Face Presentation attack Detection via Deep Reinforcement Learning

Guide

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

Team members

Arulkumaran R (422419205003)

Jabaselvi A (422419205015)

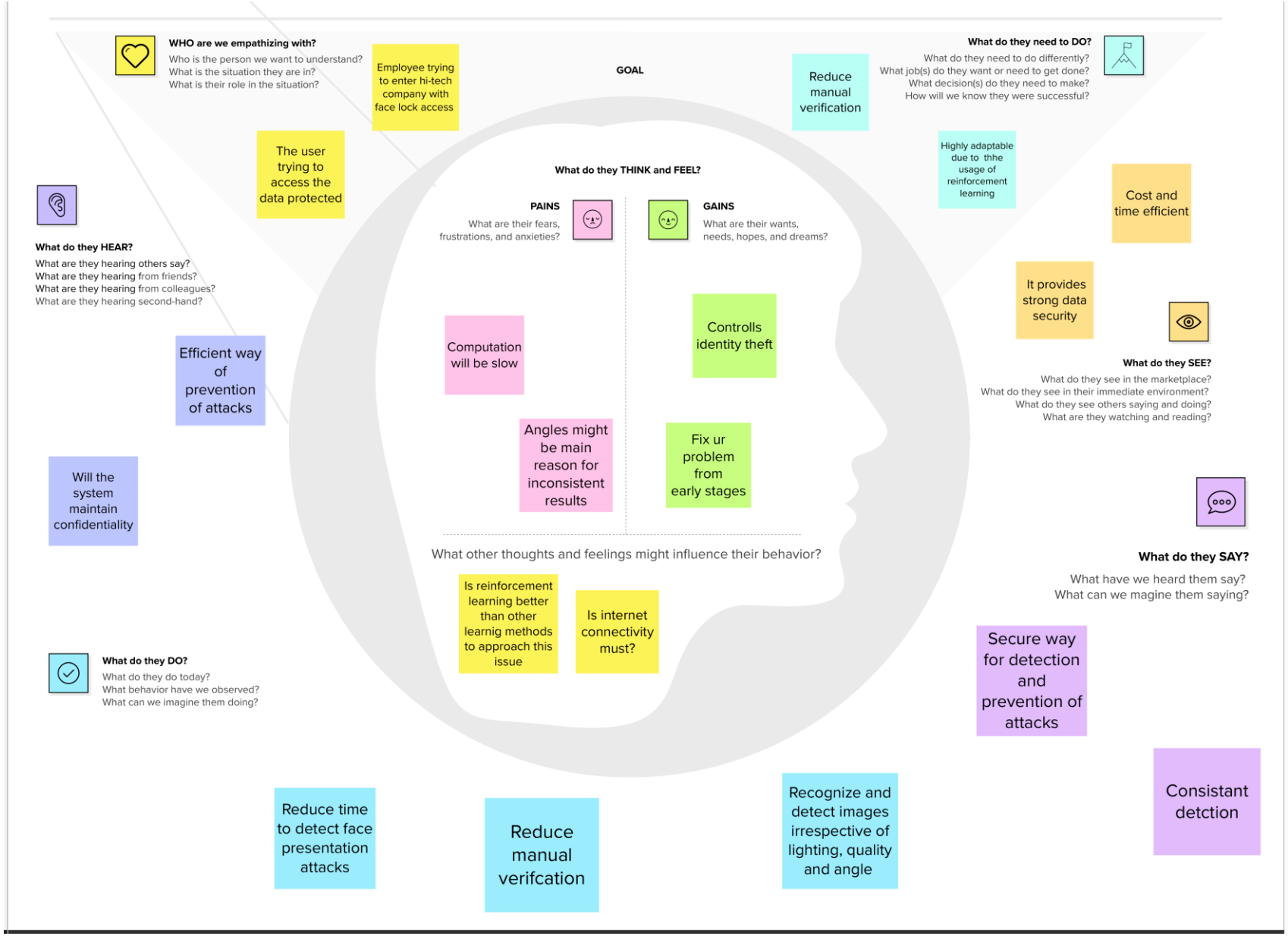
Navieen R (422419205022)

