Enhanced Document Verification Using Hybrid Algorithm (KNN And RSA Algorithm)

Ajay Vigneshwaran[1], Karthik J[2], Kirthana R[3], Dr. Palaniappan S[4]
[1, 2, 3] Dept of Computer Science and Engineering
[4]Associate Professor, Dept of Computer Science and Engineering
[1, 2, 3, 4] KCG College of Technology, Chennai, India

Abstract- *DualSec provides a means for encrypting the documents to prevent unauthorized people getting illegal access to them as well as performs matching of photos in the document to real time selfies. The number of fraudulent activities for duplication of certificates are increasing. The goal of this work is to provide a system that solves the problem of counterfeiting certificates. The proposed digital certificate system verifies the traveler's identity using a live camera, which allows faster convergence and more generalizable representations. The system proposes dual security i.e., document encryption and face recognition which is robust. KNN algorithm is one of the simplest classification non-parametric algorithm which uses a database in which the data points are separated into several classes to predict the classification of a new sample point. KNN algorithm is used for matching the photo in the document to real time selfies. The RSA, an encryption algorithm, is the most powerful form of encryption in the world. It supports incredible key lengths, and it is typical to see 2048- and 4096- bit keys and so we have used it to store the documents in encrypted form. The system requires less human intervention and is cost efficient.*

Keywords- KNN algorithm, RSA algorithm, real-time selfies.

I. INTRODUCTION

The main aim of this project is to solve the problem of counterfeiting certificates. We are proposing a digital certificate system based on block chain technology and to verify the traveler's identity using a live camera, which allows faster convergence and more generalizable representations.

Various pursuits in our everyday life need us to check who we are by displaying our id documents that include face images, like passports and driver licenses, to human operators. However, this procedure tends to be sluggish, labor intensive and untrustworthy. For the very reason, an automated system for matching ID document photos to live face images (selfies) in real time and with greater degree of precision is the need of the hour. Here, we propose a system to meet this objective. Initially we demonstrate that gradient-based optimization technique intersects slowly in the case of various classes with a smaller number of samples, an attribute of the present ID-selfie datasets. To subjugate this flaw is to upgrade the classifier weights, which permits quicker intersection and better generalizable depiction. Succeeding it is a couple of sibling networks with partly sharing criteria that are given training to grasp amalgamated face depiction with domain-specific parameters. Inter-validation on an ID selfie dataset depicts that a publicly available general face matcher only achieves a true acceptance rate of 88.78% at a false acceptance rate of 0.01% on the problem. In the proposed work, we have decided to make use of two algorithms: 1) KNN algorithm 2) RSA algorithm. K-Nearest Neighbor is outstanding amongst other Machine Learning calculations dependent on regulated Learning strategy. KNN computation acknowledges the closeness between the recently shown case/information and available cases and put the new case into the class that is generally similar to the open classes. K-NN calculation reserves all the open data and orders a cutting edge data point dependent on the comparability. This infers when present day data appears by then it tends to be viably characterized into a well suite class by using KNN calculation. KNN is a non-parametric calculation, which infers it doesn't make any assumption on essential data. It is in like manner called the languid student calculation since it doesn't pick up from the preparation set rapidly rather it stores the dataset and at the hour of request, it plays out a movement on the dataset. Assume, we have an image of a creature that is by all accounts like pooch and feline, anyway we have to know whether it is a canine or feline. So for this distinctive confirmation, we can use the KNN figuring, as it manages a closeness measure. Our KNN model will find the tantamount features of the new instructive record to the canines and felines pictures and reliant on the most practically identical features it will put it in either pooch or feline arrangement. Next comes the RSA calculation. The RSA calculation is the reason of a cryptosystem - a set-up of cryptographic computations that are used for express security organizations or purposes - which engages open key encryption and is comprehensively used to ensure about fragile data, particularly when it is being sent over a questionable framework, for instance, the web. Open key cryptography, in any case called as lopsided cryptography, uses two remarkable anyway numerically associated keys -

one open and one private. The open key can be conferred to everyone, however the private key must remain circumspect. In RSA cryptography, the open key just as the private keys can encode a message; the opposite key from the one used to encode a message is used to unravel it. This component is one inspiration driving why RSA has become the most by and large used topsy-turvy computation: It gives a methodology to ensure the security, dependability, validity, and non-denial of electronic trades and data accumulating. RSA gets its security from the difficulty of considering huge entire numbers that are the aftereffect of two enormous prime numbers. Item these two numbers are basic, yet choosing the primary prime numbers from the total - or figuring - is seen as impractical in light of the time it would take using even the current supercomputers.

