International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I8P218

Volume 71 Issue 8, 201-215, August 2023


*Original Article*

# A Novel Authentication Model Based on Multi-Biometric Hashing

Ahmed Y. Mahmoud[1], Mohammed Hazem M. Hamadaqa[2]

*[1,2]Department of Information Technology, Faculty of Engineering and Information Technology, Al-Azhar University-Gaza, Gaza, Palestine.*

*[1]Corresponding Author : ahmed@alazhar.edu.ps*

Received: 19 June 2023 Revised: 02 August 2023 Accepted: 05 August 2023 Published: 15 August 2023

***Abstract*** - *Authentication systems based on biometrics have been widely used in recent years as a means to enhance security and improve the user experience. However, traditional biometric authentication systems that rely on a single biometric modality, such as fingerprints or facial recognition, may not be able to provide a sufficient level of security and accuracy. This is particularly true in scenarios where the quality of the biometric samples is poor or when the users are trying to impersonate someone else. In this paper, we proposed a novel approach for biometric authentication that addresses these limitations by combining multiple biometric modalities. The proposed system uses fingerprints and the iris eye as the primary means of identification to increase security, reliability, and accuracy. The use of multiple modalities enables the system to account for variations in the quality of individual samples, thus reducing the chances of false rejections or acceptances. Furthermore, this paper proposes the use of hash functions for data retrieval as a way to reduce storage costs and improve the speed of the system. The paper investigates various hash algorithms, such as SHA1, SHA-256, and SHA-512; SHA3-256 and SHA3-512 give a 10% success rate in matching and also demonstrates that the use of Perceptual Hash, Average Hash, and Difference Hash algorithms result in an 83.33*% success rate *in matching.*

***Keywords*** - *Average Hash, Biometric authentication, Difference Hash, Multi-biometric, Perceptual Hash.*

## 1. Introduction

Authentication is the process of verifying the identity of a user or a device, and it is a crucial security measure in various applications, including online banking, access control, and e-commerce. With the widespread use of computers, user impersonation has become a significant security hazard, and the first line of defense against this type of attack is through proper authentication [1]. The term "biometric" is a combination of the words "bio" for life and "metrics" for measurement. Due to greater security and demonstrated superior performance as a result of rising societal demand, biometric authentication systems are becoming more and more common.

It can identify an authorized person from a forged one using measurable human physiological or behavioral features to validate the subject's identity. The fingerprint, face, retina, DNA, iris, and other physiological traits/characteristics are among those that do not change over time [2]. The term "biometric technology" refers to automated techniques for confirming or recognizing a living person's identity based on a physiological or behavioral characteristic [3, 4]. The unimodal system refers to biometrics based on a single characteristic. It has a number of issues, including noisy data, false rejection, intra-class variance, fake biometric traits, non-universality, inter-class similarity, and spoofy attacks. Multimodal biometrics are employed to overcome these issues. In multimodal, many indications or qualities are gathered from several sources about the same person [2]. Hash functions convert arbitrary-length inputs to a fixed-length string known as the hash code. These mappings can be used to safeguard the integrity of data if they meet some extra cryptographic requirements. Other cryptosystems use hash functions for different purposes, for example, improving digital signature methods, safeguarding passphrases, and committing to a string without disclosing it [5].

## 2. Overview of Biometric Authentication and Hashing

### *2.1. Biometric Authentication Characteristics*

The automated biometric authentication system uses a variety of physiological and behavioral traits. The selection is based on the application and the strengths and weaknesses of each biometric parameter. No single biometric characteristic is expected to fully satisfy every application's needs. The compatibility of a particular biometric authentication method with a given application depends on both the way the application is used and the characteristics of the biometric feature [6, 7].

In practice, the most common biometric features used for identification and verification include fingerprint, palm print, hand geometry, iris, retina, face, and ear. Each of these biometric characteristics/traits has its own strengths and weaknesses and can be suitable for different applications based on specific requirements. Below we highlight these biometric features:

#### *2.1.1. Fingerprint*

For human identification and verification, fingerprint-based authentication has been the most reliable, effective, and widely used method [8].

#### *2.1.2. Palm Print*

The palms of human hands have a distinctive pattern of ridges and valleys, much like fingerprints. Since the area of the palm is far larger than the area of a finger, palm prints should be even more recognizable than fingerprints. Palm print scanners are larger and more expensive than fingerprint sensors since they need to record a larger area [9].

#### *2.1.3. Hand Geometry*

Identification methods based on hand geometry make use of the geometrical characteristics of the hand, such as the length and width of the fingers, the diameter of the palm, and the perimeter. Biometric technologies based on hand geometry are becoming more popular in low- to medium-security applications [10].

#### *2.1.4. Iris*

The diameter and size of the pupil, as well as the amount of light that reaches the retina, are regulated by the iris, a small, round structure in the eye. Like fingerprints, each iris is unique, and identical twins' irises might differ from one another. The iris's texture cannot be altered surgically for any reason. Furthermore, fake irises are rather simple to spot [8].

#### *2.1.5. Retina*

The human retina is a delicate tissue made up of neural cells that are found in the back of the eye. Each person's retina is distinct due to the intricate capillary network that supplies it with blood. Even identical twins do not have a similar pattern in their retinal blood vessel network because it is so intricate. Although diabetes, glaucoma, and retinal degenerative illnesses can cause changes to retinal patterns, the retina normally does not change from birth until death [8].

#### *2.1.6. Face*

Since humans frequently use faces to identify people, recent advances in computing power have made automatic face recognition possible. Face recognition algorithms can be categorized into two main categories: geometric, which examines distinguishing features (the positioning and shape of facial features like the eyes, brows, nose, lips, and chin, as well as their spatial relationships), or photometric, a statistical approach that breaks down an image into values and compares the values with templates to remove variances [11].

