International Journal for Modern Trends in Science and Technology, 8(11): 01-10, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0811001
Available online at: http://www.ijmtst.com/vol8issue11.html

Deepfake - An Analysis of Opportunities and Threats

Anjali Rameshwar Nimje[1] | Gauri Ansurkar[2]

[1]Department of Information Technology, KSD'S MODEL COLLEGE
[2]Assistant Professor, Department of Information Technology, KSD'S MODEL COLLEGE

To Cite this Article
Anjali Rameshwar Nimje and Gauri Ansurkar. Deepfake - An Analysis of Opportunities and Threats. International Journal for Modern Trends in Science and Technology 2022, 8(11), pp. 01-10. https://doi.org/10.46501/IJMTST0811001

Article Info
Received: 09 October 2022; Accepted: 28 October 2022; Published: 01 November 2022.

ABSTRACT

First "deep learning" and second "fake" this two words were combined and keyword deepfake was invented deepfake is one the franchise of deep learning deepfake is the technology which deals with the audio-visual content that is artificially developed mostly with use of GAN. GAN is one of the technology in machine learning that connects the data set with neural networks to make it forgery using technology of deepfake one can mask others face on desired picture to make it look realistic and natural and with the help of ai we can recognise and study a particular face from dissimilar angles so GAN works by using ai algorithms against the original image or video with the duplicate we want to create which looks very similar with the original one.

KEYWORDS:Deepfake, Security, Threat, Privacy

1. INTRODUCTION

The automation called as deepfake is used by apple now which was discovered in 2014 by Ian goodfellow the mechanism of deepfake is to merge combine replace and superimpose images and audiovisual clips to create a video which is not original but appear to be one the deepfake can be also be capable to create a humorous instance pornographic or political video of an individual without knowing them or without their consent there image or voice can be used deepfake also point out or target the social network where misinformation gets scattered easily due to this people don't really believe on the social media platform unless and until they received the news with proper justification.

STRUCTURE OF PAPER

The paper is organized as follow : In section 1, the introduction of the paper is provided along with the structure, important terms, objectives and overall description. In section 2 we have discussed background , how deepfakes are made , who makes deepfake , technologies required to make AI deepfake and deepfake detection is explained. In section 3 consequences of deepfake , negative and positive sides of deepfake is evaluated. In section 4 possible solutions for deepfake is provided. In section 5 research methodologies is explained. In section 6 survey question and results are displayed. In section 7 testing of survey result is done using descriptive statistics and displayed it through histogram. In section 8, 9 and 10 finding, conclusion and bibliography of the research is provided.

2.BACKGROUND

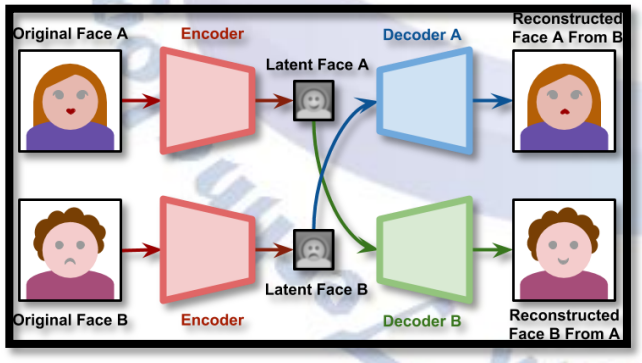
2.1 HOW ARE DEEPFAKES MADE

Higher university experimenter and computer studios of graphic have worked hard to have a check that what is the possibilities of having video and image exploitation. It requires more attempts to create a face-swap video. Firstly, you take numerous face shots of 2 individuals

through an AI algorithm known as an encoder. The work of an encoder is to find out and learn the likeness between the faces of 2 individual and reduces them to similar features, to reduce the images during the process. A second AI algorithm known as decoder is trained to regenerate those faces from the reduced images. As the faces are not similar you educate the first decoder to revive the first individuals face and same for the second individual. To carry out the face swap you rarely serve encoded images into the incorrect decoder. Then the reduced image of first individuals face is served by the decoder educated on second individual. Thus, the work of the decoder is to interchange the facial expressions with each other and for perfection it has to be repeated for every single frame.

Gan is another tool to create deepfake. A Gan merges couple of AI algorithms against each other. The first algorithm is named as generator having noise and changes it into a image this duplicate image is then merged with a couple of real images that are pushed into the second algorithm known as discriminator.

At the beginning the duplicate images will not appear to be like the original one but repeating this mechanism for period of instance the discriminator and the generator will enhance with the feedback on performance after providing the loops and feedback the generator will be able to create real like pictures of faces of nonexistent personalities.



2.2WHO MAKES DEEPFAKE?

