International Journal of Innovative Information Systems & Technology Research 9(3):120-130, July-Sept., 2021

 www.seahipaj.org ISSN: 2467-8562

An Improved Blockchain Ledger Wallet Identification System

C. J. Nwagbara & E. F. Jumbo

Department of Computer Science,
University of Port Harcourt, Port Harcourt, Nigeria

ABSTRACT
There have been challenges with cryptocurrency wallets and the identification of owners in the Blockchain digital ledger system even though the wallets may be viewable on the blockchain. Exchanges often take the know-your – customer information without linking it to the wallets. In this project, an improved blockchain ledger wallet identification system is developed to check theft of coin and the use of the blockchain for money laundry. We introduced a facial recognition using JPEG2000 for proper image recognition of the registered user. The facial recognition was integrated with the username and password of the owner to provide better secured system that can be used to identify users on the cryptocurrency space. The system was designed using structured system analysis and design methodology. The system is implemented using PHP and MySQL programing languages and database. PCA is adopted in this work to reduce image dimension and make it possible to select the hyperplane. Selecting the hyperplane makes it easier to get the axis of maximum variance as all the points will spread out maximally when projected onto the hyperplane. Studies have shown that it is easier for the system to separate faces when the data are spread out as opposed to clustered images. The result shows that facial recognition can increase security of the wallet.
Keywords: Cryptocurrency, Data Mining, Blockchain, Ledger, Blockchain Wallet.

INTRODUCTION

A blockchain, as the name implies, is a chain of digital "blocks" that contain records of transactions. Each block is connected to all the blocks before and after it. This makes it difficult to tamper with a single record as that would mean to change the block containing that record as well as those linked to it to avoid detection. Blockchains are also decentralized and distributed across peer-to-peer networks that are continually updated and kept in a consensus state. Blockchains are not contained in a central location, as such do not have a single point of failure and cannot be changed from a single computer (Buterin, 2014).
Blockchain has been introduced as an effective technology for solving the transaction security problems. Furthermore, it has been implemented successfully in many applications, e.g., Bitcoin Wallet (Bamert et al., 2014), Ethereum (Buterin, 2014), and Internet-of-Things (IoT) (Dorri et al., 2013). Generally, blockchain is a distributed database that is replicated and shared among members of a network (Lin and Liao, 2017). With blockchain, when a transaction is created, it will be verified parallelly and transparently by some nodes in the network through mining processes. After that, transactions are grouped into blocks, and the links between blocks and their content are protected by cryptography and cannot be forged. Once entered into a blockchain, transactions cannot be erased. Thus, a blockchain contains an accurate, time-stamped and verifiable record of every transaction, and hence the network does not need a central authority. As a result, the blockchain technology is popularly used in systems requiring high security and transparency, such as, Bitcoin (Nakamoto, 2009) and smart digital contract Ethereum (Buterin, 2014). In blockchain technology, the mining process plays a crucial role in verifying and adding transaction records to the public ledger, i.e., the blockchain. In a mining process, the miner, i.e., the node taking the responsibility for mining a transaction, is required to verify the transaction and solve the proof of-work

problem in order to find a new hash for the incoming block to store the verified transaction. This process is complicated and usually executed on powerful devices with high computational capacities and energy supply, e.g., servers and super computers.

Blockchain is the mechanism that allows transactions to be verified by a group of unreliable actors. It provides a distributed, immutable, transparent, secure and auditable ledger. The blockchain can be consulted openly and fully, allowing access to all transactions that have occurred since the first transaction of the system, and can be verified and collated by any entity at any time. The blockchain protocol structures information in a chain of blocks, where each block stores a set of Bitcoin transactions performed at a given time. Blocks are linked together by a reference to the previous block, forming a chain (Buterin, 2014).

2. REVIEW OF RELATED WORKS:

2.1 Blockchain

Blockchain technology enables the creation of a decentralized environment, where the cryptographically validated transactions and data are not under the control of any third party organization. Any transaction ever completed is recorded in an immutable ledger in a verifiable, secure, transparent and permanent way, with a timestamp and other details.

The blockchain term, originally block chain, was first coined in 2009, by (the still unknown) Satoshi Nakamoto, in the original source code for the virtual currency Bitcoin: "Nodes collect new transactions into a block, hash them into a hash tree"; "when they solve the proof- of - work, they broadcast the block to everyone and the block is added to the block chain" (Nakamoto, 2009).

The interrelated terms Blockchain, Cryptocurrency (currency that only exists digitally, using a decentralized system to record transactions) and Initial Coin Offering.

A blockchain is characterized by censorship resistance, immutability and global usability, and has a global network of validators called miners, who maintain it through block rewards, named cryptotokens (Jeremy and Shulman, 2018).

