

Face Presentation attack Detection Using Deep Reinforcement Learning

Guide

Dr. R. Shyamala M.E..Phd.,AP/IT

Team members

Arulkumaran R (422419205003)

Jabaselvi A (422419205015)

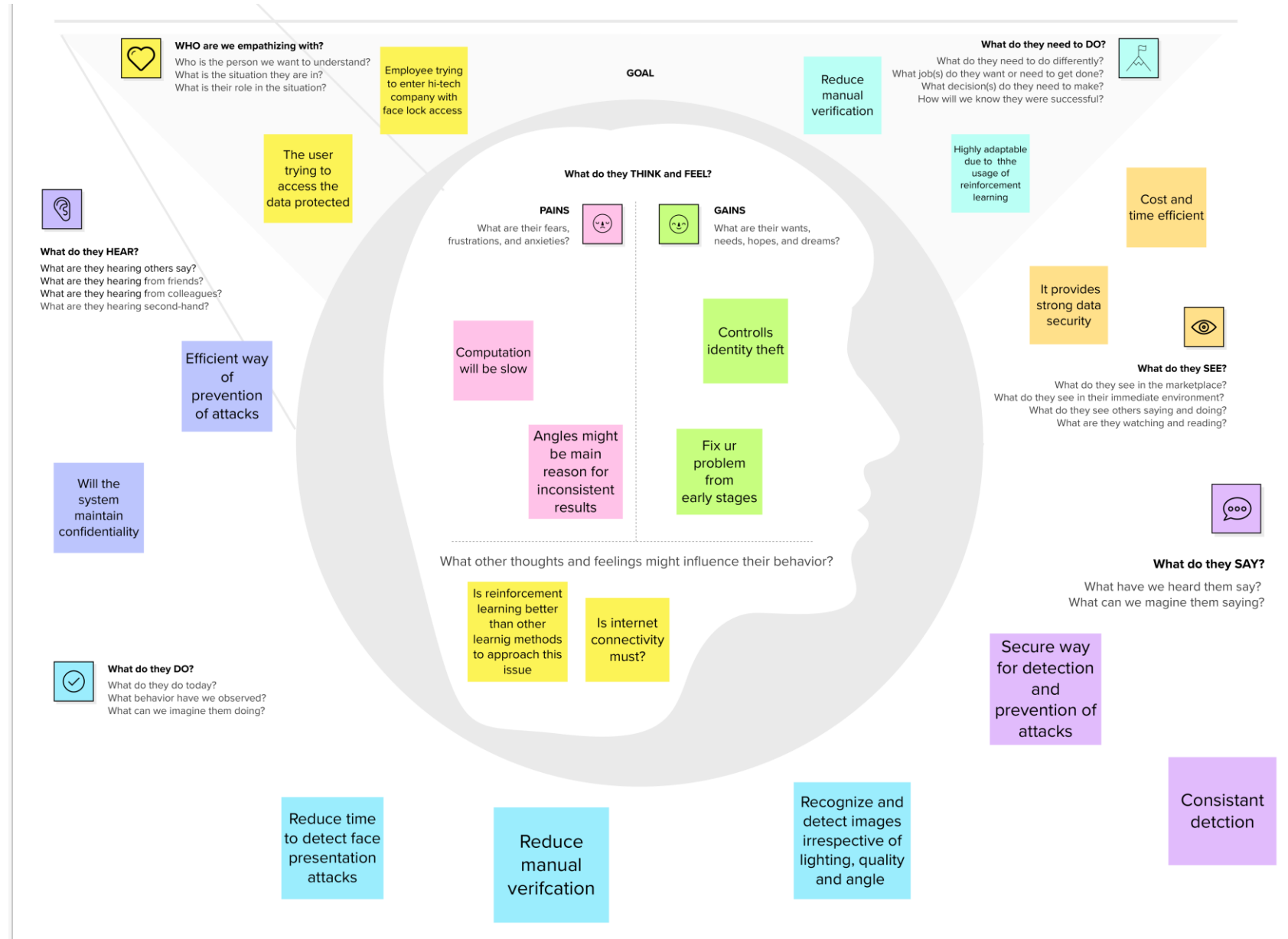
Navieen R (422419205022)