#### *2.1.7. Ear*

According to research, an adult's ear shape and appearance do not change much over their lifespan [12], making each person's ear distinctive. Between the ages of four months and eight years, ear growth is roughly linear, and from then on, it remains steady until it increases once more at the age of 70 [13]. Ear recognition is being looked into as a viable biometric because of its stability and predictable changes [12, 13].

### ***2.2. Multi-Biometric Authentication***

Multi-biometric authentication refers to the use of multiple biometric traits for the purpose of identity verification. This approach can potentially improve the accuracy and security of authentication systems, as it combines the strengths of different biometric traits and reduces the impact of individual weaknesses. The following integration scenarios are intended for use by recognition systems that combine several biometric traits:

#### *2.2.1. Multi-Sensor Systems*

Information from the same biometric collected by various sensors is aggregated for everyone. The information is then combined using a technique called sensor-level fusion [14]. Multimodal systems: User identification involves the use of many biometric characteristics. To establish the user's identification, for instance, information gathered through voice and face features or other methods can be combined [15].

#### *2.2.2. Multi-Instance Systems*

A single biometric feature is recorded many times. For iris recognition, for instance, pictures of the left and right irises can be used [16].

#### *2.2.3. Multi-Sample Systems*

For enrollment and recognition, different samples with the same biometric feature are used. For instance, the left and right faces are recorded together with the frontal face [14].

#### *2.2.4. Multi-Algorithm Systems*

One biometric attribute is subjected to numerous feature extraction and matching algorithm approaches. Final determination of which matching fusion approach can be used on the outcomes of several matching algorithms [14].

Figure 1 illustrates the different types of multi-biometric systems. These systems integrate multiple biometric features to increase accuracy and reliability. The figure shows five main multi-biometric systems categories: multi-sensor, multi-modal, multi-algorithm, multi-instance, and multi-sample systems.

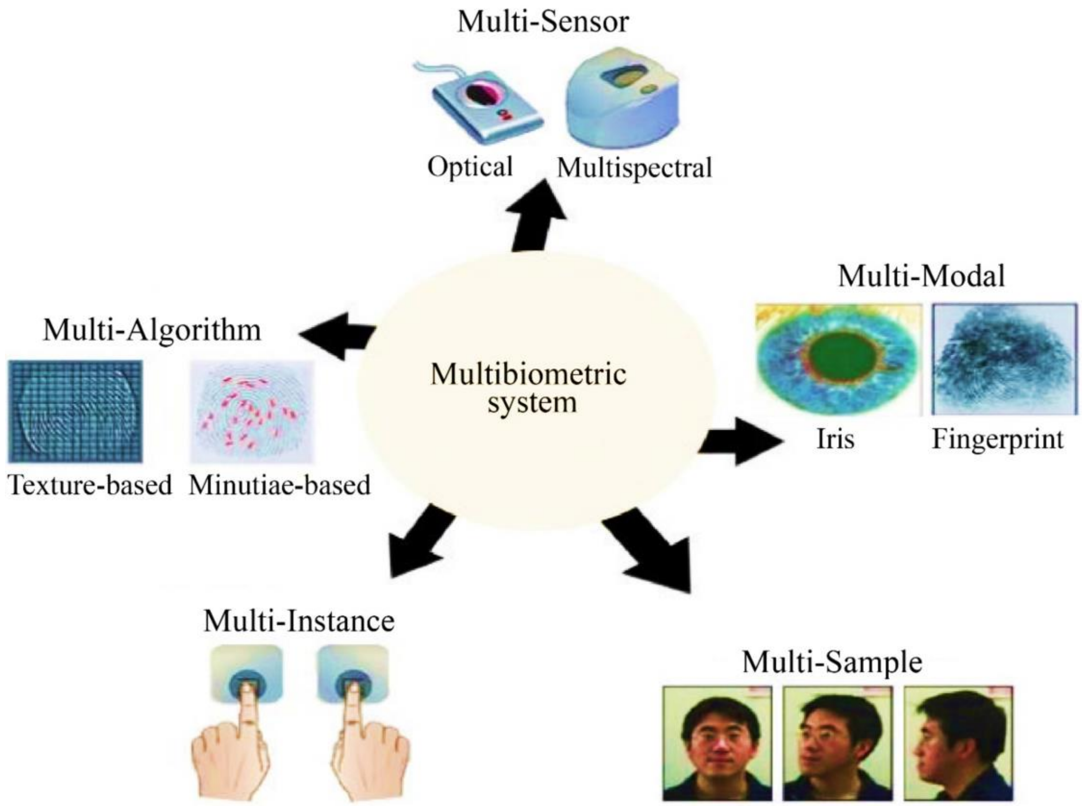



**Fig. 1 The various forms of Multi-Biometric systems**

### *2.3. Hashing*

A Mathematical formula that accepts any length as an input and outputs a fixed length that is unique and unrecoverable (one-way function). The one-way function prevents one from extracting the original data or recovering/disclosing the inputs from the hashed output. Different data cannot have the same hash. The outcome will be radically different if the input is altered even a single bit. Hash function algorithms are employed for integrity see, for example, [17], which refers to no change in the data, and for storing passwords in databases as hashes since if the database is breached, all of the passwords will be obtained with ease [18].

In this subsection, we present a discussion and comparison between the various types of hashing algorithms that have been proposed for use in biometric authentication. These include cryptographic hashing algorithms, such as MD5, SHA1 (Secure Hash Algorithm), SHA-256, SHA-512, SHA3-256 and SHA3-512, and perceptual, difference and average hashing; most of the aforementioned hashing algorithms can be found in [18] and [19].