2.2.2 Blockchain Wallets

A blockchain wallet is a digital wallet that allows users to manage bitcoin, ether and other cryptocurrencies. Blockchain wallets allow individuals to store cryptocurrencies. Creating an e-wallet with Blockchain Wallet is free, and the account setup process is done online. Individuals must provide an email address and password that will be used to manage the account, and the system will send an automated email requesting that the account be verified.

Once the wallet is created, the user is provided with a Wallet ID, which is a unique identifier similar to a bank account number. Wallet holders can access their e-wallet by logging into the Blockchain website, or by downloading and accessing a mobile application.

The Blockchain Wallet interface shows the current wallet balance for both bitcoin and ether tokens and displays the user's most recent transactions. Users can send a request to another party for a specific amount of bitcoin or ether, and the system generates a unique address that can be sent to a third party (Prisco, 2016).

Bank transfers will incur a small payment fee (e.g., 0.25%), and it may take several days before bitcoins are received. Using a credit or debit card provides instantaneous access to bitcoin but incurs a larger convenience fee (e.g., 3%). Buy and sell services are not available in all locations.

Wallet security is an important consideration for users, as having one's account illegally accessed may result in the user losing bitcoin and ether. Blockchain Wallet has three levels of security:

Level 1: Security is designed to prevent users from losing account access. It allows users to verify their email address, create a 12-word backup recovery phrase that can be used if a password is forgotten, and set up a password hint (Blockchain does not store the password).

Level 2: Security is designed to prevent others from gaining unauthorized access to the wallet and includes linking a phone number to the account to receive a one-time password when the account is logged into, and creating two-step authorization.

Level 3: Security allows users to block Tor requests.

2.2.3 Blockchain Wallet Identification

A wallet identifier, also known as a wallet ID, is like a username. You use it, along with your password, to log into your Blockchain wallet and access your digital assets. A wallet identifier is composed of 32 alphanumeric characters and 4 dashes, and takes the following format:

xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Every wallet has a unique identifier. When you create a wallet, an email containing your identifier and prompting you to verify your email will automatically be sent to the email address you signed up with. If you didn't get the email or otherwise lost your identifier, you can also find your wallet identifier within your wallet, under Settings > General.

If you ever need to use your 12-word recovery phrase to restore your funds, this action will create a new wallet that is an exact copy of your original one. This new wallet will have a new and unique identifier associated with it. Make sure to store this updated wallet information privately in a safe place.

3. Analysis of the Existing System

The existing work by (Hackett, 2016) proposed a model for Cryptocurrency as a digital currency based on cryptography, or the process of converting plaintext into ciphertext, thus making readable text non-decipherable (Hackett, 2016). He further explained that the use of cryptography in the transfer of data has four main objectives: Confidentiality as the information cannot be understood by anyone for whom it was unintended to be, Integrity by ensuring the information sent remains unaltered, Non-repudiation the sender of the information cannot deny that they sent the information at a later date and time and Authentication, where the sender and receiver have the ability to confirm each other's identity and the origin and destination of the information.

