JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Data Security Enhancement using Two Segment Graphical Pattern

[1] Ramkaran Devanda,[2] Mrs. Geeta Tiwari

[1]Research Scholar,[2] Assistant professor
[1,2]Department of Computer Science &Engineering
[1,2]Compucom Institute of Technology & Management, Jaipur

Abstract : The cutting edge banking framework and other association where the information trade is pivotal, expected to the safeguarded from the unapproved access and the hacking endeavor. To work with and further develop the security gauges, the area of exposition is information security and in the proposed work , we have proposed the idea of security which is connected with the graphical idea of password pattern generation. The idea includes the picking of the space for the realistic picture which is to be picked, then, at that point, from the area chose we will picked the specific picture from the accessible choices, then, at that point, includes the powerful division of the pictures and the turn of the picture on its place and the division and pivot will be associated with the generation of the password pattern. Together, with that the double confirmation is performed utilizing the SHA-512 two section code , which is produced based on the picture picked by the client for splitting. The resultant password which is shaped is then contrasted and the past methodologies and with devices and utility projects for testing the password strength and the outcome got are very better compared to the past methodologies.

***IndexTerms* – Data Security , Picture Password , SHA-512**

I. Introduction

Data security alludes to the most common way of shielding information from unapproved access and information defilement all through its lifecycle. Information security incorporates information encryption, hashing, tokenization, and key administration rehearses that safeguard information across all applications and stages. Information security is a bunch of guidelines and innovations that shield information from purposeful or inadvertent annihilation, alteration or exposure. Information security can be applied utilizing a scope of methods and advancements, including authoritative controls, actual security, legitimate controls, hierarchical norms, and other protecting strategies that limit admittance to unapproved or vindictive clients or cycles. [1]

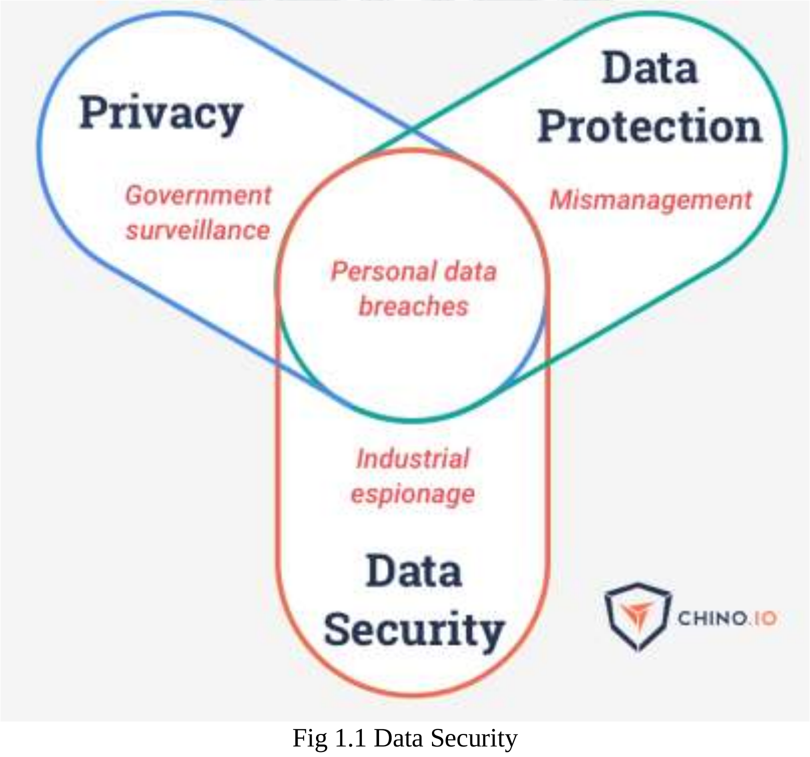


Fig 1.1 Data Security

Associations all over the planet are putting vigorously in data innovation (IT) network safety abilities to safeguard their basic resources. Regardless of whether an endeavor needs to safeguard a brand, scholarly capital, and client data or give controls to basic framework, the means for episode identification and reaction to safeguarding hierarchical interests have three normal components: individuals, cycles, and innovation. [1]

Data innovation comes in many shapes and frames and safeguards information from a developing number of dangers. Large numbers of these dangers are from outer sources, however associations ought to likewise zero in their endeavors on shielding their information from within, as well. Approaches to getting information include:

- Information encryption: Data encryption applies a code to each individual piece of information and won't concede admittance to scrambled information without an approved key being given

- Information concealing: Masking explicit areas of information can shield it from revelation to outside noxious sources, and furthermore inside staff who might actually utilize the information. For instance, the initial 12 digits of a Mastercard number might be covered inside an information base. [2]

- Information deletion: There are times when information that is presently not dynamic or utilized should be eradicated from all frameworks. For instance, assuming a client has mentioned for their name to be eliminated from a mailing list, the subtleties ought to be erased for all time.