#### *2.3.1. MD5*

The algorithm described takes in variable-length data and outputs a message process of 128 bits or 16 bytes. The algorithm divides the input message into 512-bit blocks and pads it with a 1 followed by zeros to ensure that the length of the message is 64 bits less than a multiple of 512. The remaining bits are filled with 64 bits representing the original message's length. This hashing algorithm is widely used, but it is prone to collisions. Despite this weakness, the impact attack is too slow to be useful, making it less vulnerable to collisions but still susceptible to preimages or second preimages.

#### *2.3.2. SHA1*

It is not that easy to produce SHA-1 crashes. It seems reasonable that the attack modeled after SHA-1 actually operates with a typical cost of 261 clock cycles, which is much faster than the non-specific birthday attack (which is in 280), but also highly difficult. With a lot of hand-waving that SHA-1 is more powerful than MD5 since it has more adjustments and because the introduction of the 80 message words in SHA-1 is significantly more "blending" than that of MD5. While there have been reported SHA1 attacks, they are far less credible than those on MD5. Because of this, choosing SHA1 over MD5 is a far better choice in many situations.

#### *2.3.3. SHA2*

The SHA-2 family consists of six hash functions: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA512/256, with hash values of 224, 256, 384, or 512 bits, respectively. To make the message length in this algorithm 64 bits rather than exactly an even variety of 512, the message is "cushioned" with a 1 and the corresponding amount of 0s. The end of the cushioning message has 64 bits that display the length of the unique message. 512-piece squares are used to prepare the cushioned message.

#### *2.3.4. SHA3*

The National Security Agency (NSA) institute chose the cryptographic hashing algorithm SHA-3 in 2012. SHA-3 supports the same hash lengths as SHA-2, its internal structure is completely different and resistant to attacks like length extension, which rendered both MD5 and SHA-1 defenseless; because of the potential attacks against SHA-2, the main motivation behind the development of the SHA-3 algorithm. Although no concrete evidence has been provided demonstrating the flaws in SHA-2, one cannot dismiss the possibility that it may exist.

In order to better understand the strengths and weaknesses of each algorithm and to provide a helping guideline for the selection criteria of the most appropriate hash algorithms for our proposed multi-biometric authentication model. We conduct a comparison among the different SHA functions. Table 1 provides a comparison of the most commonly used SHA functions, including SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. The key features, such as their hash size, block size, and security level, are stated. This comparison, summarized in Table 1, will provide a better understanding of different SHA functions.

**Table 1. Comparison of different SHA iunctions**

<table>
<tr><th colspan="2">Algorithm</th><th>Output size (bits)</th><th>Internal state size (bits)</th><th>Block size (bits)</th><th>Max message size (bits)</th><th>Word size (bits)</th><th>Rounds</th><th>Bitwise operations</th><th>Collisions found</th><th>Example Performance (MiB/s)</th></tr>
<tr><td colspan="2">MD5</td><td>128</td><td>128</td><td>512</td><td>2^64 − 1</td><td>32</td><td>64</td><td>and, or, xor, rotate</td><td>Yes</td><td>335</td></tr>
<tr><td colspan="2">SHA-0</td><td>160</td><td>160</td><td>512</td><td>2^64 − 1</td><td>32</td><td>80</td><td>and, or, xor, rotate</td><td>Yes</td><td>-</td></tr>
<tr><td colspan="2">SHA-1</td><td>160</td><td>160</td><td>512</td><td>2^64 − 1</td><td>32</td><td>80</td><td>and, or, xor, rotate</td><td>Theoretical attack</td><td>192</td></tr>
<tr><td rowspan="6">SHA2</td><td>SHA-224</td><td>224</td><td rowspan="2">256</td><td rowspan="2">512</td><td rowspan="2">2^64 − 1</td><td rowspan="2">32</td><td rowspan="2">64</td><td rowspan="2">and, or, xor, shift, rotate</td><td rowspan="2">None</td><td rowspan="2">139</td></tr>
<tr><td>SHA-256</td><td>256</td></tr>
<tr><td>SHA-384</td><td>384</td><td rowspan="4">512</td><td rowspan="4">1024</td><td rowspan="4">2^128 − 1</td><td rowspan="4">64</td><td rowspan="4">80</td><td rowspan="4">and, or, xor, shift, rotate</td><td rowspan="4">None</td><td rowspan="4">154</td></tr>
<tr><td>SHA-512</td><td>512</td></tr>
<tr><td>SHA-512/224</td><td>224</td></tr>
<tr><td>SHA-512/256</td><td>256</td></tr>
</table>

#### *2.3.5. Perceptual Hash (P-Hash)*

The perceptual hash uses a discrete cosine transformation as its foundation (DCT). As an image hash, the technique generates a binary sequence of 64 bits. The image's brightness is used to transform it first to a greyscale representation. The image is then subjected to a mean filter, such as a smoothing, averaging, or box filter. A 7x7-dimensional kernel is utilized to apply the filter. With the help of a unique convolution function, the kernel is applied. The image is scaled down to 32 x 32 pixels after convolution has been applied. 64 low-frequency coefficients are utilized to extract the hash, but the lowest-frequency coefficients are left out. Because they are generally stable when an image is altered, low-frequency coefficients are used. Additionally, the low-frequency DCT components retain the majority of the signal data. Because they frequently deviate greatly from others and have the potential to greatly affect the average, the lowest frequency coefficients are excluded [20].

#### *2.3.6. Average Hash (A-Hash)*

The A-hash is a perceptual image hashing technique that focuses on aspects of image structure to produce small 64-bit image hashes. Higher frequencies represent image details, and lower frequencies represent image structure, as an image is broken down into its underlying harmonics. The higher frequencies are removed from the image by shrinking to provide the smallest feasible image fingerprint.