Literature Survey

S. No	TITLE & AUTHOR	JOURNAL & YEAR	PROBLEM	SOLUTION	PARAMETER MEASURED	ADVANTAGES	DISADVANTAGES
1	Salience- Aware Face Presentation Attack Detection via Deep ReinforcementLearning - 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 DeepReinforcement Learning for Face Anti- Spoofing - Rizhao Cai, Haoliang Li	IEEE TRANSACTIONS ON INFORMATIO N 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 slowdue the usage of Recurrent Neural Network (RNN).
3	Factors Related To The Improvementof 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 andreplay attackdetection.	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 onNeural Networks (IJCNN) | 978-1-7281-8671-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/IJCNN 55064.2022.989 275	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 andLogistic 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


WHO are we empathizing with?
Who is the person we want to understand?
What is the situation they are in?
What is their role in the situation?
Employee trying to enter hi-tech company with face lock access
GOAL
Reduce manual verification
What do they need to DO?
What do they need to do differently?
What job(s) do they want or need to get done?
What decision(s) do they need to make?
How will we know they were successful?
The user trying to access the data protected
Highly adaptable due to thhe usage of reinforcement learning
Cost and time efficient
What do they THINK and FEEL?
PAINS
What are their fears, frustrations, and anxieties?
GAINS
What are their wants, needs, hopes, and dreams?
What do they HEAR?
What are they hearing others say?
What are they hearing from friends?
What are they hearing from colleagues?
What are they hearing second-hand?
Computation will be slow
Controlls identity theft
It provides strong data security
Efficient way of prevention of attacks
What do they SEE?
What do they see in the marketplace?
What do they see in their immediate environment?
What do they see others saying and doing?
What are they watching and reading?
Angles might be main reason for inconsistent results
Fix ur problem from early stages
Will the system maintain confidentiality
What do they SAY?
What have we heard them say?
What can we magine them saying?
What other thoughts and feelings might influence their behavior?
Is reinforcement learning better than other learnig methods to approach this issue
Is internet connectivity must?
Secure way for detection and prevention of attacks
What do they DO?
What do they do today?
What behavior have we observed?
What can we imagine them doing?
Reduce time to detect face presentation attacks
Reduce manual verifcation
Recognize and detect images irrespective of lighting, quality and angle
Consistant detction

