International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 05 | May - 2022 Impact Factor: 7.185 ISSN: 2582-3930

GRAPHICAL IMAGE PASSWORD AUTHENTICATION USING JARO DISTANCE

M.S.R. Deepak , P.N.V.C Mukesh Kumar , T.Sushma
GITAM University, Visakhapatnam

Abstract:

This research proposes a new authentication mechanism called Graphical Image Password Authentication Using Jaro Distance. A user can register five different related photographs using the suggested technique. To identify the similarity of the five pictures, a Gaussian mixture and the Jaro Distance method are used to preprocess the provided five similar images. All five photographs will be saved in the System database if they are comparable. The user connects in using their permitted information and a picture password based on a drawing. The password is processed by using a Gaussian mixture and implemented using the Jaro Distance technique to compare with the registered passwords in the database for authentication. The suggested method is tested with some example input image passwords, and the performance is evaluated using recall and precision measures. By ensuring authentication for user security, the proposed effort might achieve an accuracy of over 87%.

Introduction:

Generally, humans tend to forget text passwords. Even if they do remember passwords, there might be a chance of getting hacked using different techniques. So, the idea of eliminating this risk is by using graphical image passwords. The password would be in the form of an image, so it would be hard for the hackers to get. The graphical image passwords use two main strategies or techniques, namely

(i) Recognition Based and (ii) Recall Based.

The recognition-based strategy involves presenting the user with a selection of photos from which he or she must select the proper image.

Recall Based is the technique in which the user has to memorise the password and use it.

Problem Identification And Objectives:

Now-a-days the hacking of passwords has increased, the user information is being leaked. OTP's, biometrics, retina scanning can be used as an alternatives to text passwords. But they have also become vulnerable to attacks. Using Sim swapping technique the OTP can be diverted from getting it to you. Usage of retina scans frequently may cause eye problems. Biometric passwords are also compromised because of the use of artificial passwords. So to decrease the brute force attacks on the usernames and passwords of the users, some researchers have proposed an idea of using graphical passwords. Our idea is completely based on the recall-based approach where the user has to memorise the passwords.

The user is asked to draw five similar images at the time of registration. The images are pre-processed by cropping and reducing the noise of the image. The five images drawn are checked with each other whether the images are similar or not. If they are not similar, then the registration gets failed and the user is asked to draw the images again. If the user wants to access the website, he/she must draw the image that he/she set as their password during registration. If they fail to draw the same image at the time of login, then the login fails.

The graphical passwords can be added as an additional level of security to the existing security mechanisms which makes the website or an application more secure. The user need to undergo and get authenticated at all the other security levels and can reach the level of graphical passwords. This might take a lot of time for the user to get authenticated but it really keeps the data of the user safe from the malicious attacks.

Methodology:

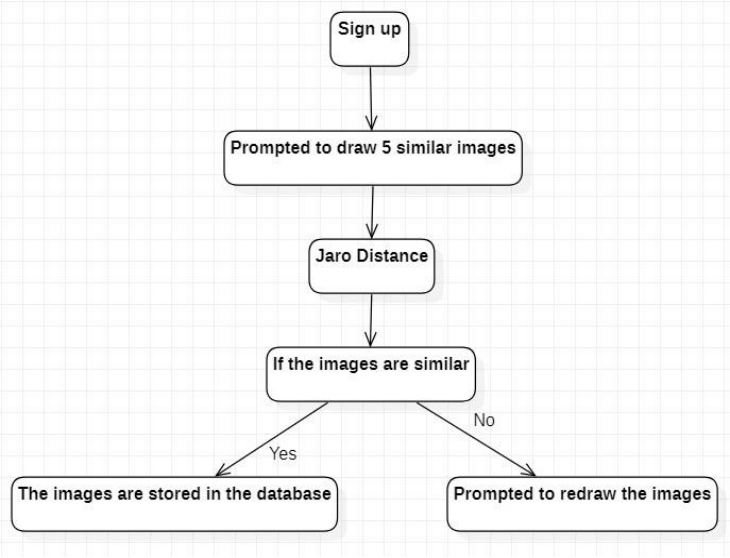

Fig-1: Architecture for the signup page

Fig-1 depicts the registration flow. First the user attempts to sign up. Now the user is asked to draw five similar images. After the images are drawn, they are compared using the jaro distance algorithm. If the drawn images are not similar then the user is asked to redraw all the images again. If the images drawn are similar, then the user is registered successfully.

