Journal of Theoretical and Applied Information Technology

30th November 2023. Vol.101. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AUTHENTICATED SECURITY SYSTEM BASED ON FREEHAND SKETCH USING FUZZY-WUZZY PARTIAL RATIO

N. KESAVA RAO[1], G. SRINIVAS[2], P.V.G.D. PRASAD REDDY[3], S. AMARNADH[4]

[1]Research Scholar, AU College of Engineering, Andhra University, Department of CS&SE, India, Associate Professor, Narayana Engineering College, Gudur, Department of CSE, India
[2]Professor, GITAM Deemed to be University, Department of C.S.E., India
[3]Professor, AU College of Engineering, Andhra University, Department of CS&SE. India.
[4]Assistant Professor, GITAM Deemed to be University, Department of C.S.E., India
Email: [1]kesavarn@gmail.com, [2]srinivas.gitam@gmail.com, [3]PrasadReddy.vizag@gmail.com, [4]amarnadh07@gmail.com

ABSTRACT

This document presents the FreeHand Sketch-based Authentication Security System, a novel methodology for validation purposes. In the current digital world, security plays a significant role. The administrator takes many security measures, but still, it is getting hacked in different ways. To take digital data security to the next level, a new methodology is proposed with Fuzzy-Wuzzy with better accuracy. The approach allows users to register by sketching five similar images on their choice. These sketches undergo pre-processing using threshold with Gaussian mixture and Fuzzy-Wuzzy algorithm to assess their similarity. If all five pictures are deemed alike, they are stored in the database. For login, user can utilize their authorized information along with an image-based sketch password, which is also processed with threshold and Gaussian mixture and compared to the registered image passwords in the database for authentication using the Fuzzy-Wuzzy method. The proposed methodology's performance is evaluated using input sample image passwords and metrics like precision and recall. The proposed work demonstrates that user security can be ensured with an accuracy level of around 90% through authentication measures.

Keywords: *Biometric Systems, Authentication, Security, Fuzzy-Wuzzy, Authorization, Free Hand Sketch-Based Authentication, Security and Safety Patterns.*

1. INTRODUCTION

The paramount concern in the digital world is safety and security. The convenience and efficiency of online platforms, such as swift data transfers, financial transactions, and booking of travel and entertainment tickets, among other things, cannot be overstated. However, this convenience comes with a downside - security vulnerabilities. Potential attacks can occur through methods such as SIM swapping[1][2], password guessing, and more, compromising the overall security of the online system.

In response, various entities like corporations, educational institutions, and government agencies have adopted multiple online safety measures like finger biometrics, text-based passwords[3],one-time passwords (OTP), recognition of patterns, retina scanning, voice recognition, and many more. Yet, these protective measures do not guarantee absolute security. There is always the risk of unauthorized individuals deciphering these security protocols using strategies like SIM swapping, guessing text passwords, using artificial fingerprints, voice mimicry, etc. Furthermore, some measures, such as retina scanning, can pose health risks due to infrared radiation, thus discouraging its use.

Pattern security systems that involve nine-dot patterns can also be compromised, as unauthorized individuals might track the pattern after multiple attempts. A novel security system called Free Hand Sketch Based Authenticated Security System (F.H.S.B.A.S.S.) employing Fuzzy-Wuzzy has been proposed to overcome these challenges. The Fuzzy-Wuzzy algorithm determines the longest common subsequence elements between two distinct strings, with a comparison ratio of 0 to 100.

In this system, Fuzzy-Wuzzy compares the sketch-based login image with pre-registered sketch-based image passwords in the database, thoroughly explaining this validation procedure in

the projected methodology section. Registration involves the official individual drawing their unique image patterns while providing a username, text password, and other relevant information. The same details, including the sketch pattern, are required for login. This innovative method makes it challenging for unauthorized individuals to crack the image-based password. Thus, the proposed methodology potentially elevates the level of online security.

2. PROBLEM STATEMENT

In today's digital age, most tasks are carried out online and safeguarded with various security measures, including biometrics, text passwords, OTPs and less frequently, speech recognition and scanners of the retina. However, these measures are still susceptible to breaches by unauthorized users who employ various illicit tactics. These tactics range from guessing text passwords[13] through numerous attempts, cloning biometrics with artificial fingerprints[5], SIM card cloning via social engineering[4], and voice imitation of authorized users, cracking smart phone patterns through various combinations of the nine-dots on screen. The use of eye retina scanners presents its own set of challenges. Prolonged exposure of the eyes to infrared rays from a distance of fewer than two centimetres for over ten seconds can potentially cause temporary or permanent damage, making this method less popular.