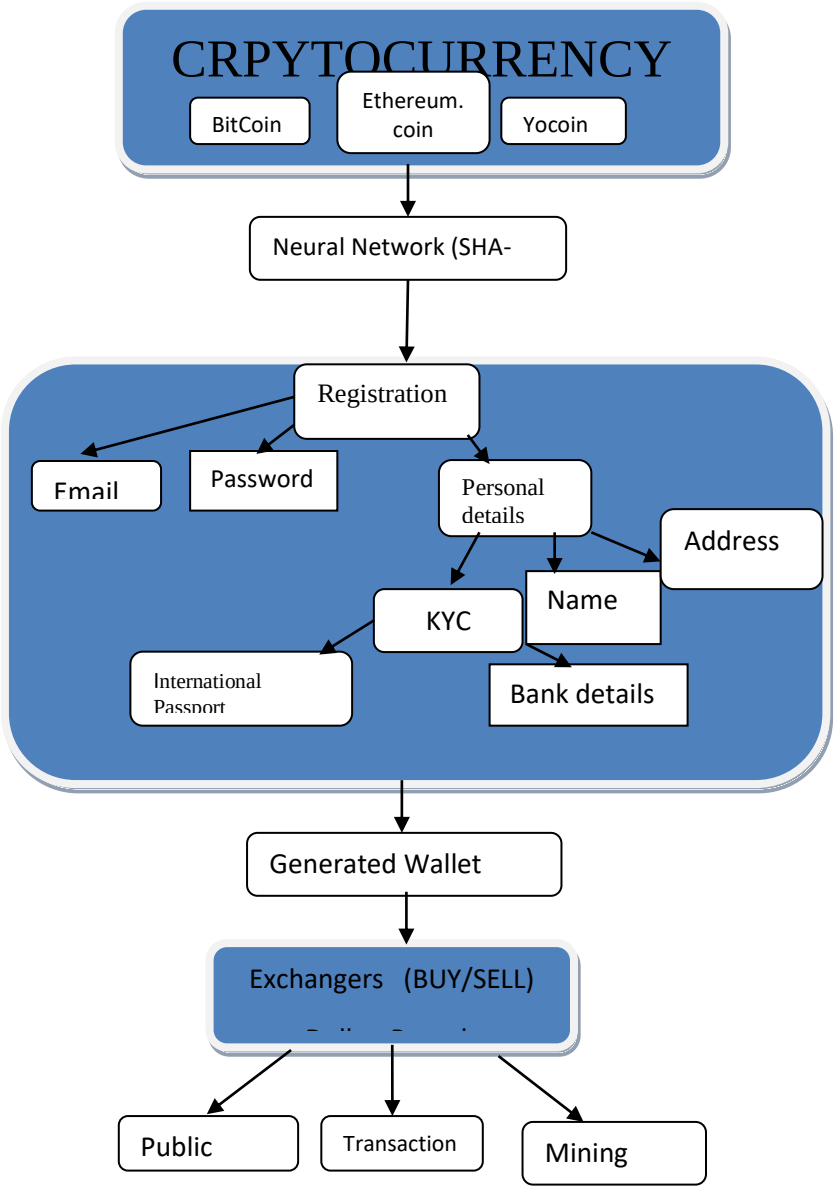

Figure 3.1: Existing Cryptocurrency System (Hackett, 2016).

3.1.1 Current Wallet Identification in the Existing System

Public Ledgers serves as a platform where all transactions from the start of a cryptocurrency's creation are stored in a public ledger. The identities of the coin owners are encrypted, and the system uses other cryptographic techniques to ensure the legitimacy of record keeping. The ledger ensures that corresponding "digital wallets" can calculate an accurate spendable balance. Also, new transactions can be checked to ensure that each transaction uses only coins currently owned by the spender. Bitcoin calls this public ledger a "transaction block chain".

3.2 Analysis of Proposed System

The proposed system is to improve on Hackett, 2016 work by enhancing the security of the user wallet. The existing system uses a one way authentication to trade which does not guarantee the security of the wallet from unauthorized access.

In the proposed system, an improvement on the security of the wallet is made with the inclusion of facial recognition as a form of biometric authentication, which uses body measurements to verify user's identity. Facial recognition is a subset of biometrics that identifies people by measuring the unique shape and structure of their faces. Facial recognition uses the same principles as other biometric authentication techniques, such as fingerprint scanners and voice recognition.

