

A Presentation on  
**Project**  
**“Adversarial Captcha System”**

By

- 1. Soham Mirajgaonkar (B190315039)**
- 2. Kartik Ballal (B190315006)**
- 3. Shantanu Badgujar (B190315054)**

Under the guidance of  
**Prof. Mrs. Laxmi Jadhav**



Department of Electronics and Computer Engineering PES's Modern College of Engineering,  
Shivajinagar, Pune ACADEMIC YEAR: 2023-2024.

# Outline of Presentation

Content

Introduction

Literature Survey

Gap Identification

Aim/ Problem Statement

Objectives

Methodology

Results & Discussion

Future Plan

References

# Introduction

The substantial and automated access to Web resources through robots has made it essential for Web service providers to make some anticipation about whether "user" is a human or a robot.

A Human Interaction Proof (HIP) like Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) offers a way to make such a distinction. Captcha is a reverse Turing test used by Web service providers to secure human interaction assumed services from Web bots.

Several Web services that include but are not limited to free email accounts, submission of e-mail, online polls, chat rooms, search engines, blogs, password systems, etc. use Captcha as a defense mechanism against automated Web bots.

This paper presents various aspects of Captcha methods that include its types, generation methods, robustness against attacks and various usability aspects.

It presents a review of existing Captcha schemes besides relative merits of text and image based on them.

# Literature Review

Sr No.	Paper Title	Author	Paper Details
1	The Robustness of Hollow CAPTCHAs	Haichang Gao, Wei Wang, Jiao Qi, Xuqin Wang, Xiyang Liu	A main feature of such hollow CAPTCHAs is to use contour lines to form connected characters with the aim of improving security and usability simultaneously, as it is hard for state-of-the-art character recognition programs to segment and recognize such connected characters, which are however easy to human eyes.
2	Research on the Security of Microsoft's Two-layer Captcha	Haichang Gao, Mengyun Tang, Yi Liu, Ping Zhang and Xiyang Liu	In this paper, systematically analyzed the security of the two-layer Captcha. A novel two-dimensional segmentation approach is proposed to separate a Captcha image along both vertical and horizontal directions, which helps create many single characters and is unlike traditional segmentation techniques
3	The End is Nigh: Generic Solving of Text-based CAPTCHAs	Elie Bursztein, Jonathan Aigrain, Angelika Moscicki, John C. Mitchell	The paper introduces a novel approach to solving captchas in a single step that uses machine learning to attack the segmentation and the recognition problems simultaneously.

# Literature Review

Sr No.	Paper Title	Author	Paper Details
4	Flexible, High Performance Convolutional Neural Networks for Image Classification	Dan C. Cireş,an, Ueli Meier, Jonathan Masci, Luca M. Gambardella, Jurgen Schmidhuber	The paper presents a fast, fully parameterizable GPU implementation of Convolutional Neural Network variants. All structural CNN parameters such as input image size, number of hidden layers, number of maps per layer, kernel sizes, skipping factors and connection tables are adaptable to any particular application.
5	Breaking text-based CAPTCHAs with variable word and character orientation	Oleg Starostenko n , Claudia Cruz-Perez, Fernando Uceda-Ponga, Vicente Alarcon-Aquino	A novel approach for automatic segmentation and recognition of CAPTCHAs with variable orientation and random collapse of overlapped characters is presented in paper.

# Gap Identification

Analyzing image-based CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) involves assessing the strengths and weaknesses of such systems.

While image-based CAPTCHAs have their strengths in distinguishing between humans and bots, they also exhibit weaknesses that need to be addressed for improved security, accessibility, and user experience.

Continuous innovation and a balanced approach to security and usability are essential for effective CAPTCHA implementation.

# Problem Statement:

To design and implement novel an image-based Captcha known as Style Area Captcha (SACaptcha) that is based on the neural style transfer techniques that are user friendly, require less server processing and offer improved security control against bots.