- Information strength: By making reinforcement duplicates of information, associations can recuperate information would it be advisable for it be eradicated or undermined inadvertently or taken during an information break.[2]

II. Literature Survey

K. Irfan, A. Anas, S. Malik and S. Amir,2018 Traditional substance based password plans are presented to dictionary attacks for a gigantic scope. As a response, graphical password plans are a promising choice as opposed to content based affirmation plans where instead of satisfying, pictures are picked for a password. In any case, these plans are again affected on account of shoulder surfing and less effective due to tremendous word reference space. This paper bases on offering a response reliant upon content based graphical password systems, a blend of Déjà vu and Moveable Frame plot. An impression that this has occurred before is moreover replaced by content based pictures than just plans. Our investigation has two standard objections: 1) To agitate shoulder riding 2) To restrict the request season of pass pictures on the login screen. The endeavor was completed as an ensuing android application using Android Studio. Results exhibit the proposed arrangement of graphical password structure with various letters all together pictures is dynamically undeniable and has less mental weight on client when appeared differently in relation to picture based graphical password plans. The incorrect login rate for quite a long time set based pictures with compact packaging was 15% more than graphical password plots subsequently a predominant solution for guarantee shoulder surfing.

A. B. Yazid, M. M. Boukar and S. I. Yusuf,2018 The graphical thought of graphical password nearly makes each and every graphical password defenseless against shoulder attack. Individuals need a basic strategy for affirmation and historic to the extent that security. The issue in numerous systems nevertheless, less feeble passwords are frustrated, less simple to utilize lastly, login time takes particularly long. In this paper, a graphical password affirmation technique exhibited to be dynamically impenetrable to bear surfing and various types of potential attacks have been proposed. PandaLock framework is a cross variety approach, which joins survey based and affirmation based technique. Blend lock interfaces in with variable pointers are used to check the clients in this proposed system. A Portable handheld contraption was used to copy and test the proposed system.

B. Bilgi and B. Tugrul,2018 The security systems should give approval as a help of their clients. The present generally ordinary and extensively used affirmation procedure is content based passwords; yet it is past the domain of creative mind to hope to make strong and easy to-use passwords with this methodology. Arranging a safeguarded and easy to-use affirmation system is a critical target for security structures. Graphical passwords (or Graphical User Authentication (GAU)) have created as a choice as opposed to old style content based passwords methods without scarcely making the slightest effort of use and constancy. The early phase of graphical confirmation relies upon the standard that people remember visual things more than works. As a result of the people's penchant to use the check instrument in open spots, for instance, open transportation, bistros and study lobbies, shoulder riding attacks have actually extended. Hybrid pictures are made by mixing different features of two pictures. The person who looks at the cross variety picture sees one of the photos creating the cream picture while the others can see the resulting picture. In this examination, creators have developed a graphical affirmation system that is impenetrable to bear riding using mutt pictures. The proposed system is differentiated and other graphical and content based methods to the extent that security level and accommodation.