Moreover, guessing text passwords can be relatively straightforward for unauthorized individuals, especially if the password is short or based on personal details such as relative names, birth dates, or mobile phone[9]. Longer, more complex passwords offer better security but are harder for users to remember. OTP security can also be compromised if an unauthorized user clones a cell phone and SIM using social engineering techniques. Similarly, fingerprint systems can be stolen with the artificial fingerprints of a legal user. Although general passwords and fingerprint information require less memory and facilitate quicker registration and login processes for online digital accounts, they offer limited security.

Figure 1: Hacking Identity Theft System

Some models have already been designed earlier to secure the data using sketch-based image passwords like Convolutional Neural Network[10], Levenshtein Distance[6]& Coordinators Similarity[11], and Sequence Matcher[6][12].These existing models have their advantages and disadvantages when compared with each other. However, the accuracy of all these current models ranges between 84% to 90%. So, to get a better percentage than the existing models, a new model is proposed using Fuzzy-Wuzzy[7] with a partial ratio. Fuzzy-Wuzzy can also be used to check the similarity of two different strings. It was taken as a reference and implemented in the proposed model to study the similarity of two other sketch-based images.

3. METHODOLOGY

Typically, the human brain struggles more with recalling long text passwords than short ones. However, shorter passwords offer considerably less security. Likewise, biometric security systems are vulnerable to breaches using unnatural fingerprints, while OTPs could be compromised through SIM-swapping methods employing social engineering.

To counter these security issues, an enhanced security feature, "F.H.S.B.A.S.S. using FuzzyWuzzy Partial Ratio", has been proposed. In this system, users can create an image password of their choice during registration and login. During registration, users are required to draw five identical sketch-based images of their selection. Once registration is successful, users can log in by reproducing their chosen image password.

This system has shown promising results, with authorized users achieving approximately a 92% success rate, as detailed in the experimental results section. This new method offers a robust defense against conventional security breaches while enhancing user-friendliness and memorability.

3.1. Registration of Image Password

The graphic, titled Fig-2, illustrates the process of creating an image-based password in the database. Users initiate online account registration by generating five sketches of their selection, which should bear similarities. In the subsequent pre-processing stage, Gaussian Blur is deployed to lessen the images' noise, thereby refining them. This technique, a type of low-pass filter kernel, turns the RGB(Red-Green-Blue) image into a gray scale image after eliminating the noise from all five images.

A binary inverse threshold is implemented to trim and bind the image for optimized outcomes. The sketches are cropped considering the object boundaries since the user can draw anywhere on the canvas .Afterward, these five images are resized to a standard format of 100X100 pixels.

The proposed model then counts the number of black pixels in each row and column for every image, storing these values in an array list. This list is converted into strings and forwarded to the Fuzzy-Wuzzy Partial Ratio. The Matcher checks if the five images are alike, using ten different combinations ($^5C_2$), as demonstrated in Figure 3.

If the Fuzzy-Wuzzy determines the five images are sufficiently similar, the system will store these resized and cropped images in its database. If they aren't, the system will prompt the user to sketch another set of five similar photos again. Fig. 3 provides a visual depiction of this process: I1, I2, I3, I4, and I5 represent the five similar sketches made by the user. The notation F(1,2), F(1,3), F(1,4), F(1,5), ... F(4,5) denotes the Fuzzy-Wuzzy percentages calculated across ten combinations of these input images.

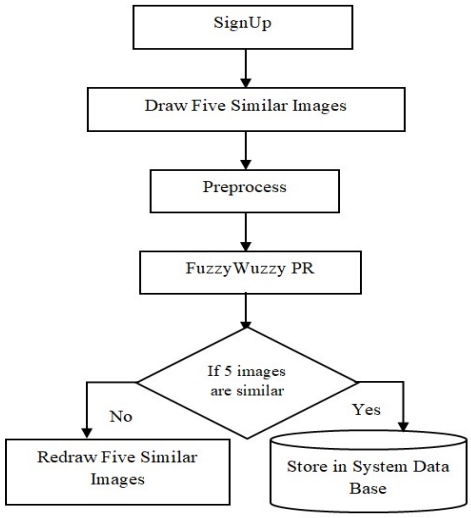

Figure 2: Architecture of Image Password Registration Process

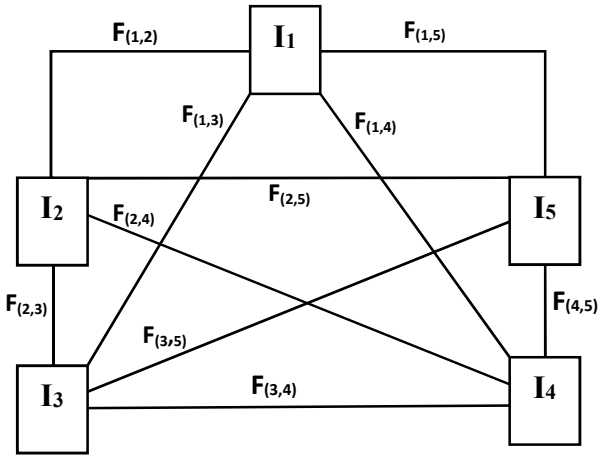

Figure3: 5 Images (Im) with Ten combinations to Calculate Fuzzy-Wuzzy Partial Ratio F(i,j)