# Objectives

The primary objective of image-based CAPTCHAs is to distinguish between human users and automated bots or scripts.

To authenticate human users, ensuring that the user interacting with a website or service is indeed a real person and not a computer program.

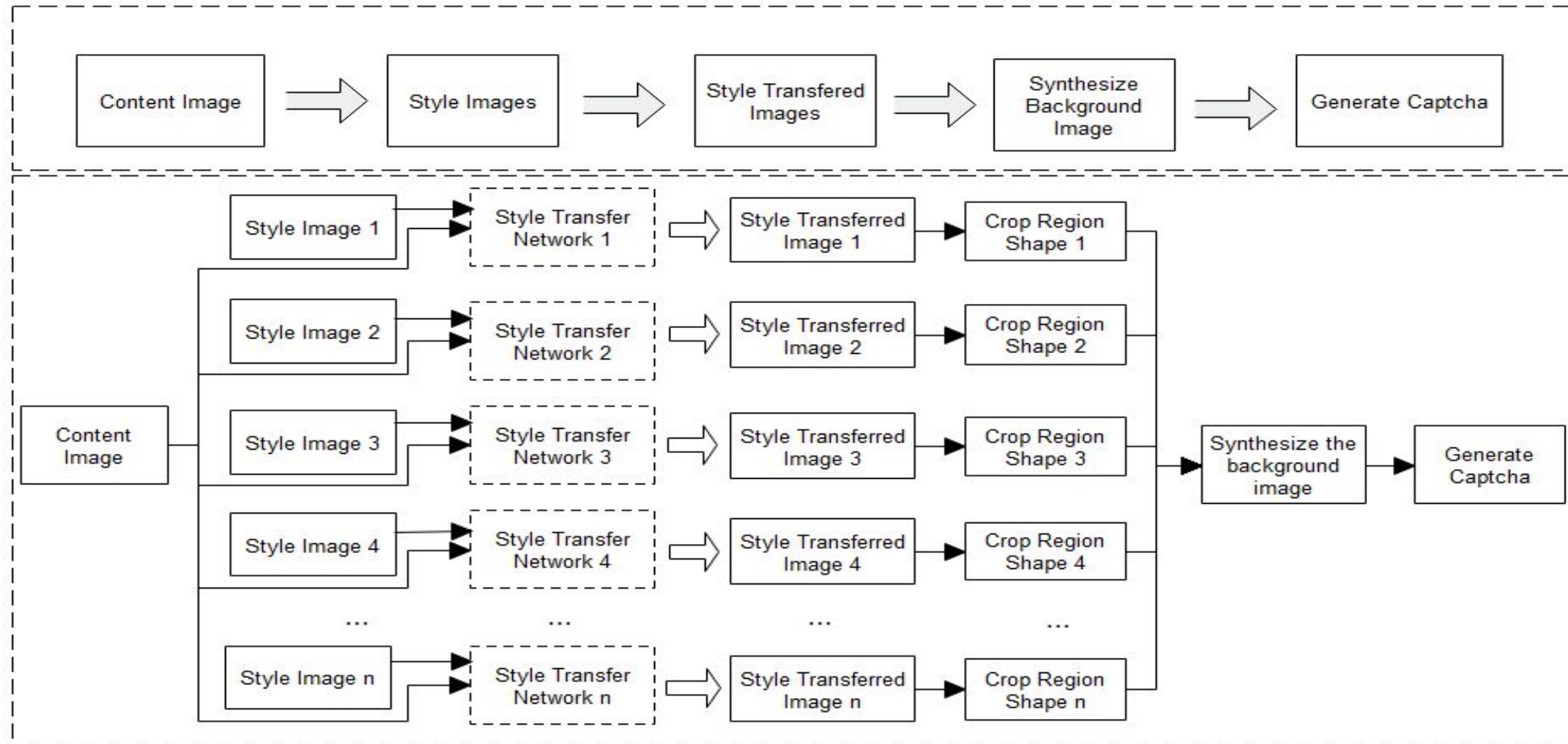
To improving security measures against advanced bot attacks.