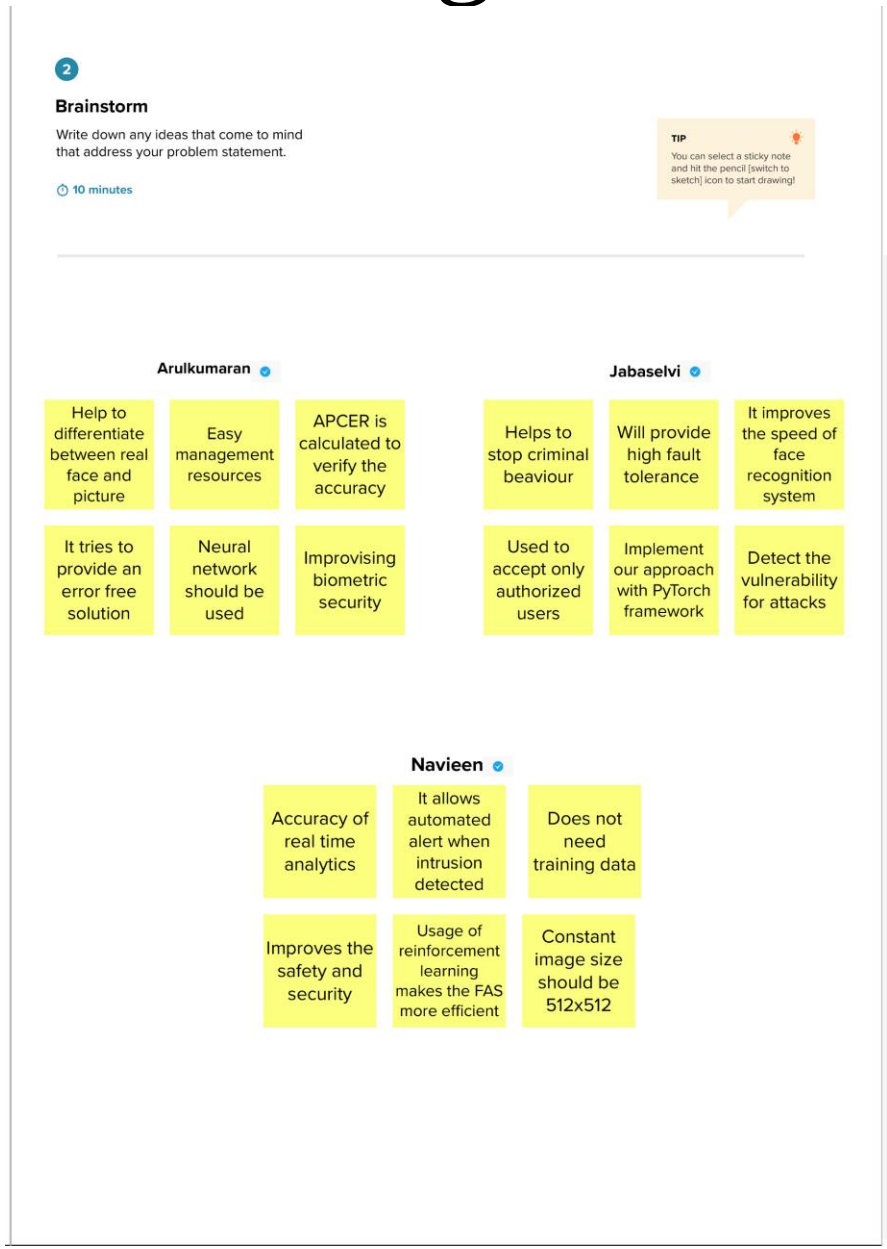
Problem Statement

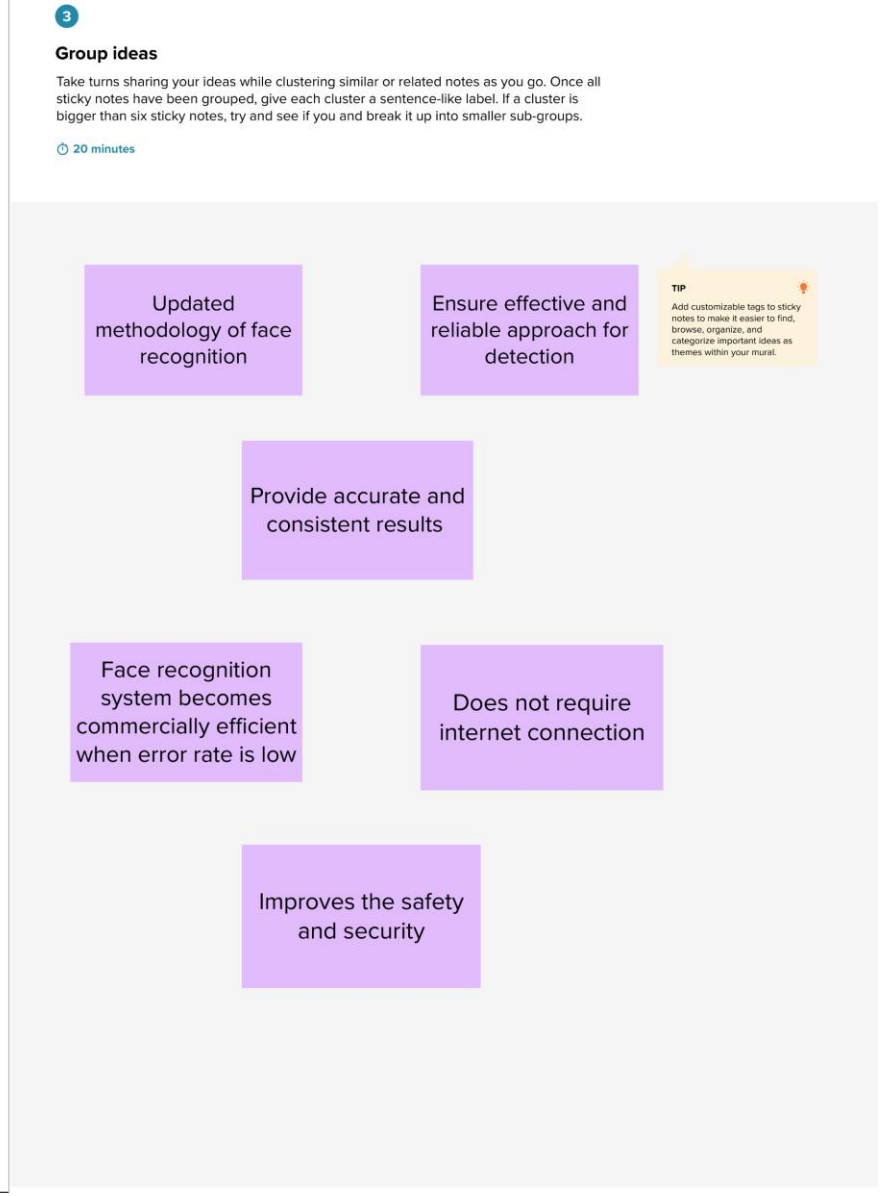
Mr. Walter White is a 45 year old successful businessman. He has a own business for past 20 years. In these 20 years he faced a lot of security issues and trouble in preventing the data from attackers.

