Smart Home Security Using Facial Authentication

Rakshitha M.V.[1] , Chitra K.[1]

[1] Dayananda Sagar Academy of Technology and Management, Karnataka, India

Email: rakshithamv2001@gmail.com; chitra-mca@dsatm.edu.in

Abstract

Smart home security enhances security by allowing only authenticated individuals to enter the home. The technology uses advanced algorithms to recognize faces, making them safer and easier to access. The main objective is to improve privacy and security by using facial recognition based on the LBPH technique. The proposed application allows users to keep track of the happenings at their homes using mobile phones, Tablets, or PCs. The system records a flow of people at the door and identifies their faces against the database of the allowed people. If the face is recognized it allows the homeowner access but if the face is not recognized it will sound a warning that there is intrusion. The new face is captured and compared to the existing one and the homeowner then decides where to add the new face for storage.

Keywords

LBPH algorithm, Face recognition, Home security, Smart home authentication

Introduction

Smart home security enhances security by identifying and penetrating trusted individuals. The technology combines convenience and security, reducing unauthorized access through advanced biometrics. Some of the other familiar crimes that are also carried out inside people's homes are robbery and theft. To tackle these problems, the Smart Home Security systems can be introduced in the homes and in this the owner of the house can operate his or her house through a single gadget. Preferably there should be cameras installed at all entries to capture the person visiting. Other features integrated with the Advanced Home Security are Facial Recognition for additional security. Thus, based on the conclusion of this study, there is a proposed Home Security method that incorporates the used LBPH for facial authentication. The system then captures from the same feed an identity match with the owner's database. In the event that a stranger is encountered the owner is informed and could choose to enroll the person or permit restricted access. Speaking of facial authentication and consequently, security, the use of LBPH algorithm boosts the degree of accuracy.

Design a home security system employing real-time face detection with a Facial Recognition Algorithm; Local Binary Patterns Histogram (LBPH). This system will effectively authenticate the allowed persons, prevent the prohibited persons from gaining access, and perform well in different light status. It may include simple management of users, the

Submission: 16 October 2024; **Acceptance:** 10 December 2024

availability of logs that are detailed, chances of being alerted of an attempt that is unauthorized among other advantages that make it a secure and convenient home protection system.

Literature Review

Dhobale et al. described the work and research on cost effective smart home security system based on IoT with real-time facial recognition. It alerts the homeowner when there are strangers at the door through their Gmail (Dhobale et al., 2020). (Durga et al., 2021) integrated Gabor wavelet features with Deep CNN features for enhanced masked face recognition. It provided better performance than benchmark CNN approaches.

Rahim and team presented a smart home security system with the aid of CNN real-time facial recognition method. It recognised people with the ability to control who has access to the smart home and is compatible with already existing smart home systems (Rahim et al., 2023). The potency of the system entails high accuracy, efficiency and instant security resolutions. Irjanto and Surantha have suggested six hybrid models for detecting anomalies as well as face recognition in the IoT smart home devices (Irjanto and Surantha, 2020). Based on identified features, the use of logistic regression, gradient boosting classifiers, and CNNs in integrated models results in the best model named LR-HGBC-CNN. Future work should improve the generalization, the stability, and applicability scenarios of the proposed IDs. These models enhance the smart home IoT protection to a higher level.

Rahim and team experimented FRS at distances of 1 (Rahim et al., 2023). This means that the enhanced clerk can work five meters away, one meter away and 0. 5 meters and, during different moments of the day. The errors were more common at 1. 5 meters because of too much of background light. The suggested method yielded 97 percent. 5% accuracy while OpenCV method was found at 95% and there has been an improved accuracy of up to 97%. 83%. It is planned that in the next work, data augmentation techniques will be improved, the camera's resolution will be increased, and the latest Raspberry Pi model will be used to increase computing power.