3.2. Authentication Validation:

Fig-4 illustrates the authentication procedure via sketch-based password. To start, the approved user sketches their password image and account name. This is followed by the pre-processing phase, where a low-pass filter kernel, Gaussian Blur,is employed to decrease the noise within the password image, making it smoother. The original B.G.R. (Blue-Green-Red) image is then transformed into a grayscale picture when the noise is cleared.

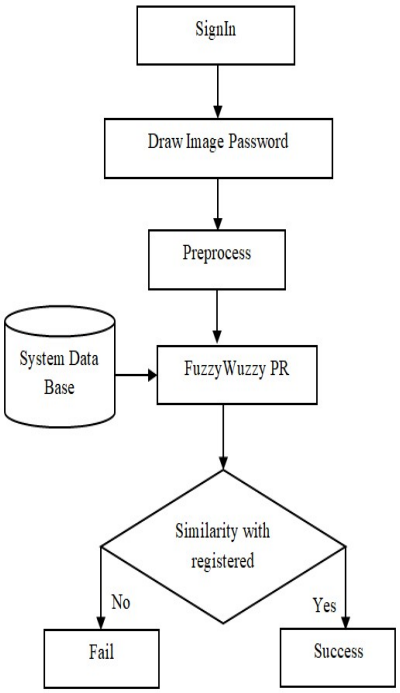

Figure 4: Image Password Login Architecture

A binary inverse threshold is used to confine and trim the image to enhance the picture. The cropping process considers the object's edges, considering the user can draw the sketch anywhere on the canvas. Subsequently, the input image is resized to a standardized size of 100X100 pixels. The system then calculates and stores the count of black pixels in each row and column of the input image into an array list. This list is converted into strings and relayed to Fuzzy-Wuzzy to verify if the input password image corresponds with images based on registered sketches.

If the registered sketch matches the input image, the system acknowledges the login attempt as successful. If it does not, it's marked as failed. These sketches, which are registered, are stored in the database for reference.

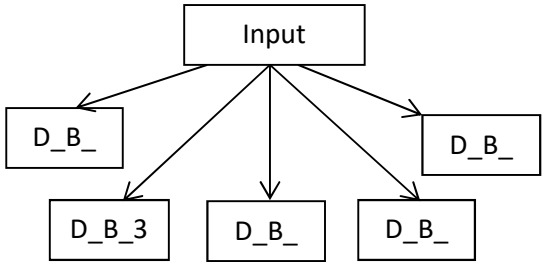

Figure 5: The comparison of Input Image and Data Base Pictures (D-B-i) to calculate Fuzzy-Wuzzy Partial Ratio F(in, i)

In Fig-5, D_B_1, D_B_2, D_B_3, D_B_4, and D_B_5 signify the stored sketch-based images. The Input Image stands for the user's sketch-based image password at login. The terms $F_{(in,1)}$, $F_{(in,2)}$,$F_{(in,3)}$,$F_{(in,4)}$,and $F_{(in,5)}$ denote the Fuzzy-Wuzzy percentages calculated across the five combinations.

3.3. Fuzzy-Wuzzy:

Fuzzy-Wuzzy is an algorithm that can used for matching the strings. It employs the Levenshtein Distance method in a user-friendly package to measure sequence variations. This is useful for scenarios where you want to find "fuzzy" matches of a string within a certain dataset or when you want to compare two similar but not identical strings.

Fuzzy-Wuzzy produces a ratio that indicates the similarity between two strings, ranging from 0 (entirely dissimilar) to 100 (identical). The library has functions like fuzz.token_sort_ratio, fuzz.ratio, fuzz.token_set_ratio and fuzz.partial_ratio, which can be utilized based on the specific requirements of your string comparison.

For example, suppose you have a list of words and must find the closest match to a particular word. In that case, you can use Fuzzy-Wuzzy to identify the most similar match, even if there's a typo or slight variation in the name you're searching for.

The proposed model leverages the Fuzzy-Wuzzy algorithm to assess the similarity percentage between two sketch-based images. The pixel count of a sketch-based image input password is typically high when initially drawn by the user, leading to increased time complexity during authentication evaluation. To alleviate this issue and save on memory, the input sketch-based image is set to 100x100 pixels tailored to the user's sketch.