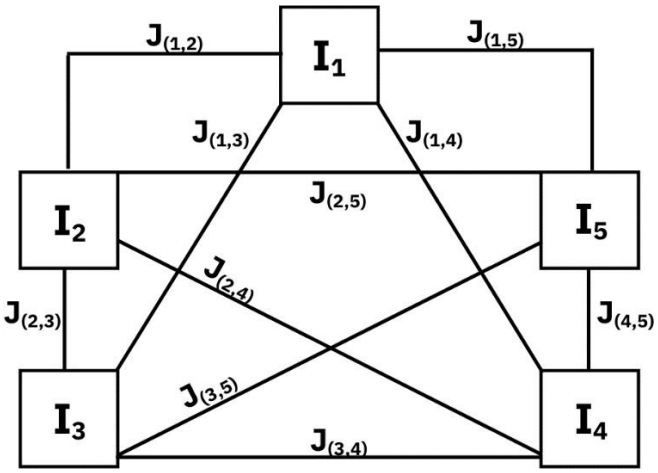

Fig-2: Five images with 10 combinations to compute Jaro Distance J(i,j) at the time of registration

Fig-2 depicts how each and every image is compared using the Jaro similarity algorithm. I1, I2, I3, I4, I5 are the images drawn by the user. J(1,2), J(1,3)….J(4,5)are the jaro distance percentages that are computed. Each and

every image is compared with the other image and the similarity between them is calculated. There is a value called threshold value where the similarity between the two images should be more than that of the threshold value. Even if one image is not drawn correctly, the user gets a message stating that the image patterns are not same and needs to be redrawn.

Image Comparisons with Combinations	If all the images are similar		If one image is dissimilar		If all the Images are Dissimilar	
	Row %	Col %	Row %	Col %	Row %	Col %
C1: Img[1,2]	51.67	27.43	49.19	49.15	31.1	45.42
C2: Img[1,3]	53.14	42.48	24.24	29.63	40.14	31.18
C3: Img[1,4]	53.33	48.7	59.23	49.37	15.15	27.62
C4: Img[1,5]	56.19	56.28	57.26	51.67	28.27	26.25
C5: Img[2,3]	58.82	63.39	21.01	22.39	43.82	34.53
C6: Img[2,4]	65.7	59.65	55.51	60.76	34.22	30.71
C7: Img[2,5]	69.57	52.4	61.66	49.58	21.99	24.09
C8: Img[3,4]	62.44	60.53	19.92	30.26	24.24	23.31
C9: Img[3,5]	57.56	59.39	20.82	29.41	26.86	27.27
C10: Img[4,5]	65.38	58.37	65.55	51.45	15.97	18.32
	S=9 and F=1		S=6 and F=4		S=4 and F=6	

Table-1: The count of Jaro Distance Success(S) and Failure(F) during the process of Graphical image password registration

There are three cases that are considered in table-1.

First case: All the images drawn are similar.

In this each and every image is compared with the other image and the row% and col% values are returned. If the values are greater than 30% then the value of S is incremented by 1 and if not the value of F is decremented by 1. Here since the value of f is less than 4, the images drawn are termed to be similar and are accepted.

Second case: One image drawn is dissimilar.

In this each and every image is compared with the other image and the row% and col% values are returned. If the values are greater than 30% then the value of S is incremented by 1 and if not the value of F is decremented by 1.Here, since the value of F is not greater than 4, the images are termed to be not similar and are asked to redraw again.

Third case: All the images drawn are dissimilar.

In this each and every image is compared with the other image and the row% and col% values are returned. If the values are greater than 30% then the value of S is incremented by 1 and if not the value of F is decremented by 1.Here, since the value of F is not greater than 4, the images are termed to be not similar and are asked to redraw again.

Table-1 gives the values of row% and col% for the above 3 mentioned cases. It checks the similarity score between images and returns it. If the similarity score is greater than 30% and less than or equal to 100% then the value of S is incremented and f not the value of F is incremented.

Image Comparisons with Combinations	If all the images are similar		If one image is dissimilar		If all the Images are Dissimilar	
	Row %	Col %	Row %	Col %	Row %	Col %
Comb [1:2]	1	15	25	20	9	14
Comb [1:3]	2	21	10	0	16	18
Comb [1:4]	5	29	8	3	3	19
Comb [1:5]	7	36	28	27	13	11
Comb [1:6]	14	32	6	12	3	15
Comb [1:7]	18	25	12	0	9	21
Comb [1:8]	11	33	29	19	7	22
Comb [1:9]	6	32	28	20	4	18
Comb [1:10]	14	31	16	2	15	27
Comb [2:3]	0	6	35	20	25	4
Comb [2:4]	3	14	33	22	12	5
Comb [2:5]	6	21	3	7	4	3
Comb [2:6]	13	17	31	31	6	0
Comb [2:7]	16	10	37	20	18	7
Comb [2:8]	9	18	4	1	16	8
Comb [2:9]	4	17	3	0	13	4
Comb [2:10]	12	16	41	22	24	13
Comb [3:4]	3	8	2	2	13	1
Comb [3:5]	5	15	38	27	29	7
Comb [3:6]	12	11	4	11	19	3
Comb [3:7]	16	4	2	0	7	4
Comb [3:8]	9	12	39	19	9	4