Uddin and team have designed a mobile application for the smart home security with facilities to control different gadgets and monitor the activities remotely (Uddin et al., 2022). Other options are a PIN cod lock and a facial recognition system implemented with the help of Raspberry on doors. It seeks to lower property crime rates with efficient and specific attributes. Action plan for the period ahead implies the use of blockchain to enhance PIN safety and neural networks to strengthen cyber protection.

Anbazhagu have suggested hybridized approach has the potential to deliver more precise and effective decision-making processes for energy management in smart homes, allowing users to optimize their energy consumption while preserving comfort and lowering environmental impact (Anbazhagu et al, 2024).

Methodology

The currently used system of smart home security with the help of the facial recognition mechanism is generally implemented as follows: After that, patterns such as LBPH (Local

Binary Patterns Histogram) or Haar cascades choose visual attributes like eyes, nose, and mouth for examination. This extracted data is then used in a database containing other faces to verify the identities of the users. Recognition leading to successful identification provides access control decisions which are twofold, to allow or deny a user entry, usually combined with door or some other hardware locks. These systems differ with some relying on third-party services for computation and data storage while others main concentration is on local computation on such platforms as Raspberry Pi for secure operations and more control.

The smart home security system that has been suggested involves monitoring the home's security using facial recognition through a application only for controlling it stresses on the use of a smartphone for effective security. Users would take facial images in real time in the app and the app automatically processes the images with LBPH (Local Binary Patterns Histogram) technique for facial features formatting and recognition. Some of them include facial detection, feature extraction, and facial recognition to check against other recognized data to issue a credential. Thus, successful recognition permits unlocking doors, managing the security of a home, or other options right from the application, providing one with more control over the Smart Home environment without needing to rely on IoT gadgets. Figure 1 shows the overview of the LBPH algorithm.

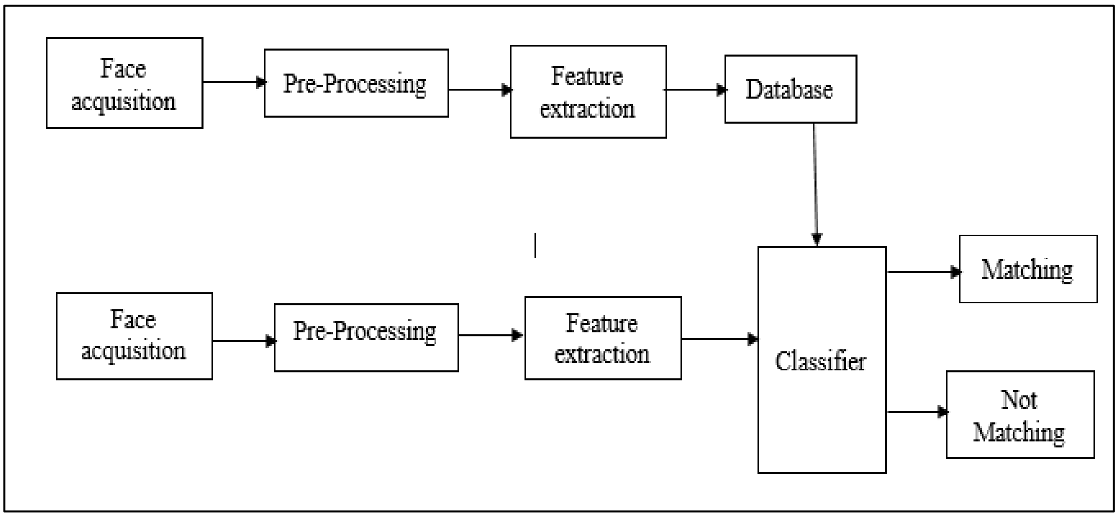

Figure 1. Overview of the LBPH algorithm

The LBPH algorithm has the operation where it will first extract the Local Binary Patterns from an image or a Region of Interest in an image. LBP is a basic feature that describes the texture distribution of local pixels and their relations. The simplest form of this idea is to look at the value of the central pixel and compare it with the neighboring pixels and then convert the outcomes to binary sequences most of which involves use of a threshold value. These binary patterns are then put together to from a histogram and this histogram forms a feature vector that represents the texture of the image or the Region Of Interest (ROI).