In this method, the gray scale sketch-based image only contains two types of pixels: black and white, with pixel values of 255 and 0, respectively. The sketch-based image predominantly consists of white pixels, with a minimal number of black pixels. In this scenario, the Fuzzy-Wuzzy tends to return a more percentage (similarity), regardless of whether the sketch-based images are similar or dissimilar.

For more accurate results, black pixel values are extracted and saved in 2 separate arrays to yield a more similarity percentage for similar images and a low one for non-similar images. The first array keeps the computed count of row-wise black pixels, while the other one saves the count of black pixels column-wise for each image.

Both row-wise and column-wise array lists are then converted into strings to execute the Fuzzy-Wuzzy operation, which computes the similarity percentage. This process is reiterated for all sketch-based images. Finally, the model counts the instances where similarity percentages exceed 25% to ascertain whether the user is authorized.

Fuzzy-Wuzzy Partial Ratio Algorithm:

The Partial Ratio method in the Fuzzy-Wuzzy algorithm[14]measures the similarity between two strings based on the highest-scoring substring. Here is a conceptual explanation of how it works:

Step 1: Take two strings as input. Let's say "New York Mets" and "New Mets" for illustration.

Step 2: Identify the shorter of the two strings. In this case, it's "New Mets".

Step 3: For the longer string, find all substrings with the same length as the shorter string. Here, we have "New York", "ew York ", "w York M", " York Me", "York Met", and "ork Mets".

Step 4: Use the fuzzy ratio method (which calculates the standard Levenshtein Distance similarity) between the shorter string and each of the substrings identified in the previous step. This would give us a similarity score for each pair.

Step 5: Return the maximum of these similarity scores. The Partial Ratio score indicates the similarity between the original two strings based on the closest matching substring.

Note that the Partial Ratio method works best when a small string is expected to be a subset of a larger string, not necessarily at the beginning of the string.

3.4. Gaussian Filtering Method

Images obtained from various sources, such as camera sensors, may contain different kinds of noise. As depicted in Fig-6, Gaussian Filtering[15]reduces such disturbances and creates a smooth image, thus yielding superior results. This technique is especially effective in removing Gaussian noise from images. Moreover, it maintains the crispness of edges in images while minimizing unwanted blurring.

The Gaussian filtering technique is implemented in the projected model to trim the image according to the pattern edges. This method entails three parameters: (a) Border Type(B.T.), (b) Width(w) and Height(h), and (c) Source Image(S.I.). Both width and height are required to be odd positive integers.

Blur=cv2.GaussianBlur(SI,(h,w), BT)

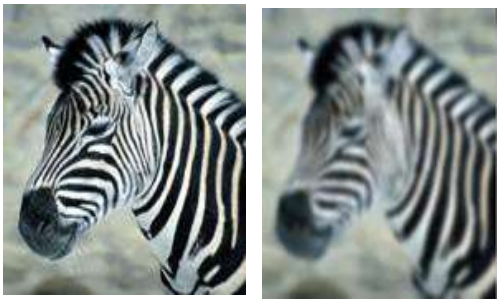

Figure 6: Before Blur Image and After Blur Image

4. EXPERIMENTAL RESULTS

In the proposed study, approximately 500 sketch-based images from 50 categories were examined. Each category had five images that were similar. Measurements such as Recall, Precision, and Accuracy were calculated across these 50 categories, yielding an impressive accuracy rate of 92%. The system requires users to create an account by drawing five sketches of their choice that should be similar. All five images are stored in the system's database if they match. However, if they do not match, the user must create five new similar sketches. For the sign-in process, users must draw an image. This drawn image is then compared to the previously registered sketches within the system's database. The login is successful if there's a match between the input and the stored sketches. If not, the login attempt fails.

Registration Process with experimental results:

During registration, the proposed system might come across three potential scenarios related to the user's input of image passwords.

These scenarios can be described as follows:

Scenario 1: All the image passwords given are alike.
Scenario 2: Only one of the image passwords provided is not similar to the others.
Scenario 3: All the image passwords input by the user are dissimilar to each other.

Scenario 1: All the image passwords given are alike:

Figure 7: Identical image-based passwords at the time of registration

During the sign-up phase, should a user provide five identical image passwords as depicted in Fig-7, the results of the Fuzzy-Wuzzy's successful and unsuccessful matches for the ten possible combinations ($^5C_2$) from these five password images are presented in Table-1. From this set of ten combinations, the neighbouring differences for the 45 possible pairings ($^{10}C_2$) of images are displayed in Table-2.