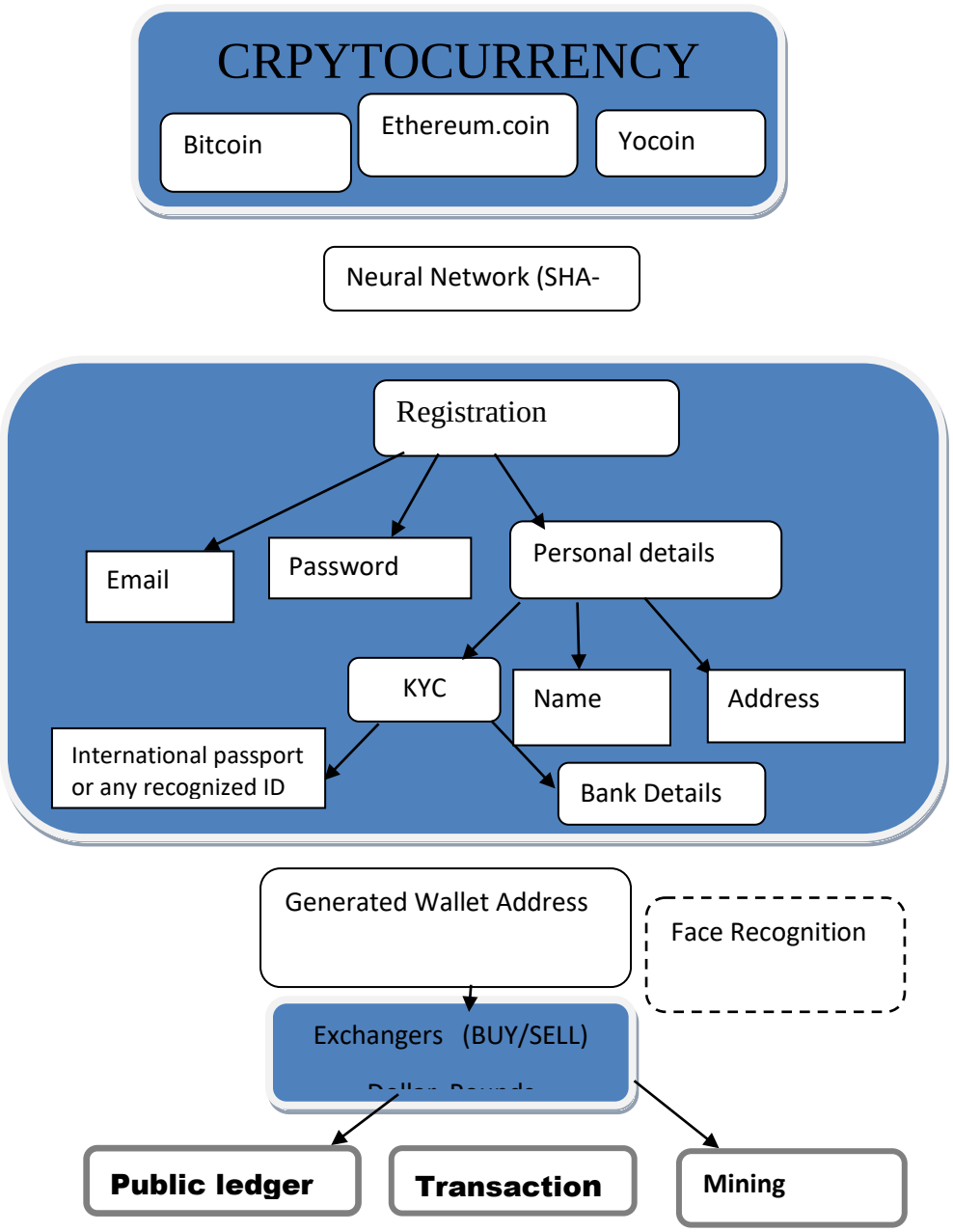

Figure 3.2: Architecture of the propose System.

3. Proposed System

3.1 The Proposed Crypto-currency System with Face Recognition

In the architecture of the proposed system, a face recognition system was integrated into the system to function as an added layer for the creation of the wallet. The detail of the face recognition is illustrated in figure 3.3 where the architecture of the face recognition system was shown. During registration for the wallet image is captured from the camera via the image interface like web cam or phone camera into the face detection subsystem. In the system, Down Sampling and Face Recognition Subsystem is also integrated to allow wallet users gain access to their wallet by simply showing their face to be recognized. The system also ensure that when coin is sent to that wallet that the system can detect the owner and supply other detailed information.

3.2 Algorithm of the PCA used in the Proposed System

PCA method is used to extract features from face images. PCA calculates the Eigenvectors of the covariance matrix, and projects the unique features onto a lower dimensional feature. These Eigenvectors are also referred to as Eigenfaces.

The advantage of the PCA method is that it reduces the dimension of the eigenvectors by some technique.

To perform PCA some steps are undertaken. Assuming there are 'K' training images, denoted by M. M=1, 2, 3, 4…k.

Step 1: Convert the 2D image vector in 1D image form.

Step 2: Calculate the average image vector from all trained images.

$$Avg = 1/k \sum_{i=1}^{k} M_i$$

Step 3: Subtract the average image vector from each 1D image vector to get the unique image vectors. Resultant vectors are also known as normalized image vectors.

$$S_i = M_i - Avg$$

Step 4: Calculate a covariance matrix

$$C = 1/k \sum_{i=1}^{k} S_i^T S_i$$

Step 5: Calculate Eigenvectors and Eigenvalues from the covariance matrix.

Step 6: Choose a feature vector. Only that Eigenface should be selected which have the maximum eigenvalues. The additional Eigenvalues describes the features of a face images better.

4. RESULTS AND DISCUSSION

Software implementation has to do with testing the designed and developed program as well as the overview of the system for optimal performance and delivery; it also depicts the programming languages, tools that lead to the successful testing and achievement of the program, also outlined emphasis on why such tools and languages were adopted for this work.

4.2.1 System Deployment

After testing we can deploy the application to a server that allows access via a web browser, the system can also be deployed to a local server within a company and be accessible to only employees within that company. To do this, the project folder will have to be archived as a zipped file and deployed on a standards server that has all the software specified earlier and hardware support, another alternative is git deployment, which involves uploading the entire files to a git repository and pulling from the repository directly from your server.