The deepfake is made from the studios of special effect or porn makers, industrial academy. In order to avoid, terrorist clan and other misleading activity government may also be involved in the technology. For example

There is minimum four categories of deepfake producers 1. Deep-seated groups of hobbyists. 2. Social actors 3. Other actors 4. Legal actors (TV Companies).

Usually, the group of hobbyists try to watch videos created using AI technology as a way of social media comic rather to make people angry for using their pictures in wrong comic manner. The deep fake generation are supposed to be for entertainment purpose, comic or political videos and it can be also utilized to achieve a certain amount of fan followers on online platform.

The different types of misleading activities can be performed by the terrorist, hackers, political enemies and foreign countries can use this technology for defaming about campaigns and idea to change public opinion according to their vision. The deepfake can also be used as weapon during the period of warfare to create wrong information.

Deepfake are also rapidly followed by the fraud people to perform stock and currency contrivances. Criminals are already started using fake AI generated voice to carry out a transaction by asking for money transfer in urgency.

2.3 TECHNOLOGIES REQUIRED TO MAKE AI DEEPFAKE

It is very difficult to create a true deepfake on normal computer many are created on high performing computers with powerful processor and graphic cards or else it can be still done by computing power using clouds. This helps to convert the duration of work from long period to short period of time. It also requires expert opinion for at least a touch-up to the completed videos to monitor flicker and other visual defects. Hence different types of tools are available to help people create deepfake; there are also the companies who will assist you to make deepfake videos using clouds, e.g. Deepfakesweb.com There are applications also which are available for mobile to create Deepfake videos and images e.g. Zao.

2.4 DEEPFAKE DETECTION

The deepfake video which are not created with proper scales are easy to acknowledge as the lip sync are out of match, the person who is speaking doesn't blink his eyes or there could be flicker on the screen. But due to rise in technology and NLP algorithms it has become more advanced, it is also getting difficult for the people to recognize(justify) deepfake and other advance(enhanced) technology scam. AI is one of the most powerful tools to combat AI developed attacks. AI is capable of understanding the patterns and it can

automatically sense unusual patterns quickly and precisely than a normal person can.

But we cannot just depend on the technologies. Education and people should be aware of all these activities, which are important. Hence 61% IT leaders are already started their campaign for educating their workers about the dangers created by Deepfake and remaining 27% have plans to do so. Several studies use characteristics like visual artifacts, image quality, lip-sync, blinking, or wrapping for classification. This work is used to give a general frame work which have a guarantee on its reliability.

3.EVALUTION

3.1CONSEQUENCES OF DEEPFAKE

It seems scary for many of them to avail artificial intelligence the use of ai technology is plenty of ethical dilemmas and unpredictable future uses one of the most danger possibilities of AI are the invention of deepfake. Deepfake provide many opportunities of malicious and terror use it is very difficult to find the solution or bring a positive light to creation so that one can believe it.

The intention behind creating videos using deepfake was to create harmless and advance research of authentic video creation which can be used for movies, storytelling and day to day activities. But unfortunately, this tool can also be used in a wrong manner to spread wrong information, to harass individual or defame the individual's personality. The rise in creations of fake videos by using social media platforms has raised a question mark on the workability of digital media. But every technology has its merits and demerits.

3.2 POSTIVE IMPACTS

1.Educational benefits:

there is a plus point of deep fake technology on tutoring it could change the way of teaching and also make the lessons interactive for example the chapters of history can be taught to students using deepfake and think how interactive session is would be for the learner and the tutor as well with deep samples of historical figures it could preserve tales and help catch interest

2.Unifying the global audience:

as we know with the help of deepfake we can change the voice and audio visual so interpret movies that use the real actors can be allowed

3. The movie industry:

take representatives case of the days when the role of the ghost was used to played by a person the role of CGI can be filled by deep fake mechanization recreate the same features of inapproachable past performer with the help of deepfake AI.

4. Art World:

we can build the virtual museums this will build an interest in people to watch the skill work from different nation for whom it is not feasible to go in the museum physically we should share the planets compelling profound artwork

5.Medical:

This will offer a boost to data protection thus assisting with the emergence of current diagnostic and tracking procedures infirmary can produce deep-fake sufferer by using the applied science backing deep-fakes that is sufferer information that is practical for research and test but does not place actual sufferer at risk so rather than actual sufferer details experimenters apply natural deep-fake sufferer there is space to examine new diagnostic and keep an eye on techniques or even teach other ai to help with medical decisions .

6.Training:

It takes many of details and information to train unnatural technology often questions arises as to what is the source of all this knowledge comes from there's also the matter of probabilistic prejudice induced by an absence of knowledge difference .However, generate natural difference unnatural data with deep-fake innovation and so the issue of requiring further training statistics could come to an end or for new colleagues contemplate some preparation take paradigm of trouble shooting training its can be possible to create the near enough client to give the training to the candidates you will train your recently joined colleague without instead directly making them face to the actual customers.