II. LITERATURE SURVEY

Title: DocFace+: ID Document to Selfie Matching
Authors: Yichun Shi, Anil K. Jain
Year: 2019

The paper gives an outline of the primary methodologies utilized for document encryption and face confirmation. The base model is prepared for a huge scope unconstrained face informational index and its highlights are focused to the area of ID selfie sets. It features the difficulties in the advancement and approval of such strategies for confirmation of face identity. The author contrasts the proposed framework and the current general face acknowledgment frameworks on the private informational collection and sees a noteworthy improvement with the framework demonstrating the need of the area explicitly displaying the ID selfie informational collections.

Title: Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks
Authors: Kaipeng Zhang, Zhanpeng Zhang
Year: 2016

Face recognition and plan in unconstrained conditions are troublesome because of various stances, illuminations and obstructions. Late examinations show that significant learning approaches can achieve essential execution on these two assignments. In this paper,the creator proposes a profound task structure which uses the trademark connection between them to help up their creation. In particular, the framework abuses a fell structure with three periods of meticulously arranged significant convolution frameworks that anticipate face and achievement region in a coarse-to-fine way. Additionally, in the learning strategy, the creator proposes another online hard model mining philosophy that can improve the introduction normally without manual test assurance. This procedure achieves better accuracy over the front line frameworks on the troublesome FDDB and WIDER FACE benchmark for face area, and AFLW benchmark for face game plan, while keeping progressing execution.

Title: CosFace: Large Margin Cosine Loss for Deep Face Recognition
Authors: Hao Wang, Yitong Wang
Year: 2018

Face affirmation has gained wonderful ground owing to the progress of significant convolutional neural frameworks (CNNs). The central undertaking of face affirmation, counting face check and distinguishing confirmation, includes face feature detachment. For any situation, the standard softmax loss of significant CNNs when in doubt misses the mark on the intensity of isolation. To address this issue, starting late a couple of misfortune limits, for instance, center misfortune, huge edge softmax misfortune, and exact softmax misfortune have been proposed. All these improved misfortunes share a comparable idea: amplifying between class distinction and limiting intra-class vacillation. Right now,the creator proposes a novel misfortune work, specifically colossal edge cosine misfortune (LMCL), to comprehend this idea from a substitute point of view. Even more expressly, we reformulate the softmax misfortune as a cosine misfortune by L2 normalizing the two features and weight vectors to remove winding assortments, in perspective on which a cosine edge term is acquainted with further amplifying the decision edge in the exact space. Hence, least intra-class vacillation furthermore, most noteworthy between class variance are practiced by uprightness of normalization and cosine decision edge increase. The creator suggests their model arranged with LMCL as CosFace. Wide test evaluations are coordinated on the most notable open territory face affirmation datasets, for instance, MegaFace Challenge, Youtube Faces (YTF) and Labeled Face in the Wild (LFW). They achieve the top tier execution on these benchmarks, which asserts the practicality of our proposed approach.

Title: NormFace: L2 Hypersphere Embedding for Face Verification
Authors: Feng Wang, Xiang Xiang
Year: 2017

Because of the ongoing advancements of Convolutional Neural Networks, the execution of face confirmation strategies has expanded quickly. In a run of the mill face confirmation strategy, normalization is a basic advance for boosting execution. This inspires the author to

present and study the impact of normalization during training. Be that as it may, we discover this is non-trivial, in spite of normalization being differentiable. They recognize and study four issues identified with normalization through scientific investigation, which yields comprehension and assists with parameter settings. In view of this investigation the authors propose two procedures for preparing utilizing standardized highlights. The _rst is a modi_cation of softmax loss, which enhances cosine likeness rather than inward item. The second is a reformulation of metric learning by presenting a specialist vector for each class. It is shown that both methodologies, and little variations, reliably improve execution by between 0.2% to 0.4% on the LFW dataset dependent on two models. This is signi_cant on the grounds that the execution of the two models on LFW dataset is near immersion at over 98%.