To create CAPTCHAs that are effective against bots while remaining user-friendly and ensuring that legitimate users can easily pass through without undue hassle or frustration.

To maintain security, verify human presence, prevent abuse, and continually adapt to counter evolving threats from automated scripts and bots.



# Proposed Methodology : Block Diagram



# Process Overview (Model)

SIGN IN PAGE

---

**Your Time Starts: 95**

Email-ID

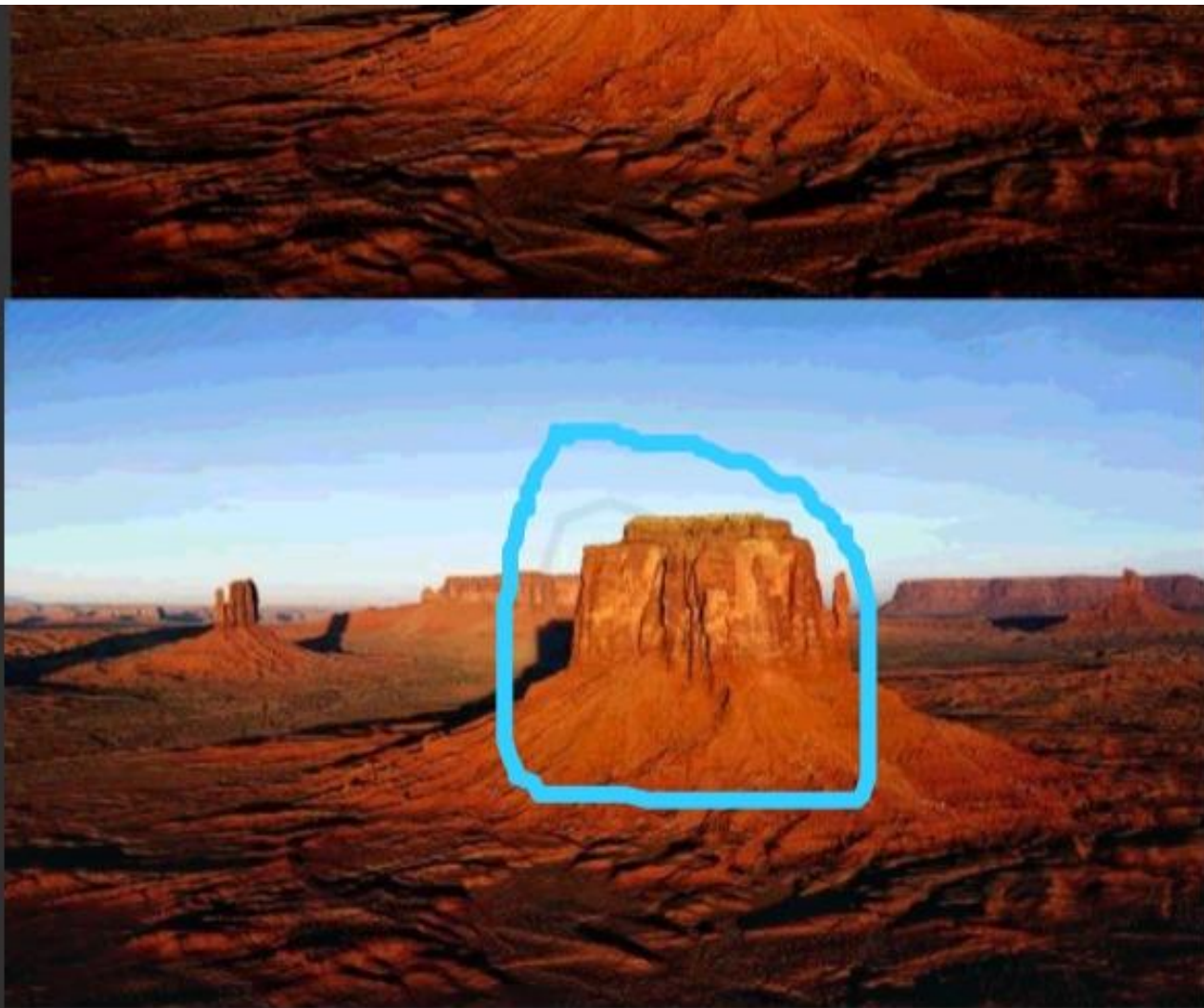
Password

Click Triangle



Click Pentagon

Click Octagon



SIGN IN

RESET

Click Octagon

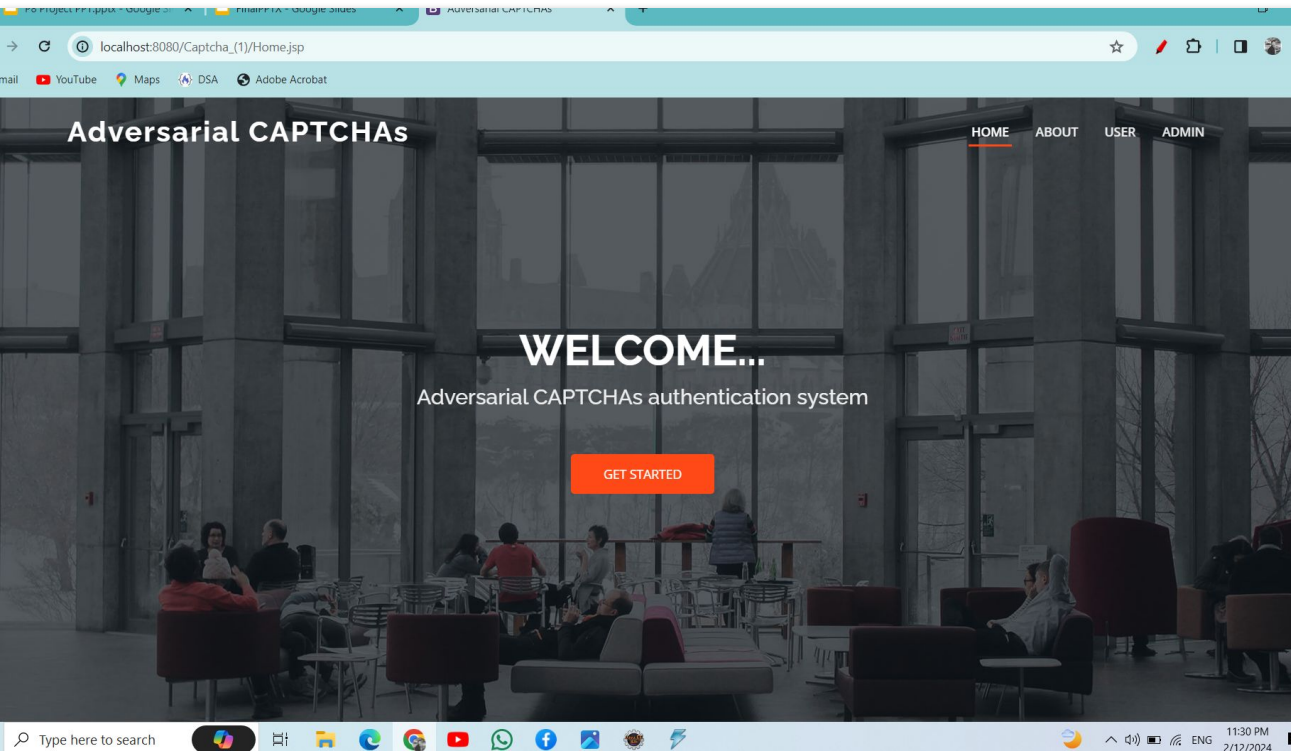


SIGN IN

RESET



# Static Website:



LOGIN HERE

LOGIN

[Register here!!!](#)



# Proposed Methodology : Explanation

Previous image-based Captchas have describes various issues: some schemes require humans to manually select source images or add labels to images.