Table-1 is segmented into three distinct types they are (a) All the image passwords given are alike, (b) Only one of the image passwords provided is not similar to the others, (c) All the image passwords input by the user are dissimilar to each other. These categories are divided into two sub-types: (i) Row-wise Percentage(ii) Column-wise Percentage. Percentages are derived from the ratio provided by the Fuzzy-Wuzzy.In Table-1, the initial column displays labels from C_1 through C_{10}. For instance, C_1 represents the pairing of Images 1 and 2, C_2 signifies the combination of Images 1 and 2, and so on for the remaining combinations. The introduced model examines row and column image pairs, providing both row and column percentages. If the Fuzzy-Wuzzy indicates a similarity range between 30% to 100% for two images, and both row and column percentages are at least 30%, then the success (S) tally increases by one. If not, the failure (F) count rises by one.

Table-2, akin to Table-1, is organized into three primary categories: (a) All the image passwords given are alike, (b) Only one of the image passwords provided is not similar to the others, (c) All the image passwords input by the user are dissimilar to each other. These primary categories are divided into i)Differences adjacent to rows, (ii)Differences adjacent to columns. The initial column of Table-2 lists combinations like (C_1-C_2), (C_1-C_3), (C_1-C_4), up to (C_9-C_{10}). These combinations denote the adjacent differences of row% and column% values from Table-1. The adjacent differences, both row-wise and column-wise, are derived from percentages provided by the Fuzzy-Wuzzy. If the adjacent difference for rows is at least 30%, its tally increases by one. Similarly, if the adjacent difference for columns is 30% or more, its count also increases.

Table-1. FuzzyWuzzy Fail(F) count during Registration Process of Image Password

Image Comparisons with Combinations	5 Similar Images		1 Dissimilar Image		All Dissimilar Images	
	R %	C %	R %	C %	R %	C %
C_1: Img[1,2]	50	64	11	36	51	28
C_2: Img[1,3]	62	43	7	24	9	35
C_3: Img[1,4]	70	43	7	41	15	29
C_4: Img[1,5]	50	44	7	42	4	22
C_5: Img[2,3]	43	42	43	42	12	48
C_6: Img[2,4]	46	37	46	37	43	17
C_7: Img[2,5]	63	37	63	37	14	14
C_8: Img[3,4]	63	75	63	75	16	30
C_9: Img[3,5]	58	59	58	59	45	14
C_{10}: Img[4,5]	80	68	80	68	17	17
Failure Count<30 (Threshold)	F= 0		F= 4		F= 10	
	Registration Success		Registration Failed		Registration Failed	

From Table-1, among the 10 combinations, there are no failures (F = 0) in cases fewer than 4. From Table-2, from 45 combinations, the column-wise and row-wise counts are 4 and 8,which are<9.If these criteria are met, the proposed model determines the images to be sufficiently similar for registration and stores them in the system database. If not, the user is prompted to input five consistent images again.

Scenario 2: Only one of the image passwords provided is not similar to the others:

Figure 8: Five Identical and One Unique image-based passwords at the time of registration

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

When a user provides a distinct input image password, as depicted in Fig-8, the suggested model yields varied results displayed in table-1 and table-2. In table-1, 4th and 5th columns, for image combinations ranging from C_1 to C_4, both the row and column percentages are less than 30% and are marked in yellow. However, for combinations from C_5 to C_{10}, both percentages are 30% or more. Based on the conditions outlined in case-1, there are four failures. In table-2, 4th and 5th columns, the number of adjacent differences in rows and columns that are 30% or more stands at 0 and 15, respectively.

Table-2. The Count Of Fuzzy-Wuzzy Column And Row Wise Adjacent Differences Count During The Development Of Password Registration Of A Sketched Image