- Mr. Walter White wants to setup a face recognition system that prevents others from accessing 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 the problem?	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 fix the 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 solve the issue?	We use deep reinforcement learning to prevent from attacks.

Brainstorming



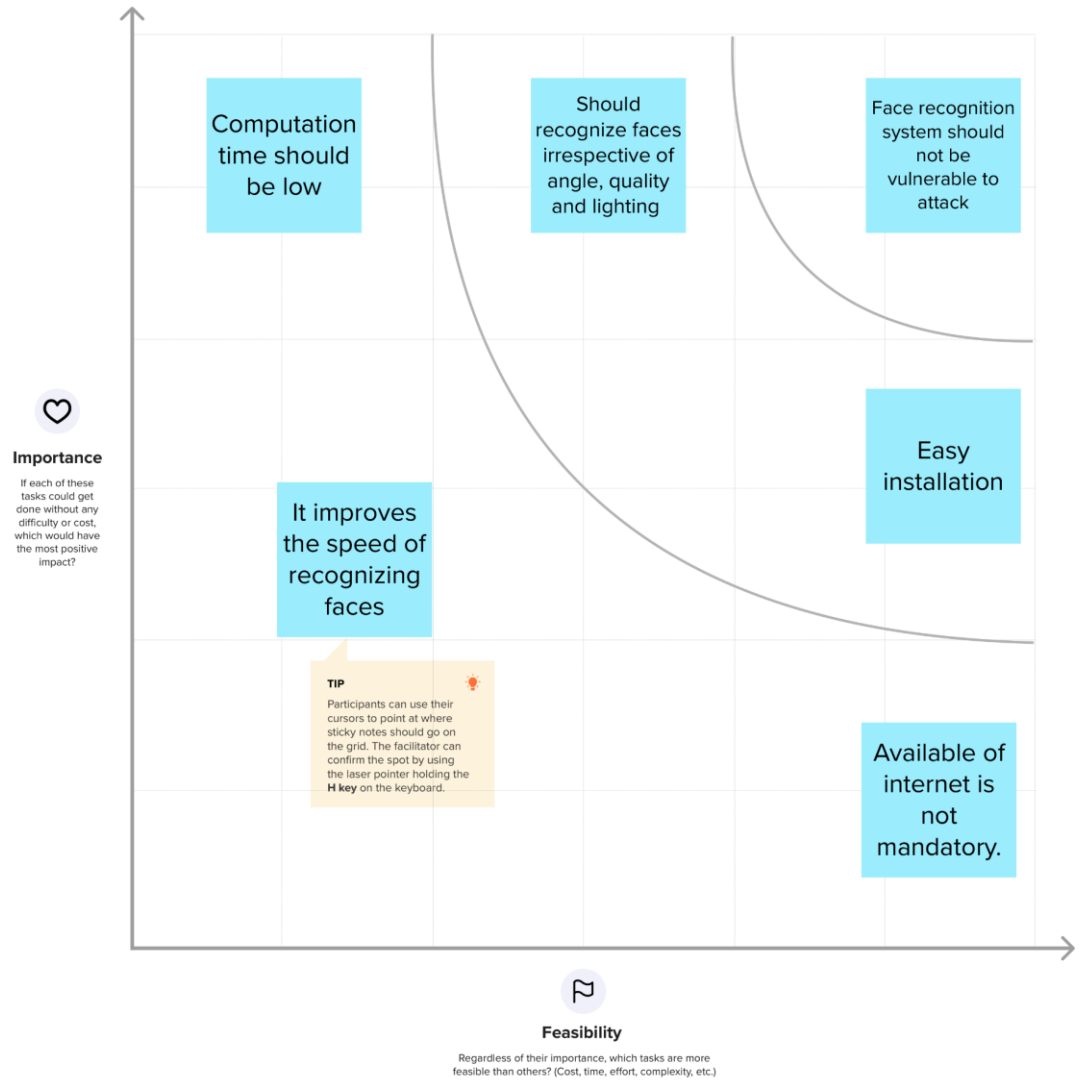


4

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