Title: No Fuss Distance Metric Learning using Proxies
Authors: Yair Movshovitz-Attias, Alexander Toshev
Year: 2017

We address the issue of Distant Metric Learning (DML), described as learning a separation unsurprising with a thought of semantic similarity. For the most part, for this issue management is imparted as sets of centers that follow an ordinal relationship – a catch point x resembles a great deal of positive centers Y , and not under any condition like a ton of negative centers Z, and a misfortune portrayed over these separations is restricted. While the focal points of the smoothing out fluctuate, at the present time all around call this sort of management Triplets and all systems that follow this plan Triplet-Based techniques. These procedures are attempting to smooth out. An essential issue is the prerequisite for finding educational triplets, which is ordinarily practiced by an arrangement of tricks, for instance, growing the bunch size, hard or semi-hard triplet mining, etc. In reality, even with these tricks, the mixing pace of such systems is moderate. At this moment the creator proposes to improve the triplet misfortune on a substitute space of triplets, comprising of a catch data point and practically identical and different mediator centers which are found out too. These go-betweens inaccurate the principal data centers, with the objective that a triplet misfortune over the go-betweens is a tight upper bound of the main misfortune. This middle person based misfortune is tentatively better continued. Likewise, the delegate misfortune enhances state-of-craftsmanship results for three standard zero-shot learning datasets, by up to 15% center, while meeting on different occasions as brisk as other triplet-based misfortunes.

A) Existing System

In the current framework, Identity check assumes a significant job in our everyday lives. For instance, get to control, physical security and worldwide outskirt crossing expect us to confirm our entrance (security) level and our identities. To confirm what our identity is by indicating our ID records containing face pictures, for example, visas and driver licenses, to human administrators. In any case, this procedure is moderate, labor-intensive and unreliable. All things considered, a computerized framework for coordinating ID record photographs to live face pictures (selfies) continuously and with high precision is required. In the wake of confirming an explorer's character by face examination, the entryway is consequently opened for the voyager to enter. For IDselfie coordination, they are looking at a filtered or computerized archive photograph. Various mechanized ID-selfie coordinating frameworks have been deployed at international border crossings. Sent in 2007, SmartGate in Australia is the soonest of its sort. Because of an increasing number of explorers in Australia, the Australian government presented SmartGate at a large portion of its worldwide air terminals as an electronic visa check for ePassport holders. To utilize the SmartGate, explorers just need to let a machine read their ePassport chips containing their advanced photographs and afterward catch their face pictures utilizing a camera mounted at the SmartGate. After confirming a voyager's personality by face examination, the door is naturally opened for the explorer to enter Australia. Comparable machines have additionally been introduced in the U.K. (ePassport doors), USA (U.S. Computerized Passport Control) and different nations.

In China, such check frameworks have been sent at different areas, including train stations, for coordinating Chinese ID cards with live faces. Notwithstanding global fringe control, a few organizations, are using face acknowledgment answers for ID report confirmation for online administrations. The issue of ID-selfie coordinating represents various difficulties that are not quite the same as general face acknowledgment. For ordinary unconstrained face acknowledgment assignments, the primary difficulties are because of posture, light, and appearance (PIE) varieties. Then again, in ID-selfie coordinating, we are contrasting an examined or computerized archive photograph to an advanced camera photograph of a live face. Expecting that the client is agreeable, both of the pictures are caught under obliged conditions and huge PIE varieties would not be available.

However, (1) the low quality of document photos because of picture compression2 and (2) the enormous time hole between the report issue date and the check date stay as the essential challenges. Also, since cutting edge face acknowledgment frameworks depend on profound systems,

another issue looked in our concern is the absence of a huge preparing dataset (sets of ID photographs and selfies.

