5 results in a reduction in the success rate. Striking a balance between minimizing computational strain and attaining a targeted success rate of 94%, users are mandated to submit 5 images during registration.
2. Within the designated canvas dimensions of 1368x730, users can freely craft their sketch-image patterns. Gaussian Filtering supports object detection, followed by image processing, resizing to 100x100, and

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024

subsequent storage. Employing an image size beyond 100x100 amplifies computational requirements. Conversely, sizes below 100x100 tend to compromise the rate of accuracy, aiming for a benchmark of 94%.

Table 5: Damerau–Levenshtein distance with 25% Threshold on 50 Images

	FN	TP	FP	TN	Recall	Precision	Accuracy
IN1	4	46	4	46	92	92	92
IN2	6	44	3	47	88	94	91
IN3	1	49	5	45	98	91	94
IN4	0	50	3	47	100	94	97
IN5	0	50	5	45	100	91	95
IN6	0	50	5	45	100	91	95
IN7	5	45	3	47	90	94	92
IN8	3	47	3	47	94	94	94
IN9	0	50	2	48	100	96	98
IN10	5	45	2	48	90	96	93
					95	92	94

4.4 Different FHSBASS Models Comparison results:

Table-6 displays a comparative analysis of different models, which encompasses the FreeHand Sketch Base Authenticated Security System, employing FuzzyWuzzy & DLD.

Table 6: Comparison Results of FHSBASS FuzzyWuzzy Partial Ratio and DLD Models

Model Name	Images used during registration	Images used for testing and training	Time Complexity		Memory occupied for registered images	% of Accuracy
			SignIn	SignUp		
FuzzyWuzzy	5	500	1 to 2	1 to 2	20KB	92%
DLD	5	500	1 to 2	1 to 2	20KB	94%

Five sketch-based pictures were utilized for registration in the FuzzyWuzzy and DLD models. For testing and training purposes, 500 images were utilized in both models. The image is cropped in the FuzzyWuzzy Model based on the edges of the pattern using the Gaussian Filtering Technique to diminish the noise in the images, whereas Gaussian Blur Model is used in Damerau Levenshtein Distance to reduce image noise. This technique works as a Low Pass filter kernel, effectively removing noise from the RGB images to produce Grayscale images. A binary inverse threshold is used to precisely cut and restrict the image in order to get better results.

Where FHSBASS is Free Hand Sketch Based Authenticated Security System.

When evaluating the two models, FHSBASS with FuzzyWuzzy and DLD, both models necessitate users to choose 5 sketches at the time registration. The registration and login period for two of the models ranges from 1 to 2 seconds. Each model utilizes 20KB of memory in the data memory to save these image sketches. The newer model underwent training and testing on the 500 sketch-based images. While the original model success frequency views at 92%, the newer one attains a superior success frequency of 94%.

5. Conclusion

This study presents a FreeHand Sketch-based Authentication Security System that utilizes the DLD algorithm. In the broader context, security mechanisms fall into two main categories: sketch-based and text-based password systems. The primary objective of this research is to streamline the user's effort in memorizing passwords and to increase the security of digital accounts. The proposed approach allows users to register, using a distinctive sketch-based image pattern as their password, which was drawn on their own pattern. This enables a straightforward

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024

login process using their own image password, posing a challenge for unauthorized users attempting to try the passwords.

The efficacy of the DLD algorithm in user authentication is demonstrated in Table-3. Analysis was done on the sample image passwords, calculated their precision, accuracy and recall using DLD, with detailed results provided in Table-5. The proposed system achieves an authentication accuracy of 94% in verifying valid users. In Fig-12, the accuracy, recall and precession are graphed for 10 sample passwords across 50 trails based on the obtained results as per table-5. Exploring this avenue exhibits potential for robust user identification, enhancing data security against intruders. This process may evolve as a prominent validation method in the digital realm in the future.

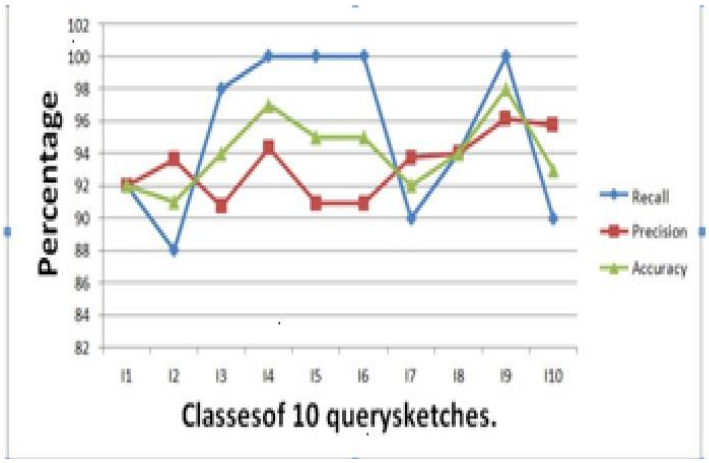

Figure 12. Graphical representation of Recall, Precision and Accuracy of different Image Passwords (Sketch-Based)

Acknowledge

I am very much thankful to my Supervisor Prof. P.V.G.D Prasad Reddy, Co Supervisor Dr.G.Srinivas for their Guidance, Support and constant Monitoring of my PhD work and heartfelt gratitude to my family members and Almighty.