Literature Survey

S. No	TITLE & AUTHOR	JOURNAL & YEAR	PROBLEM	SOLUTION	PARAMETER MEASURED	ADVANTAGES	DISADVANTAGES
1	Salience- Aware Face Presentation Attack Detection via Deep Reinforcement Learning - Bingyao Yu, Jiwen Lu, Xiu Li, Jie Zhou.	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 17, 2022	Face spoofing detection, replay attack, print attack detection..	They propose SAFPAD approach, which takes advantage of DRL to exploit the salient local part information in face images.	Ablation Study, Cross-Dataset Testing, Salient Local Patches Number, Salient Local Patches Size	Usage of Reinforcement learning makes the FAS more efficient.	Needs to be improved in the generalization capability for the complicated face presentation attack detection,.
2	DRL-FAS: A Novel Framework Based on Deep Reinforcement Learning for Face Anti- Spoofing - Rizhao Cai, Haoliang Li	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 16, 2021	Face spoofing detection, replay attack, detection..	Reliable FAS techniques are highly desired and essential for developing secure face recognition systems.	We particularly employ a GRU to learn local features from f1, f2,...ft in a sequential and recursive manner.	We take advantage of RNN to memory information from all “observations” from sub-patches to reinforce extracted local features gradually.	The Computation of this FAS is slow due the usage of Recurrent Neural Network (RNN).
3	Factors Related To The Improvement of Face Anti-Spoofing Detection Techniques With CNN Classifier - Ms. Sonali R.Chavan, Dr. Swati S. Sherekar, Dr. Vilas M. Thakre.	2021 International Conference on Computational Intelligence and Computing Applications.	Face spoofing detection and replay attack detection.	This paper adopted comprehensive presentation of proposed Anti-spoofing techniques followed by features, datasets, parameters.	HTER, ACER, ACPER, BPCER, EER, EPR, FNR	CNN based algorithms approaches are most effective, depending on the type of spoof attack	Although many researchers have put their efforts to develop face detection systems but it fails to give adequate results in all situation.

S. No	TITLE & AUTHOR	JOURNAL & YEAR	PROBLEM	SOLUTION	PARAMETER MEASURED	ADVANTAGES	DISADVANTAGES
4	Spoof Face Detection Via Semi- Supervised Adversarial Training - Chengwei Chen, Yaping Jing, XuequanLu.	2022 International Joint Conference on Neural Networks (IJCNN) 978-1-7281-8671-9/22/\$31.00 ©2022 IEEE DOI: 10.1109/IJCNN55064.2022.989275	Face spoofing detection and print attack detection.	In this paper, we propose a semi-supervised adversarial learning framework for spoof face detection, which largely relaxes the supervision condition.	Weighting parameter, Adversarial loss, Image reconstruction loss, Maximum Mean Discrepancy.	Our approach does not need spoofing face data for training, and is thus semi-supervised and robust to different types of spoof faces.	The cross database experiments may cause errors in big scale.
5	Face Anti- spoofing Based on Image Block Difference and Logistic Regression Analysis -	2015 IEEE 5th International Conference on Consumer Electronics Berlin (ICCE-Berlin)	Face spoofing detection and replay attack detection.	The proposed method uses the difference between pairwise discrete cosine transform coefficients and logistic regression as a machine learning algorithm.	Feature extraction (HBD, VBD, HVBD), Scrambling.	The proposed anti-spoofing method is very simple, but the results of initial evaluations demonstrated its good performance on a slightly modified face anti-spoofing database.	The cross database experiments may cause errors in big scale.

Empathy Map



Problem Statement

Mr. Walter White is a 45 year old successful businessman. He has a own business for past 20 years. In these 20 years he faced a lot of security issues and trouble in preventing the datafrom attackers.

- Mr. Walter White wants to setup a face recognition system that prevents others fromaccessing his important data.
- He has faced a huge loss for a long time.
- He needs a secure face recognition system to prevent data from replay and print attacks.
- He needs to secure his system immediately.

Who does the problem affect?	Person who has the data
What are the boundaries of theproblem?	May lead to reputation loss and also leakage of models or prototypes.
What is the issue?	In business aspect, if confidential data gets released unknowingly of the user it may lead to huge financial loss.
When does the issue occur?	When attacker needs to access the data and corrupt the whole system.
Where does the issue occur?	The issue occurs in the system of the user.
Why is it important that we fixthe problem?	It will be useless if the face recognition system is vulnerable to replay and print attacks. So it is important to detect and prevent these attacks.
What solution to solve this issue?	Improved face recognition system to correlate between real face and replay/print attack.
What methodology used to solvethe issue?	We use deep reinforcement learning to prevent from attacks.

Brainstorming

2

Brainstorm

Write down any ideas that come to mind that address your problem statement.

🕒 10 minutes

TIP

You can select a sticky note and hit the pencil icon to start drawing!

Arulkumaran

Help to differentiate between real face and picture

Easy management resources

APCER is calculated to verify the accuracy

It tries to provide an error free solution

Neural network should be used

Improving biometric security

Jabaselvi

Helps to stop criminal behaviour

Will provide high fault tolerance

It improves the speed of face recognition system

Used to accept only authorized users

Implement our approach with PyTorch framework

Detect the vulnerability for attacks

Navieen

Accuracy of real time analytics

It allows automated alert when intrusion detected

Does not need training data

Improves the safety and security

Usage of reinforcement learning makes the FAS more efficient

Constant image size should be 512x512

3

Group ideas

Take turns sharing your ideas while clustering similar or related notes as you go. Once all sticky notes have been grouped, give each cluster a sentence-like label. If a cluster is bigger than six sticky notes, try and see if you can break it up into smaller sub-groups.