B) Problem Statement

- The issue of ID-selfie coordinating represents various difficulties that are unique concerning general face acknowledgment. For run of the mill unconstrained face acknowledgment assignments, the fundamental difficulties are because of posture, brightening and appearance (PIE) varieties.
- The low quality of report photographs because of picture compression1 and (2) the huge time hole between the record issue date and the confirmation date stay as the essential challenges.

C) Proposed System

We are proposing a certificate framework dependent on the RSA algorithm to defeat the issue. Information is put away in various hubs, and any individual who wishes to adjust a specific inside datum must demand that different hubs change it at the same time. Along these lines, the framework is highly reliable. We built up a decentralized application and structured an authentication framework. This innovation was chosen since it is incorruptible, encrypted, and trackable and permits data synchronization. The framework improves the effectiveness activities at each stage. The framework saves money on paper, cuts the executives costs, forestalls record fraud, and gives precise and dependable data on computerized authentications and contrast client live face and confirmed report face.

III. SYSTEM DESIGN

Identity confirmation assumes a significant job in our day by day lives. For instance, get to control, physical security and worldwide outskirt crossing expect us to check our entrance (security) level and our characters. A useful and normal way to deal with this issue includes contrasting a person's live face with the face picture found in his/her ID report. For instance, migration and customs authorities take a gander at the identification photograph to affirm an explorer's character. Assistants at general stores in the United States take a gander at the client's face and driver permit to check his/her age when the client is buying liquor. Examples of ID record photograph coordinating can be found in various situations. In any case, it is essentially directed by people physically, which is tedious, expensive, and inclined to administrator mistakes. An examination relating to the identification officials in Sydney, Australia, shows that even the prepared officials perform ineffectively in coordinating new faces to visa photographs, with a 14% bogus acknowledgment rate. Thus, a precise and computerized framework for productive coordinating of ID report photographs to constant selfies is required. Likewise, robotized ID-selfie coordinating frameworks additionally empower remote validation applications that are in any case not possible, for example, onboarding new clients in a versatile application (by checking their characters for account creation), or record recuperation on account of overlooked passwords.

A) MODULES

The following modules exist :

- User Registration and Authentication
- User Upload Certificate
- Get Certificate
- Face Verification and Response from Verification Authority

User Registration and Authentication

In this module, the user needs to register into this application and a request will be sent to the central board server for authentication. Unless the central board server approves the request, the user cannot login into his account. When the central board server approves the request, a key will be generated and the user can login into his account.

User Upload Certificate

After the user login into his account he needs to upload certificates namely pan card, aadhar card, voter id, ssc certificate to the central board server. Central board server will review the certificates and accept or decline the certificates. If the central board server accepts the certificate those details will be stored in E.C.S. If the central board server declines the certificate it won't be stored in E.C.S. or Block Chain.

Get Certificate:

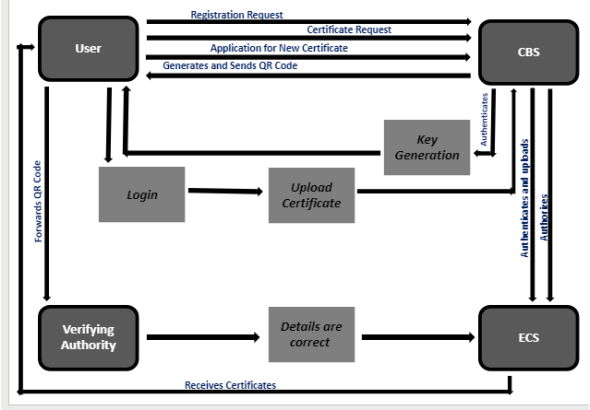
If the user needs a certificate, he will send a request to the central board server. If the central board server found the user details to be genuine, he accepts the request and forward a request to Authority where all the certificates will be there. Authority responds for the request and certificates will be provided to the user.

QR Request and Response from Verification Authority

If the user wants to apply for any certificates, he will send a request to the central board server and the central board

server will check the details and forward the request to the Authority. Authority will verify the user live face with document images and forwarded to the user via central board server. User forwards the QR code.

The below figure depicts the architecture diagram of the proposed system.



