International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

BIOMETRIC ENCRYPTION FOR SECURE AND EFFICIENT CLOUD ACCESS MANAGEMENT

Dr.Adelina Johnsana[1], Nalla Varun[2], Uppunuthala Abhilash[3], Nandhyala Sravan Kumar Reddy[4]

[1] Associate Professor, Dept. of AI-ML, Sri Indu College of Engineering and Technology, Hyderabad,
[2 3 4] Research Student, Dept. of AI-ML, Sri Indu College of Engineering and Technology, Hyderabad

Abstract

Cloud computing is a major blooming technology which has numerous applications in today's market and is rightly so hyped. Images are a major part of today's internet data traffic, especially due to widespread social media, and hence, its security is crucial. However, in the present scenario, the images in cloud are a major issue in terms of security. Since the user who has uploaded the image has no control over the security of images, the cloud provider has to ensure maximum security in terms of authentication and prevention from attacks. The main objective of this paper is to provide a method to enhance the safety of images on cloud. This paper presents an idea of securing images on cloud platform using biometric authentication. Different steps involved in biometric authentication and secure upload and access of images are explained, and integration of all the steps is done at the end as a case study which puts light on the whole process in which methods are best-regarding results and compatibility. The proposed algorithm in this paper presents the idea of authentication of images in two basic steps of image compression using standard discrete wavelet transform method followed by image encryption using the hybrid method of SHA and blowfish. This image is then stored into the database of cloud and accessed whenever the user requests it. A structured and comprehensive view of encryption methods, types of biometrics and to secure data as well as images is provided in this paper.

Keywords Biometrics · Image encryption · Image compression · Security · Cloud

1 Introduction

The drastic change in the eminence of the technological world is primarily as a result of the advancement in the speed and the performance of the internet. The real-time fast processing and storage of multimedia data on the internet in recent times have heavily relied on cloud computing. Even though the cloud is barely a decade old, it has influenced the computing world such as no other technology. Apart from providing various other advantages, the most cardinal advantage would be that this technology is straightforward and easy to understand even for a technical neophyte. The flexible nature, creation of applications across platforms, streaming multimedia and using analytic data patterns to make predictions, makes it an ideal choice for companies who rely heavily on data analytics. In addition, there is a proliferation in the production of data, and corresponding storage space is, inadequate.

On the basis of accessibility, clouds are divided as public, private, and hybrid. In public cloud, the organization needs not to worry about cloud hosting management as well as maintenance and it belongs to the service provider. While private clouds belong to an individual company. Hybrid cloud, as the name suggests, is the mixture of both public and private clouds. Although the user is free from the management of data center, there is a drawback too. They worry about that data security, because the data are under control of service provider. For this, a framework of data security is proposed (Pandey et al. 2013). In addition, there are some proposed

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

models and patents of security techniques of data storage. In Chen and Zhao (2012), privacy and security of data are analyzed. Concisely, a large number of researchers are working on security of data in cloud computing, because the trustworthy environment of the technology is the most required thing or a condition to gain confidence of users (Duarte et al. 2016).

Cloud computing is a technology which provides flexibilities such as infrastructure as a service, software as a service (Bothe et al. 2012), Web-based cloud computing (Wang et al. 2013a, b), platform as a service (Thieling et al. 2014), managed service, utility services, and many more. These produced data can be stored on storage provided by cloud system providers. The main advantage of the cloud is that whenever a user or any organization or an employee of a company wants to access that data authentication is done before. From 2014 to 2018, there is 0.79 billion increase in some cloud storage users. However, it includes some drawbacks such as cost, vulnerability to attack, limited control and flexibility, vendor lock-in, and most importantly security and privacy. Authentication such as traditional methods can be done by passwords and PINs, but its drawback is that users have to remember them. To relieve from remembering many such passwords, they generally use the same passwords everywhere which is not troublesome work for a hacker. Nowadays, multi-factor authentication is also used by cloud services and mobile phones, but cost imbalance is created along with IT onerous (Rathi et al. 2012).

In addition, Keystroke dynamics is used for authentication, but again, it has disadvantages too. This system is of lower accuracy and permanence. The soft token is another alternative, but in this, users always need to carry token with them. Furthermore, cost of the token and any replacement fees are also augmented. Smart cards are also considered superior. They contain a lot of sensitive data, so if stolen, crucial information of users gets leaked, and security and privacy are compromised. Fingerprint along with multi-factor authentication is also one of the widely used systems, but in it, the fingerprint scanner does not consider any physical changes. Nowadays, biometric identification is the most used authentication system. It uses metrics related to human characteristics such as palm veins, face recognition, DNA, palm print, retina, and odour. These are unique characteristics. The main disadvantage of this system is that if any of those unique characteristics stolen, the actual user cannot replace it with a new one. Once stolen, the characteristic becomes useless for the user. This kind of data is also not known by cloud storage servers itself, but due to lack of authenticity, infidelity inside the team itself, systems developed by people which can read the data used for authentication and misuse it, and they do not feel safe to store any critical data on cloud storage. Until date, many researchers have tried and are trying to find an authentication system without such disadvantages,

and therefore, this review paper shows the advantages and disadvantages along with accuracy based on a case study.

In addition, there is a small relevance between cloud computing and grid computing. A single operating system is used in grid computing which amalgamate and control varied resources to provide computing services with high performance. While in cloud computing, discrete operating systems control system resources and computing, provid- ing users' services such as extensive storage of data and exorbitant performance computing. Thus, the whole scenario of grid computing has been changed by cloud computing. Due to such useful characteristics and salient features, it has attracted a lot of researchers.

Today, multimedia are the main feature of all the applications related to the internet including the cloud. The multimedia mostly consists of the images and videos. Images are the most widely used modes of communication in almost every field be it business, medical, or research. Even though image transfer and exchange is one the most popular activ- ity online, most of the channels through which the images' transfer is mostly unsafe and the security is quite low. Hence, the unauthorized access of images is very common, and normally, people do not think much before sending or receiv- ing images. Even though the person that one is sending the images to is safe, the channel might not be safe, and hence, the image gets tampered **(**Madhu et al. 2016**)** Watermarking an image refers to the act of applying a transparent layer of text or another image over the original image to protect it. This text or image which overlaps the original image is known as the signature of that image, which may be visible or cryptically hidden as per the function of the image.

Data storage in cloud computing can be both, text and images. Those images might include much of the user's important data. Various methods for protection of data in cloud computing have developed and improvised, but that in privacy protection of images in cloud computing are very few. In addition, as stated in Business Insider, approximately
1.2 trillion images will be captured this year which is a lot to be managed and processed. The smart systems releasing their burden by outsourcing data constantly is no big deal, but their privacy protection is the biggest concern and especially that of images.

Furthermore, there are lots of image processing applica- tions based on cloud computing for different motives such as agricultural and remote sensing. Their protection is of utmost concern. Therefore, many encryption methods have been pro- posed to date (Chnag et al. 2001; Fridrich 1998; Guan et al. 2005). Survey of encrypting schemes of chaotic images is provided in (Rajput and Sharma 2015).

There are numerous methods of encryption and watermarking of images.

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

1. One of them is using recursive cellular automata substitu- tion in which the image in which the concept of dynamic keys is used to generate the cipher image from the plane image. This method has been successful in various sci- entific problems and systems (Zefreh et al. 2011).
2. Another method, which is comparatively mainstream, is the usage of public keys and private keys for encryption and decryption in which the digital signature is produced using a secure hash algorithm (SHA) (Murty et al. 2011).
3. A different method to encrypt the image is superimposi- tion of the original images with another image if the same frequency range by applying discrete cosine transform (DCT) and fast Fourier transform (FFT) which has its set of drawbacks due to its incompatibility with hardware, these disadvantages are overcome by a method proposed in *International Journal of Future Computer and Com- munication*, which proposes a watermarking technique in which digital signature is embedded in the least sig- nificant bits of the pixels of the original image (Bhansali et al. 2013).

Many efforts and research works are going on for real- time privacy protection of images based on cloud computing. Many of these systems with the implementation of image processing have other uses such as face recognition (Rathi et al. 2012), security (Mannapur et al. 2018), feature extrac- tion (Wang et al. 2013a, b), smart campus (Xia et al. 2018), copyright protection, and many more. Therefore, various methods used for privacy protection of images are water- marking technology (Reza et al. 2012), where data are linked with contents of digital multimedia (Bhattacharyya et al. 2009). Local binary pattern [LBP] which is used as descriptor of contents of images as well as videos with the help of neighbouring pixels and can be used for classification in high level understanding of digital images (Huang et al. 2011), embedded scalable vision system (Thieling et al. 2014) using scale-invariant feature e-transformation in which local features are identified and described (Hsu et al. 2011), MapReduce technique where a large amount of data goes through input-map-shuffling-reduce-output processes run- ning independently and in a distributed manner (Potisepp 2013; Zhang et al. 2014).