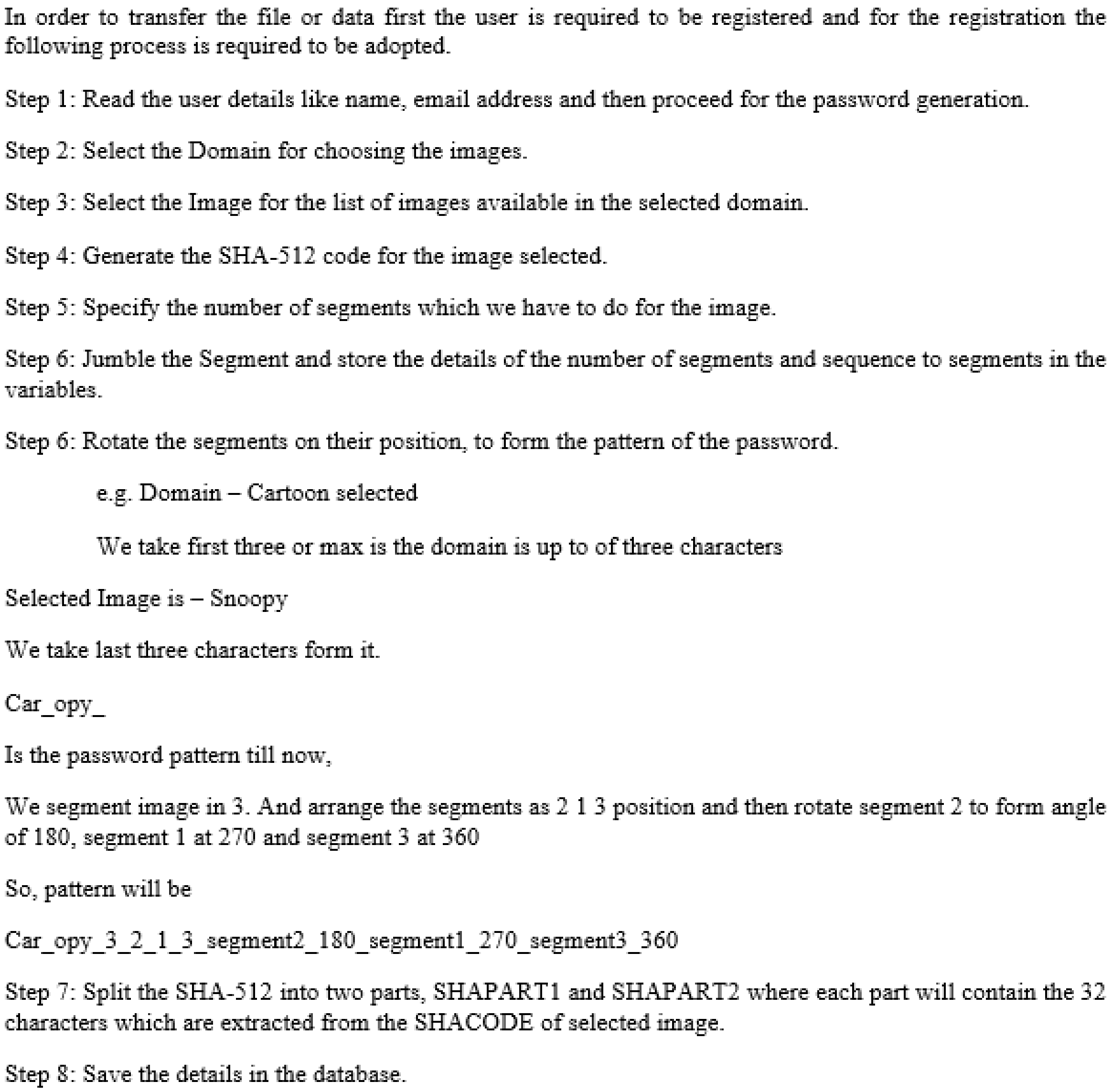
R. Tolosana, R. Vera-Rodriguez, J. Fierrez and J. Ortega-Garcia,2018 This work evaluates the positive conditions and ability of combining contact biometrics to versatile one-time passwords (OTP). The new e-BioDigit information base, which incorporates online physically composed mathematical digits from 0 to 9, has been acquired using the finger contact as commitment to a cell. This data set is used in the assessments declared in this work and it is straightforwardly open to the investigation organization.

An examination of the OTP circumstance using interpreted digits is finished as for which are the most discriminative composed by hand digits and how generous the system is while extending the amount of them in the client password. Likewise, the best incorporates for each physically composed mathematical digit are considered to redesign our proposed biometric system..

III. Proposed Work

In the proposed work we have implemented the two concepts of the authentication and data sharing ,

3.1Algorithm User Registration



In order to transfer the file or data first the user is required to be registered and for the registration the following process is required to be adopted.

Step 1: Read the user details like name, email address and then proceed for the password generation.

Step 2: Select the Domain for choosing the images.

Step 3: Select the Image for the list of images available in the selected domain.

Step 4: Generate the SHA-512 code for the image selected.

Step 5: Specify the number of segments which we have to do for the image.

Step 6: Jumble the Segment and store the details of the number of segments and sequence to segments in the variables.

Step 6: Rotate the segments on their position, to form the pattern of the password.

e.g. Domain – Cartoon selected

We take first three or max is the domain is up to of three characters

Selected Image is – Snoopy

We take last three characters form it.

Car_opy_

Is the password pattern till now,

We segment image in 3. And arrange the segments as 2 1 3 position and then rotate segment 2 to form angle of 180, segment 1 at 270 and segment 3 at 360