The user initially makes a request to the Central Board Server (CBS) to register into the application. The CBS approves or rejects the request depending upon the authentication. If approved the user can login into his/her account. The user then uploads various certificates. The CBS checks the certificates for authenticity and stores them in ECS. If the user wants to apply for any document, then the user again makes a request to CBS. After verification from the CBS, the ECS will generate a QR code and forward it to the user who forwards it to the authority. The authority issues the documents if all the details are correct and the face matches with the live face.

B)Algorithms Used:

i) **KNN Algorithm**

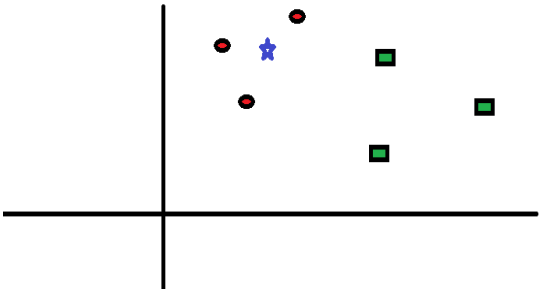
KNN can be utilized for both characterization and relapse prescient issues. Be that as it may, it is all the more broadly utilized in grouping issues in the business. To assess any system, we by and large gander at 3 significant angles:

1.Straightforwardness to decipher yield

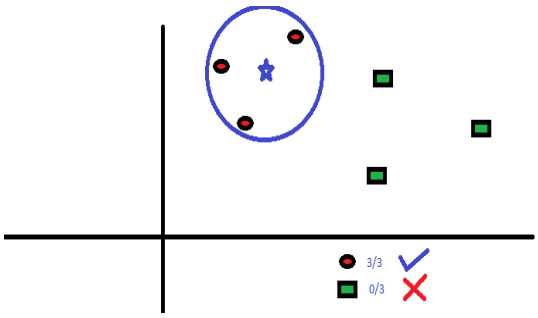
2.Estimation time

3. Prescient Power

How about we take a basic case to comprehend this calculation. Following is about the scatter of red circles and green squares:



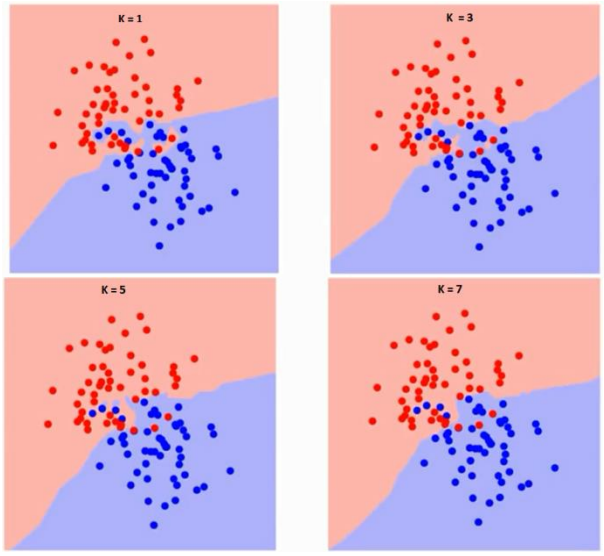
You are expected to discover the class of blue stars (BS). Blue Star can either be Red Circles or Green Squares and that's it. "K" in the KNN algorithm is the closest neighbor we have to take points. Suppose K = 3. Henceforth, we will currently make a hover with BS as focus similarly as large as to encase just three information focuses on the plane. Allude to the following graph for more subtleties:



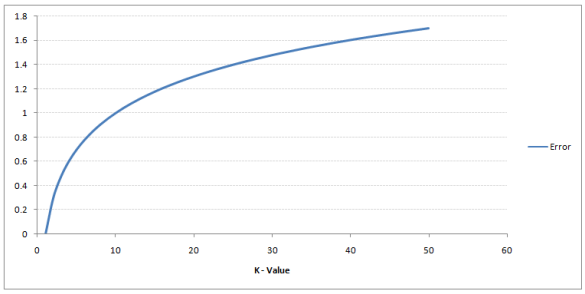
The three nearest focuses on BS is all RC. Thus, with great certainty level, we can say that the BS ought to have a place with the class RC. Here, the decision turned out to be extremely clear as every one of the three votes from the nearest neighbor went to RC. The decision of the parameter K is extremely vital right now.

