A SURVEY ON SMART SECURITY SYSTEM USING ARTIFICIAL INTELLIGENCE

Deep Shikha[1], Sayali Mahajan [2], Pratiksha Shinde[3], Prakash Solanki[4]

[1]Deep Shikha: Student, Dept. of Computer Engineering, DR. D.Y. Patil School of Engineering and Technology, Pune, Maharashtra.

[2]Sayali Mahajan: Student, Dept. of Computer Engineering, DR. D.Y. Patil School of Engineering and Technology, Pune, Maharashtra.

[3]Pratiksha Shinde: Student, Dept. of Computer Engineering, DR. D.Y. Patil School of Engineering and Technology, Pune, Maharashtra.

[4]Prakash Solanki: : Student, Dept. of Computer Engineering, DR. D.Y. Patil School of Engineering and Technology, Pune, Maharashtra.

[5]Nutan Borkar: Assistant Professor, Dept. of Computer Engineering, DR. D.Y. Patil School of Engineering and Technology, Pune, Maharashtra.

---***---

Abstract – *Many Artificial Intelligence system is used to replace the traditional means of security. A traditional security system can be easily breached. Traditionally in societies/business complex Entry of visitor is done manually to overcome these security threats we have implemented a security management system for private sector and societies which helps to secure registration and profile management facilities for visitors using Face detection & Text Mining. To improve the recognition performance, many things have been improved which are implemented such as color processing, edge detection, etc.*

Key Words: Artificial Intelligence, Text Mining, Face Detection, Color Detection, Edge Detection.

1. INTRODUCTION

In the era of growing technology, the internet has become one of the major components of our life. One cannot imagine its life without the internet. Internet of Things is used to collect and handle the huge amount of data that is required by the Artificial Intelligence algorithms. The algorithms convert the data into a useful result. Nowadays a concept of RF-ID is introduced which is quite good than earlier but it does not provide automation. While our system provides a full automation system for visitors to make their entry automatically. The smart security system is designed to replace traditional visitor registration and visitor information management activities in the premises, with this system that will be able to assist the visitor registration process, to know who is still inside of the premises after meeting and notify the system. This system solves the problem of electively capturing all-relevant information about the visitors and that information is recorded in a centralized database server, which provides data management and manipulation through searching for future purposes in the organization. The benefits of the Smart Security System are enhancing the level of security enforced in premises, providing an organized view of visitor records and reducing the time spent on managing visitor information. The primary objectives of smart security system is to implement the company's security policies, obtain reliable information about visitors and visits, and to give a professional impression without excessive costs. Optimizing this process can lead to significant cost reduction, improved security, and access to valuable visitor data. Smart Security System is used to take input automatically from the Aadhar card or any other valid Id proof through text mining and make an entry in the database. If the user is not registered in the database then they will get registered so that whenever they'll come next time they don't have to make any entry.

1.1 Haar cascade

Haar Cascade is an ML-based object disclosure algorithm that is used to analyze objects in pictures or documentaries and based on the approach of Lienhart and Maydt the concept of a tilted (45°) Haar-like feature.
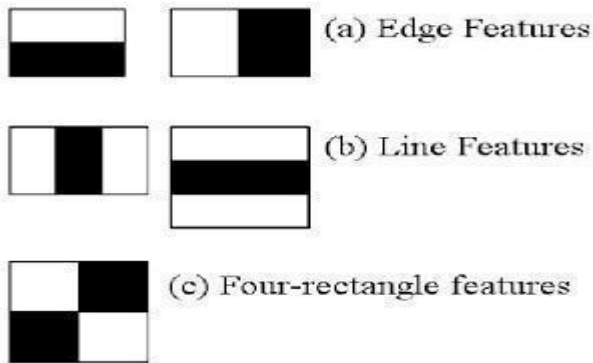
It is an ML-based approach where a cascade function is qualified from a lot of affirmative and abrogating images. It is then used to disclose object s in other pictures or documentary.