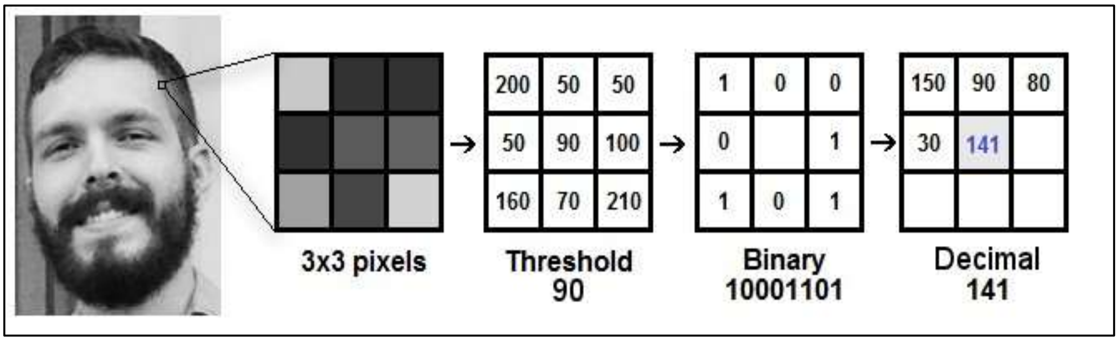

Figure 2. LBPH operation

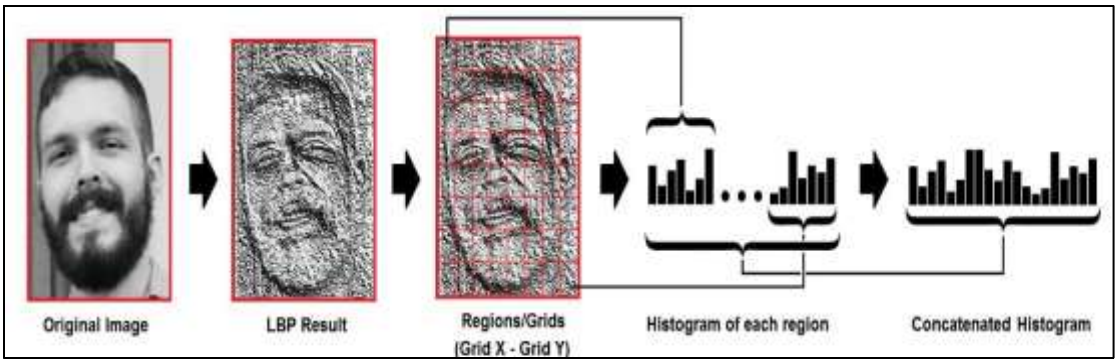

Figure 3. LBPH Extraction Procedure

Texture category is critical for face reputation, and the local binary sample (LBP) approach is a very powerful tool for this motive. LBP is a trustworthy and efficient texture operator that labels the pixels of a picture by means of evaluating each pixel with its pals, ensuing in a binary variety First introduced in 1994. LBP has confirmed itself to be a complicated aspect for texture type. Its effectiveness is in addition improved with the aid of the addition of oriented-gradient (HOG) annotations to histograms, which substantially improves detection overall performance for positive statistics units LBP technique estimates neighborhood texture positions by way of pixel evaluate it with its surroundings. The picture ought to be transformed to grayscale for texture description. Using LBP in mixture with a histogram, face pix can be represented as easy information vectors.

Results and Discussions

The facial authentication for clever domestic safety the use of the Local Binary Patterns Histogram (LBPH) algorithm showed promising effects, showing high accuracy and robust common overall performance in the course of several environmental situations. The LBPH set of policies reliably diagnosed faces with a excessive real remarkable fee and espresso faux pleasant charge, coping with extraordinary lighting fixtures conditions and facial expressions efficiently. Its computational performance enabled real-time processing, making it well-proper for sensible use in clever homes. The system greater protection by using minimizing unauthorized get right of entry to incidents compared to standard strategies like passwords or

PINs. However, it faced challenges which include sensitivity to facial occlusions (e.g., glasses, hats) and reduced performance in low-slight situations. Future enhancements will focus on overcoming those obstacles and incorporating multi-element authentication methods to further decorate protection and reliability in smart domestic settings.