How would we pick the factor K?

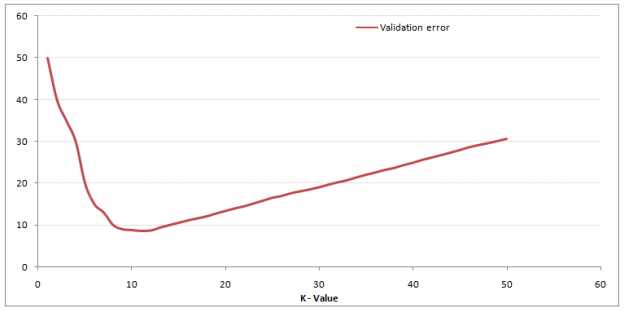
First, let us attempt to comprehend what precisely does K impact in the calculation. On the off chance that we see the last model, given that all the 6 preparing perceptions stays consistent, with a given K esteem we can make limits of each class. These limits will isolate RC from GS. It is a similar way; how can we attempt to predict the impact of significant value "K" on the class limits. The following are the various limits isolating the two classes with various estimations of K.



In the event that you observe cautiously, you can see that the limit becomes smoother with expanding estimation of K. With K expanding to vastness it at long last turns into all blue or all red relying upon the absolute greater part. The two parameters to access on K-esteems are the preparation mistake rate and the approval blunder rate. Following is the bend for the preparation mistake rate with fluctuating values makes the story all the clearer.



As should be obvious, the blunder rate at K=1 is constantly zero for the preparation test. This is because the nearest point to any preparation information point is itself. Thus the forecast is constantly precise with K=1. On the off chance that approval mistake bend would have been comparable, our decision of K would have been 1. Following is the approval blunder bend with a fluctuating estimation of K



:

At K=1, we were overfitting the limits. Thus, the blunder rate at first declines and arrives at an insignificant. After the minima point, it at that point increments with expanding K. To get the estimation of K, we isolate the preparation rate and approval rate from the underlying datasets. Presently plot the approval mistake bend to get the ideal estimation of K. This estimation of K ought to be utilized for all forecasts.

Breaking it down – Pseudo Code of KNN

We can implement a KNN model by following the below steps:

1. Give the input
2. Initialize k
3. For getting the anticipated class, iterate from 1 to total number of training data points

a. Calculate the distance between test data and each row of training data. Here we will use Euclidean distance as our distance metric since it's the most popular method. The other metrics that can be used are Chebyshev, cosine, etc.

b. Sort the calculated distances in ascending order based on distance values

c. Get top k rows from the sorted array

d. Get the most frequent class of these rows

e. Return the predicted class

ii) RSA Algorithm

RSA algorithm is an open key encryption procedure and is considered as the most secured method for encryption. It was designed by Rivest, Shamir and Adleman in 1978 and consequently named the RSA algorithm. The following are the steps:

Step 1: Create the RSA modulus

The underlying technique starts with choosing two prime numbers say p and q, and computing their product N i.e., N=p*q

Here, let N be the predetermined huge number.

Step 2: Derived Number (e)

Consider a number e > 1 and e < (p-1) and (q-1). The foremost constraint is that (p-1) and (q-1) should not have any other common factor other than 1.

Step 3: Public key

The predetermined pair of numbers n and e serves as the RSA open key and it is made public.

Step 4: Private Key

Private Key d is determined from the numbers p, q and e. The numerical connection between the numbers is as per the following $e^d = 1 \bmod (p-1)(q-1)$

This is the essential equation for the Extended Euclidean Algorithm, which accepts p and q as the input parameters.