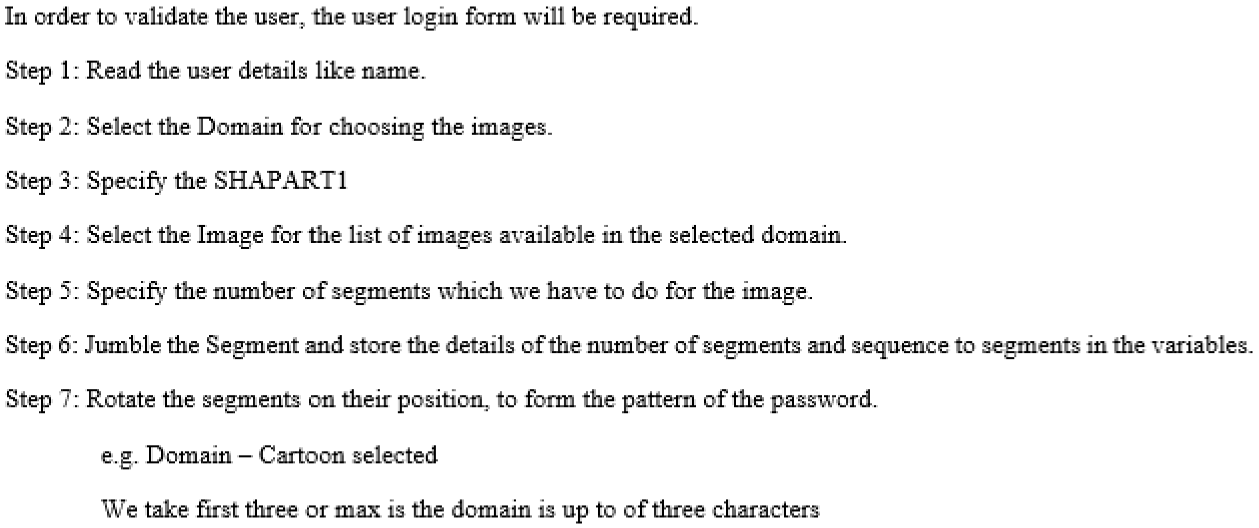
So, pattern will be

Car_opy_3_2_1_3_segment2_180_segment1_270_segment3_360

Step 7: Split the SHA-512 into two parts, SHAPART1 and SHAPART2 where each part will contain the 32 characters which are extracted from the SHACODE of selected image.

Step 8: Save the details in the database.

3.2Algorithm For User Login



In order to validate the user, the user login form will be required.

Step 1: Read the user details like name.

Step 2: Select the Domain for choosing the images.

Step 3: Specify the SHAPART1

Step 4: Select the Image for the list of images available in the selected domain.

Step 5: Specify the number of segments which we have to do for the image.

Step 6: Jumble the Segment and store the details of the number of segments and sequence to segments in the variables.

Step 7: Rotate the segments on their position, to form the pattern of the password.

e.g. Domain – Cartoon selected

We take first three or max is the domain is up to of three characters

Selected Image is – Snoopy

We take last three characters form it.

Car_opy_

Is the password pattern till now,

We segment image in 3. And arrange the segments as 2 1 3 position and then rotate segment 2 to form angle of 180, segment 1 at 270 and segment 3 at 360

So, pattern will be

Car_opy_3_2_1_3_segment2_180_segment1_270_segment3_360

Step 8: Check the generated password with the Database.

Step 9: Specify the SHAPART2.

```
Step 10: If Match Exists then
          Login Success
         Else
         Login Failed
         [End of If structure]
Step 11: Stop
```

IV. Implementation and Result Analysis

V. 4.5 Proposed Work

The proposed work is designed in the software framework , VS 2010 and making use of the database SQL Server 2008 Express edition and we have concentrated over designing the Window Based Application environment for the simulation of the proposed work.