2 Cloud-computing: architecture

There is much hype around cloud computing. According to Forrester in 2010, an American market research company, the cloud computing industry will expand from a 40.7 bil- lion dollars industry in 2010–241 billion dollars industry in 2020. Microsoft Azure, Google Compute Engine, 10gen etc. are the most famous cloud providers (Rani and Ranjan 2014). The cloud is generally divided into private which is accessible to only c entities, public clouds which provide services to all its customers, community cloud which is a cloud shared by various organizations having common functionalities and domain, and finally, hybrid cloud which is a fabrication of two or more private, public, and community cloud structures. Cloud is a better option for its customers than any other service, because customers save time and money. Quoting Steve Jobs, Co-founder, CEO and Chairman of Apple Inc. “I do not need a hard disk in my computer if I can get to the server faster… carrying around these non-connected computers is Byzantine by comparison.” Cloud is a cluster of servers and computers in considered as a collection of different components. A cloud data center is made up of several compute nodes, switches, network topologies, storage nodes, and front end to submit responses to the received requests (Varsha et al. 2015). Conceptually cloud services’ architecture is divided into SaaS, PaaS, and IaaS.

- SaaS (Software as a Service): it runs a list of programs on the server of the cloud, and it is usually billed to the customer in proportion to its usage. It can also be accessed anywhere by various clients via the applications present on the network.
- PaaS (Platform as a Service): it acts as an operating system and database on the cloud environment. The user generally does not have to pay separately for this service.
- IaaS (Infrastructure as a Service): the flexible infrastructure of the cloud permits the users to use all the other software services irrespective of the type of devices used.

2.1 Security issues in cloud

Although the cloud provides a multitude of advantages and vast opportunities, it does come with a baggage of some secu- rity issues which are trivial. Some of the issues related to security in the cloud are: users interact with cloud via inter- faces or application program interfaces (Varsha et al. 2015; Archer et al. 2010). Hence, the security of the cloud also depends on the overall security of the APIs. These APIs, if not protected properly, can easily be hacked and be taken advantage of by the malicious attacks. This can be prevented by implementing strong access control protocols and secure authentication. Usage of encryption is also advised. Second, the IaaS services provided in the cloud are provided via a shared infrastructure in which the access of different operat- ing systems and physical compute resources is mediated by a virtual hypervisor. Even though the hypervisor maintains security regarding the access levels of administrators, users, and guests, there have been instances when even the guests have been able to access a certain level of data well out of their range due to security loopholes. Matthew Garret, cloud company Nebula’s senior security engineer claims that—”On the balance of probabilities, you have to assume that hypervi-

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

sors probably do contain vulnerabilities, that they do contain flaws that can be exploited to gain access and allow guests to break out into the hypervisor". Furthermore, there are other major risks involved such account hijacking or data leakage.

3 Image compression in cloud

Going a step deeper into data protection, we consider the protection of images. Since images constitute of the major- ity part of everything online including cloud, it is extremely important to protect private and copyrighted images. In recent times, there is a shift towards the trend of outsourcing, i.e., saving personal images and videos on the cloud as a backup. However, this not only does not ensure security, but also gives birth to various other security issues which prove that images and data might not be completely safe on the cloud. Accord- ing to an article written by Dave Lewis in Forbes Magazine, there was a massive breach on iCloud which resulted in pri- vate celebrity photos getting leaked. Hence, images need to be protected through an efficient algorithm. The images need to be compressed first, before loading or storing to minimize storage space. Compression is a representation of an image in a minimal number of bits (Chowdhury and Khatun 2012). The compression achieved is quantified by the compression ratio given by the following formula:

$$CR = n1/n2,$$

where $n1$ and $n2$ denote, and the number of bits in original image and $n2$ denotes bits in the compressed image. In most cases, only bits carrying important information are taken into consideration. Some of the existing methods for image com- pression in cloud computing are:

1. Image compression using DWT (discrete wavelet trans- formation):

In this process, as explained in Fig. 2, the wavelets are discretely sampled. There are various steps to this pro- cess. First, the type of wavelet and the numbers of levels that it has to be decomposed into is chosen. In gen- eral, biorthogonal waves are used in image processing (Gupta and Choubey 2015). First, the wavelets and coef- ficients are obtained from a single wavelet known as the mother wavelet. These wavelets created are used and stored more efficiently than pixel blocks. This is gen- erally one dimensional, but a two-dimensional wavelet can be seen as one-dimensional wavelet along rows of a matrix. As shown in Fig. 1, the image is first decomposed into wavelets which divides the image matrix into two vertical halves in which the first half stores the average coefficients and the second half stores the detailed coef- ficients (Gupta and Choubey 2015; Shelly 2015). Even though DWT is a complex transformation, the compres- sion ratio that it provides is the highest.
Cabeen and Gent have suggested that two types of wavelets are generally used:

1. High-pass filter—high-frequency information is stored, and low frequency is let go.
2. Low-pass filter—low-frequency information is stored, and low frequency is let go of.

Major steps performed for the compression process are given in the following:

- High-pass and low-pass filter are applied to the image rowwise.
- Now, both are combined into a tuple/horizontal matrix form (say, T).
- Now, again, high pass and low pass are applied to T columnwise.
- Their output is stored in a tuple T'.

Now, the decompression process during the image retrieval or request is not the exact opposite of the com- pression process. The major steps involved are as follows:

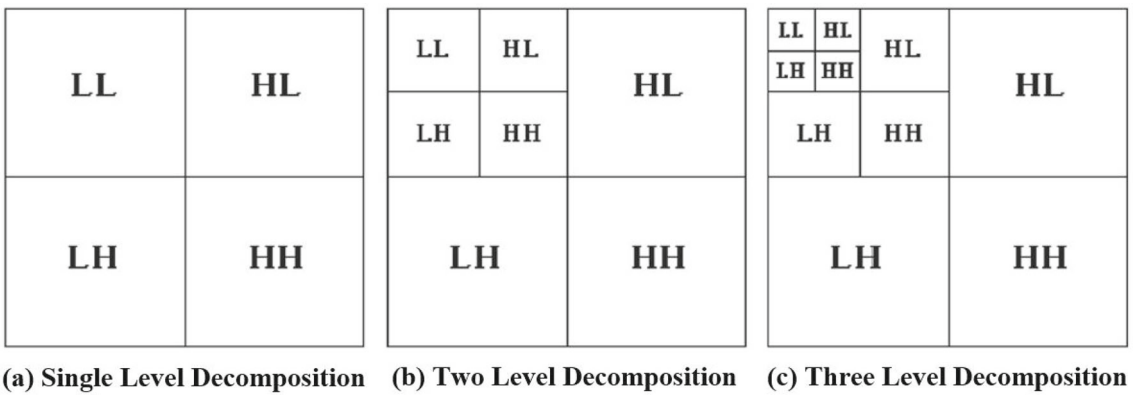

Fig. 1 Division of image matrix into wavelets after passing it through high-pass and low-pass filter

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

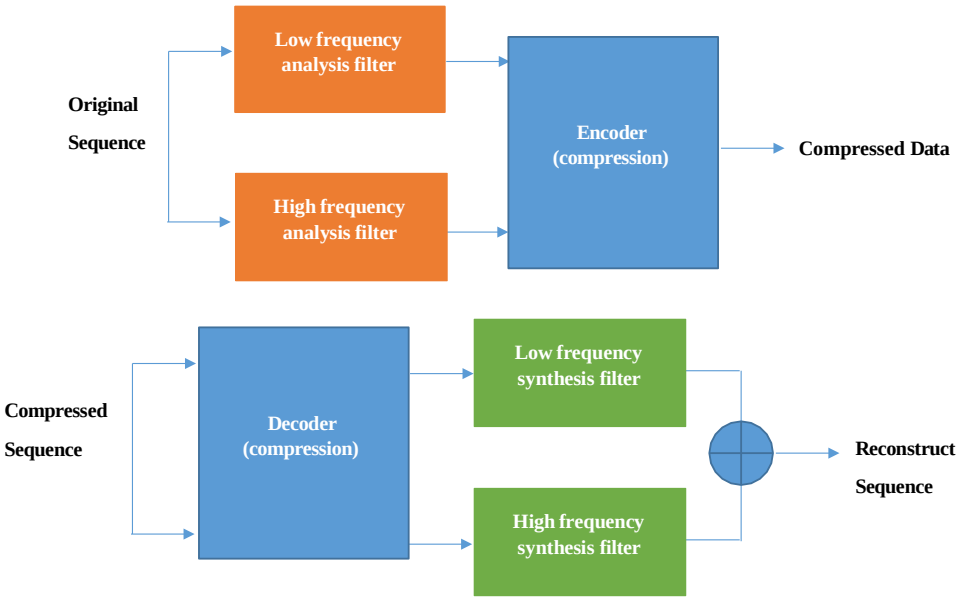

Fig. 2 Discrete wavelet transformation process on an image for compression and decompression

- The upper half of the matrix is low-pass filter, and the lower half is high pass filter, and they are extracted.
- These images are summed into a single image.
- Again, the low-pass and high-pass filtered images are extracted and separated by dividing the image vertically.
- These images are then combined and reconstructed into the original image.
- Compression using DCT (discrete cosine transform).