3.3NEGATIVE IMPACTS

Deepfake cause serious threat to our community, government and business due to 1. It creates a lot of stress on journalists to identify the difference between real and fake news 2. The deepfake can also be used to trouble national security by misusing the tool for election purposes. 3. To break the citizens trust towards the information provided by the authority. 4. Increase cyber

security problems for individuals and organization of a country.

There is a high possibility that the journalism industry will be facing a big amount of trust issues by the citizens and the credit goes to deepfake. The deepfake allows the assemblers of various data which look almost similar to the original one hence judging the journalist and putting them in conflict.

Due to the misuse of deepfake it makes more difficult for the people to identify that the video they watch comes from a true source with subjective norms constraints or not. This is same as phenomenon of fake news. Hence one can only tell the story is trustable or not by seeing the source which is subjected to norms and constraints.

One of the incident between India in Pakistan in the year 2019 where 30 fake footages were posted which we old from the other event posted with a new captions and title.

It is believed that the deepfake will be used to threaten the national security of the nation which will lead to cause a disturbance in the election campaigns. Editing a video and changing the vocal with wrong or misleading words can be biggest weapon in today's world.

Not always deepfake is responsible for creating a fake video but due to misusing of this tool it leads to trust issue between people whether to trust it or not.In other words, the best threat isn't that folks are going to be deceived, but that they're going to come to take everything as deception.

4. POSSIBLE SOLUTIONS FOR DEEPFAKE

According to the latest articles it shows that there are four different methods to stop the miss use of deepfake 1) rules and regulation,2) business strategies and immediate action,3) education and training, and4) a tool named as anti-deepfake technology which will include identification of deepfake and hence help to stop misuse of deepfake.

Legislation and legislation are also transparent forms of profound forgery. Deepfakes are not currently explicitly addressed by civil or criminal legislation, while legal scholars have proposed adapting existing laws to cover libel, slander, identity theft, or using deepfakes to mimic a government official.

The social media companies of today enjoy strong immunity for the content shared on their sites by users. One legislative alternative may be to remove the legal immunity of social media sites from the content shared by their users making not only users but also websites more accountable for posted information.

The detection of audio and video for fake content is very easy as per recent studies. Recently, a fake detection method was inconsistencies that exist between the dynamics of the mouth shape (visemes) and the spoken phoneme. In this observation they kept the mouth close in the video and checked that this did not happen in specially the length of video was found to be increased.

The social media should follow some ethic and stay away from the truth that having wrong content pushed to the top can help them to make a lot of money but still it is wrong thing to do. Few of the social media platform companies still have the policies which are related to deepfake as they try their best to prevent the information which is not 100% true towards the community. The policies consist of blocking and deleting deep faced content. Many of the platforms do not actually delete the deepfake content but lower it down so that no one can reach it. There is a rise in hate speech, false news, and misinformation polluting digital networks

Has led to many businesses to take against it such as deceiving their account and investing a lot of money in the fastest technology for detection of deepfake.

5. RESEARCH METHODOLOGIES HYBRID MODEL

A model may include both descriptive and analytical components. A descriptive model's logical relationships can be examined, and conclusions can be drawn to reason about the system. Nonetheless, logical analysis yields quite different conclusions than a quantitative chemical investigation of system properties.

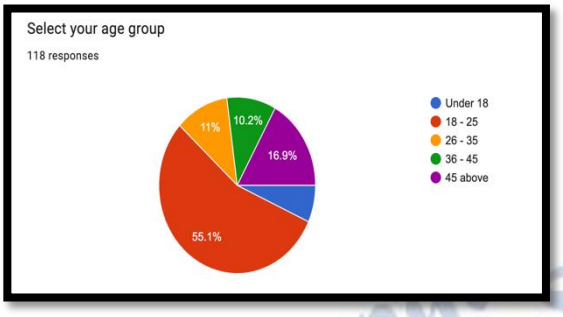
We first conducted a poll of people utilizing an online form creator and data collection service to acquire information regarding people's awareness.

6. PUBLIC SURVEY

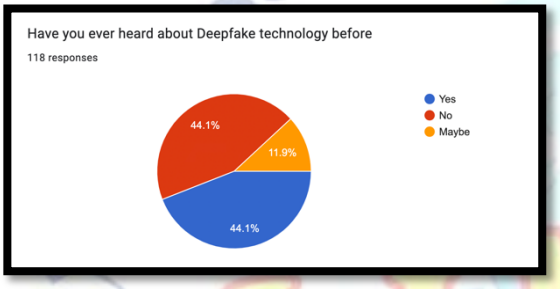
We deployed our data gathering utility, often known as a survey bot, to a variety of people and collected information on various facets of their understanding of AI deepfake.