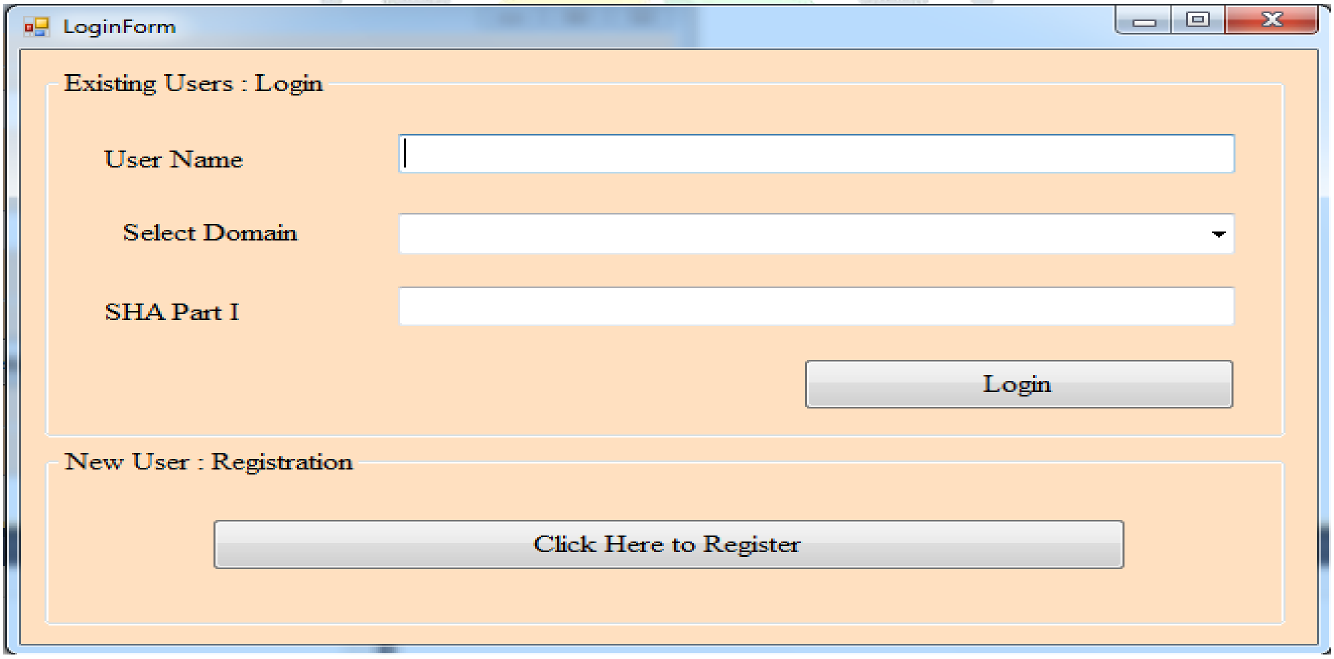
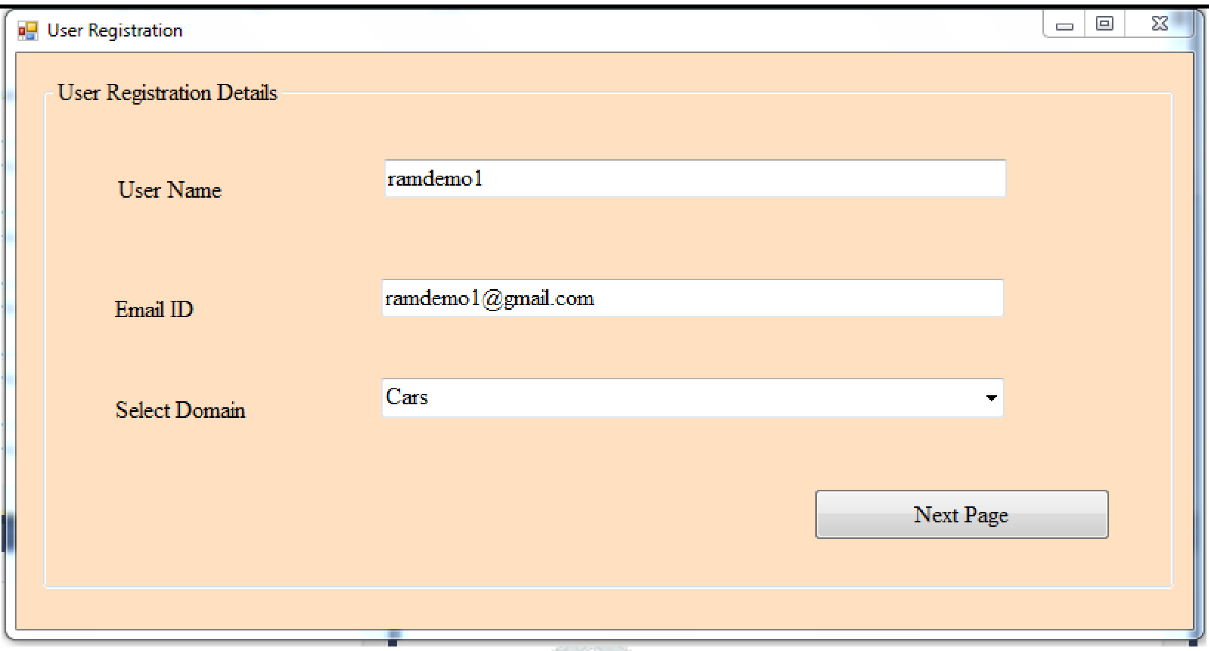