2. Compression using DCT (discrete cosine transform)
In this method of compression, the image is divided by different frequencies of different parts of the image. To compress an image, the parts of the image containing the less important frequencies are discarded. This step is known as quantization step. Due to its tendency to discard the unimportant frequencies, it is known as a lossy image compression method. The leftover frequencies are used to determine the image during its retrieval. The main process includes the following steps during the compression process:

- Breaking of the image into $n \times n$ blocks.
- Applying of DCT algorithm in each block.
- Quantization is applied to each block to compress them, and they are stored in dramatically less storage space.
- During retrieval, the inverse DCT procedure is applied to decompress the image.

Decoding the compressed image using DCT is the reverse process of the compression procedure. The steps for decompressing using DCT are (Katharotiya et al. 2011):

- The image is broken into $n \times n$ blocks.

Table 1 Comparison of discrete wavelet transform and discrete cosine transform: image compression and decompression methods

Method of compression	Advantages
1. DWT (discrete wavelet transform)	1. Has a larger compression ratio 2. Identifies which data is more important to human perception 3. Uses a more optimal set of functions for the sharp edges
2. DCT (discrete cosine transform)	1. Has better performance time 2. Uses coefficients optimally 3. Does not result in block-like appearance

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

- De quantization is applied on each block.
- Inverse DCT is applied to each block.
- These blocks are then combined into an image which is not a replica of the original image but is identical to it.
- The value of *n* remains constant throughout the com- pression and decompression of image.

Image compression is the first step towards the image protection, and uploading of the images needs to be accu- rate. Hence, we need to select the best method that would be compatible with our proposed biometrics encryption sys- tem. Hence, we try to compare which method would be most suitable for our cloud computing system. Table 1 will demon- strate the advantages and disadvantages of the discussed methods of image compression (Katharotiya et al. 2011).

Since we are concerned primarily with the compression ratio to minimize the storage space, the method of compres- sion in this paper is the DWT method.

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

4 Biometrics and their types

Identification of a person is the most crucial step today to minimize fraud and identity theft (Bhattacharyya et al. 2009). Hence, biometrics are used to identify an individual uniquely by comparing the original image with the data set governed by different attributes. Biometry means applying statistical analysis on biological data. Biometrics classification is shown in Fig. 3. It is a computerized method of identifying a person by any of these two characteristics—physiological or behavior (Alsaadi 2015).

Such systems comprise four stepped modules including a sensor, feature extraction, matching, and decision making. As shown in Fig. 4, biometrics authentication and identification is done of three steps.

4.1 Fingerprint

Fingerprints are the most important and unique thing, the ridges which help people to hold things. These get developed until the 7th months in the womb. Those ridges of twins are also unique, and there is also a very small possibility that any two people in the world can have those same. As they are unique, they are used as a tool for authentication. In addition, as stated in Table 5, its results are also of high accuracy.

In cloud computing, a large amount of important data are stored which is to be accessed by the owner of data only, so Fingerprint sensors are used greatly in specifically biometric authentication in cloud computing. This is divided into two parts. It is, as a matter of fact, computerized matching of two people (Batool et al. 2015). In addition, some algorithms are fixed with fingerprints scanner like, it can measure the distance between minutiae (splitting of ridges into two) which is also unique. It also depends on finger's state, because those scanners are not able to scan them properly many a times when fingers are moist or greased. Government organizations and international schools also rely on this for the attendance of staff and students. In addition, nearly, 67% smartphones embedded fingerprint scanner worldwide. Therefore, this system is useful till the user's fingerprints are not damaged. Once damaged, they are useless.

4.2 Retina

A person's retina is scanned by a retina scanner in which the retina blood vessels are scanned. As it is unique as well as unchanging characteristics, the retina is seemingly dependable and maximum precise biometric (Abdullah and Aziz 2016). The infrared light with minimal energy is cast on a person's eye, because blood vessels in the retina can absorb

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

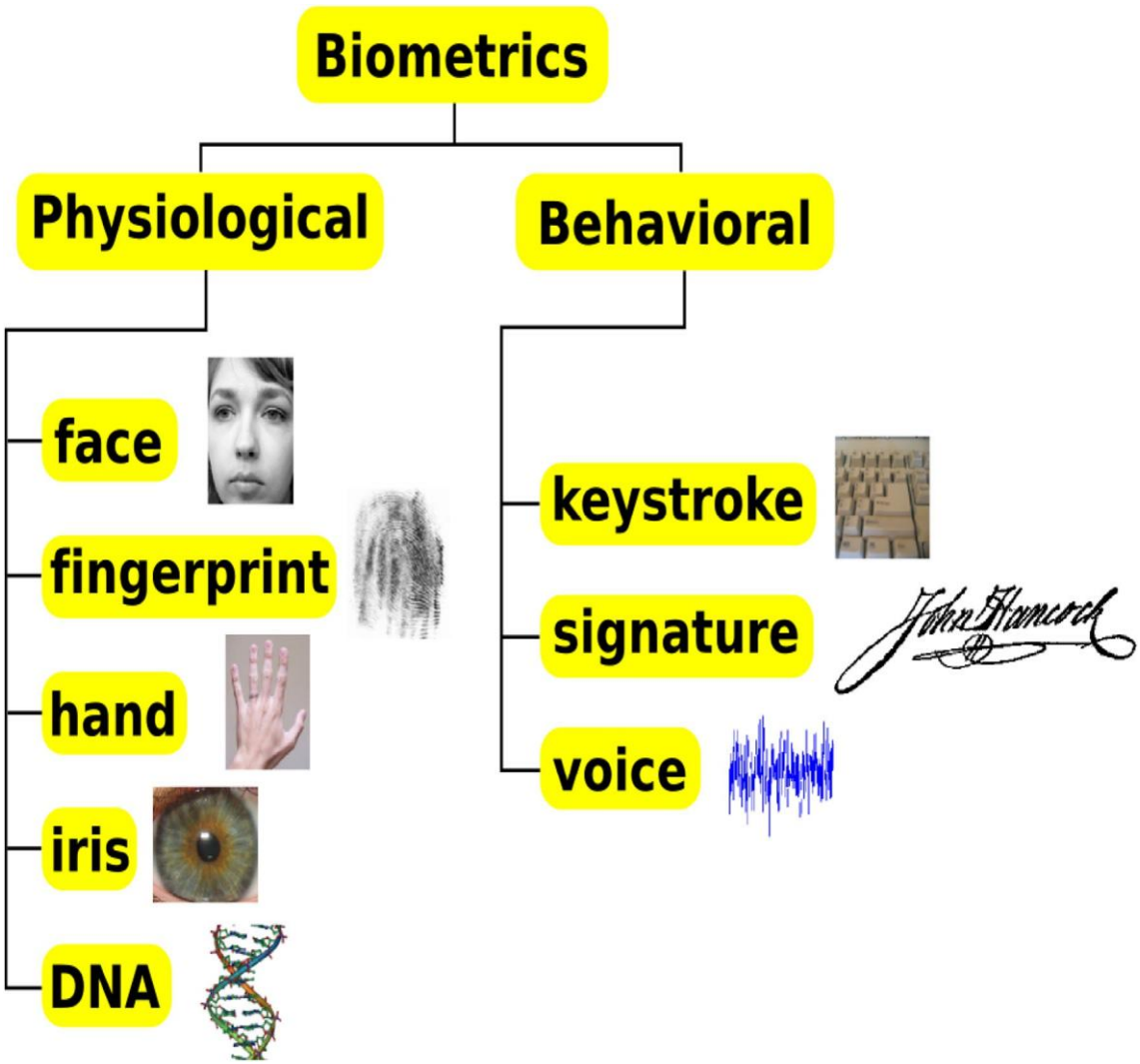

Fig. 3 Major biometrics classification on the basis of physiological and behavioral traits for biometric authentication