Adj. Diff.	5 Similar Images		1 Dissimilar Image		All Dissimilar Images	
	RWAdj-Df	CW Adj-Df	RW Adj-Df	CW Adj-Df	RW Adj-Df	CW Adj-Df
(C1-C2)	12	21	4	12	42	7
(C1- C3)	20	21	4	5	36	1
(C1-C4)	0	20	4	6	47	6
(C1-C5)	7	22	32	6	39	20
(C1-C6)	4	27	35	1	8	11
(C1-C7)	13	27	52	1	37	14
(C1-C8)	13	11	52	39	35	2
(C1-C9)	8	5	47	23	6	14
(C1-C10)	30	4	69	32	34	11
(C2-C3)	8	0	0	17	6	6
(C2-C4)	12	1	0	18	5	13
(C2-C5)	19	1	36	18	3	13
(C2-C6)	16	6	39	13	34	18
(C2-C7)	1	6	56	13	5	21
(C2-C8)	1	32	56	51	7	5
(C2-C9)	4	16	51	35	36	21
(C2-C10)	18	25	73	44	8	18
(C3-C4)	20	1	0	1	11	7
(C3-C5)	27	1	36	1	3	19
(C3-C6)	24	6	39	4	28	12
(C3-C7)	7	6	56	4	1	15
(C3-C8)	7	32	56	34	1	1
(C3-C9)	12	16	51	18	30	15
(C3-C10)	10	25	73	27	2	12
(C4-C5)	7	2	36	0	8	26
(C4-C6)	4	7	39	5	39	5
(C4-C7)	13	7	56	5	10	8
(C4-C8)	13	31	56	33	12	8
(C4-C9)	8	15	51	17	41	8
(C4-C10)	30	24	73	26	13	5
(C5-C6)	3	5	3	5	31	31
(C5-C7)	20	5	20	5	2	34
(C5-C8)	20	33	20	33	4	18
(C5-C9)	15	17	15	17	33	34
(C5-C10)	37	26	37	26	5	31
(C6-C7)	17	0	17	0	29	3
(C6-C8)	17	38	17	38	27	13
(C6-C9)	12	22	12	22	2	3
(C6-C10)	34	31	34	31	26	0
(C7-C8)	0	38	0	38	2	16
(C7-C9)	5	22	5	22	31	0
(C7-C10)	17	31	17	31	3	3
(C8-C9)	5	16	5	16	29	16
(C8-C10)	17	7	17	7	1	13
(C9-C10)	22	9	22	9	28	3
Count of AD ≥ 30	4	8	26	12	15	4

Table-2. The count of Fuzzy-Wuzzy Column and Row wise Adjacent Differences count during the development of Password Registration of a Sketched Image

Adj. Diff.	5 Similar Images		1 Dissimilar Image		All Dissimilar Images	
	RW Adj-Df	CW Adj-Df	RW Adj-Df	CW Adj-Df	RW Adj-Df	CW Adj-Df
(C1-C2)	12	21	4	12	42	7
(C1- C3)	20	21	4	5	36	1
(C1-C4)	0	20	4	6	47	6
(C1-C5)	7	22	32	6	39	20
(C1-C6)	4	27	35	1	8	11
(C1-C7)	13	27	52	1	37	14
(C1-C8)	13	11	52	39	35	2
(C1-C9)	8	5	47	23	6	14
(C1-C10)	30	4	69	32	34	11
(C2-C3)	8	0	0	17	6	6
(C2-C4)	12	1	0	18	5	13
(C2-C5)	19	1	36	18	3	13
(C2-C6)	16	6	39	13	34	18
(C2-C7)	1	6	56	13	5	21
(C2-C8)	1	32	56	51	7	5
(C2-C9)	4	16	51	35	36	21
(C2-C10)	18	25	73	44	8	18
(C3-C4)	20	1	0	1	11	7
(C3-C5)	27	1	36	1	3	19
(C3-C6)	24	6	39	4	28	12
(C3-C7)	7	6	56	4	1	15
(C3-C8)	7	32	56	34	1	1
(C3-C9)	12	16	51	18	30	15
(C3-C10)	10	25	73	27	2	12
(C4-C5)	7	2	36	0	8	26
(C4-C6)	4	7	39	5	39	5
(C4-C7)	13	7	56	5	10	8
(C4-C8)	13	31	56	33	12	8
(C4-C9)	8	15	51	17	41	8
(C4-C10)	30	24	73	26	13	5
(C5-C6)	3	5	3	5	31	31

If the count of failure reaches four or more, or if the count of adjacent row differences or adjacent column differences is nine or more, the recommended method indicates a negative result. It then advises the user to recreate five similar sketch-based image passwords.

Scenario 3: All the image passwords input by the user are dissimilar to each other:

Figure 9: Five dissimilar image-based passwords at the time of registration

If the user-provided input image passwords are all different, as depicted in Fig-9, the method yields distinct results, as highlighted in Table-1 and Table-2. In column-6 and column-7 of Table-1, specific row% and column% values for image combinations from C_1 to C_{10} are below 30%. Based on the criteria outlined in Case-1, there are ten failures. Similarly, in columns 6 and 7 of Table 2, there are 12 row-wise counts and one column-wise count where adjacent differences are 30% or

greater. If the count of failure is four or more, or if the row or column adjacent difference counts are nine or more, the method advises the user to generate five new sketch-based password images.