To be more precise, the image is shrunk to an 8x8 block, giving it a total of 64 pixels, before the hash is calculated. A greyscale rendition of each pixel follows. Because the crucial semantic information is kept in a picture's luminance component, this step is used by all perceptual image hashing techniques. The 64 pixels are then averaged to determine the color. Then, the hash is built such that each bit denoting a single pixel is set depending on whether that pixel's colour value is below or above the estimated image average [20].

*2.3.7. Difference Hash (D-Hash)*

The D-hash is similar to the A-hash method and makes use of visual structure. The hashing approach concentrates on the image structure and does so by shrinking the image, which means taking away higher frequencies from the image spectrum. The D-hash approach records image gradient as opposed to the A-hash approach, which produces the fingerprint by averaging the pixels. Each image is reduced to a 9x8 block and made grayscale before being hashed, making a total of 72 pixels.

The difference between each pair of adjacent pixels is then calculated for each row, yielding a total of 8 differences per row. As a result, 64 differences are calculated for each image and utilized to build the fingerprint. Each bit is set based on the determined difference d to accomplish this. As an illustration, if $d < 0$, the hash bit is set to 0, and if $d \geq 0$, the bit is set to 1 [20].

In order to fully understand the capabilities and limitations of different hash algorithms, it is important to compare and contrast cryptographic and perceptual hash. Cryptographic hash algorithms, such as SHA-1 and MD5, are designed to provide a secure data integrity and authentication method. They are widely used in security applications such as digital signatures and message authentication codes. On the other hand, perceptual hash algorithms are designed to generate a hash that is based on the visual content of an image.

These algorithms are particularly useful for image authentication and retrieval and are resistant to image manipulation. Table 2 provides a comparison between cryptographic and perceptual hash.

**Table 2. Comparison between the cryptographic and perceptual hash**

| Feature | Cryptographic Hash | Perceptual Hash |
|---|---|---|
| **Essential feature** | Sensitive to the input message at all times | Sensitive to the variations in perceptual characteristics |
| **Properties** | Preimage resistance; Second preimage resistance; Strong collision resistance | Robustness; Discriminability; Unpredictability; Compactness |
| **Application scenario** | verifying the integrity of messages; files or data identification; password verification | Content-based image retrieval; image authentication |

When compared to cryptographic hash methods like MD5 and SHA1, perceptual hashes are a distinct idea. The hash values used in cryptographic hashes are arbitrary. Since the data used to build the hash functions as a random seed, different data will provide different results, while the same data will produce the same result. In reality, comparing two SHA1 hash values only reveals two things. The data will differ if the hashes are different. The data is probably the same if the hashes are the same. In comparison, you may compare perceptual hashes to understand how similar the two data sets are.

## 3. Literature Review

Numerous endeavors have been undertaken to reconstruct and reconfigure biometric authentication to improve its effectiveness. The intention of the author [21] was to engage a large audience to discuss the merits of the Biometric encryption approach to confirming identity, safeguarding privacy, and ensuring security. The authors of [22] discussed the future trend of increasing the security of information systems through secure individual authentication. The article highlights the importance of considering usability aspects during the development of authentication solutions and how user acceptance is crucial for the success of any authentication method.

The article also states that biometric systems are seen as the most efficient and secure solution for user authentication and that it is essential to consider privacy concerns when implementing these systems. The article emphasizes that biometrics are the only method to authenticate the user or the mobile phone's owner; however, it is also important to use as many authentication factors as necessary to increase the security of an information system.

Recent advances in multi-biometrics have mostly focused on quality-based fusion, for example, [23] - [27][60], where the decision-level fusion takes into consideration the quality associated with both the template and the query biometric sample. Numerous quality metrics have recently been introduced in the literature for application in this situation, including classifier-dependent measures (confidence), iris, face, speech, signature, iris, fingerprint, and fingerprint [29]-[36]. The main objective of the provided quality measures is to rate the quality or compliance of biometric samples to some specified criteria known to influence system performance.

These, for instance, assess the accuracy of face detection, image focus, and contrast. Fingerprint, palmprint, and hand geometry integration have been suggested by G. Prabhu and S. Poornima [37] for the identification and verification process. In order to improve accuracy, the author suggests classifying gender using hand geometry data that has been extracted from diverse sources while minimizing search time. The preprocessing of the photos in this study begins with the employment of filters for fingerprint and palmprint images, followed by the application of the 2D discrete wavelet transform and the Gabor filter and the extraction of common biometric features by normalization.

The characteristics of the face and finger veins were integrated by Muhammad Imran Razzak et al. [38] to improve the biometric identification system's accuracy, according to Mohamed Soltane et al. In order to increase the robustness and reliability of the biometric authentication system, face and speech are combined. The lip movement and gestures suggested by Piotr Dalka [40]. A multimodal biometric system was employed to enhance security, incorporating both the face and ears. A.A. Darwish proposed the idea of combining these two biometric features as a means of increasing security [41]. For a better fusion outcome and to increase the biometric system's accuracy, C.K. Verma [42] suggested combining soft biometrics with fingerprint and facial recognition.

The multimodal biometric system that records three fingerprints and a vein in the palm of the hand is proposed by Shigefumi Yamada [43]. For raising FAR's recognition accuracy, the author's goal in this paper is to assess whether or not biometric features are independent. The properties of a fingerprint and a palm print are combined by V. D. Mhaske. [44] to get around some of the drawbacks of unimodal biometrics. The author employed a customized gabor filter as opposed to a standard Gabor filter, applied the Fourier transformation after that, and then categorized features using Euclidean distance to ensure that the final image perfectly matched database templates. The author of [44] integrates a biometric system's palmprint and fingerprint features to provide a superior performance and consequent image of higher quality.