Haar cascade algorithm has 4 stages:
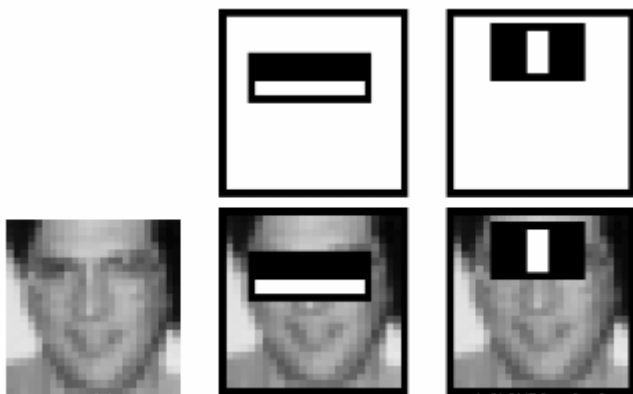
1.   Haar Feature Selection

2.   Creating Integral Image

3.   Adaboost Training

4.   Cascading Classifiers

It is recognized for being able to identify faces and body parts in an image but can be trained to detect any object ..Let us take facial detection as an example Initially, the algorithm needs a lot of affirmative images of faces and abrogating images without faces to train the classifier. Then we need to select features from it. The Initial step is

---

to collect the Haar Features. A Haar feature examines various regions at a specified location in a detection window, later it gross up the pixel depth of each part and calculates the difference between these sums.

(a) Edge Features

(b) Line Features

(c) Four-rectangle features

Integral Images are used to make the process super quick. But from all these features we estimated, most of them are pointless. For example, examine the image below. The top row shows two excellent features. The first feature target on the approach that the zone of the eyes is often dusky than the zone of the nose and cheeks. The second feature target on the approach that the eyes are dark than the link of the nose. But the same cases targeting on cheeks or any other place is unrelated.

So how do we decide the best appearance out of 180000.0+ countenance? This is achieved using a concept called Adaboost which both selects the best appearances and caravan the classifiers that use them. The algorithm buildup a "strong" classifier as a precise merge of weighted simple "weak" classifiers. The process is as follows.

During the detection process, a window of the specified size is moved over the input figure, and for each classification of the figure and Haar features are estimated. You can notice this response in the video. This change is then equalized to original that distinguishes non-objects from objects.

As each Haar feature is only a "weak" classifier an enormous Haar features are mandatory to define an object

with satisfactory skills and are therefore standardized into cascade classifiers to design a strong classifier.

2. OCR – Classification Interaction Mathematical Model

The significance in the Information retrieval area keeps on increasing, because of the constantly growing number of numeric data available on the Internet. However, there is a huge database of digital documents, there also exist non-digital data such as handwritten documents, machine printed documents, set of papers.

For deterministic OCR, we use type-I, which will provide a single candidate word with no confidence score. For Probabilistic OCR, we use "type-II" and "type-III" which will provide a single word with the score.

In this paper, we "Type-III" OCR is used. Type III OCRs prove to be stronger than types I or II, especially for low-performance OCRs

2.1 Type-III OCR global Mathematical Model:

In this paragraph, we want to compare the quantity:

$$C_k | X_1,...,X_i,...,X_n) \quad (1)$$

to:

$$P(O_k | C_j) \quad (2)-$$

and to:

$$P(O_k | X_i) \quad (3)$$

The $P(C_k|X_1,...,X_i,...,X_n)$ are the probabilities that a document made of the vector of patterns

$X_1,...,X_i,...,X_n$ belongs to class C_k.

The $P(P_k|C_j)$ are the conditional probabilities to search the word "k", in document class "j". These probabilities are the "ideal" probabilities, that would be the ones found for digital documents, that is, documents generated by an text editor.

Finally, the $P(O_k|X_i)$ are the "OCR" probabilities that the object with form, or characteristic vector Y_i belongs to the class O_k.

Therefore, we will match our document classification scores, on one hand to the purely semantic characteristics of the problem, described by the $P(O_k|C_j)$, and on the other hand, to the OCR features of the problem, described by the $P(O_k|X_i)$.