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

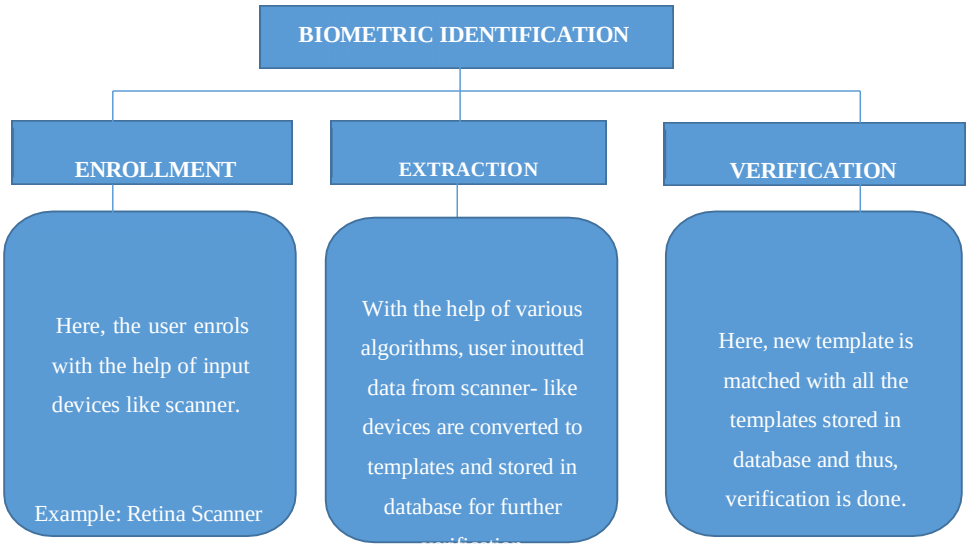

Fig. 4 Steps included in thorough process of biometric authentication and identification

them and a retinal image is captured. It will not allow the user to either enrol or verify until the retinal image is not captured qualitatively. Due to this reason, a situation arises, where a user needs to try three-to-four times for verification, as the retinal image is not clicked properly for cross-checking into a database, where these data are stored in a coded format. Blood vessels in the retina are the most important thing here, plus they are so complicated that even twins cannot possess identical blood vessels. Once scanned, it just takes a fraction of a second to verify a user. However, due to certain diseases such as cataract, retina scanner is unable to verify the per- fectly valid user, and this is one of the major drawbacks. This technique is used for high-level military applications, and in many government organizations and, therefore, as shown in Table 5, it is less acceptable socially.

4.3 Face recognition

Facial recognition is one of the latest technologies used for security issues. Woodrow Bledsoe first developed the first system of face recognition in 1960. The working of the face recognition system is divided into the following steps:

1. *Enrolment:* here, in this step, the user stands two feet from the digital camera and then according to the sys- tem, that is, in 2D systems, the face is scanned directly, while in 3D systems, the live video is captured and then converted into a 2D image by digital camera.
2. *Extraction*: in this step, unique features are extracted to create a template and stored in the database. Each human face has unique nodal points, and they are nearly 80 per person. They could be anything such as distance from one eye to another, nose's width, jaw line's length, cheekbones' shape, and many more. Complexion is also checked off a user (Al-hamami and Al-juneidi 2015). Many algorithms work simultaneously to extract these data, and from these data, a numerical code is created known as face print which represents face in the database.
3. *Comparison:* here, in this step, new template is compared with data stored in a database.
4. *Matching:* person stands at two feet distance, his tem- plate is compared with the database, and then, if the template matches any data in the database, then he is allowed further otherwise not. Decision-taking time for the system is nearly 5 s. Many a time person has to reat- tempt after moving and getting perfectly in the frame.

There is another system added known as surface texture analysis in which a photo is captured of a skin patch, and it is divided into smaller ones. With the use of some interesting algorithms, these patches are converted to mathematical and measurable space with the help of which difference, even between twins can be recognized. Using this, 20–25% accu- racy is increased. It is mostly used to avert terrorist activity. It is also used to identify a criminal from a large crowd and also to check the criminal status of a person. Thus, it has used in the verification process, attendance systems, and activity logs, in bank tellers (automated), railway stations, airports, financial institutions, government offices, stadiums, and many such places. This technology is cheap, and the response is also very quick (Kim et al. 2012) (Table 2).

4.4 Hand geometry

Hand geometry is the oldest biometric identification system which measures dimensions of a person's hand, creates a

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

Table 2 Literature work on face recognition in biometric

authentication Sr. no.	Developments
1	A simple face recognition technique was proposed in Pawle and Pawar (2013) which checks username with image of face
2	In addition, face recognition by implementation and application of Eigenface and REST concept, respectively, was proposed in Siregar et al. (2018)
3	A system of face recognition, using PCA-characterized instances and in which invariant points of SIFT are reduced was showcased in Kisku and Rana (2016)
4	In Deshpande and Ravishankar (2017), a system working in two stages out of which, in first stage, human face is detected in the image using algorithm violaJones and in second one, detected face is recognized using mixture of PCA and FFNN

Table 3 Literature work on hand geometry along in biometric authen- tication

Sr. no.	Developments
1	A system using hand contour matching was proposed in Rathi and Dubey (2013) in which Euclidian distance was used to measure various distances in hand from specific point
2	Along with traditional methods, a method with merits such as mutual authentication, secure password changeability, user anonymity, and revocation was proposed in Yassin et al. (2016a, b)
3	Weakness of Xu-Zhu-Feng scheme along with a new and more secure method is presented in Wangsuk and Amornkul (2013)
4	On the basis of dissolution of two models-vascular pattern and hand geometry, a new method which measures hand's side view thickness is prepared in Yassin et al. ((2016a, b). It is based on K-curvature and VPE

template, stores that in the database, and uses that data in the verification process. However, as hand geometry is not always unique, other biometric identification systems were comparatively used more. In this system, a camera is used to capture outlines of hand. The user places palm with down- ward position and data are captured by charge-coupled device along with top and side views using an angled mirror. Thus, in this process, analysis of nearly 31,000 points of hand is done and measurements of 90 things such as knuckles' dis- tance, fingers' length and thickness, and many more. These data are stored in a database with minimal memory storage. Thus, three images are taken sequentially; the template is created and compared with a database for the verification process. Its major advantage is that environment does not have any effect on the results. This system, for a medium range of people, has shown success 97 times and errors 10 times out of 100. In 1996, the Olympic games used hand geometry recognition to protect access to the Olympic vil-

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

lage. In addition, many institutes and companies collaborated it with time to make attendance system. Some literature work in this field is shown in Table 3.

4.5 Iris

Iris scanning is one of the most used biometric identifica- tion methods in which person's iris' images are computed with the help of mathematical techniques of pattern recogni- tion. Iris' structure does not change, and they are unique as well. In addition, detailed images are produced, because in this technique, infrared illumination is used which shows its complete structure. Initially, a person's iris is scanned with the help of iris scanner, and then, after computing it with statistical as well as mathematical algorithms, the unique dig- ital template in encoded form is generated and stored in the database. Thus, a person is enrolled. Then, matcher engines search the database consisting of plenty of templates and try to find the one matching the newly scanned template. Matcher engine searches the database with the speed of mil- lions of templates per second. Moreover, the error rate is also very less. According to NIST, the accuracy of iris recognition systems is 90–99%.

As stated in Table 5, since iris is unique, accuracy of this method is high. In addition, a user has to just stand at a nor- mal distance from the camera, and the whole process is done within seconds. This process is similar to taking a casual photograph. Some people use the lens, but that does not act as an obstacle for the scanner, and results are not affected. However, if a reflection occurs by any case, the iris scanner is not able to scan properly, and thus, the result gets affected. In addition, as there is the use of infrared light, Iris can get harmed by its more and more usage. Template consumes much memory. As pupil changes its size, non-elastic defor- mation of iris takes place which is a major drawback. This device is very expensive. Many a time, it happens that the iris is blocked by eyelids because of blinking, and thus, scanning is not done properly. Due to its small size, iris should be near to the scanner for proper images to be captured by dig- ital camera. In addition, verification of iris is done in light medium, because actions of iris are dynamic in light (Desh- pande 2015). Many times, it happens that due to contact lens or glasses, iris design is darkened (Delac and Grgic 2004).

4.6 Keystroke

The keystroke is the technology used in biometric identi- fication in which a person needs to type something in the keyboard, and from that, a template is created for further ver- ification. Such characteristics are unique. It is a subclass of major behavioral class. Many right-handed people are com- fortable in typing the letters focused on the right side in the keyboard, and it usually takes time for them to type letters

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

Table 4 Literature work on keystroke in biometric authentication

Sr. no.	Developments
1	A system proposed in Monrose and Rubin (2000) analyzes rhythm patterns which are habitual for a specific user
2	In Teh et al. (2013) a detailed survey of various keystroke authentication methods is given
3	In Patil and Renke (2016) another system which stores additional timing information in database along with dwell and flight time was proposed
4	In Chen and Zhao (2012) Keystroke dynamics method of authentication is proposed in which username typing behavior is verified using trajectory dissimilarity

on the opposite side. People also have weakness in finding some letters, and therefore, this consumes time. In addition, the key pressing and leaving time are also different. The speed of typing also plays a major role in the enrolment process. Some people, instead of pressing one specific key, always press another key which is also observed and the template is created accordingly. Therefore, here, two main things are calculated without failure that is dwell time and flight time. Dwell time is the duration of the key pressed by a person, while the flight time is the duration between after leaving a key and pressing the next key. In other words, its duration is between different keystrokes.