In [45], various secure hashing methods are evaluated and compared. Each algorithm optimizes the timing of the hash estimation process. By considering the time taken by each of these algorithms and identifying the one that minimizes the duration for the hash estimation algorithm, the security of the transmitted information can be enhanced by employing a well-structured security algorithm. The author of [46] recommends assigning greater importance to SHA algorithms over MD5 due to their superior performance compared to other cryptographic hash algorithms. But by gathering additional information, new questions can be raised, leading to creative testing of cryptographic hashing algorithms. These new findings would reinforce the previously reached conclusion, endorsing SHA algorithms as the primary choice for cryptographic hash algorithms.

For processing a packed portrayal of a message, the Secure Hash Algorithm (SHA-1) is used. If we provide an information message with a discretionary length of 264 bits, the message process, a 160-piece yield, is produced. The SHA1 method is said to be safe because it is virtually impossible to figure out the message by comparing it to a given messaging process. Furthermore, finding two messages hashing to the same value is quite rare. In this way, the majority of people still use MD5 or SHA1 today, faulty or not. Since the current state of hashing technology is that we have some capacities that we know have speculative weaknesses but no actual, tangible breaks and some problematic capacities that we know virtually nothing about. Although SHA1 has not been successfully compromised to date, it may become vulnerable to attack as computers become more powerful in the future. In order to make the web safer, huge businesses like Google, Microsoft, and others plan to terminate the use of SHA-1 in the near future [62].

Based on the previous discussion of SHA family hash, it is important to examine another popular type of hashing algorithm called perceptual hash. Perceptual hash algorithms are designed to produce a hash that is based on the visual content of an image rather than the image's file format or the file's binary data. These algorithms are particularly useful for image authentication and retrieval, as they are resistant to image manipulation and can be used to find similar images. In order to identify near-duplicate photos, researchers have developed a number of image hashing methods that extract well-known image features (such as HOG, DOG, SIFT, etc.) as big, high-dimensional vectors that are afterwards reduced using dimensionality reduction techniques.

For instance, in [50], the authors extract local features for picture representation based on DOG and then employ locality-sensitive hashing as the primary indexing structure. In [51], the data are fitted to a multidimensional rectangle using spectral hashing after primary component analysis (PCA) has been used to identify the data's primary components. The proposed approach in [52] uses PCA to discover the maximum variance direction similarly to the preceding method, with the exception that the original covariance matrix is "adjusted" by a different matrix derived from the labeled data. In [52], the authors present the Min-Hash algorithm for retrieving related images and leverage bag-of-words approaches for text analysis to create bag-of-visual-words utilizing vector quantized local feature descriptors (SIFT).

Additionally, it is suggested that geometric image hashing [63] be used to enhance standard Min-Hash by considering the spatial dependency of visual words. In [54], a wonderful new graph-based methodology is presented that automatically identifies the neighborhood structure present in the data. The author of [55] suggested using kernelized locality-sensitive hashing for scaled picture search. Deep learning frameworks are suggested in more recent research to produce binary hash codes for quick image retrieval [56] and [57].

In [18], the authors studied the robustness of perceptual image hashing algorithms (A-hash, D-hash, W-hash and P-hash) with respect to visible physical image modifications and image upload on social networks. They created a dataset of original images and their modifications and used common measures (Precision, Recall and F1 score) to compare the performance of the different algorithms. The evaluation results show that P-hash is the most robust algorithm, achieving an F1 score of 0.738 on the image modifications dataset and 0.864 on the social networks uploaded dataset.

In [58], the authors presented a feature-level fusion and binarization framework using deep hashing to design a multimodal template protection scheme that generates a single secure template from each user's multiple biometrics. They employed a hybrid secure architecture combining the secure primitives of cancellable biometrics and secure sketch and integrated it with a deep hashing framework, making it computationally prohibitive to forge a combination of multiple biometrics that passes the authentication. They proposed two deep learning-based fusion architectures and analyzed the matching performance and security, and also performed an unlinkability analysis of the proposed secure multimodal system. Experiments using the WVU multimodal dataset, containing face and iris modalities, demonstrate that the matching performance does not deteriorate with the proposed protection scheme. In fact, both the matching performance and the template security are improved when using the proposed secure multimodal system. However, the authors note that further validation is required to show how well the system works with other biometric modalities. The goal of the paper is to motivate researchers to investigate how to generate secure, compact multimodal templates.

In [59], the authors proposed a secure biometric-based authentication scheme that employs a user-dependant one-way transformation combined with a secure hashing algorithm. They discussed its design issues, such as scalability, collision-freeness, and security. They tested their scheme using the ORL face database and presented simulation results. The preliminary results show that the proposed scheme offers a simple and practical solution to one of the biometrics-based authentication systems' privacy and security weaknesses. The author of [21] proposed a novel method that generates a safe signature for each authorized individual in the enrolment phase by utilizing a hash function, even though the iris is only derived from a segment (not the entirety) of the iris image. The best way to provide great security to the permitted database is to use SHA-256, which is also quicker than other forms of hash functions. In the future, iris and hash function-based mobile biometric authentication may be used.

In the current study, we proposed a multi-biometric authentication model combining multiple biometric traits to enhance the security and performance of authentication systems. The proposed model can provide a high level of security, minimize storage requirements by using perceptual and average hash functions and satisfy the integrity of the data in addition to the protection against impersonation and other forms of attacks.