Experimental Results along with Process of Login:

The proposed methodology identifies two scenarios during the user's login process:

Case 1: Login valid Image Password

Case 2: Login Invalid Image Password

Case 1: Login valid Image Password:

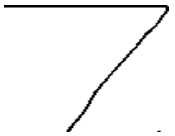

Figure 10: Login with a valid Image Password

When a user sketches a login valid image password, as depicted in Fig-10, the method provides the Fuzzy-Wuzzy column and row percentages between the login image password and the stored image passwords, visible in columns 3 and 2 of Table-3. This Fuzzy-Wuzzy assesses the login image password (I.N.P.) against the five saved database images (DB1 to DB5) and lists the row% and column% in Table 3. If both row% and column% are 30% or higher, the success tally increases by one; otherwise, the failure tally does. According to Table-3, with the specified conditions, the percentages in columns 2 and 3 indicate five successes and 0 failures. With the success count of 5 surpassing the failure count of 0, the model verifies the user as authorized and allows a successful login.

Case 2: Invalid login Image Password:

Figure 11: Invalid Login Image Password

When a user sketches an invalid login image password, as illustrated in Fig-11, the method outputs the Fuzzy-Wuzzy's row and column percentages, comparing this login image password with the stored ones, seen in columns 4 and 5 of Table-3. This Matcher evaluates the login image (I.M.P.) against the five saved database images (DB-1 to DB-5), detailing the row% and column% in Table-3. If row% and column% are at least 30%, the success tally rises by one, but if not, the failure count does. Given the criteria, Table 3's columns 4 and 5 indicate no successes (0) but five failures. With the success tally of 0 being outnumbered by the five failures, the system determines the user isn't authenticated and prompts them to input the image password again.

Table-3. Count of Failures (F) and Successes (S) for FuzzyWuzzy during the Sketch-based Image Password Login process.

Image Combinations	Authenticated Image Password for Login		Unauthenticated Image Password for Login	
	RW %	CW%	RW%	CW%
[IMP-DB-1]	60.95	35.64	15.24	28.85
[IMP-DB-2]	73.08	61	8.65	30.77
[IMP-DB-3]	71.96	67	5.61	29.81
[IMP-DB-4]	68.93	59	11.65	25
[IMP-DB-5]	51.46	51	11.65	26.92
Outcome	S=5	F=0	S=0	F=5
	Successful Login		Unsuccessful Login	

4.1. Performance Evaluation:

The results from the Fuzzy-Wuzzy model were assessed based on its performance metrics. To evaluate accuracy, we utilized both recall and precision as reference measures. The metrics of False Positive, False Negative, True Positive and True Negative served as the basis for determining precision, recall, and overall accuracy. Table-4 displays the metric formulas[8] used to compute the model's accuracy. These findings are summarized and presented in table-5.

Table -4. Metric Formulas Of Accuracy, Recall And Precision

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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table-5. RECALL, ACCURACY AND PRECISION USING FUZZYWUZZY ON SKETCH-BASED IMAGE PASSWORDS

FuzzyWuzzy Partial Ratio with 25% threshold on 50 Images							
	FN	TP	FP	TN	Recall %	Precision %	Accuracy %
IN1	5	45	8	42	90	85	87
IN2	1	49	3	47	98	94	96
IN3	2	48	2	48	96	96	96
IN4	1	49	7	43	98	88	92
IN5	0	50	6	44	100	89	94
IN6	0	50	9	41	100	85	91
IN7	4	46	8	42	92	85	88
IN8	2	48	3	47	96	94	95
IN9	5	45	5	45	90	90	90
IN10	3	47	3	45	94	94	94
Average Percentage					95%	90%	92%

NOTE:

1. When registering, if the number of input images exceeds 5, it increases processing time and memory usage, creating a computational burden. Conversely, with fewer than 5 input images, the success rate drops. To balance reducing computational strain with achieving a desired success rate of 92%, During the registration process, users are required to submit 5 images.

2. Users can create sketch-image patterns anywhere within the specified canvas dimensions of 1368x730. Gaussian Filtering aids in object detection, after which the image is processed, resized to 100x100, and saved. Using an image size larger than 100x100 intensifies computational demands. On the other hand, sizes below 100x100 tend to reduce the accuracy rate, targeting a 92% benchmark.

4.2. Comparison results of different F.H.S.B.A.S.S. Models:

Table-6 compares various models, including the FreeHand Sketch Base Authenticated Security System, using both Sequence Matcher[11] and Fuzzy-Wuzzy.

Table-6. Comparison Results of F.H.S.B.A.S.S. Sequence Matcher and Fuzzy-Wuzzy Partial Ratio Models

Model Name	Images used during registration	Images used for testing and training	Time Complexity		The memory occupied for registered images	Percentage of Accuracy
			Sign In	Sign Up		
Sequence Matcher	5	300	1 to 2	2 to 3	20 K.B.	90%
Fuzzy Wuzzy	5	500	1 to 2	1 to 2	20 K.B.	92%

Where F.H.S.B.A.S.S. is a Free Hand Sketch-Based Authenticated Security System.

