Paper Format

While writing your section if you feel like anything needs to be addressed in other sections, then please write that in the paper with red color mentioning the section in which it needs to be addressed and how (if possible). In this way all the sections will be interconnected and paper will have a proper flow.

1. **Introduction (1½ Page) Hasky**
2. **Background and Motivation (1½ Page) Jaskirat Sudan**
    1. **Background:**
        i. Explain the physics behind the pattern and how we are getting different colors in a step-by-step manner with diagrams.
    2. **Motivation:**
        i. How will the camera see color variations as we rotate the pattern? We need to add a figure with 0-degree, 45-degree, and 90-degree rotations to illustrate this.
        ii. Depending on the flexibility we need from the model, we can register the patterns visible from -15 to 15 degrees.
3. **Threat Model: (1 Page) Hasky**
    1. **What is the system's goal, and what are you trying to protect?**
        i. Focus on what assets are valuable, e.g., authentication access, biometric uniqueness
    2. **Who is the adversary?**
        i. Define the attacker's role clearly: outsider, insider, remote observer, etc.
        ii. If possible, relate them to realistic threats, e.g., video-based spoofers, casual attackers.
    3. **What does the adversary know?**
        i. What the attacker can observe or learn (e.g., system outputs, tag patterns).
        ii. Limit or bound this knowledge.
    4. **What can the adversary do?**
        i. Describe the actions they can take: printing patterns, replaying images, forging materials.
        ii. State whether they can interact with the system directly.
    5. **What are your assumptions about the system and environment?**
        i. Mention any operational constraints: camera setup (need polarizer sheet on camera), lighting conditions, and user distance.
        ii. Avoid over-assuming; state only what you can reasonably enforce or control.
    6. **What types of attacks are out of scope?**
        i. Acknowledge what you're not protecting against, but do so confidently.
4. **System Overview: (½ Page) Fatima Qasem Fatima Mohammed**
    1. **Overview of the System Architecture**

        Start with a short paragraph summarizing the main components and how they connect. Optionally include a figure showing the full pipeline.

    2. **High-Level Goal:** Start with one sentence like, What is our system trying to achieve and why?
    3. **Core Idea:** Explain what makes our method different or novel in one or two sentences.
    4. **Key Components:** Break down your system into major modules, ideally 2–4, and describe their roles.

Next two sections are the technical core of the paper. The reader should leave these section with a clear understanding of:

- What did we build?
- How does each part work?
- How do they all connect?

5. **Passive Tag (1½ Page) Fatima Qasem Fatima Mohammed**
    1. **TapeNail Tag Creation**
        i. What materials are used (e.g., polarizer sheet, crisscross print)?
        ii. Why did we choose this shape/design (e.g., rotation detection, spoof-resistance)?
        iii. Any physical properties that matter (e.g., thickness, size, visibility under light),

iv. How it's applied (e.g., on nail like a sticker, no batteries or electronics).

6. Reader (1½ page) Jaskirat Sudar Hasky

1. **Image Capture Pipeline**
   i. Camera setup (distance, resolution, angle),
   ii. Lighting conditions (ambient vs. flashlight, importance of polarization),
   iii. Any preprocessing steps (resizing, normalization).
2. **Tag Detection and Feature Extraction**
   i. YOLOv11 model setup,
   ii. What labels did we train on (bounding box, rotation angle, etc.)?
   iii. Training dataset creation (how many samples, augmentation, etc.)?
   iv. Output of the model: location + angle (or other features)?
   v. Why did we choose this model (lightweight, fast, accurate)?
3. **Authentication Mechanism**
   i. How are features matched to a registered profile?
   ii. Any thresholds (e.g., rotation difference margin)?
   iii. What triggers successful/failed authentication?
4. **Deployment on an Android Device**
   i. How is the model converted and deployed (e.g., TFLite, on-device inference)?
   ii. Efficiency on phone (latency, memory usage, real-time inference)?
   iii. User interaction flow (tap the app, show finger, get result)?
   iv. Why is this practical for real-world use?

7. Security Analysis or Threat Mitigation (¾ Page) Hasky Jaskirat Sudan

1. **Restate Key Threats**
   i. Briefly reintroduce the attacker capabilities from our Threat Model, just to frame the reader again.
2. **Explain How We Defend Against Each**
   i. Go through each threat and explain why it fails against your system.

8. Evaluation (1½ Page) Hasky

1. **Experimental Setup**
   i. Hardware used (camera type, phone model)
   ii. Number of users, sessions, and lighting conditions
   iii. Dataset size for training/testing
   iv. Environment setup: indoor, lighting variability, angles
2. **Authentication Accuracy**
   i. Show precision, recall, F1-score, or ROC-AUC for authentication success
   ii. Accuracy across distances (show with a bar chart or confusion matrix)
3. **Latency and Resource Usage**
   i. Time taken per authentication on the mobile device (camera + model + decision)
   ii. Model size, inference time (on CPU/GPU), memory usage
   iii. Does it run in real time?

9. Discussion (½ Page) Jaskirat Sudan

Talk about Limitations, Assumptions, Design Trade-offs, and Future Opportunities.

10. Conclusion (½ Page) Jaskirat Sudan

To summarize your contribution, restate the problem you solved, and briefly mention results and future directions in a concise, confident tone.

- The problem you tackled (e.g., secure, practical, spoof-resistant authentication),
- Your core idea (TapeNail: passive crisscross tag + vision-based authentication),
- A quick mention of key results (e.g., accuracy, real-time deployment, spoofing resistance),
- A forward-looking statement about future work or applications.

Note: The page numbers are without diagrams.