## 4. Proposed Model and Methodology

### *4.1. Dataset*

The dataset in this study consists of a collection of Iris images from the MMU-Iris dataset and fingerprint images from the fvc2004 fingerprint dataset for the purpose of the research; we create a comprehensive dataset for our proposed model. The MMU-Iris-Database contains iris images of both the left and right eyes of 30 individuals, with each individual having 5 samples for both eyes. Similarly, the fvc2004 fingerprint dataset contains 5 samples for each of the 30 individuals. To create our dataset, we combined the iris and fingerprint images of the 30 individuals, resulting in a total of 30 individuals, each with 5 samples of both iris and fingerprint images. The dataset is divided into a training set and a testing set, where 4 samples of each modality per individual are used for hashing and storing, while the remaining sample is used for validation and testing purposes. By using a combination of both iris and fingerprint samples, we aim to increase the accuracy and robustness of our proposed model.

This approach allows us to take advantage of both modalities' unique features and characteristics and ends by improving the performance of our proposed multimodal biometric authentication system. The sampling and selection criteria for the data are based on the data's diversity and quality. The diversity of the data is ensured through the use of multiple sensors, multiple subjects, multiple scenarios, and multiple variations. The data quality is ensured through the use of high-resolution and high-contrast images and the removal of noise, blur, and artifacts. We have four samples for storing and one sample for testing. This data size is sufficient to represent the population and estimate the performance of the hashing algorithm during testing.

**Table 3. Sample 1 of compound dataset**

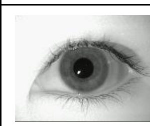
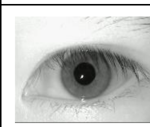
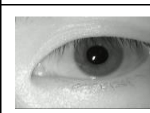
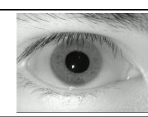
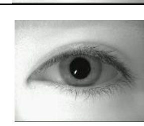
| Person | Fingerprint | Left iris | Right iris |
|---|---|---|---|
| **1** |  |  |  |
| **2** |  |  |  |
| **3** |  |  |  |
| **4** |  |  |  |
| **5** |  |  |  |

Table 3 shows the first fingerprint sample, left iris and right iris images, respectively, for 5 individuals.

### *4.2. Evaluation Metrics*

We employed three assessment metrics in this study to gauge the effectiveness of the suggested classification model: accuracy, recall, precision, and F1-score. These metrics are defined by equations (1), (2), (3), and (4), respectively. The computations rely on the statistical findings from numerous experiments.

$$Precision = \frac{TP}{TP + FP} \tag{1}$$

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{3}$$

Where TP, FP, TN and FN are true positive, false positive, true negative and false negative, respectively [59].

### *4.3. Proposed Model and Experimental Discussion*

The proposed model is illustrated in Fig. 2; it depends on two main phases as follows:

#### *4.3.1. Enrolment Phase*

During the enrollment phase, users are requested to submit four fingerprint images, four left iris images, and four right iris images. These input images undergo preprocessing and conversion to a standardized format (JPEG) utilizing the ImageMagick library. The images are hashed using a reliable, secure hashing algorithm. The resulting hash values are then stored in a database for future utilization during the authentication phase.

#### *4.3.2. Authentication Phase*

The user is prompted to provide one fingerprint image, one left iris image, and one right iris image. These images are pre-processed and converted to JPEG format. Subsequently, they are hashed using the same secure hashing algorithm employed during the enrollment phase. A query is performed on the database to compare the newly hashed images with the previously stored hashes. If a match is discovered, the user is granted access. However, if no match is found, the user is prompted to attempt again.

In summary, the proposed model utilizes a two-phased approach for biometric authentication, leveraging fingerprint, left iris, and right iris images to verify user identity. This is achieved by converting the images to a standardized format and employing a secure hashing algorithm. By doing so, the model prioritizes the privacy and security of user data while offering a dependable and efficient authentication method.