6.1 SURVEY QUESTIONNAIRE AND RESULTS

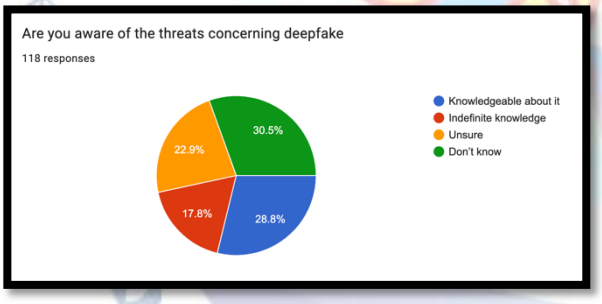
1.Select your age group.



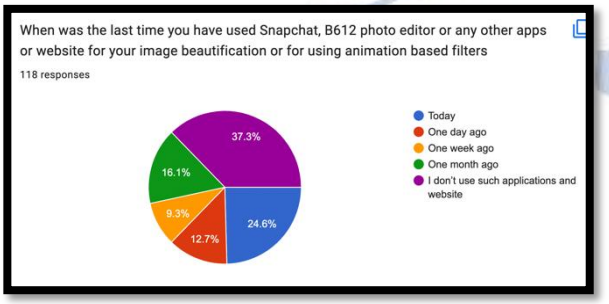
2.Have you ever heard about Deepfake technology before?



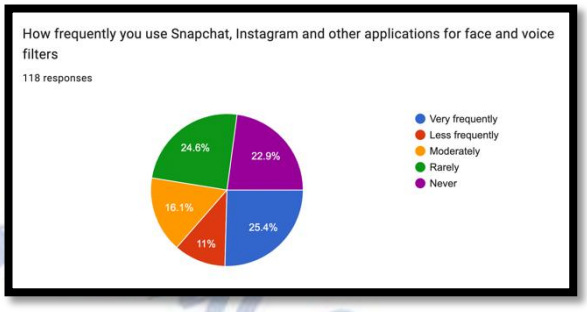
3. Are you aware of the threats concerning deepfake?



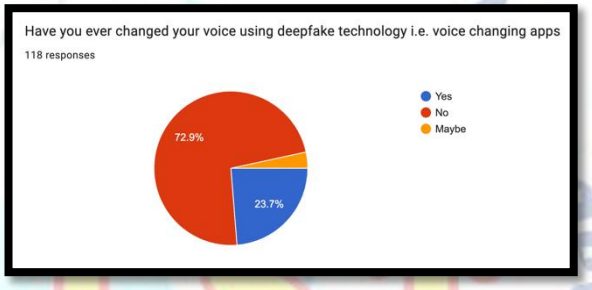
4.When was the last time you have used Snapchat,B612 photo editor or any other applications and websites for your image beautification or for using animation based filters?



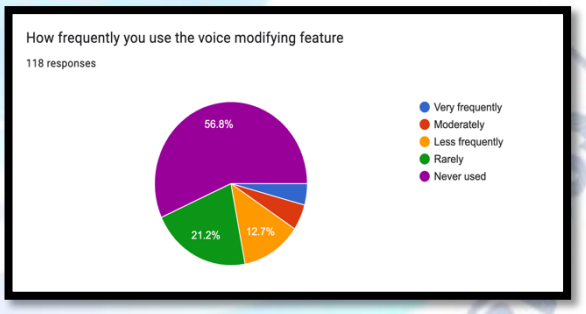
5.How frequently you use Snapchat, Instagram and other applications for face and voice filters?



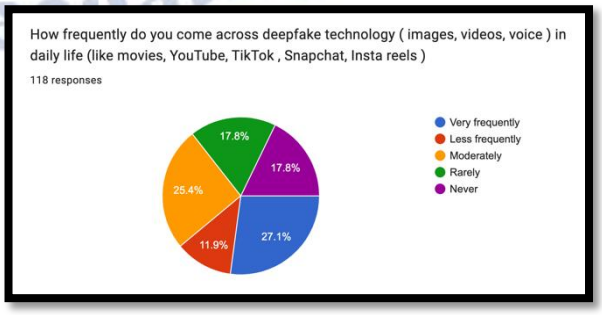
6.Have you ever changed your voice using deepfake technology i.e. using voice changing apps ?



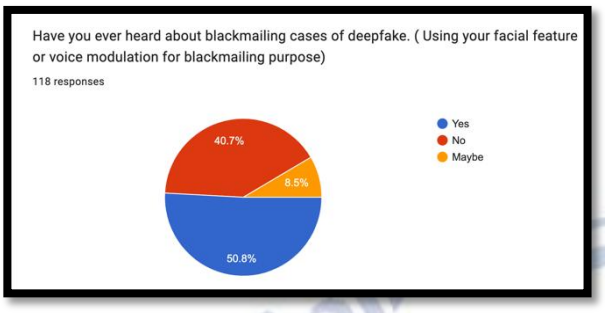
7.How frequently you use the voice modifying features?