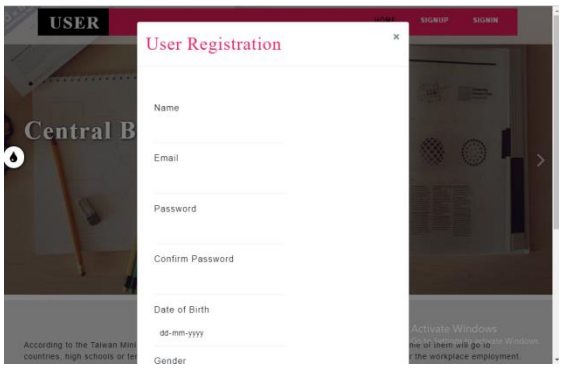
Encryption Formula

Let us assume a person sends a plain message to another person for which the public key is (n,e). To encrypt the plain message in the mentioned example, use −
$C = P^e \bmod n$

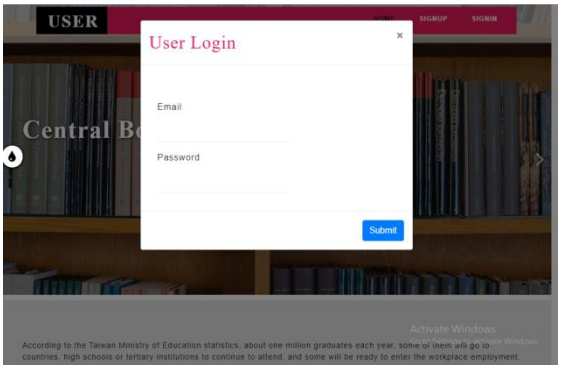
Decryption Formula

The decoding procedure is extremely clear and incorporates investigation for count in an orderly methodology. Considering recipient C has the private key d, the outcome modulus will be determined as −
Plaintext = $C^d \bmod n$

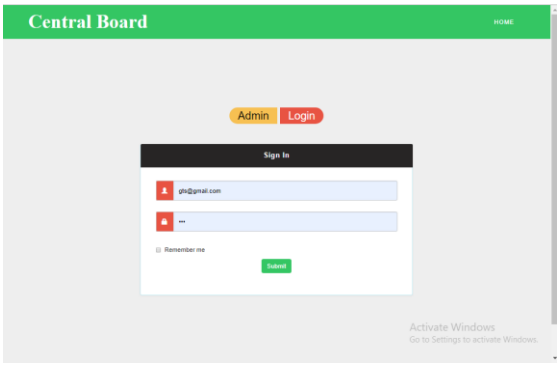
IV. RESULTS AND DISCUSSIONS



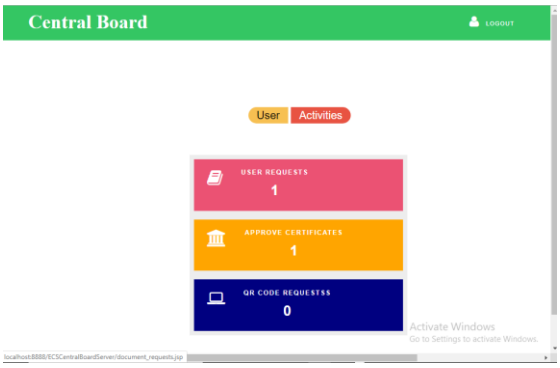
This is the user registration form wherein the user fills the necessary details.



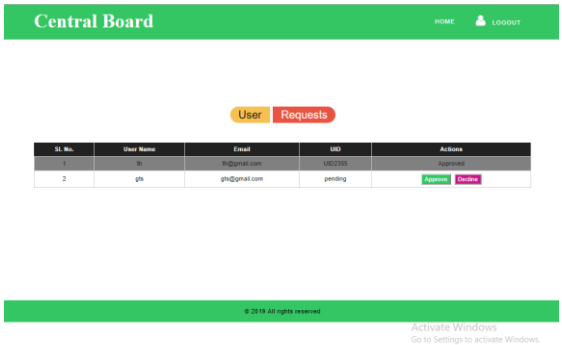
Once the registration request of the user is accepted by CBS, the user can login into his/her account.