The keystroke is completely based on software, and there is no requirement of any sensor at all (Kalyani 2017). In addition, when the keystroke is combined with PIN or password-type authentication, then, its results are good compared to just keystroke-based authentication. However, physiological characteristics of biometrics are more preferred than such behavioral characteristics, because along with these advantages, there are many such disadvantages which cannot be ignored. Some literature work in this field is stated in Table 4.

4.7 Signature

Signature scanning is a type of biometric identification system in which the signature of a person is taken by any of the two ways. First, which is also known as 'offline' system, the signature of a person is taken on paper, and then, this signature is digitized with the help of a camera or a scanner. This signature is recognized by its shape. While in a second way, the signature of a person is taken digitally with the help of tablet or PDAs or smartphones. This is also known as 'online' method. Signature scanning comes under behavioral characteristics of biometrics. In this method, various characteristics which identify a person uniquely such as stroke, pressure, speed, acceleration, and curvature are measured in X, Y, and Z paths. X and Y are used to measure velocity and acceleration and Z measures respective pressure. These characteristics are nearly impossible to replicate. Using the clustering method, signature recognition shows the accuracy of 70%, but it majorly depends on the technique used to recognize signature (Suryani et al. 2017). In addition, it is instant, easy to use, easily integrated with other systems and inexpensive. In addition, this type of identification is universally accepted. Banks, credit cards, and checks have major use of signature for authentication. However, as detailed in Table 5, this method requires many devices such as optic pen and touch panel.

4.8 Table of comparison of biometrics

5 Encryption and decryption

Encryption means converting data into an unreadable format by any method. This plays a major role in cryptography. Encryption, as well as decryption, are used by it. Cryptography provides authentication, integrity, and confidentiality (Abdullah and Aziz 2016). Encryption has two categories which are symmetric and public key encryption. The same key is used in symmetric encryption for encrypting and decrypting in symmetric, while different keys are used for encrypting and decrypting messages in public key kind (Dongare et al. 2017; Patterson and Hennessy 1994; Vaudenay 1996).

Even after ensuring safe and secure storage and access methods of biometrics in cloud architecture, the database in which the information of biometrics is stored has to be

Table 5 Comparison of biometric characteristics on the basis of different performance parameters

Biometric technology	Accuracy	Cost	Devices required	Social acceptability
DNA	High	High	Test equipment	Low
Iris recognition	High	High	Camera	Medium–low
Retinal Scan	High	High	Camera	Low
Facial recognition	Medium–low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hard geometry	Medium–low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature recognition	Low	Medium	Optic pen, touch panel	High

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

protected from outside attackers. Various risks involved in the database are:

- privilege abuse by the users to gain access to data other than what they are authorized to access;
- SQL injection to send unauthorized queries to access the database;
- denial of service to the users by network flooding, tamper- ing with the access codes or excessive resource consump- tion.
- Even if the database has a backup, there have been cases, where even backup tapes and hard disks have been com- promised.

Even though there are these vulnerabilities associated with the database, the encryption technique will minimize the threats associated with it. Some of the encryption techniques are given in the following.

5.1 Homomorphic encryption

Specific biometric characteristics of the client are taken and are asked to generate two keys, public, and secret keys. Secret key will be used to encrypt the plain text into cipher text. The public key will be used by the server to compute on this cipher text using any specific function. These encrypted data can be decrypted by the client just using a secret key, and the client will get original data (Parmar et al. 2014).

In Yang et al. (2017), a homomorphic encryption algo- rithm is proposed in which both additions, as well as multiplication operations, can be used on floating num- bers. Before uploading an image in the cloud, the image is encrypted and then stored in the server, because if any- one gets access to the stored image, it would still be in an encrypted form so. Thus, whenever a user wants to access that image, it is only decrypted using that key used to encrypt in homomorphic encryption.

5.2 Biometric inspired homomorphic encryption algorithm

Homomorphic encryption works as a base for BIHEA. Here, it works as follows:

m1 and m2 be the two messages, and E(x) be a function for encryption. c1 and c2 will be two cipher texts produced after applying E(x) on plain texts m1 and m2:

$c1 = E(m1)$

$c2 = E(m2)$.

After c1 and c2 are produced, arithmetic operations are done on them, and encrypted data are produced. Thus, here, operations are done on cipher text, and in decryption process, the key is applied only on the decrypted data, and the plain message will be displayed, no two-level decryption in which initially encrypted data are decrypted to cipher, and then, again, the same process is applied to get a plain text message. In BIHEA, as proposed in Bala and Malik (2018), user's iris is scanned in iris scanner. Iris scanner is because they are a unique characteristic of a person. The fovea is a kind of pit which is captured in retina image. Initially, the image is taken in RGB and then converted to grey scale image. Therefore, from scanning, it is pre-processing, key features are extracted, and from that, an OTP is generated of vary- ing length. Every time, new OTP is generated, and hence, every time, a user has to go through this process. The encryp- tion and decryption are done with the help of homomorphic encryption only.

Input iris image → image pre-processed → features extracted →OTP generated →(key passed) → data encrypted/decrypted

5.3 Advanced encryption standard

AES works as follows:

Cryptographic transformations take place by key size. 128, 192, and 256 bits are key sizes and ciphers are of the 128- bit block size. In addition, cryptographic transformations are repeated various times based on the key selection. For 128, 192, and 256 bits, 10, 12, and 14 rounds of transformations are performed, respectively. In Maraghy et al. (2013), the AES-128 algorithm is used for of area as well as a speed optimization.

As proposed in Ghoradkar and Shinde (2015), the AES encryption algorithm is divided into four steps:

(i) *SubstituteBytes:* here, there is a substitution table which is pre-calculated only once called S-box. It has 256 numbers as in 0–255 and corresponding values. There- fore, every state bytes are substituted non-linearly using this S-box in SubstituteBytes step.

(ii) *ShiftRow:* in this step, the process of shifting of bytes in a row is done. However, the bytes of zeroth row remain unchanged. First row shifts left by one byte, second by two, and so on.

(iii) *MixColumns:* here, columns of state, i.e., of block, are considered to be polynomial of $GF(2^8)$. In addition, product of this and modulo $x^4 + 1$ [with c(x), which is fixed polynomial] is done, where

$$c(x) = \{03\} + \{01\} + \{01\}x + \{02\}.$$

(iv) A*ddRoundKey:* a round key is calculated from main key with the help of key expansion. This is XORed with the result of MixColumns in this step.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

AES decryption is again divided into four steps:

(i) *AddRoundKey*: as XOR is its inverse function only, the same step AddRoundKey of encryption is repeated.
(ii) *InverseShiftRow:* here, this step is exactly inverse of ShiftRow. The bytes of the rows are shifted in the oppo- site direction, but zeroth row remains unchanged.
(iii) *InverseSubstituteByte:* here, there is a substitution table which is pre-calculated only once called InvS box. It has 256 numbers as in 0–255 and corresponding values.
(iv) *InverseMixColumns:* polynomials with a degree not more than three over GF(2^8) of which the coefficients are elements present in state's columns, reduce modulo ($x4 + 1$) and then multiply by $d(x)$ (a polynomial which is fixed). $d(x) = \{0B\}x3 + \{0D\}x2 + \{09\}x + \{0E\}$, where {0B}, {0D}; {09}, {0E} denote hexadecimal values.

5.4 Quantum cryptography

The algorithm proposed in Singh et al. (2018) is given in the following:

(a) The image is divided by blocks with equal size.
(b) Each block is divided by the frequency band.
(c) Random exchange of pixels is performed with neigh- bour ones.
(d) With the help of modulus concept, the sub-blocks of each block are encrypted.
(e) Every sub-block is conjugated, and a complete block is created.
(f) Again, the random exchange of pixels is performed with neighbour ones.
(g) Encryption is performed using modulus function.
(h) Repeat these steps in reverse order, i.e., (g–a), and the original image is produced.

5.5 Blowfish algorithm

Blowfish is a block cipher kind of encryption which uses the same key for encryption as well as decryption (Valmik and Kshirsagar 2014). Here, key length is varying in 32–448 bits. In this method, the message is broken down to fixed length blocks of 64 bits.