References

[1] **"**Cloning SIM Cards Usability Reduction in Mobile Networks", Mustafa A. Al-Fayoumi, Nidal F, Shilbayeh, J NetwSyst Manage(2014)22:259-279, DOI 10.1007/s10922-013-9299-8.

[2] "Forensic SIM Card Cloning Using Authentication Algorithm", Nuril Anwar, Imam Riadi, Ahmad Luthfi. , Int. J. of Electronics and Information Engineering, Vol 4, No.2, PP. 71-81, June 2016.

[3] "An Alternative Method for Understanding User-Chosen Passwords", Zhixiong Zheng, Haibo Cheng, Zijian Zhang, Yiming Zhaoand Ping Wang. , Hindawi Security and Communication Networks, Volume January, 2018, Article ID 6160125.

[4] "Social Engineering Threats and Awareness- A Survey", Anshul Kumar, Mansi Chaudhary and Nagresh Kumar. , European Journal of Advances in Engineering and Technology, 2015, 2(11): 15-19, ISSN: 2394 - 658X.

[5] "Impact of Artificial Gummy Fingers on Fingerprint Systems", Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino. Optical Security and Counterfeit Deterrence Techniques IV, Rudolf L. van Renesse, Editor, Proceedings of SPIE Vol. 4677 (2002) © 2002 SPIE · 0277-786X.

[6] "Characteristic mining of Mathematical Formulas from Document - A Comparative Study on Sequence Matcher and Levenshtein Distance procedure", G.AppaRao, G.Srinivas, K.VenkataRao, P.V.G.D. Prasad Reddy, Volume-6, Issue-4 E-ISSN: 2347-2693, 30th April, 2018.

[7] "A Partial Ratio And Ratio Based Fuzzy-Wuzzy Procedure For Characteristics Mining Of Mathematical Formulas From Documents", G. AppaRao, G. Srinivas, K. VenkataRao and P.V.G.D. Prasad Reddy. , ISSN: 2229-6956, ICTACT Journal On Soft Computing, July 2018, Volume: 08, ISSUE: 04.

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024

[8] "A Heuristic Ranking of Different Characteristic Mining Based Mathematical Formulae Retrieval Models", K.N.BrahmajiRao, G.Srinivas, P.V.G.D.PrasadReddy,T.Surendra,, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019.

[9] "Mobile phone cloning", Kareena Bisht, Pragya Chimnani, and Rajveer Marwal., March 2018 | IRE Journals | Volume 1 Issue 9 | ISSN: 2456-8880.

[10] "FreeHand Sketch-based Authenticated Security System using Convolutional Neural Network", S. Amarnadh, P.V.G.D. Prasad Reddy and N.V.E.S. Murthy., International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019.

[11] "FreeHand Sketch-based Authenticated Security System using Levenshtein Distance and Coordinates-Similarity", S.Amarnadh, P.V.G.D.Prasad Reddy and N.V.E.S.Murthy., International Journal of Scientific & Technology Research (IJSTR) ISSN: 2277 – 8616, Volume-9 Issue-3, March, 2020.

[12] "FreeHand Sketch-based Authenticated Security System using Sequence Matcher", S.Amarnadh, P.V.G.D. Prasad Reddy and N.V.E.S. Murthy., International Journal of Advanced Science and Technology (IJAST) ISSN: 2005-4238, Volume-29 Issue-4, 2020.

[13] "Words Versus Pictures: Leveraging the Research on Visual Communication", Pauline Dewan. The Canadian Journal of Library and Information Practice and Research, Vol 10, No. 1(2015).

[14] "Authenticated Security System based on FreeHand Sketch using FuzzyWuzzy Partial Ratio", N.KesavaRao, G.Srinivas, P.V.G.D.Prasad Reddy, S.Amarnadh, Journal of Theoretical and Applied Information Technology(JATIT), ISSN:1992-8645 , Volume-101 , Issue-22, 30th Nov, 2023.

[15] "Investigation on the Effect of a Gaussian Blur in Image Filtering and Segmentation", Estevao S. Gedraite, Murielle Hadad. Research Gate Conference Paper, January 2011.

[16] "DamerauLevenshtein distance for indonesian spelling correction", Puji Santosoa, Pundhi Yuliawati, Ridwan Shalahuddin, AjiPrasetya Wibawa, JURNAL INFORMATIKA, ISSN: 1978-0524, Vol. 13, No 2, July 2019, pp. 11-15.

[17] "Spelling Correction Application with DamerauLevenshtein Distance to Help Teachers Examine Typographical Error in Exam Test Scripts", Viny Christanti Mawardi ,Fendy Augusfian , Jeanny Pragantha , and Stéphane Bressan. E3S Web of Conferences, Vol-188, Article No. 00027 (8th Sept, 2020), ICESTI 2019.

[18] "A Levenshtein Transpose Distance Algorithm for approximating String Matching", Meena Malviya, Rajendra Gupta, World Academics Journal of Management, E-ISSN: 2321-905X, Vol.6, Issue.2, pp.01-04, 31st December, 2018.

[19] "Damerau-Levenshtein Distance Algorithm Based on Abstract Syntax Tree to Detect Code Plagiarism", Ahlijati Nuraminah, Abdullah Ammar, Scientific Journal of Informatics, e-ISSN 2460-0040, p-ISSN 2407-7658, Vol. 11, No. 1, 2024.

DOI: https://doi.org/10.54216/JCIM.150128
Received: April 16, 2024 Revised: June 15, 2024 Accepted: August 18, 2024