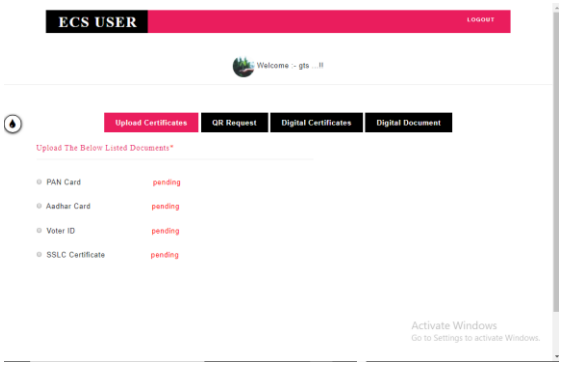
This is the login page of the admin of CBS.



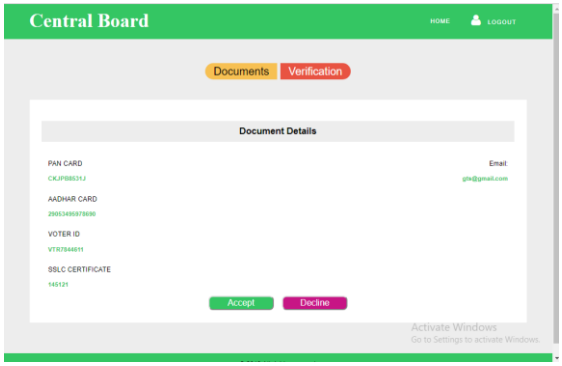
This page depicts the various number of requests which the admin needs to approve so that the user can further proceed.



This shows the various user registration requests that the admin of CBS needs to approve.



Once the user has logged in, he/she needs to upload the required documents. The above page states a pending status as the user has not uploaded any document.



Once the necessary certificates are uploaded the admin will check the document details and approve/decline them depending upon their trueness.

V. CONCLUSION

Nowadays, the number of fraudulent activities for duplication of certificates are increasing. The proposed system provides a technique to encrypt the user's document kept in the block chain. The system also proposes an approach to eliminate the manual process and enable automated matching of photographs in documents/. to live face images. It also enables remote authentication. The proposed system gives a solution to prevent the maximum number of intruders from getting illegal access to the user's credentials. Thus, the system will be able to successfully match photographs in documents to live face images and will avert frauds and augment security.

REFERENCES

[1] D. White, R. I. Kemp, R. Jenkins, M. Matheson, and A. M. Burton, "Passport officers' errors in face matching," *PLoS ONE*, vol. 9, no. 8, 2014, Art. no. E103510.

[2] Wikipedia. (2018). *Australia Smartgate*. [Online]. Available: https://en.wikipedia.org/wiki/SmartGate

[3] Wikipedia. (2018). *Epassport Gates*. [Online]. Available: https://en. wikipedia.org/wiki/EPassport_gates

[4] U.S. Customs and Border Protection. (2018). *Automated Passport Control (APC)*. [Online]. Available: https://www.cbp.gov/travel/uscitizens/ apc

[5] Xinjiang Heng An Perimeter Security Equipment Company. (2018). *What Is ID-Person Matching?* [Online]. Available: http://www.xjhazj. com/xjhazj/vip_doc/8380983.html

[6] Jumio. (2018). *Netverify ID Verification*. [Online]. Available: https://www.jumio.com/trusted-identity/netverify

[7] Mitek. (2018). *Mitek ID Verification*. [Online]. Available: https://www.miteksystems.com/mobile-verify

[8] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," Univ. Massachusetts, Amherst, MA, USA, Rep. 07-49, Oct. 2007

[9] V. Starovoitov, D. Samal, and B. Sankur, "Matching of faces in camera images and document photographs," in *Proc. ICASSP*, 2000, pp. 2349–2352.

[10] T. Bourlai, A. Ross, and A. Jain, "On matching digital face images against scanned passport photos," in *Proc. IEEE Int. Conf. Biometrics Identity Security (BIDS)*, 2009, pp. 1–10.

[11] Y. Shi and A. K. Jain, "DocFace: Matching ID document photos to selfies," in Proc. BTAS, 2018, pp. 1–8.

[12] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint face detection and alignment using multitaskcascaded convolutional networks," IEEE Signal Process. Lett., vol. 23, no. 10, pp. 1499–1503, Oct. 2016.

[13] H. Wang et al., "Cosface: Large margin cosine loss for deep face recognition," in Proc. CVPR, 2018, pp. 5265–5274.