As a first step, we will build the conditional probabilities to find the shape X_i, on document class C_j, as a sum over all possible paths :

$$P(X_i|C_j) = \sum_k P(X_i|O_k)P(O_k|C_j)$$

$$(4)$$

Where the C_j are the document classes, the O_k are the objects making up the document, and the X_i are the forms produced by the generating process, from the O_k. In a second step, using Bayes inversion formula in the case of n stochastic variables :

$$P(C_j|X_1, ..., X_n) = \Pi_i P(X_i|C_j) \frac{P^n(C_j)}{P(X_1, ..., X_n)}$$

$$(5)$$

and write this equation, $P(X_i|C_j)$ by its value given in the former equation, we get :

$$\Rightarrow P(C_j|X_1, ..., X_n) = \Pi_i (\sum_k P(O_k|X_i)\frac{P(X_i)}{P(C_j)}P(O_k|C_j)) \frac{P^n(C_j)}{P(X_1, ..., X_n)}$$

$$(6)$$

Where the $P(O_k|X_i)$ is the probability vector produced by the OCR process applied on form X_i.

$$\Rightarrow P(C_j|X_1, ..., X_n) = \frac{P^n(C_j)\Pi_i P(X_i)}{P(X_1, ..., X_n)P^n(C_j)} \Pi_i (\sum_k P(O_k|X_i)P(O_k|C_j))$$

$$(7)$$

If the X_i may be considered as stochastically independent, then:

$$P(X_1, ..., X_n) = \Pi_i P(X_i)$$ $$(8)$$

$$\Rightarrow P(C_j|X_1, ..., X_n) = \Pi_i (\sum_k P(O_k|X_i)P(O_k|C_j))$$

$$(9)$$

which is the relation we were looking for.

This equation merges together two conditional probabilities with different origins : the first set of probabilities, the $Q(O_{k(i)}|Y_i)$ are generated by the low level OCR process, while the second set, the $Q(O_{k(i)}|C_j)$ corresponds to the upper level document classification process.

We will now use this relation to link the performances of the classifier with the performances of the OCR, and to the ideal problem difficulty.

However, we will first start by a discussion around this equation.

First, we recognize in the set Q($Ok|Yi$), a vector belonging to the *n-dimensional* space we met earlier, in Type I OCR. Here, the vector can span the whole space. It is not limited to the vertices of the hypercube.

3. CONCLUSION:

Security is a crucial issue nowadays worldwide. This project aims at improving the security issues for private as well as public sectors. Face Recognition and Optical Character Recognition is an emerging technology used for identifying the person intelligently. To improve recognition performance, MANY things have been improved here, some of them being fairly easy to implement. For example, we have added color processing, edge detection, etc. We have usually improved face recognition accuracy by using more input images, at least 50 per person, by taking more photos of each person, particularly from different angles and lighting conditions.

REFERENCES

[1] Rong Jin; Chengxiang Zhai; Hauptmann Alex G., "Information Retrieval for OCR Documents : A Content-based Probabilistic Correction Model", Electronic Imaging Conference (EI'03), Document Recognition and Retrieval Conference DRR(X), Santa Clara, CA, January 20-24, 2003, vol. 5010, pp. 128-135.

[2] J. Bass, Eléments de Calcul Probabilités (théorique et appliqué). Masson et Cie.

[3] J. Oswald, Théorie de l'Information ou Analyse Diacritique des Systèmes. Masson et Cie.

[4] Jean-Marie, "OCR Classification Mathematical Model" unpublished.

[5] Liying Lang,Weiwei Gu, "Study of Face Detection Algorithm for Real-time Face Detection System",Second International Symposium on Electronic Commerce and Security.

[6] Li Cuimei1, Qi Zhiliang 2, Jia Nan 2, Wu Jianhua , "Human face detection algorithm via Haar cascade classifier combined with three additional classifiers", IEEE 13th International Conference on Electronic Measurement & Instruments .

[7] Mrs. Madhuram.M1, B. Prithvi Kumar2, Lakshman Sridhar3, Nishanth Prem4, Venkatesh Prasad, "Face Detection and Recognition using OpenCV",

International Research Journal of Engineering and Technology (IRJET)2018.

[8] Dr. Naveen Kumar Gondhi, Er. Navleen Kour, "A Comparative Analysis on various Face Recognition Techniques" International Conference on Intelligent Computing and Control Systems ICICCS

[9] Menglu Wu, Tongwei Lu, "Face Recognition Based On LBP And LNMF Algorithm",15th International Symposium on Parallel and Distributed Computing

[10] Moataz M. Abdelwahab, Wasfy B. Mikhael , "A New Fast Facial Recognition Algorithm Applicable to Large Databases