Comb [3:9]	4	11	38	20	12	0
Comb [3:10]	12	10	6	2	1	9
Comb [4:5]	3	7	36	29	16	8
Comb [4:6]	10	3	2	9	6	4
Comb [4:7]	13	4	4	2	6	2
Comb [4:8]	6	4	37	21	4	3
Comb [4:9]	1	3	36	22	1	1
Comb [4:10]	9	2	8	0	12	8
Comb [5:6]	7	4	34	38	10	4
Comb [5:7]	11	11	41	27	22	10
Comb [5:8]	4	3	1	8	20	11
Comb [5:9]	1	4	0	7	17	7
Comb [5:10]	7	5	45	29	28	16
Comb [6:7]	4	7	6	11	12	7
Comb [6:8]	3	1	36	30	10	7
Comb [6:9]	8	0	35	31	7	3
Comb [6:10]	0	1	10	9	18	12
Comb [7:8]	7	8	42	19	2	1
Comb [7:9]	12	7	41	20	5	3
Comb [7:10]	4	6	4	2	6	6
Comb [8:9]	5	1	1	1	3	4
Comb [8:10]	3	2	46	21	8	5
Comb [9:10]	8	1	45	22	11	9
Count of AD ≥ 30	0	5	20	4	0	0

Table-2: Count of adjacent differences row and column wise during the process of graphical image password registration

In table-2, Each and every image is compared with the other image and the adjacent distance is calculated.The difference in row% and col% between 2 images are noted down and this is termed to be the adjacent distance. A note of number of values greater than 30 is noted down.

This is the activity diagram that depicts the login page of the project.

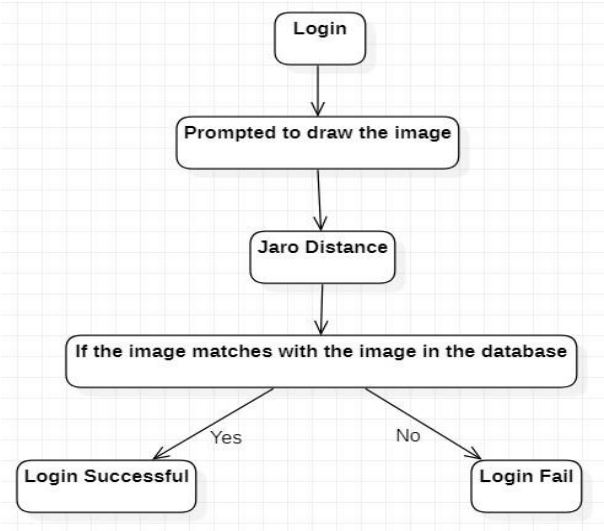

Fig-3: Architecture for the login page

Fig-3 depicts the login flow .First the user attempts to login. The user is asked to draw the image inorder to get authenticated. The image drawn by the user is compare with the images drawn at the time of registration using jaro distance algorithm. If the image matches with the images in the database, then th euser is authenticated and is asked to proceed to the next step else the user is asked to redraw the image again.

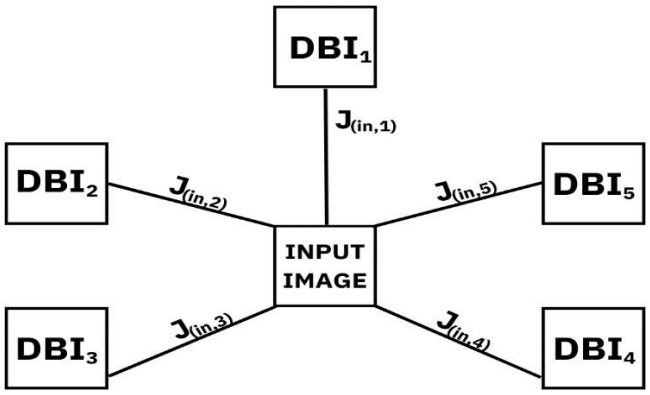

Fig-4: Comparision of input image with the images in the database to compute Jaro Distance J(I,j) at the time of login

The above figure depicts the process that takes place during the time of login. The image which is drawn at the time of login is compared with each and every image in the database using the jaro distance algorithm and the similarity score is calculated. If the image matches with all the images in the database, only then the user is authenticated and the user is asked to proceed to the next step.