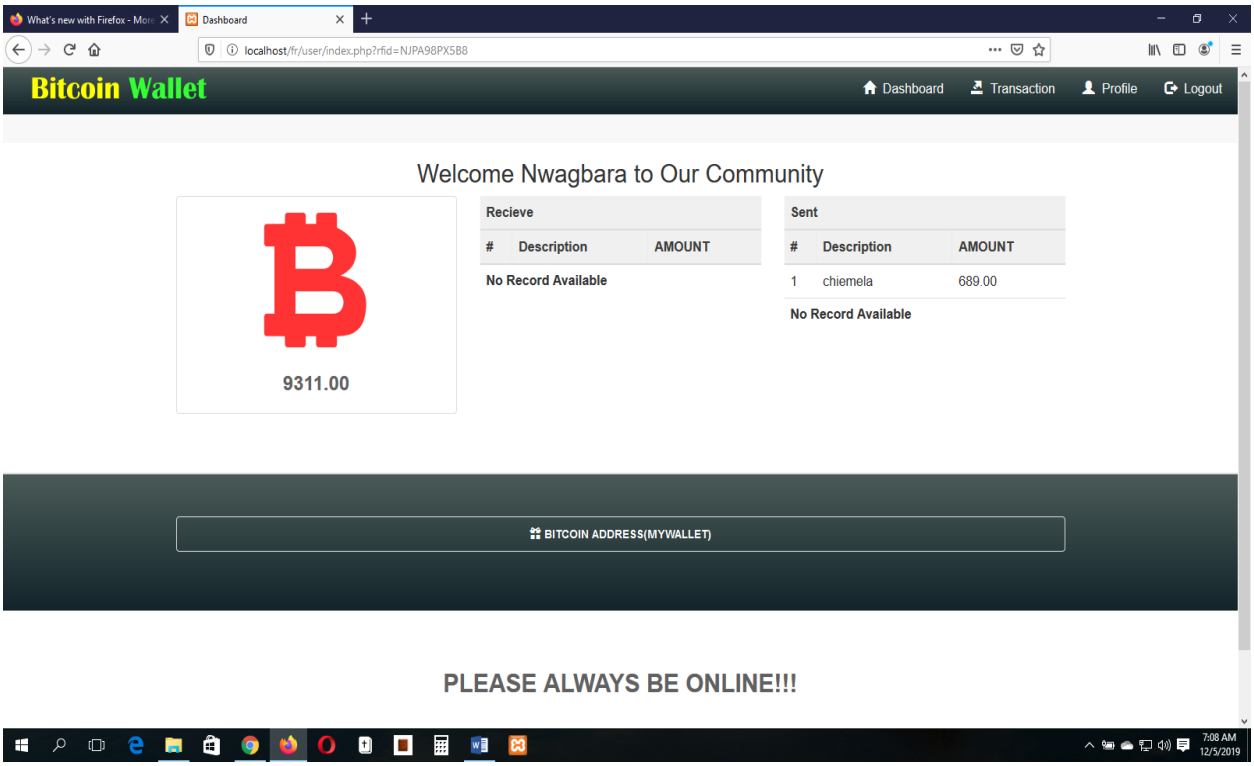

Figure 4.1. Welcome page of the Improved Blockchain Wallet.

4.3 Experimental Results

Preprocessing on face picture like changing over the picture into dark and white and resizing is finished by utilizing standard MATLAB® capacities for example image resize. The pictures are resized into 157x128 measurements. The preparation set currently contains pictures with same measurements. The figure 4.2 demonstrates preparing set of face space. The standardized preparing set is created by changing the mean and standard deviation everything being equal and transposing all pictures network.