The whole process includes two steps:

1. The first step is key expansion in which inputted key gets expanded into an array of sub keys of 4168 bytes in total. P array, containing 18 boxes of 32-bit length, is there along with S boxes consisting of four arrays of 32 bits and each of these arrays comprised of 256 entries. Therefore, P and S boxes are initialised first. After this, XOR oper- ation is performed between key's starting 32 bits and P1. Similarly, another same operation is performed between key's next 32 bits and P2, and this goes on until P and is XORed completely. Moreover, if the key is shorter, again, the same key is taken from starting, and the same operation goes on with the next element of P.
2. Now, comes the second step, encryption. All the zero strings are encrypted using this algorithm with the help of P array which we just modified. Hence, we get a block of 64 bits. Now, P1 is replaced with first 32 bits which we get in output and P2 with next 32 bits. This, the 64-bit output is given as input to blowfish cipher form which we get a new block of 64 bits. The next values of P array are replaced with this block. This is repeated for every value in P array as well as the S boxes. Hence, data are encrypted. In Shelly (2015), usage of compression of the image for fast transfer, similarly for security, encryption, and also blurring of that image is done.

5.6 Hybrid of blowfish and SHA

In this method, we use a combination of both blowfish and Secure Hash Algorithm (SHA) algorithms. Here, the SHA is used for calculating a hash value of images uploaded on the cloud framework and blowfish is used to encrypt and decrypt the binary form of the image. The following method is proposed in Gore et al. (2016) and is described in Fig. 5:

1. SHA algorithm takes an image and calculates the hash value of that image by converting the image into a matrix form having binary values. This matrix is then stored in a temporary file. This file is then passed as a parameter in the SHA algorithm.
2. On that file, blowfish encryption algorithm is applied, and the encrypted file is then split into three equal sized chunks. For these chunks, the hash value is calculated using SHA algorithms. These chunks are then stored on the cloud framework corresponding to their hash values. The cloud server will maintain the hash table of each chunk.
3. When a user wants to access or download the image, cor- responding chunks are located, and new hash values are calculated which are then compared to the old hash val- ues. If both values are identical, the chunks are combined to form a temporary file.
4. Now, the encrypted file is then decrypted using the blow- fish algorithm. New SHA value is calculated and is compared to the old SHA value. If a match occurs, the decrypted image is then fetched to give access to the user by converting the binary file into the matrix and then subsequently converting it into its original form.

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

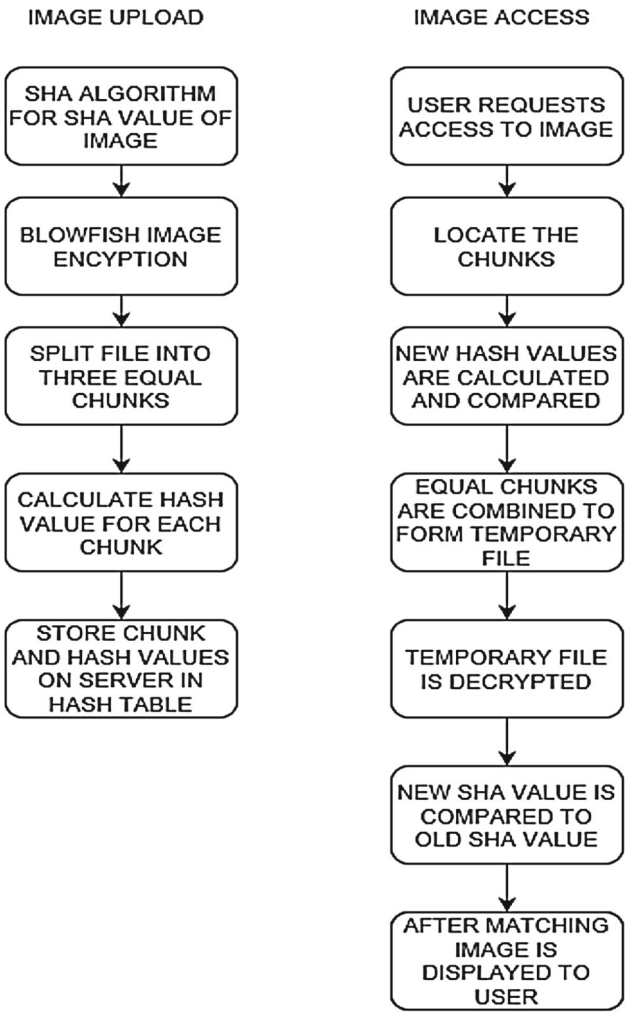

Fig. 5 Flowchart describing image upload and access process using hybrid encryption method of blowfish and SHA

5.7 Security-as-a-service

In this method, pixels of the image are separated to individ- ual red, green, and blue coloured bands (Mahalakshmi and Kuppusamy 2016). Each coloured bands are separated from that image. These image pixels are converted to binary for- mat. This binary sequence is stored in a matrix for red, green, and blue bands individually as 8 × 8 blocks. Now, the initial- ization vector is set using the binary input of 8-bit length. After this, cipher block chaining mode is followed. Key is generated as a result of the previous step. It is XORed with the original matrix. Similarly, the second key matrix K is to be computed, where the input of size 8-bit is given as any random number. XOR operation is performed on bands of those three colours with K. Hence, modified binary sequence is generated, as intended. Finally, all these individual bands are combined. These steps are repeated until all pixels are encrypted.

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

5.8 RSA algorithm

As proposed in Deen et al. (2014), two prime numbers, p and q, which are distinct and large are chosen, and $n = pq$ called public modulus is calculated. Similarly, e (public exponent) is chosen in a way that it should be coprime to $(p - 1)$ (q$-$ 1) and $1 < e < (p - 1)$ $(q - 1)$. Hence, we got the public key as a pair (n, e). Private key is unique integer d, such that $1 < d < (p - 1)$ $(q - 1)$ and ed $=$ 1 mod $(p - 1)$ $(q - 1)$. Encryp- tion is processed by splitting the message into blocks as M1, M2,…Mt and Mi should satisfy $0 \leq$ Mi $< n$. Encryption and decryption are done by the equations, as given in Deen et al. (2014). The decryption key is of the form (d, n). The code is implemented on MATLAB simulating RSA algorithm by the author. RSA algorithm is used by the author on images.

6 Middle man attack

Even after encryption, there is still a possible threat of man- in-the-middle attack. In this case, the intruder secretly relays and changes the communication between two entities. All the cloud users should be provided with a level of security and securing and this would ensure a certain level of privacy amongst the users. One of the methods to ensure security from this type of attack is the usage of secure sockets layer (SSL) (Shubh and Sharma 2016). It is a standard encryption link between a client and the server which consists of three protocols:

- *Handshake protocol:* it is used to establish a secure connec- tion between client and server using common parameters that both have agreed upon.
- *Record protocol:* this protocol encrypts the data that have to be sent through the network via the key that is exchanged during the handshake protocol.
- *Alert protocol:* this is generally used to send mainstream messages to the users and the system whenever any error is detected.

7 Proposed cloud structure using a case study

Nowadays, social media are widely used. Along with this, lots of images are captured and uploaded on this platform. Therefore, image privacy and protection is of crucial impor- tance currently. Similarly, in cloud-computing image, privacy is at most needed. We also know that biometric characteris- tics are the unique characteristics of a person. Therefore, in this paper, we have used biometric characteristics of a person for image protection in cloud computing.

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

7.1 Synopsis and findings

The images stored on the cloud have a different approach than the data stored, as the security of images is far more threatened than that of the data stored. Hence, after consid- ering all approaches for biometrics, the optimal method of biometric authentication has been explained using an exam- ple idea (Tiwari and Saklani 2013). The following steps are mainly involved in this idea:

1. Consider any IaaS cloud provider (e.g., Google Cloud or Microsoft Azure) in which pay-as-you-go services are provided to its registered user. Our user, a layman is reg- istered on this cloud infrastructure and has a bunch of private photos to upload on the cloud. The user uploads the photos on cloud framework via his mobile device, and the photos are to be saved on the network.
2. Next is the biometric authentication. After uploading images, the user's iris scan takes place. The iris is the dark ring that controls the aperture of the pupil. The colour of the iris is determined by genetics, and even though the colour could be same, the difference in arrangement of ligament patterns is what makes it so unique that the odds of two irises being same are almost negligi- ble (Kaware and Yadav 2016). Now, the dynamic eye image is captured using a scanning device such as the CCD camera and segmentation is performed, i.e., the iris region is located. After successful segmentation, normal- ization is performed, where the image is divided into fixed dimensions for pattern matching. Then, the impor- tant features are extracted from the image using Gabor and wavelet transformations. Next step, pattern matching of these extracted features is done using Manhattan Dis- tance which requires minimum computation as compared to other computation methods. Consider the following distance as the maximum distance between the trained image that is the image stored in the database and test- ing image (say D), which when is less than Manhattan distance; the person is authorized. Moreover, it is greater than or equal to Manhattan distance; the person is unau- thorized.
3. Uploaded image is to be compressed to minimize the cloud storage space for the database. For the compression of the image, in this example, we take up the method of DWT (discrete wavelet transform). The compression ratio of this method is higher than the DCT method and hence would be more efficient when the size of data is huge (Cabeen and Gent 2019).
4. After compression of the image, it has to be encrypted before storing it on the server database. The hybrid encryption algorithm is used in this case, as it has capabil- ities to provide a better level of security. The compressed image is converted into a binary matrix which is stored on a temporary file. This, the file is passed inside of the SHA algorithm, is used to find SHA value of compressed image file, followed by the Blowfish algorithm used to encrypt the file. In this, the file is split into three equal chunks, and hash values for each chunk are calculated. Those chunks, along with their hash values, a form of hash table are stored in the database.
5. When the user requests to access the image from the database, again, the real-time biometrics scan takes place by scanning the iris and comparing it with the template biometrics in the database. After successful authenti- cation, the image is retrieved and decrypted from the database also using the hybrid SHA and Blowfish algo- rithm. The image is then decompressed using the DWT algorithm and then displayed to the user.
6. Whenever another user wants to access this image, the actual user has the OTP, data are decrypted, to com- pressed form using Blowfish decryption and is decom- pressed using DWT decompression method and made available to the user.
7. Whenever a use of the *r* wants to access another cloud user's data, the request is sent to a cloud server. Cloud server sends the user encrypted data. If a user has the same OTP used for encryption, he can decrypt it. Clearly, he can access data, but if not, the user is not able to access that data (Fig. 6).