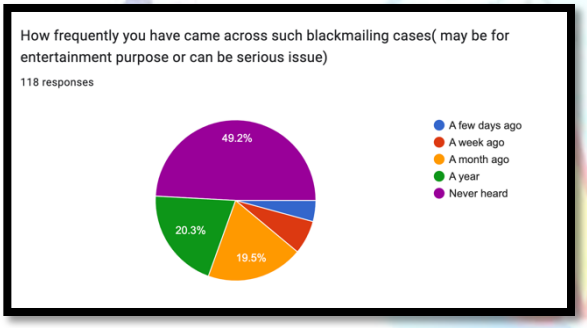
8.How frequently do you come across deepfake technology(images, videos, voice) in daily life(like movies, YouTube, TikTok, Snapchat, Instagram reels, etc)?



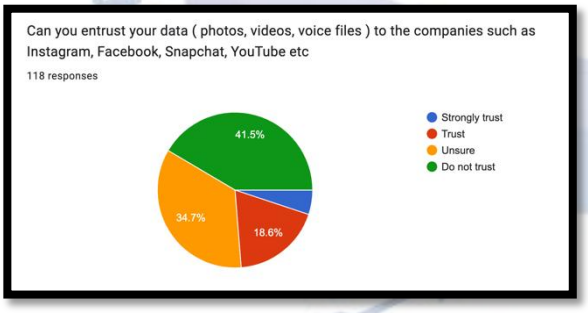
9.Have you ever heard about blackmailing cases of deepfake? (Using facial features or voice modulation for blackmailing purpose)?



10.How frequently you have come across such blackmailing cases(may be for entertainment purpose or can be serious issue)?



11. Can you entrust your data (photos, videos, voice files) to the companies such as Instagram, Facebook, Snapchat, YouTube, etc?



7.TESTING

7.1DESCRIPTIVE STATISTICS

Descriptive statistics is a means of describing features of a data set by generating summaries about data samples.

Have you ever heard about Deepfake technology before	
Mean	1.66942149
Standard Error	0.06142077
Median	2
Mode	1
Standard Deviation	0.67562847
Sample Variance	0.45647383
Kurtosis	-0.7489587
Skewness	0.51365217
Range	2
Minimum	1
Maximum	3
Sum	202
Count	121
Confidence Level(95.0%)	0.12160885

Are you aware of the threats concerning deepfake	
Mean	2.55371901
Standard Error	0.10943784
Median	3
Mode	4
Standard Deviation	1.20381625
Sample Variance	1.44917355
Kurtosis	-1.5374528
Skewness	-0.0991775
Range	3
Minimum	1
Maximum	4
Sum	309
Count	121
Confidence Level(95.0%)	0.21667931

When was the last time you have used Snapchat, B612 photo editor or any other apps or website for your image beautification or for using animation based filters	
Mean	3.2892562
Standard Error	0.14819298
Median	4
Mode	5
Standard Deviation	1.63012278
Sample Variance	2.65730028

Kurtosis	-1.5591623
Skewness	-0.302493
Range	4
Minimum	1
Maximum	5
Sum	398
Count	121
Confidence Level(95.0%)	0.29341179

How frequently you use Snapchat, Instagram and other applications for face and voice filters	
Mean	3.08264463
Standard Error	0.13665967
Median	3
Mode	1
Standard Deviation	1.50325634
Sample Variance	2.25977961
Kurtosis	-1.4127904
Skewness	-0.1878284
Range	4
Minimum	1
Maximum	5
Sum	373
Count	121
Confidence Level(95.0%)	0.27057663

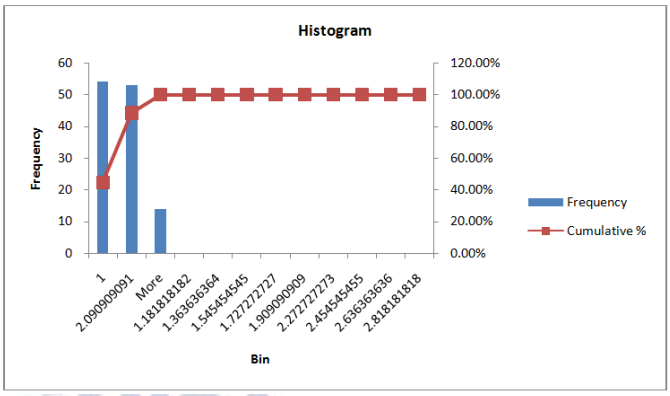
Have you ever changed your voice using deepfake tech2logy i.e., voice changing apps	
Mean	1.79338843
Standard Error	0.04378346
Median	2
Mode	2
Standard Deviation	0.48161803
Sample Variance	0.23195592
Kurtosis	0.20114645
Skewness	-0.5066605
Range	2
Minimum	1
Maximum	3
Sum	217
Count	121
Confidence Level(95.0%)	0.0866882