Fig 4.1 StartUp Form



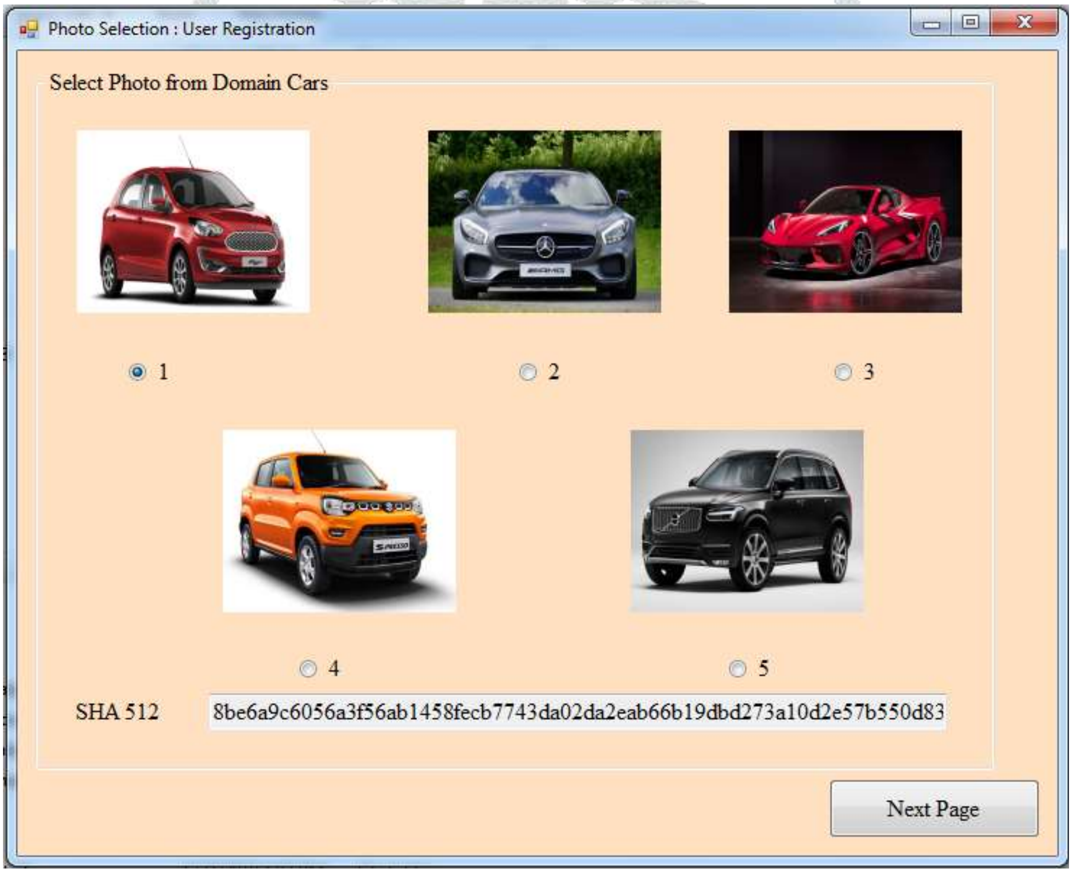
User Registration Details

User Name: ramdemo1

Email ID: ramdemo1@gmail.com

Select Domain: Cars

Fig 4.2 Registration Phase 1



Select Photo from Domain Cars

● 1 ○ 2 ○ 3

○ 4 ○ 5

SHA 512: 8be6a9c6056a3f56ab1458fecb7743da02da2eab66b19dbd273a10d2e57b550d83

Fig 4.3 Registration: Picture Selection Phase 2

Once the image we have selected, then we will click on the Next Page , in this form the user have to select the number of segments or parts of the images which we want to create and once the parts are created then we can click over the image to rotate the image and the image can be rotated in 4 positions , default is 90 , then 180 and so on .