Conclusion

Altogether, it is possible to state that the investigated Local Binary Patterns Histogram (LBPH) algorithm is the most efficient one when it comes to facial authentication in smart home security systems. The ability to offer accurate and real-time facial recognition exclusively improves home security because of minimization of intrusion. With the limitations like sensitivity to occlusions (example – glasses and hat) and the performance dramatically differs under varying light conditions there is a question about the performance and accuracy the LBPH algorithm has the required characteristics for being the candidate for the smart home security system. This technology restricts entry to those persons who have passed through the biometric scan and thus the homeowners can feel more secure knowing that their home cannot easily be accessed by unauthorized persons.

The further research should be focused on the development of the suggestions for the improvement of the disadvantages which were mentioned above related to the LBPH algorithm. More research should be dedicated aiming at enhancing the algorithm’s noise resistance, especially regarding the occlusions and irregular illumination, potentially succeeded by more elaborate preprocessing or integrated LBPH with other algorithms. On the same, the systems could be coupled with multi-factor authentication techniques like Face ID together with fingerprint/voice recognition to enhance the level of security and reliability. In the above-discussed areas, smart home security systems can be made more safe and reliable to provide maximum protection and comfort for the homeowners.

References

Alghassab, M. A. (2024). Fuzzy-based smart energy management system for residential buildings in Saudi Arabia: A comparative study. *Energy Reports*, *11*, 1212-1224. https://doi.org/10.1016/j.egyr.2023.12.039

Anbazhagu, U. V., Koti, M. S., Muthukumaran, V., Geetha, V., & Munrathnam, M. (2024). Multi-Criteria Decision-Making for Energy Management in Smart Homes Using Hybridized Neuro-Fuzzy Approach. Distributed Generation & Alternative Energy Journal, 83-110. https://doi.org/10.13052/dgaej2156-3306.3914

Dhobale, M. R., Biradar, R. Y., Pawar, R. R., & Awatade, S. A. (2020). Smart home security system using Iot, face recognition and raspberry Pi. International Journal of Computer Applications, 176(13), 45-47. https://doi.org/10.5120/ijca2020920105

Durga, P., Divya, G., Ayeshwariya, D., & Sivakumar, P. (2021). Gabor-deep CNN based masked face recognition for fraud prevention. In *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 990-995). IEEE. https://doi.org/10.1109/ICCMC51019.2021.9418044

Irjanto, N. S., & Surantha, N. (2020). Home security system with face recognition based on convolutional neural network. International Journal of Advanced Computer Science and Applications, 11(11). https://dx.doi.org/10.14569/IJACSA.2020.0111152

Kurniawan, I., & Sumitra, I. D. (2023). A Smart Home Architecture for Energy Conservation and Multiple Energy Source Management. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *31*(2), 101-116. https://doi.org/10.37934/araset.31.2.100116

Rahim, A., Zhong, Y., Ahmad, T., Ahmad, S., Pławiak, P., & Hammad, M. (2023). Enhancing smart home security: anomaly detection and face recognition in smart home IoT devices using logit-boosted CNN models. Sensors, 23(15), 6979. https://doi.org/10.3390/s23156979

Shahgoshtasbi, D., & Jamshidi, M. M. (2014). A new intelligent neuro–fuzzy paradigm for energy-efficient homes. IEEE Systems Journal, 8(2), 664-673. https://doi.org/10.1109/JSYST.2013.2291943

Uddin, K. M. M., Shahela, S. A., Rahman, N., Mostafiz, R., & Rahman, M. M. (2022). Smart home security using facial authentication and mobile application. International Journal of Wireless and Microwave Technologies (IJWMT), 12(2), 40-50. https://doi.org/10.5815/ijwmt.2022.02.04