How frequently you use the voice modifying feature	
Mean	4.21487603
Standard Error	0.10110043
Median	5
Mode	5
Standard Deviation	1.1121047
Sample Variance	1.23677686
Kurtosis	1.15958862
Skewness	-1.3976571
Range	4
Minimum	1
Maximum	5
Sum	510
Count	121
Confidence Level(95.0%)	0.20017181

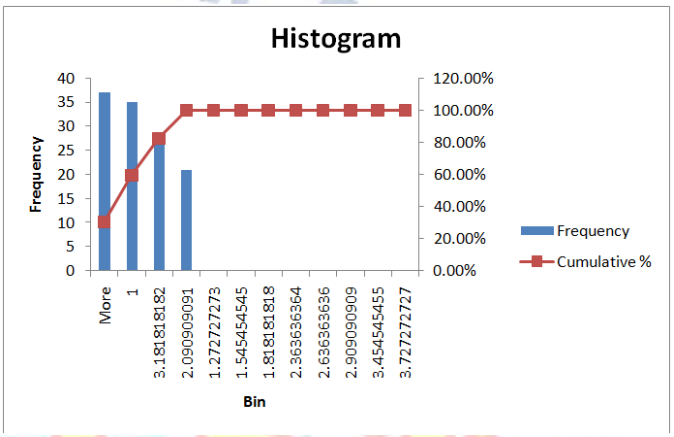
How frequently do you come across deepfake technology (images, videos, voice) in daily life (like movies, YouTube, TikTok , Snapchat, Insta reels)	
Mean	2.85123967
Standard Error	0.13208497
Median	3
Mode	1
Standard Deviation	1.45293471
Sample Variance	2.11101928
Kurtosis	-1.3215906
Skewness	0.04821097
Range	4
Minimum	1
Maximum	5
Sum	345
Count	121
Confidence Level(95.0%)	0.26151906

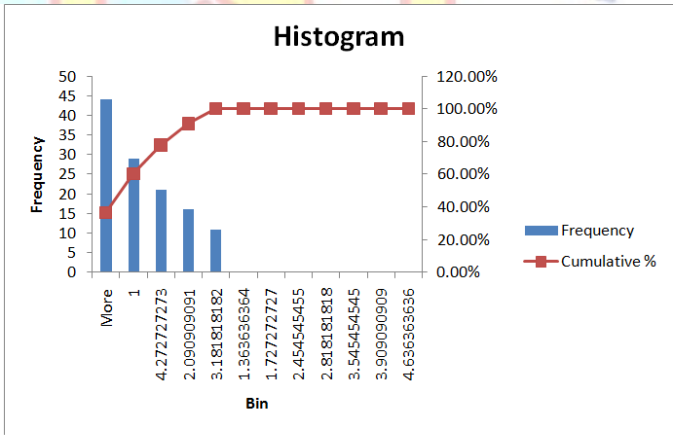
Have you ever heard about blackmailing cases of deepfake. (Using your facial feature or voice modulation for blackmailing purpose)	
Mean	1.58677686
Standard Error	0.05946203
Median	1
Mode	1
Standard Deviation	0.65408233
Sample Variance	0.42782369
Kurtosis	-0.561878
Skewness	0.67164276
Range	2
Minimum	1
Maximum	3
Sum	192
Count	121
Confidence Level(95.0%)	0.11773068

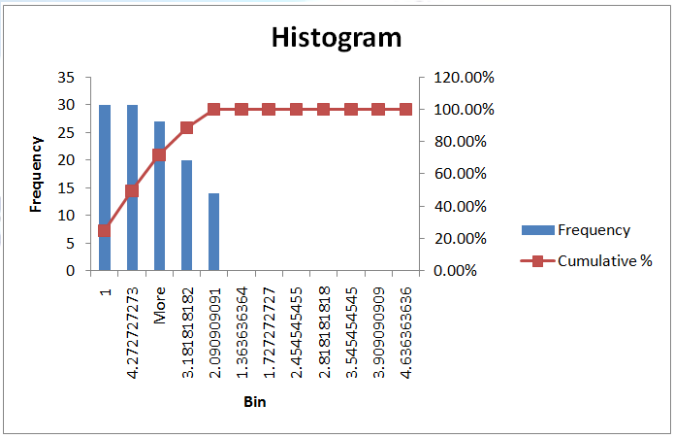
How frequently you have come across such blackmailing cases(may be for entertainment purpose or can be serious issue)	
Mean	2.14876033
Standard Error	0.04176076
Median	2
Mode	2
Standard Deviation	0.45936835
Sample Variance	0.21101928
Kurtosis	1.02144645
Skewness	0.55076912
Range	2
Minimum	1
Maximum	3
Sum	260
Count	121
Confidence Level (95.0%)	0.0826834