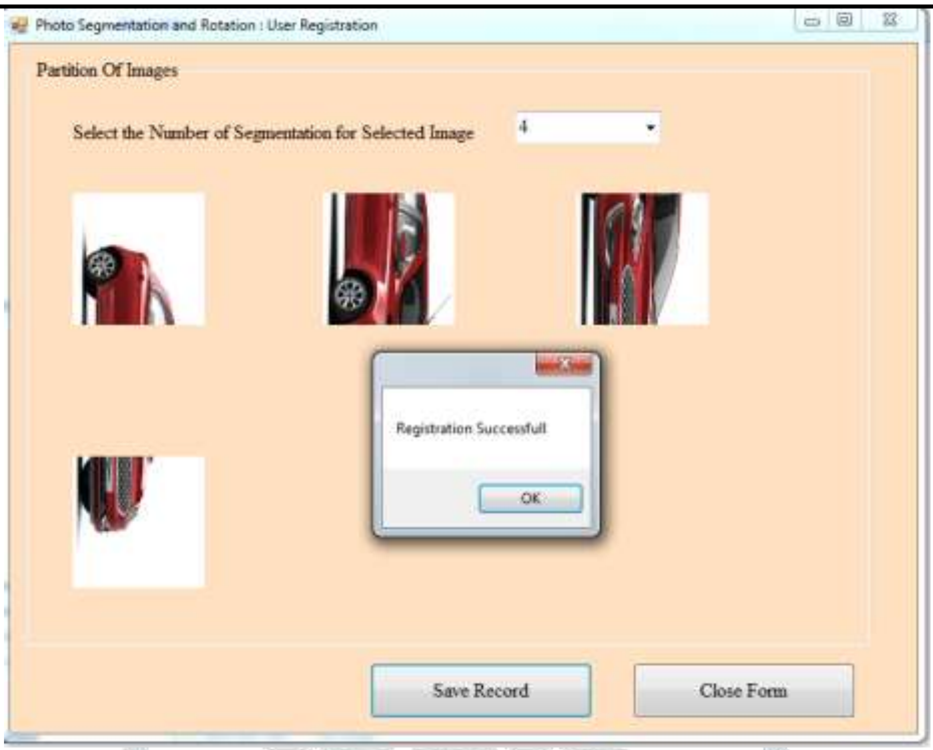


Photo Segmentation and Rotation : User Registration
Partition Of Images
Select the Number of Segmentation for Selected Image
4
Registration Successfull
OK
Save Record
Close Form

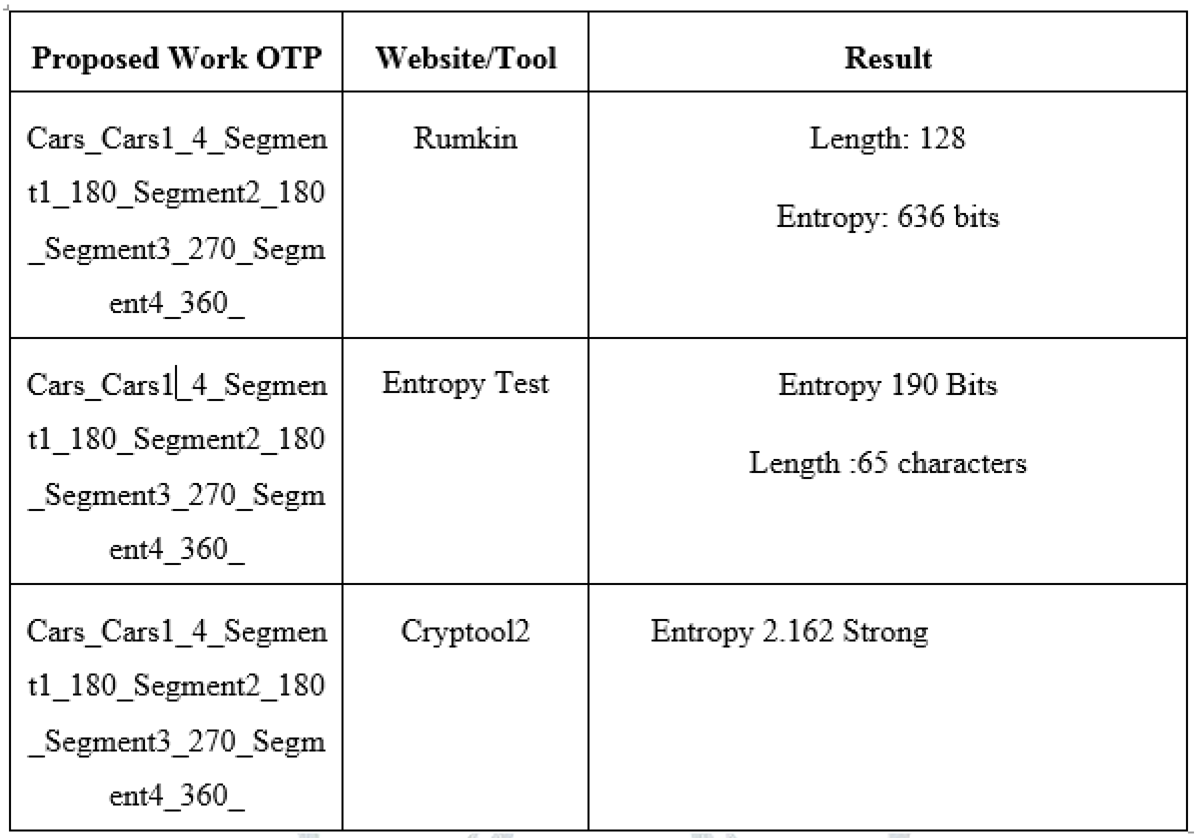
Fig 4.4 Registration: Picture Segmentation and Rotation Phase 3

Once all done we have to save the details and we will click on the Save Record button and the details of the user like the user name , email id and password generated using the method which we have followed will get saved in the register table which is maintained in the Microsoft SQL Server 2008 database.