Some are based on a database, and if the database is compromised, they become vulnerable; some schemes incur a high transmission cost; and, most importantly, almost all of them have been proven to be insecure.

To overcome these issues, proposes a novel image-based Captcha named Style Area Captcha (SACaptcha), which is based on semantic information understanding, pixel-level segmentation and deep learning techniques.

# Proposed Methodology : Explanation

In this work, select single input content image. After create the number of foreground style-transferred regions in each Captcha image to 4 to 7 the style transfer images.

The shape of each region is randomly selected: it can be a rectangle, a triangle, a circle or other irregular shapes such as a heart, a leaf, a moon and so on.

One of these style-transferred images is synthesized with the original image. Randomly crop regions with different shapes from other style-transferred images and relocate them in the synthetic background to generate a Captcha.

After, generate a brief description to guiding users on how to pass the test. The output is the generated SACaptcha.



# Flow Chart / Algorithm

To overcome these issues, proposes a novel image-based Captcha named Style Area Captcha (SACaptcha), which is based on semantic information understanding, pixel-level segmentation techniques.

The proposed system describes in given fig.1. In this work, select single input content image. After create the number of foreground style-transferred regions in each Captcha image to 4 to 7 the style transfer images.

The shape of each region is randomly selected: it can be a rectangle, a triangle, a circle or other irregular shapes such as a heart, a leaf, a moon and so on. One of these style-transferred images is synthesized with the original image.



# Proposed Methodology : Database

Mysql 5.0

# Proposed Methodology : Implementation System Details

Sr No.	System	Name of system tools	Specification
1	IDE	Eclipse	Eclipse Oxygen(J2EE)
2	Database	MySQL	MySQL 5.0
3	Server	Apache Tomcat	Apache Tomcat 9
4	Language	Java	Java 8
5	Operating System	Windows OS	Windows 10

# Experimental Results & Discussion

Image-based CAPTCHA systems are designed to distinguish between human users and automated bots by presenting challenges that are easy for humans to solve but difficult for automated scripts or bots.

When discussing experimental results, it's important to consider the context, the specific implementation of the CAPTCHA system, the types of images used, and the metrics measured to draw meaningful conclusions.

# Future Plan

The proposed a novel image-based Captcha named SACaptcha using neural style transfer techniques.

Most early image-based Captchas are based on the problem of image classification, whereas SACaptcha will rely on problems of semantic information understanding and pixel-level segmentation.

A positive attempt to improve the security of Captchas by utilizing deep learning techniques.

The future work will promote more-effective ways to enhance the security of text Captchas.

# References

H. Gao, W. Wang, J. Qi, X. Wang, X. Liu, and J. Yan, “The robustness of hollow captchas,” in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 1075–1086.

H. Gao, M. Tang, Y. Liu, P. Zhang, and X. Liu, “Research on the security of microsoft’s two-layer captcha,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1671–1685, 2017.

E. Bursztein, J. Aigrain, A. Moscicki, and J. C. Mitchell, “The end is nigh: Generic solving of text-based captchas.” in WOOT, 2014.

D. C. Ciresan, U. Meier, J. Masci, L. Maria Gambardella, and J. Schmidhuber, “Flexible, high performance convolutional neural networks for image classification,” in IJCAI Proceedings-International Joint Conference on Artificial Intelligence, vol. 22, no. 1. Barcelona, Spain, 2011, p. 1237.

O. Starostenko, C. Cruz-Perez, F. Uceda-Ponga, and V. Alarcon-Aquino, “Breaking text-based captchas with variable word and character orientation,” Pattern Recognition, vol. 48, no. 4, pp. 1101–1112, 2015.

Thank You .