In comparing the two models, F.H.S.B.A.S.S. with Sequence Matcher and Fuzzy-Wuzzy, both require five user-selected sketch-based images during the registration phase. The login time for both models is 1 to 2 seconds. However, Fuzzy-Wuzzy is quicker during registration, taking only 1 to 2 seconds compared to Sequence Matcher. Each model requires 20 K.B. of memory in the database to store these sketches. The initial model was trained and tested on 300 images, while the newer model was trained and tested on 500 images. The success rate of the original model stands at 90%, while the newer one achieves a 92% success rate, making it superior.

5. CONCLUSION

This study introduces a FreeHand Sketch-based Authentication Security System that leverages the Fuzzy-Wuzzy partial ratio algorithm. Security mechanisms can be categorized into sketch-based and text-based password systems. This research aims to increase the security level of digital data by overcoming different threats. With the suggested approach, users can register using a unique image pattern as a password selected by them. This facilitates easy login using the designated image password, making it challenging for hackers to guess. The Fuzzy-Wuzzy partial ratio algorithm has proven effective in user authentication, as indicated in table-3. Analysis done on some sample image passwords, computing their recall, precision, and accuracy using the Fuzzy-Wuzzy partial ratio; results are detailed in table-5. The proposed system boasts a validation accuracy of 92% for authenticating genuine users.

Fig-12 graphs the accuracy, precision and recall across 50 trials for 10 sample passwords. Study in this direction holds promise for robust user

identification, safeguarding data from intruders. In the future, such a method may emerge as a primary authentication technique in the digital realm.

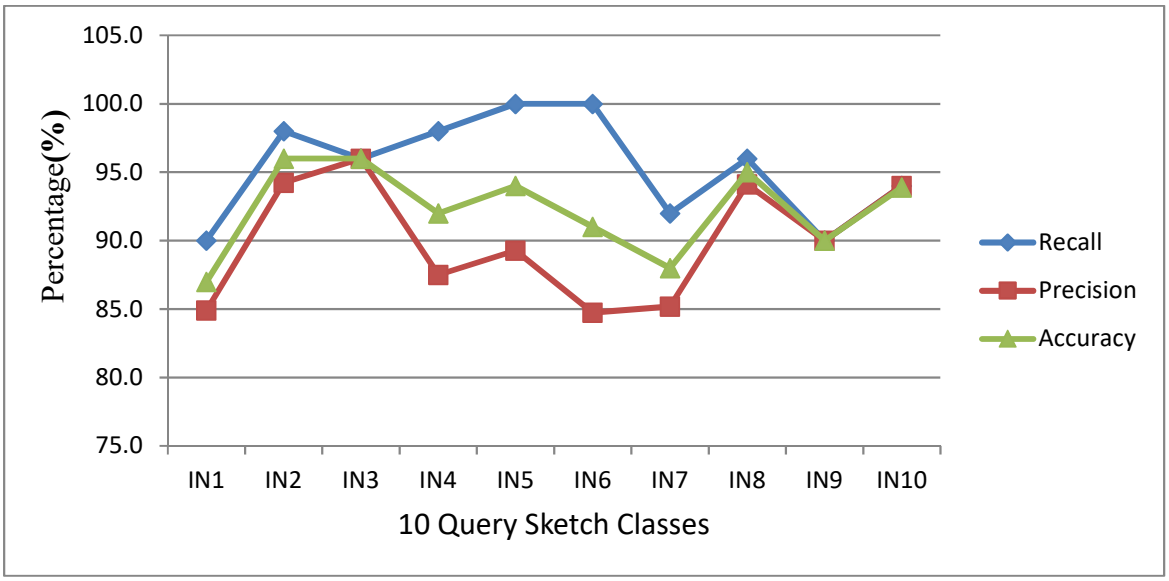

Figure 12: Accuracy, Precision and Recall of different Sketch Based Image Passwords.

REFERENCES:

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

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

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

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

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

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

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

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

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

[10] S. Amarnadh, P.V.G.D. Prasad Reddy and N.V.E.S. Murthy, "FreeHand Sketch-based Authenticated Security System using

Convolutional Neural Network", International Journal of Engineering and Advanced Technology (I.J.E.A.T.) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019.

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

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

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

[14] Krishna, Marlapalli, G. Srinivas, and P. V. G. D.Prasad Reddy, "Image smoothening and morphological operators-based JPEG compression.", *Journal of Theoretical and Applied Information Technology* 85.3 (2016): 252-259.

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