8 Alternatives

Various methods such as a DCT compression method for image compression, AES, and RSA encryption methods for image encryption and decryption were available individually for biometrics authentication, image processing, encryption, and decryption. However, we scrutinized best from bio- metrics and encryption methods and used them for image protection for real-time cloud framework.

9 Conclusion

Many studies and research papers have analyzed the con- cept of security of images on cloud based on confidentiality, integrity, and availability. In this paper, a method of biomet- rics authentication coupled with image encryption to ensure that the security of images on the cloud architecture is pro- posed. Numerous amounts of attacks everyday conclude to the fact that private images require special attention than the data on the cloud as compared to the other forms of data. Biometrics have been on rising as an authentication process to authorize the user and set some permission checks to not allow authorization to any other entity. If the procedure of authorization itself is made strong and faultless, then the

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

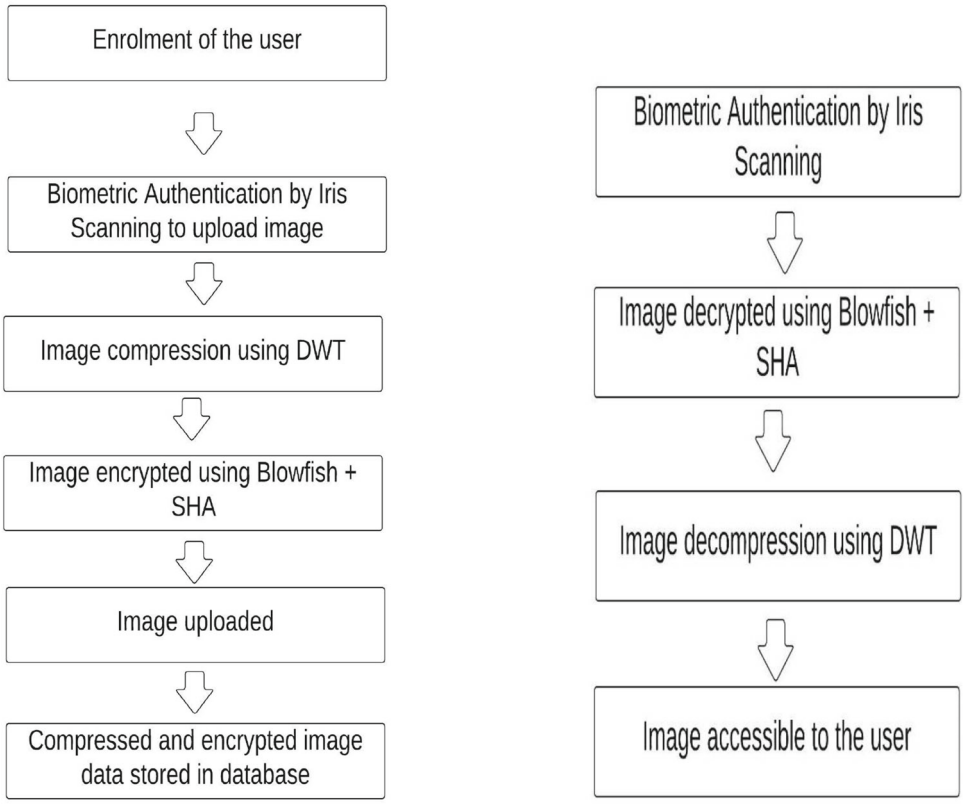

Fig. 6 Proposed process of image upload and access on cloud framework using biometric authentication and hybrid image encryption

level of security of the overall system increases. Successive steps such as compression and encryption of images get an extra level of reliability. Most modern systems have a bio- metrics scanner embedded inside of them especially when taken into consideration the iris recognition. In this paper, we have selected iris as the biometric used for the authenti- cation as most smartphones and laptops already have an iris scanner inside of them and also the chances of two peoples' iris being the same are very thin. After the image is queued for upload or access by the user, the machine will scan the iris of the user, compare it with its database image, and then authorize the user to upload or access the image. The type of hybrid algorithm proposed has proven to be highly effective regarding security as well as compatibility with the image format. Like every method, biometric authentication does have its disadvantages such as high false acceptance rates, increased cost and delay and scanning difficulty due to envi- ronmental or technical factors. Biometrics is a double-edged sword and also provides a level of security that most fellow methods cannot provide due to its scalability and versatility. The future of cloud platform must contain this bandwagon of advanced biometric technology for a hassle-free ride for its users. Our future work includes enhancement of this algo- rithm, followed up by research in this field and analyzing the thesis and algorithm based upon the experimental results and bringing detailed solutions. These solutions will lead to increased cloud usage as well user trust in upcoming years.

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

One of the aims of future research would be to put forth an algorithm which is more efficient in terms of space and time complexity. This would lead to an efficient and trustable cloud network that not only would be user friendly but also fast and cost-effective.

Acknowledgements The authors are grateful to School of Technology, Pandit Deendayal Petroleum University and Vishwakarma Government Engineering College for the permission to publish this research.

Author contributions All the authors make substantial contribution in this manuscript. VK, MP and MS participated in drafting the manuscript. VK and MP wrote the main manuscript, all the authors discussed the results and implication on the manuscript at all stages.

Availability of data and material All relevant data and material are presented in the main paper.

Compliance with ethical standards

Conflict of interest The authors declare that they have no competing interests.

References

Abdullah AM, Aziz RHH (2016) New approaches to encrypt and decrypt data in image using cryptography and steganography algo- rithm. Int J Comput Appl 143(4):11–17

Al-hamami AH, Al-juneidi JY (2015) Secure mobile cloud comput- ing based-on fingerprint. World Comput Sci Inform Technol J 5(2):23–27

Alsaadi IM (2015) Physiological biometric authentication systems, advantages, disadvantages and future development: a review. Int J Sci Technol Res 4(12):285–289

Archer J, Cullinane D, Puhlmann N, Boehme A, Kurtz P, Reavis J (2010) Top Threats to cloud computing V1.0. Cloud Security Alliance. pp 1–14

Bala Y, Malik A (2018) Biometric inspired homomorphic encryption algorithm for secured cloud computing. In: Panigrahi B, Hoda M, Sharma V, Goel S (eds) Nature inspired computing. Advances in intelligent systems and computing, vol 652. Springer, Singapore, pp 13–21

Batool R, Naveed G, Khan A (2015) Biometric authentication in cloud computing. Int J Comput Appl 129(11):6–9

Bhansali A, Barot H, Masrani K, Shah S, Chheda V (2013) Encrypting watermarked images: a transparent approach. Int J Future Comput Commun 2(6):665–667

Bhattacharyya D, Ranjan R, Alisherov F, Choi M (2009) Biomet- ric authentication: a review. Int J u- and e- Serv Sci Technol 2(3):13–28

Bothe S, Jadhao RM, Shinde S (2012) Cloud computing based image processing applications for agro informatics using 'self learning system' approach. In: Proceedings of AIPA, pp 1–4

Cabeen K, Gent P (2019) Image compression and the discrete cosine transform. Math 45, pp 1–11 (unpublished report)

Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing. In: Proceeding of the International Conference on Computer Science and Electronics Engineering, pp 647–651

Chnag CC, Hwang MS, Chen TS (2001) A new encryption algorithm for image cryptosystems. J Syst Softw 58:83–91

Chowdhury MMH, Khatun A (2012) Image compression using discrete wavelet transform. Int J Comput Sci 9(4):327–330