Image Comparisons with Combinations	Valid Login Image Password		Invalid Login Image Password	
	Row%	Col%	Row%	Col%
C1(INP-DB1)	41.63	60.61	38.05	21.46
C2(INP-DB2)	47.71	47.16	46.64	13.85
C3(INP-DB3)	32.41	54.15	43.44	14.72
C4(INP-DB4)	50.23	58.37	41.96	13.62
C5(INP-DB5)	47.49	59.83	42.86	17.8
	S=5 and F=0		S=0 and F=5	
	Login Successful		Login Fail	

Table-3: The count of Jaro Distance Success(S) and Fail(F) during the process of Graphical Image Password Login

Table-3 depicts the similarity scores of the images at the time of login. In table-3, two cases are considered where in the first case, the user draws the same image as the images present in the database. The col% and row% are greater than 30 so the count of S is incremented. Since the value of S is greater than the value of F,the user gets authenticated. So the user gets a message stating that the login is successful. In the second case, the user draws the image which is dissimilar to the images in the databse. The row% and the col% is not greater than 30% so the count of F gets incremented.Since the value of S is less than F, the user wont get authenticated. So the user gets a message stating that the login has failed.

Steps:-

- The user firsts open the portal and registers as a new user.
- In the process of registration, the user is prompted to draw five similar images and set the Image as password.
- If the five images aren't similar, the user is asked to draw the images again.
- If the images are similar, the user is registered, and the Image drawn is stored in the database.

- At the time of login, the user is prompted to draw the Image which he set as the password.
- Only if the drawn Image matches with the Image in the database the user is authenticated.

ACKNOWLEDGEMENT:

We want to thank our internal guide Dr. S. Amanadh and all the faculty members for their valuable guidance and encouragement in completing our project work.

With Regards and Gratitude:

M.S.R. Deepak(121810302001)

P.N.V.C. Mukesh Kumar(121810302005)

T. Sushma(121810302061)

Result:

A	B	C	D	E	F	G	H
Jaro distance with 50% threshold on 50 Images							
	FN	TP	FP	TN	Recall	Precision	Accuracy
IN1	4	46	15	35	92	75	81
IN2	6	44	10	40	88	81	84
IN3	1	49	17	33	98	74	82
IN4	0	50	14	36	100	78	86
IN5	0	50	10	40	100	83	90
IN6	0	50	11	39	100	82	89
IN7	5	45	10	40	90	82	85
IN8	3	47	7	43	94	87	90
IN9	0	50	5	45	100	91	95
IN10	5	45	5	45	90	90	90
					95	82	87

After training and performing tests and trails on 50 images, we found that the Jaro distance algorithm gives an accuracy of 87%, which is high among all the other algorithms.

Conclusion:

Our basic goal was to use graphical passwords as an extra added security layer to the current existing digital account security system. The proposed methodology asks the user to draw five similar images at the time of registration. The images are cropped, and the noise is reduced and checked using the jaro similarity method. If the five images aren't similar, the user is asked to redraw them again else, the images are stored in the database only when all the images are similar. Now the user can log in with the registered image password successfully.

References:

1. Akshay Karode, Sanket Mistry and Saurabh Chavan "GRAPHICAL PASSWORD AUTHENTICATION SYSTEM"

2. Ahmad Almulhem "A GRAPHICAL PASSWORD AUTHENTICATION SYSTEM BY POINT OF INTEREST"

3. Hala Assal, Ahsan Imran, Sonia Chiasson " AN EXPLORATION OF GRAPHICAL PASSWORD AUTHENTICATION FOR CHILDREN"

4. Sana Ansari, Prof. Avinash Shrivas **"**IMPLEMENTATION OF AUTHENTICATION MECHANISM USING IMAGE SEGMENTATION USING GRID SEGMENTATION FOR WEB BASED APPLICATIONS"

5. A Balamurali, M V R Harsha,V Sai Hitesh, A Sai Chaitanya "GRAPHICAL IMAGE PASSWORD BY IMAGE SEGMENTATION"

6. Rohitkumar Kolay, Animesh Vora, Vinaykumar Yadav " GRAPHICAL PASSWORD AUTHENTICATION USING IMAGE SEGMENTATION"

7. Shiksha Saxena, Nikesh Tiwari "A SURVEY ON GRAPHICAL PASSWORD AUTHENTICATION"

8. Mr.Jadhav Rajesh S., Mr.Chandole Durgesh K., Mr.Wani Milind D., Mr.Kusalkar Santosh R., Mr.Shinde Kiran G., Mr.Dighe Mohit S "GRAPHICAL PASSWORD AUTHENTICATION SYSTEM "

9. Harsh Desai, Ninaad Suvarna, Dipen Desai and Simranjeet Singh Chawla, Prof. Sowmyashree "GRID BASED AUTHENTICATION PASSWORD USING HASH TECHNIQUE"

10. 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"

11. S. Amarnadh, P.V.G.D. Prasad Reddy and N.V.E.S. Murthy. "FREEHAND SKETCH-BASED AUTHENTICATED SECURITY SYSTEM USING CONVOLUTIONAL NEURAL NETWORK"