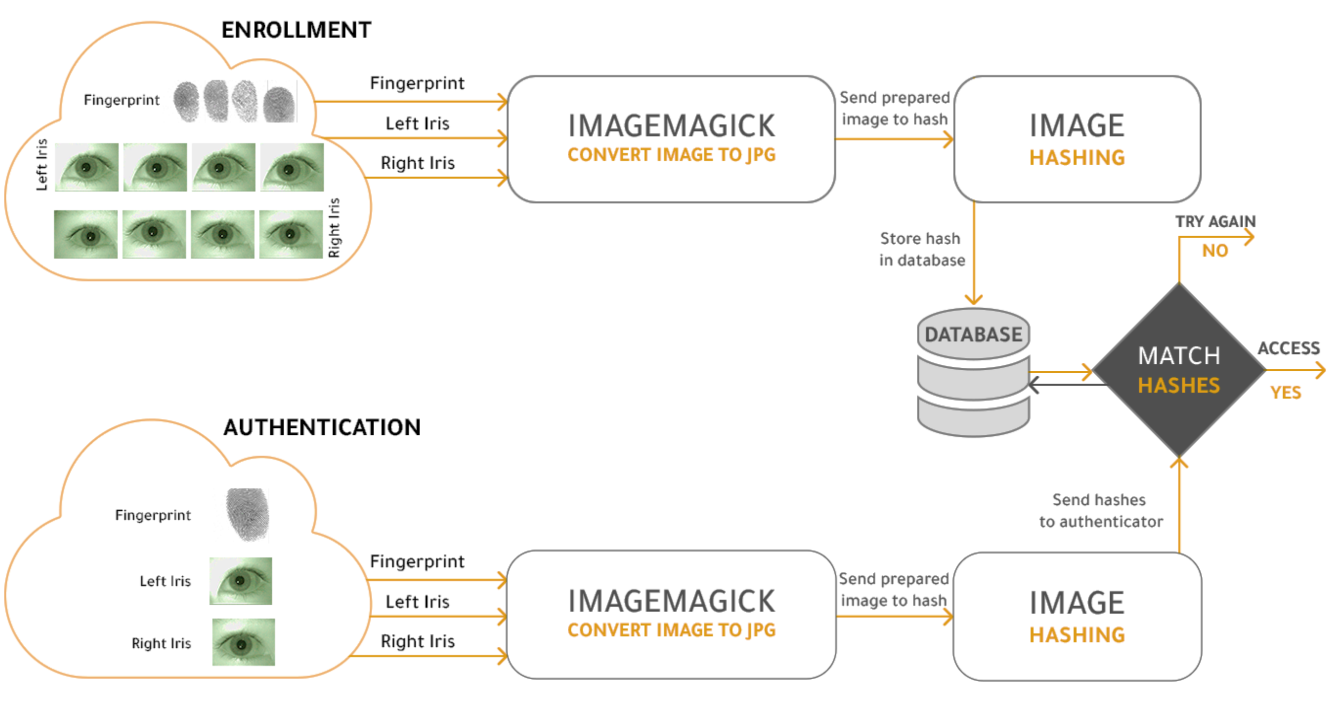



**Fig. 2 Proposed model**

**Table 4. Hashed value of SHA-1 algorithm**

| # | Left iris hash | Right iris hash | Fingerprint hash |
|---|---|---|---|
| **1** | e4fd7035fa49f0a127d21ff3adbb037adb7522b0 | d31adb056dda4d7c2107f91027a135985fb9cfea | 999e34e14b5ffcc3e3ee534fc2118fc04f0c7f51 |
| **2** | ecfe00b4b9a623d97360ad9ac964823ca0a4d473 | e444c579c0778b59d70c48be4293df199e966c57 | 346a88114651ae259cec2252cb293ddb7f78f35e |
| **3** | f78f7b0b218998b5f89924eac14d95dec875f3fe | f5f81176914242ad8907f9b2b3e49a0e5bf3de63 | 3b75c4cb076334646b637807172639238c294080 |
| **4** | 9cf9a8219e2774299f1326330c123bfc6a254a48 | 0799fa4ea0b2a10301ec17b726f675e21bc26891 | 7edc0bd97be2bb7758812a0d984fcb90702fa9ff |
| **5** | b39bb142022fc6fc51bf6adb9f563ebc5b71d2d4 | a0a1161292dd53f5060029533ed20b91257468c3 | 506d3f7cb3b36713e4862bc5aae7df732b8fd31e |

**Table 5. Hashed value of SHA-256 algorithm**

| # | Left iris hash | Right iris hash | Fingerprint hash |
|---|---|---|---|
| **1** | 32869389e4ed9d35b2e39a18a1e089616961d9f9e71f892158903ce0e63adabb | e823ff51fad10f84522ab5c23f73f7622597ffba0abc529dc09d61738ed185af | d85d749abe732ad0ea93eaf931e126fc596d9d457b213d179865d5f474df0f8e |
| **2** | 84220625a4e311667705b0e4e1624bfd7a54fcb53c6ba54f1a77b2b8618d2d35 | ff08e9c809150e8782cb58a66e8377b864794d2ea0d1a6da1a70954c049b5007 | 5f27d0c9aff46f74ca3a015ed7f0f3a5b551208b75fa6b4d2b53181fca109b39 |
| **3** | e73e3f4a9b14e36e5cab25fdc8ffd16e0b37de4f6ec0798739af7d1571dbecc9 | 39c5495c613a29cba72f0e2cb5ee73d6c8165af96b6a65fdd6a701f0f9a1ea17 | 620c614dc994c29b24b492a2e1c4f5e27dc71e000bbdbbe0fa2e027e805d6514 |
| **4** | 4c68566a573658150179bc27fa9ac610dd3d7420836de9ab4e0cc4164bba4f10 | 46035fa20241d2fab94a1ba2ee70bed630867df4a74cbc07f8c3d08f3b085dd2 | d212ce1c546a97154e10d5aa76f00149d9aaa2082e068293d2f70ce34c919c2f |
| **5** | 9e7751ec0728a48b395e71fbba93fbfd21c7e7282d47dc6a161af50a6cd4b7ff | 5653cba7f0515abf8c2bccde8e1e0a3ff9e09121d8ed524b05a1b2f6243af70c | 0a282f8dad3323358e6185d46822bb3bf09ee7566db68ad5f0e627fdbd605af3 |