Can you entrust your data (photos, videos, voice files) to the companies such as Instagram, Facebook, Snapchat, YouTube etc.	
Mean	3.1322314
Standard Error	0.08126255
Median	3
Mode	4
Standard Deviation	0.89388803
Sample Variance	0.79903581
Kurtosis	-0.4591197
Skewness	-0.6918299
Range	3
Minimum	1
Maximum	4
Sum	379
Count	121
Confidence Level(95.0%)	0.16089419

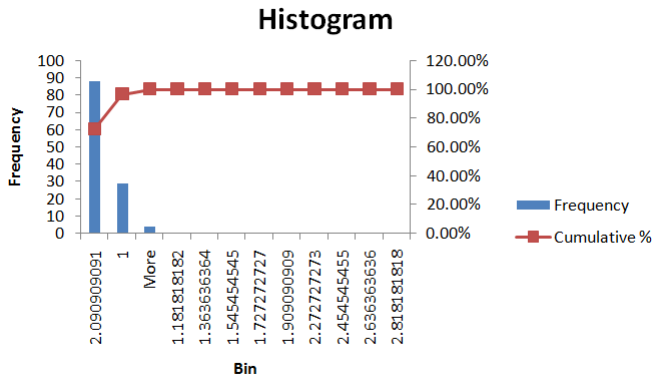


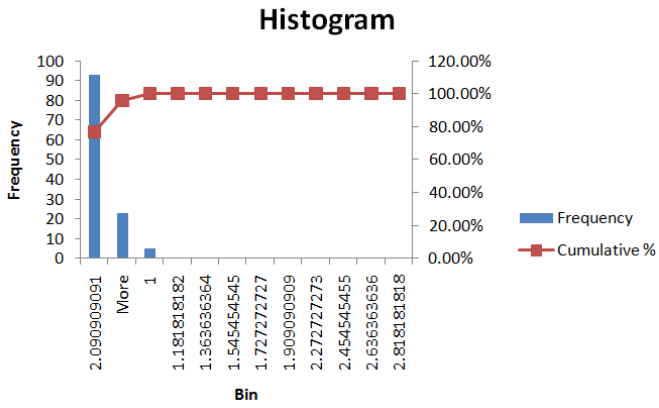


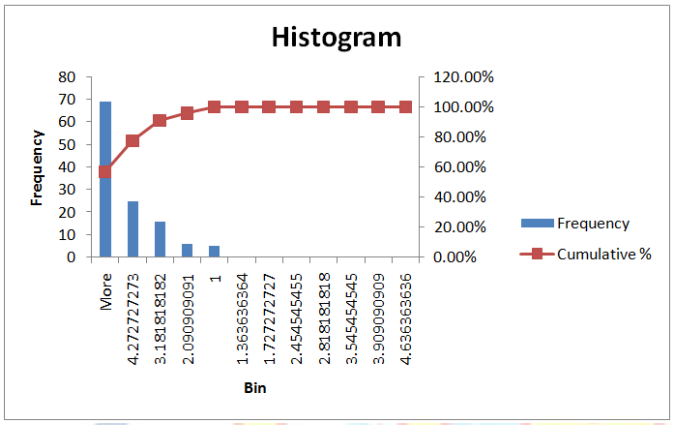


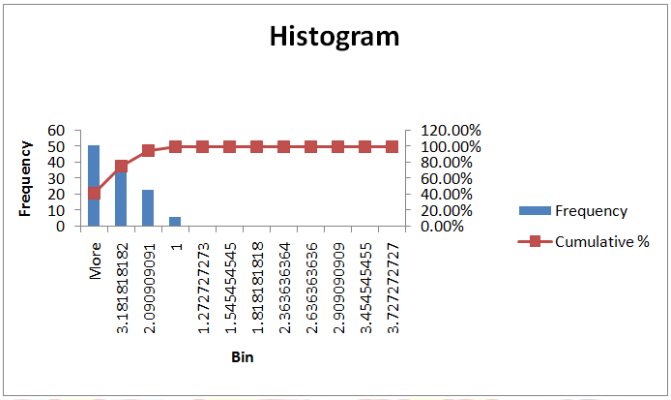
7.2 HISTOGRAM

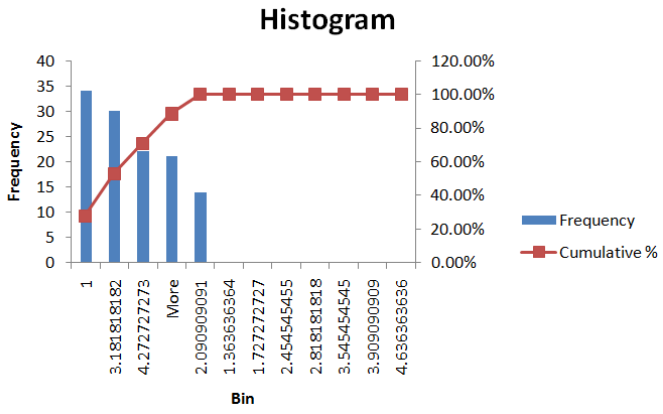
The histogram is a popular graphing tool. It is used to summarize discrete or continuous data that are measured on an interval scale. It is often used to illustrate the major features of the distribution of the data in a convenient form.