Deen AETE, El-Badawy ESA, Gobran SN (2014) Digital image encryption based on RSA algorithm. IOSR J Electron Commun Eng 9(1):69–73

Delac K, Grgic M (2004) A survey of biometric recognition meth- ods. In: 46th International Symposium Electronics in Marine, pp 184–193

Deshpande SD (2015) Advances in computational research review paper on introduction of various biometric areas. Adv Comput Res 7(1):212–214

Deshpande NT, Ravishankar S (2017) Face detection and recognition using Viola-Jones algorithm and fusion of PCA and ANN. Adv Comput Sci Technol 10(5):1173–1189

Dongare AS, Alvi AS, Tarbani NM (2017) An efficient technique for image encryption and decryption for secured multimedia applica- tion. Int Res J Eng Technol 4(4):3186–3190

Duarte T, Piementao JP, Sousa P, Onofre S (2016) Biometric access con- trol systems: a review on technologies to improve their efficiency. In: Power Electronics and Motion Control Conference (PEMC), IEEE, pp 795–800

Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurc Chaos 8(6):125901284

Ghoradkar S, Shinde A (2015) Review on image encryption and decryp- tion using AES algorithm. Int J Comput Appl 11–13

Gore A, Meena SS, Purohit P (2016) Hybrid cryptosystem using mod- ified blowfish algorithm and SHA algorithm on public cloud. Int J Comput Appl 155(3):6–10

Guan ZH, Huang FJ, Guan WJ (2005) Chaos-based image encryption algorithm. Phys Lett A 346(1–3):153–157

Gupta D, Choubey S (2015) Discrete wavelet transform for image pro- cessing. Int J Emerg Technol Adv Eng 4(3):598–602

Hsu CY, Lu CS, Pei SC (2011) Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction. SPIE-IS&T/ 7880:1–17

Huang D, Shan C, Ardabilian M, Wang Y, Chen L (2011) Local binary patterns and its application to facial image analysis: a survey. IEEE Trans Syst Man Cyberns Part C Appl Rev 41(6):765–781

Kalyani C (2017) Various biometric authentication techniques: a review. J Biom Biostat 8(5):1–5

Katharotiya A, Patel S, Goyani M (2011) Comparative analysis between DCT & DWT techniques of image compression. J Inform Eng Appl 1(2):9–18

Kaware PC, Yadav DM (2016) Iris recognition for mobile security. Int Res J Eng Technol 3(6):2000–2005

Kim MG, Moon HM, Chung Y, Pan SB (2012) A survey and proposed framework on the soft biometrics technique for human identifica- tion in intelligent video surveillance system. J Biomed Biotechnol 2012:1–7

Kisku DR, Rana S (2016) Multithread face recognition in cloud. J Sens. https://doi.org/10.1155/2016/2575904

Madhu B, Holi G, Murthy SK (2016) An overview of image security techniques. Int J Comp Appl 154(6):37–46

Mahalakshmi J, Kuppusamy K (2016) An efficient image encryption method based on improved cipher block chaining in cloud com- puting as a security service. Aust J Basic Appl Sci 10(2):297–306 Mannapur SJ, Raj S, Kumar S, Kiran B (2018) IoT based home security through image processing algorithms. Int J Adv Res Ideas Innov Technol 4(3):1598–1602

Maraghy ME, Hesham S, Ghany MAAE (2013) Real-time efficient FPGA implementation of AES algorithm. In: IEEE International SOC Conference (SOCC), pp 203–208

Monrose F, Rubin AD (2000) Keystroke dynamics as a biometric for authentication. Future Gener Comput Syst 16:351–359

Murty MS, Veeraiah D, Rao AS (2011) Digital signature and watermark methods for image authentication using cryptography analysis. Signal Image Process 2(2):170–179

Pandey A, Tugnayat RM, Tiwari AK (2013) Data security frame- work for cloud computing networks. Int J Comput Eng Technol 4(1):178–181

Parmar PV, Padhar SB, Patel SN, Bhatt NI, Jhaveri RH (2014) Survey of various homomorphic encryption algorithms and schemes. Int J Comput Appl 91(8):26–32

Patil RA, Renke AL (2016) Keystroke dynamics for user authentication and identification by using typing rhythm. Int J Comput Appl 144(9):27–33

Patterson DA, Hennessy JL (1994) Computer organization and design: the hardware/software interface. Morgan Kaufmann Inc, San Francisco

Pawle AA, Pawar VP (2013) Face recognition system (FRS) on cloud computing for user authentication. Int J Soft Comput Eng 3(4):189–193

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

Potisepp K (2013) Large-scale image processing using MapReduce. M.Sc. Thesis, Tartu University, Faculty of Mathematics and Com- puter Science, Institute of Computer Science, pp 1–56

Rajput AS, Sharma V (2015) Survey and analysis of chaotic image encryption schemes. Int J Commun Syst Netw Technol 4(1):24–27 Rani D, Ranjan RK (2014) A comparative study of SaaS, PaaS and IaaS in cloud computing. Int J Adv Res Comput Sci Softw Eng 4(6):458–461

Rathi P, Dubey S (2013) Hand geometry recognition system using feature extraction. Int J Adv Res Comput Eng Technol 2(6):2064–2067

Rathi R, Choudhary M, Chandra B (2012) An application of face recog- nition system using image processing and neural networks. Int J Comp Tech 3(1):45–49

Reza MS, Khan MSA, Alam MGR, Islam S (2012) An approach of digital image copyright protection by using watermarking tech- nology. Cornell University Library, Cornell, pp 1–7

Shelly Bawa RK (2015) Secure image transmission for cloud storage system using hybrid scheme. Int J Eng Res Dev 11(9):18–26

Shubh T, Sharma S (2016) Man-in-the-middle-attack prevention using HTTPS and SSL. Int J Comput Sci Mobile Comput 5(6):569–579 Singh RK, Kumar B, Shaw DK, Khan DA (2018) Level by level image compression-encryption algorithm based on quantum chaos map. J King Saud Univ Comput Inform Sci. https://doi.org/10.1016/j. jksuci.2018.05.012

Suryani D, Irwansyah E, Chindra R (2017) Offline signature recog- nition and verification system using efficient fuzzy kohonen clustering network (EFKCN) algorithm. Procedia Comput Sci 116:621–628. https://doi.org/10.1016/j.procs.2017.10.025

Teh PS, Teoh ABJ, Yue S (2013) A survey on keystroke dynamics and biometrics. Sci World J. https://doi.org/10.1155/2013/408280

Thieling L, Schuer A, Hartung G, Buchel G (2014) Embedded image processing system for cloud-based applications. In: International Conference on ssytems, signals and image processing, pp 1–4

Tiwari P, Saklani A (2013) Role of biometric cryptography in cloud computing. Int J Comput Appl 7(9):34–38

Valmik NK, Kshirsagar VK (2014) Blowfish algorithm. IOSR J Com- put Eng 16(2):80–83

Varsha D, Wadhwa A, Gupta S (2015) Study of security issues in cloud computing. Int J Comput Sci Mobile Comput 4(6):230–234

Vaudenay S (1996) On the weak keys in blowsh. In: Gollmann D (ed)
Fast software encryption. International workshop on fast software encryption, FSE 1996. Lecture notes in computer science, vol 1039. Springer, Berlin, Heidelberg, pp 27–32

Wang P, Wang J, Chen Y, Ni G (2013a) Rapid processing of remote sensing images based on cloud computing. Future Gener Comp Syst 29(8):1963–1968

Wang S, Nassar M, Atallah M, Malluhi Q (2013b) Secure and private outsourcing of shape-based feature extraction. In: International conference on information and communications security, pp 90–99

Wangsuk K, Amornkul TA (2013) Trajectory mining for keystroke dynamics authentication. In: 17th Asia Pacific Symposium on Intelligent and Evolutionary Systems. vol 24, pp 175–183

Xia Z, Ma X, Shen Z, Sun X, Xiong NN, Jeon B (2018) Secure image LBP feature extraction in cloud-based smart campus. IEEE Access 6:30392–30401

Yang P, Gui X, An J, Tian F (2017) An efficient secret key homomor- phic encryption used in image processing service. Secur Commun Netw. https://doi.org/10.1155/2017/7695751

Yassin AA, Yao J, Han S (2016a) Strong authentication scheme based on hand geometry and smart card factors. Computers 5:15

Yassin AA, Yao J, Han S (2016b) Strong authentication scheme based on hand geometry and smart card factors. Computers 5:1–17

Zefreh EZ, Rajaee R, Farivary M (2011) Image security system using recursive cellular automata substitution and its parallelization. In: IEEE, pp 77–86

Zhang L, Shen P, Song J, Dong L, Wang G, Cai Y (2014) An image processing system based on heterogeneous embedded mul- ticore processors. In: 2014 Second International Conference on Advanced Cloud and Big Data, pp 1–6