Table 4.1 Result Comparison Table Base Work **M Hamza Zaki Title "Secure Pattern-Key Based Password Authentication Scheme"**

Proposed Work OTP	**Website/Tool**	**Result**
bbbb n > z A n a n	Rumkin	Length 22 Entropy: 107.2 bits Charset Size: 75 characters
bbbb n > z A n a n	Entropy Test	Entropy 117.482 bits
bbbb n > z A n a n	Cryptool2	Entropy 3.96 Very Strong

Table 4.2 Result Comparison Table Proposed Work



Proposed Work OTP	Website/Tool	Result
Cars_Cars1_4_Segment1_180_Segment2_180_Segment3_270_Segment4_360_	Rumkin	Length: 128 Entropy: 636 bits
Cars_Cars1_4_Segment1_180_Segment2_180_Segment3_270_Segment4_360_	Entropy Test	Entropy 190 Bits Length :65 characters
Cars_Cars1_4_Segment1_180_Segment2_180_Segment3_270_Segment4_360_	Cryptool2	Entropy 2.162 Strong

VI. CONCLUSION

The assurance of information from the unapproved access is the superb thought process of the exposition and verification of the client is likewise extremely fundamental. To work with and further develop the security gauges, the area of exposition is information security and furthermore in the proposed work,we have proposed the idea of security which is connected with the graphical idea of password pattern generation. The idea includes the picking of the space for the realistic picture which is to be picked, then, at that point, from the area chose we will pick the specific picture from the accessible choices, then, at that point, includes the unique division of the pictures and the turn of the picture on its place and the division and revolution will be engaged with the generation of the password pattern. Together, with that the double confirmation is performed utilizing the SHA-512 two section code , which is produced based on the picture picked by the client for parting. The resultant password which is framed is then contrasted and the past methodologies and with devices and utility projects for testing the password strength and the outcome got are very better compared to the past methodologies

Later on , we will additionally prefer to broaden the exploration by chipping away at the viable execution of the work in the support or the other association which are connected with the banking business where the confirmation of clients if the premier prerequisite and furthermore alongside that we will jump at the chance to deal with the DNA cryptography , Retina Based Authentication and the sky is the limit from there..

REFERENCES

1. B. Alese and A. A. Omojo "An Enchanced Graphical Password Technique using Fake Pointers" Akure 2015.
2. X. Li and H. Zhao A Scalable Shoulder-Surfing Resistant Textual-GRaphiacl Baseed Password Authentication Scheme 2014.
3. S. Mahmood B. Amen and R. Nabi "Mobile Applcation Security Platforms" International Journal of Computer Science and Information Security vol. 133 2016.
4. K. Irfan, A. Anas, S. Malik and S. Amir, "Text based graphical password system to obscure shoulder surfing," 2018 15th International
5. Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, 2018, pp. 422-426
6. Mu, Yarong & Yao, Bing., "Exploring Topological Graph Passwords of Information Security by Chinese Culture", IAEAC, 2018, pp 1648-1652.
7. Yadav, Uma & Mohod, P.S, "Adding persuasive features in graphical password to increase the capacity of KBAM", ICE-CCN.2013 , pp. 513-517
8. M. U. Siddiqui, M. S. Umar and M. Siddiqui, "A Novel Shoulder-Surfing Resistant Graphical Authentication Scheme," 2018 4th International Conference on Computing Communication and Automation (ICCCA), 2018, pp. 1-5
9. N. A. A. Othman, M. A. A. Rahman, A. S. A. Sani and F. H. M. Ali, "Directional Based Graphical Authentication Method with Shoulder Surfing Resistant," 2018 IEEE Conference on Systems, Process and Control (ICSPC), 2018, pp. 198-202.
10. A. B. Yazid, M. M. Boukar and S. I. Yusuf, "PandaLock: Variable-Pointer Rotary-Password Authentication Technique," 2018 14th International Conference on Electronics Computer and Computation (ICECCO), 2018, pp. 1-6.
11. A.Bilgi and B. Tugrul, "A Shoulder-Surfing Resistant Graphical Authentication Method," 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), 2018, pp. 1-4.
12. Tolosana, Ruben & Vera-Rodriguez, Ruben & Fierrez, Julian & Ortega-Garcia, Javier.,"Reducing the Template Aging Effect in On-Line Signature Biometrics", IET Biometrics, 2018.
13. Yao, Bing & Sun, Hui & Zhang, Xiaohui & Mu, Yarong & Wang, Honzvu & Xu, Jin. , "New-Type Graphical Passwords Made by Chinese Characters with Their Topological Structures", IMCEC.2018 , pp. 1606-1610.