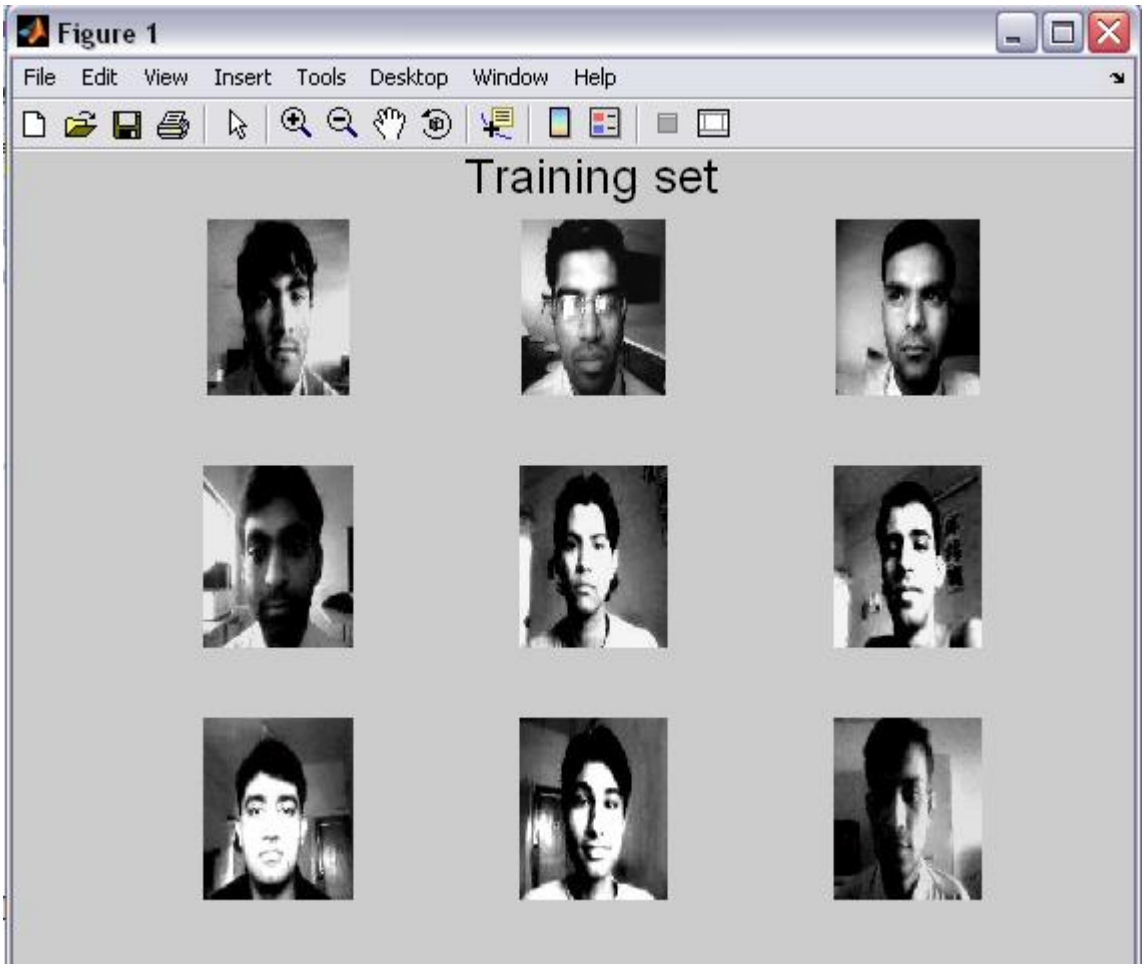

Figure 4.2 Training Set of Face-Space

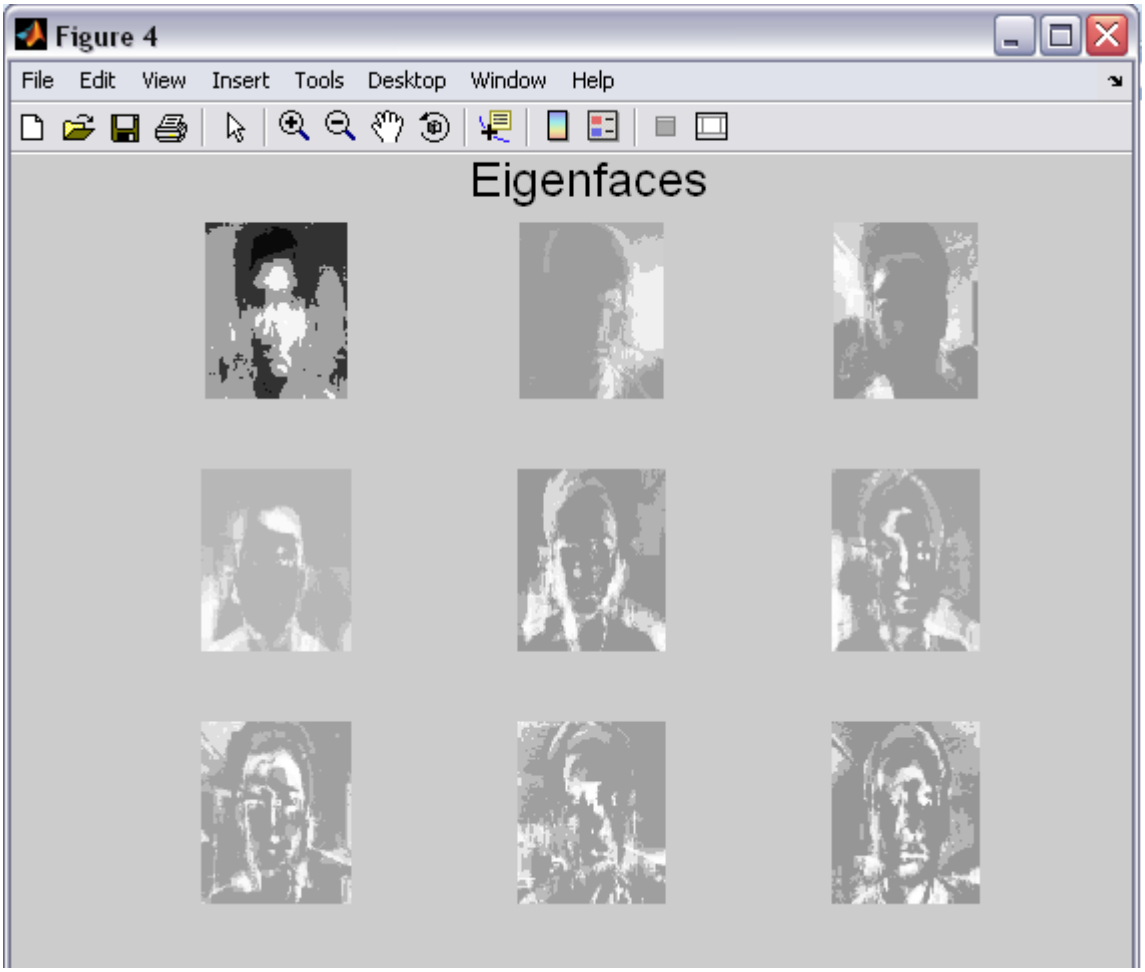

Fig. 4.3: Eigenefaces of Training Set.

Mean picture is represented in figure 4.2. Next ascertain eigenvectors and its relating eigenvalues from the covariance network and standardize it to acquire Eigen face as shown in figure 4.3. Presently taking info picture to compute weight of information picture and its separation. This is first picture of preparing set. Figure 4.2 demonstrates recreated picture of figure 4.4. The Euclidian separation and weight of info face picture is appeared in figure 4.4.