🕒 20 minutes

Updated methodology of face recognition

Ensure effective and reliable approach for detection

TIP

Add customizable tags to sticky notes to make it easier to find, browse, organize, and categorize important ideas as themes within your mural.

Provide accurate and consistent results

Face recognition system becomes commercially efficient when error rate is low

Does not require internet connection

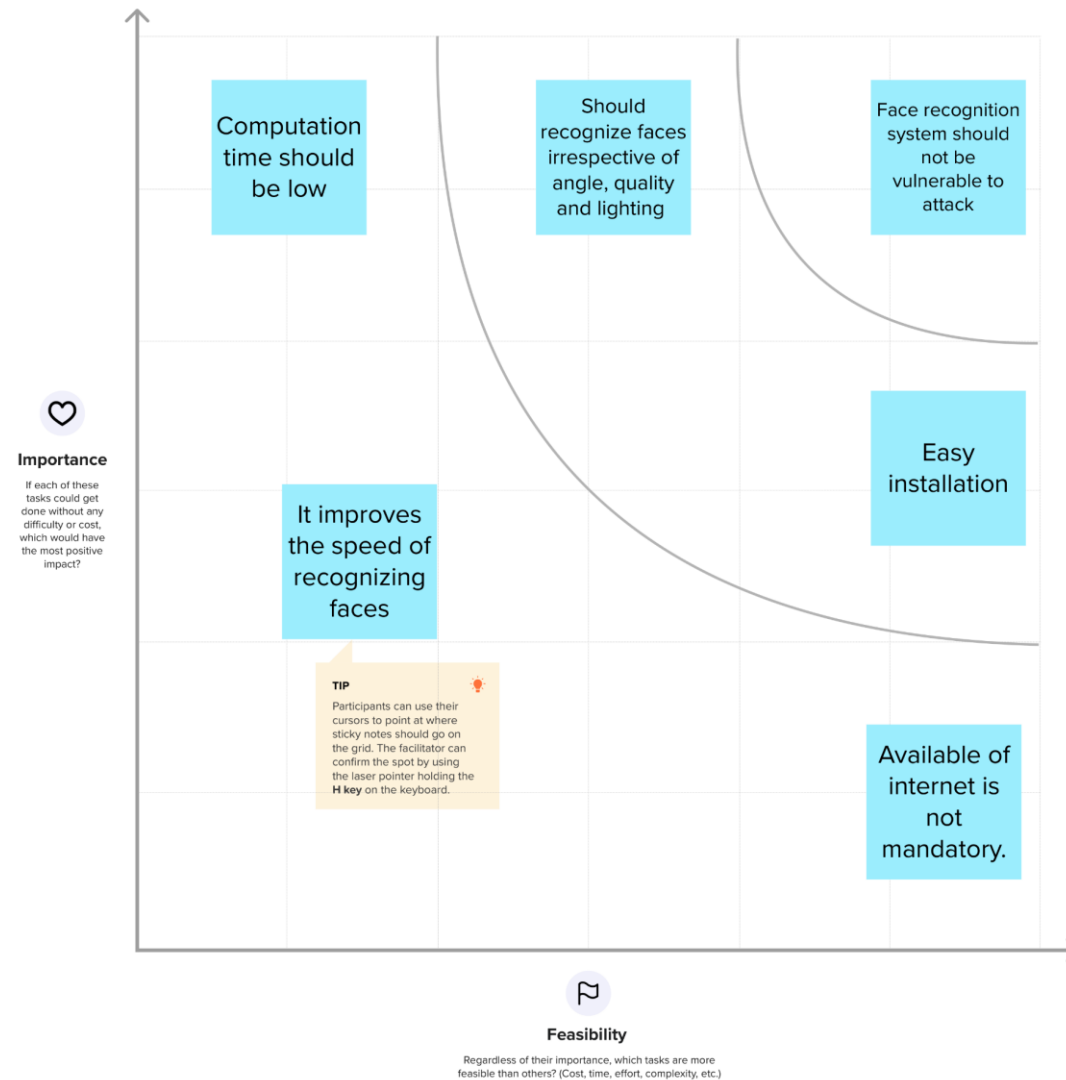
Improves the safety and security

4

Prioritize

Your team should all be on the same page about what's important moving forward. Place your ideas on this grid to determine which ideas are important and which are feasible.

🕒 20 minutes



After you collaborate

You can export the mural as an image or pdf to share with members of your company who might find it helpful.

Quick add-ons

A

Share the mural

Share a view link to the mural with stakeholders to keep them in the loop about the outcomes of the session.

B

Export the mural

Export a copy of the mural as a PNG or PDF to attach to emails, include in slides, or save in your drive.

Keep moving forward



Strategy blueprint

Define the components of a new idea or strategy.

[Open the template →](#)



Customer experience journey map

Understand customer needs, motivations, and obstacles for an experience.

[Open the template →](#)



Strengths, weaknesses, opportunities & threats

Identify strengths, weaknesses, opportunities, and threats (SWOT) to develop a plan.

[Open the template →](#)

[Share template feedback](#)