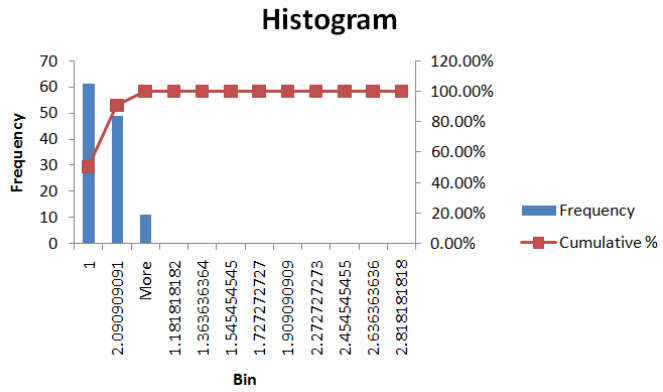












8. FINDINGS

1.People who are aware of the threats caused by deepfake technology should use any app only after reading and understanding all the terms and conditions before downloading and using it and same applies to the people who are least aware of this technology.

2.People believe just because it is one of the popular app and website to mask faces among the generation it will not cause any privacy issue.

3. While using any website to mask your face make sure the website you are using is “https://” not “http://”.

4.It is very important to keep your devices up to date to get the latest security patches the company releases that greatly enhance your privacy and security while using any application.

5.Disable the features you don’t use.

9. CONCLUSION

According to the survey and study, deepfake has its own positive and negative sides but negative is over-ruling the positive effects of deepfake.

Deepfake is used in advertisements as a Dubey for the main characters in ads. Many research is taking place to

clone the facial features of a group on a single person to know how the outcome is , this are the pros of this AI based technology. The cons of deepfake is it can be serious threat for the society. They put pressure on journalists struggling to filter real from fake news, threaten national security by disseminating propaganda that interferes in elections, hamper citizen trust toward information by authorities, and lift cyber security issues for people and organizations.

On other hand there only four possible ways to beat the deepfake issue that is 1) Legislation and Regulation, 2) corporate policies and voluntary action, 3) education and training, and 4) anti-deepfake technology. Legislation takes actions against misuse of this technology but is not effective in other countries. Also, many activists try to educate people do avoid using any pirated app. Many porn sites capture your images without your consent and willing which causes a big humiliation on the user because once they get your picture, they blackmail the user. Also, many a times it has happened that a random person calls you who is aware about you and has enough information about your life tends to make you fool using voice changing app on a phone call to get your bank data.

In short weightage of cons is more than pros. And to make this technology safe for user's appropriate security should be enabled. Arguments, both in favour and against, can be made but they will only prove to be imperative if the development of and access to Deepfake generating tools are governed properly. If closely monitored then Deepfakes can be used to benefit modern-day humanity rather than cause its downfall.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Mika Westerlund "The Emergence of Deepfake Technology: A Review" Technology Innovation Management Review, Volume 9, Issue 11, November 2019

[2] Sakshi Agarwal and Lav R. Varshney "Limits of Deepfake Detection: A Robust Estimation Viewpoint" arXiv, May 2019

[3] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales and Javier Ortega-Garcia "DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection" arXiv, June 2020

[4] F. Matern, C. Riess and M. Stamminger, "Exploiting Visual Artifacts to Expose Deepfakes and Face Manipulations," IEEE Winter Applications of Computer Vision Workshops (WACVW), ISBN:978-1-7281-1393- 2019

[5] Fallis, D. "The Epistemic Threat of Deepfakes" Springer

[6] SupasornSuwajanakorn, Steven M Seitz, and Ira Kemelmacher-Shlizerman. "Synthesizing obama: learning lip sync from audio" ACM Transactions on Graphics (TOG), Volume 36, Issue 4, July 2017.

[7] Shehzeen Hussain, PaarthNeekhara, Malhar Jere, FarinazKoushanfar, Julian McAuley "Adversarial Deepfakes: Evaluating Vulnerability of Deepfake Detectors to Adversarial Examples" arXiv, November 2020

[8] Yuezun Li, SiweiLyu "Exposing DeepFake Videos By Detecting Face Warping Artifacts" arXiv, May 2019