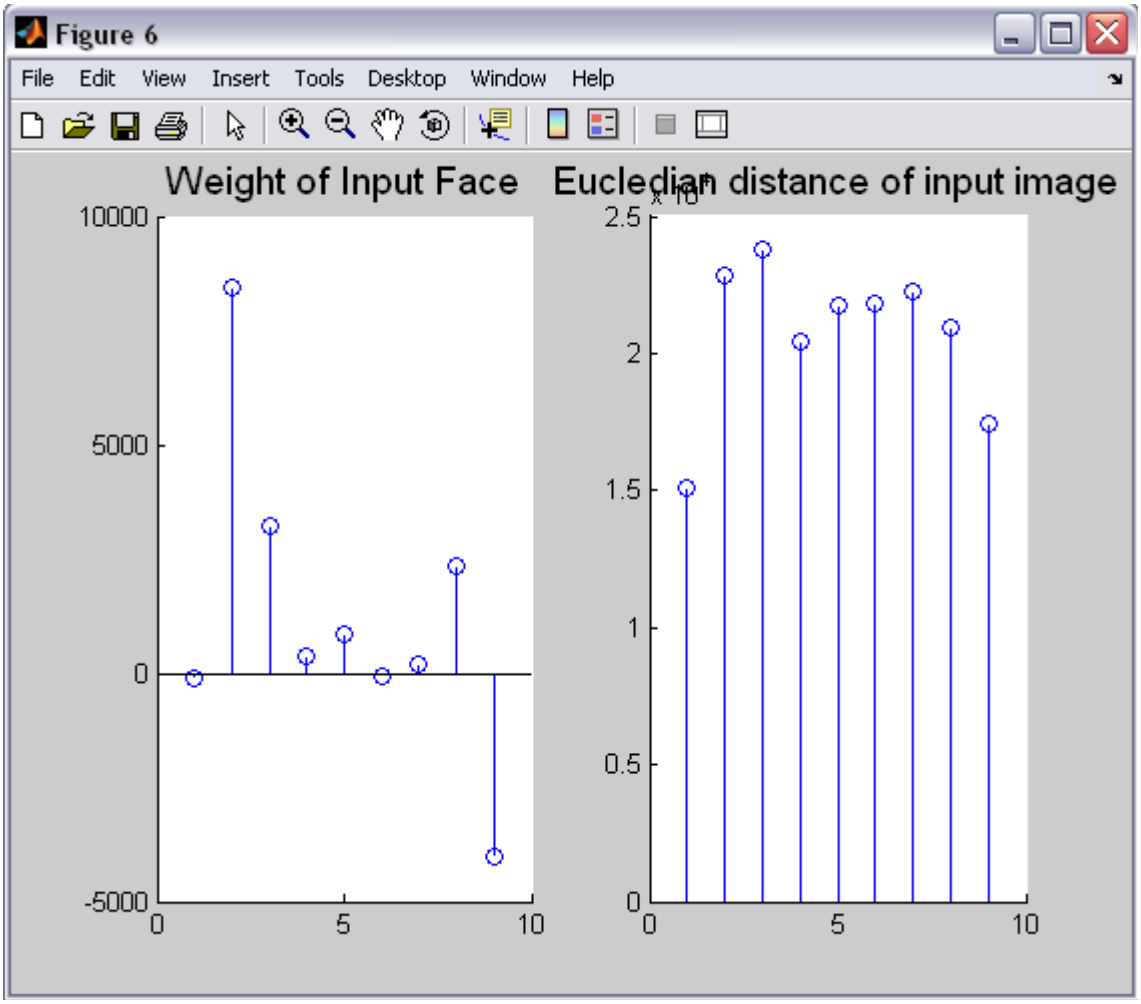

Figure 4.4: Weight of the input face and Euclidean Distance of the input face

5. CONCLUSION

In conclusion, the new approach in securing blockchain ledger wallet identification system has been developed using XAMPP as a server with the MySQL Database system as an open source software and implemented with PHP being a simple, multi-paradigm, structured, object-oriented, modern and event-driven high level programming language. PCA is adopted in this work to reduce image dimension and make it possible to select the hyperplane.

6. RECOMMENDATIONS

The under listed recommendations are made based on the findings:

i. The research is prescribed to associations both private and public that are searching for a superior and secure approach to verify enlisted clients' wallet in the digital money stage for all exchange.

ii. Moving forward, face recognition system can be fused with other biometric authentication traits like voice recognition.

REFERENCES

De Novellis, M. (2018). Blockchain, Big Data Analytics & The 5 Hottest Topics On The MBA Curriculum In 2018. Business Because.

Delfin-Vidal, R. (2014) "The fractal nature of bitcoin: Evidence from wavelet power spectra," The Fractal Nature of Bitcoin: Evidence from Wavelet Power Spectra .

DF. (2018). Discussion Paper: Virtual Currencies and Blockchain Technology. Department of Finance, Ireland.

Dhillon, V., Metcalf, D., & Hooper, M. (2017). Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You. Apress.

Dorri, A. Kanhere, S. S. and Jurdak, R. (2017). "Towards an optimized blockChain for IoT," in IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation, Pittsburgh, USA, 173-178.

Dorri, A. Kanhere, S. S. Jurdak, R. and Gauravaram, P. (2017). "Blockchain for IoT security and privacy: The case study of a smart home," in IEEE International Conference on Pervasive Computing and Communications Workshops, Hawaii, USA, 618-623,

Esposito, M. (2018). This is how new technologies could improve education forever. World Economic Forum Report. Online at https://www.weforum.org/agenda/2018/03/education-catapult.

Gers, F. A. Eck, D. and Schmidhuber, J. (2001) Applying lstm to time series predictable through time-window approaches, 669–676.

Global M-commerce Market (2016-2020). Available at: https://www.technavio.com/report/global-media-and-entertainment-servicesglobal-m-commerce-market-2016-2020.

Gorsline, E. (2018). What is Nebulas (NAS)? A Beginner's Guide. Online at https://coincentral.com/nebulas-nas-beginners-guide.

Greaves A. and Au, B. (2015) "Using the bitcoin transaction graph to predict the price of bitcoin,".

Grech, A., and Camilleri, A. F. (2017). Blockchain in Education. Inamorato dos Santos, A. (ed.). Joint Research Centre.

Hackett, R. (2016, May 23). Wait, What Is Blockchain? Retrieved from Fortune: http://fortune.com/2016/05/23/blockchain-definition/

Heaton, J. B. Polson, N. G. and Jan H. W.(2016) Deep learning for finance: deep portfolios. Applied Stochastic Models in Business and Industry.

Hobson, D. (2013). What is bitcoin? ACM Crossroads, 20(1,)

Holotescu, C. (2018). Blockchain and Open Education. Presentation for OEW. Online at https://www.slideshare.net/cami13/blockchain-and-open-education.

Holotiuk, F., Pisani, F., & Moormann, J. (2017). The impact of blockchain technology on business models in the payments industry. 13th International conference on Wirtschaftsinformatik.

Investopedia. (2016, October 15). Cryptocurrency. Retrieved from Investopedia: http://www.investopedia.com/terms/c/cryptocurrency.asp

Jordan P. (2016). "'Bitcoin Unlimited' Hopes to Save Bitcoin from Itself". Motherboard. Vice Media LLC. Retrieved 17 January 2017.