**Table 6. Hashed value of SHA-512 algorithm**

| # | Left iris hash | Right iris hash | Fingerprint hash |
|---|---|---|---|
| **1** | 6ef760557d8387229c461fd103ef050d46719ebb5f49e931c4072334d41590e64dd289ac6545e41f2a4168686b0df7c965bec69b161bab32d5f80f864a8ca964 | 496017761319d143b3449b0edd20c508ff18babe7b8f864a8c58d8d3200bed0de9d60f2d67f993f3f3c73c0ac0ddbc2aab12dc044aa88d68de52d555ba028002 | a23977009d287ff0b12127d7892d3cb27030e894aa2cca990f0889d35fb504e63864f4d6db00a7ffd2bc8c3719700db5fe954a01736b8150624a6edb8d055d62 |
| **2** | 1caee920cf7d89c5f9263be1288e9190be5bcccf94f0e38e7780a7b3925de2482264e2c86681db1342bb89e9760d4cb7d923f6ca03af75cf0aab0c42a7045bc2 | 0116877d6379d42d4e3e27c28a3ab6a2c299c469d35744465eb6bc33c5f2f94295e2df553d043864cfceab6b7c8629befd1db7e049b8c2132e1123fd3336731c | b3b4637d610e286262200b0588cac7fc129763c01dbaf1fe4c9fe3f52cbef6f6bb01234fbf1efd7c3cee98580f3fbd732461960f35eee6f3349e23e6a2cc1518 |
| **3** | 47392b9b916949e3a9b00d2f6ce4b38c2abf8dae65a7cc7bec56f4cc7546e8c4543597d7e24a6f66c51a02c27dbfd226eedc83f11600487ff5a66dedc30f383e | 41644ed61cfc13fd62317d6c65bece6c9ff3bca3f3b5cc84e2adb5d5b7471f7f398578b9db8c6e0a54913c631004e8b078685e8170beef62cc85ecfcf8b5eae5 | 5e738ac010be9e0072f516fb80188e3c203a419cfafd33b88666285b2a37a8f6cfcdd704fb02a72f87cbc7f830ffbc7b6d56c8a35de0a19cc1cd2d3ee3213d1a |
| **4** | 363910397e2c435f226c7f35f62340f558fc9e989eac4d8e487de17e242abc324eb3149079aa48d771ee82bb6740261a240dd0595fd9b0e215541e508278044d | 0a74f33471363bd092a82d790ae07fd819657069d6cf625352e663574636e16dd6491bcded1fa9a8baa3c5aa426511b6a2c0a56e222f620c5d30ccddfd8ae177 | 73a47beabbce81821c41a2e9bf4f9052f3f316ba1040f5a9b4c000babc4022c1b407ef4fd5da3adc724ed0f8717c0da7d5d1f72c3e4fdd812ffb1bd35aad1cf7 |
| **5** | eeffcc12094f9a3fb9511bf125d68c201c05fbc62b4cbd59babb12b3a0ef4809d5e27264d27145332252fae53865972d5aaeced05c69dad1988fdd2343cb86c7 | 7e963ecbbbc9f246afee94c44fd2dc38f73b762fd260b3a69f9c5bfc627153082134a78e59c3687a1236303e708e477a2b64d85c645baa30940b8862b78a2f45 | a9e2f8cf3c3b7117df52d252853788bb0bff6e3539d95f56fd4b702190544b025157ed62237ea1a79d03902576fb7737c49ed45bc5cf73cf17fb871db3c78f3e |

**Table 7. Hashed value of SHA3-256 algorithm**

| # | Left iris hash | Right iris hash | Fingerprint hash |
|---|---|---|---|
| **1** | 821bd1cd877997ca98c15883f149036efcb36c5549fd3c8f9046fab12a12ad49 | ee6671285a4b2b12469ee69da2b9a56eae41abb49d85bb766ce72ec3ed243004 | 28e5abe08e7bd2f6b26a1c309c177f604ecc9474224a9ab60a1ec01e5a89c0e4 |
| **2** | cac32e9a7fc848126364da35a8cb0b910d214dc152483522c3302fc672929fa1 | 7feff0df043ba03e6f7d5b1202d199012d38faec4cf5bf2c8f89a0ca7352e4a7 | 74cfa2aaaf3bd784309fcf2725c3cc8f18dfc93451c783a1da59ce7ef7bc78c6 |
| **3** | 053261ee807539200cea36fe8d3f643c921deb35c2aa0b172ad4ce450649602f | a34be27b226c53a1bfa86e6566edc5e15e1dfebf1d30319dd24b47edbdcd51b9 | bc1ca1bacea93ef36cdd730ad6cf5b5bb94b2fcd6de009c69e0a1f6028f62a68 |
| **4** | 64d77a6632e04f4c2c763df8eef3979781be9bc8685614fcb2584337ae03170a | 13c32de00f703056e1628481e9b467c9b393f7ed019e24874a6712d4afe3f770 | 46a52425c22531a07f33f07411c9a2469815c49de2613812e7abaf4d08c142da |
| **5** | e3140d91648445cf359cbaed23daad74f4e78fc11d4e9e1ecbfb435b824cf088 | 21ee10ff7a51eeb24856bf9137cde454c2052ac812ba542502cb61cd621beebf | e0302930f391c824d604b2bcf3dc14bd81e2da0a9f62f8b2ce84956425186411 |

## 5. Experimental Results and Discussion

In order to examine and evaluate the proposed model, we proceeded with its implementation by employing various hash algorithms, specifically SHA algorithms and perceptual algorithms. The outcomes of our implementation, which include the success rate of matching the stored templates with the input samples, are also presented. Furthermore, we thoroughly examined the obtained results from the different SHA algorithms and perceptual algorithms to determine the optimal choice in terms of matching accuracy (calculated according to equation 3) and computational efficiency based on elapsed time. This section offers a comprehensive insight into implementing our proposed model and the resulting outcomes.

To enhance comprehension and facilitate result analysis, we have introduced the obtained result of the hashed values extracted from the MySQL database for each algorithm. These tables offer a visual representation of the length and structure of the hashed values. Table 4 shows the obtained results of SHA-1; it illustrates that the hashed value length for SHA-1 consists of 40 hexadecimal characters, corresponding to the algorithm's production of a 160-bit hash value.

Table 5 shows that the length of the hashed value for SHA-256 is 64 hexadecimal characters long, as the algorithm produces a 256-bit hash value. The obtained result of SHA-256 is illustrated in Table 5. The obtained results of SHA-512 are depicted in Table 6; the hashed value's length for SHA-512 is 128 hexadecimal characters. This is because the SHA-512 algorithm generates a 512-bit hash value.

The outcomes achieved through the utilization of the SHA3-256 algorithm are presented in Table 7. This particular algorithm belongs to the SHA-3 algorithm family and is known for its robust ability to prevent collisions. The table demonstrates that the SHA3-256 algorithm generates a hashed value with a length of 64 hexadecimal characters, corresponding to its production of a 256-bit hash value.

Table 8 shows the hashed values for the SHA3-512 algorithm, known for its high security and collision resistance. The algorithm produces a 512-bit hash value, and Table 8 presents the length of the hashed values as 128 hexadecimal characters long.

We examined our model by employing the Perceptual Hashing, Average Hashing, and Difference Hashing algorithms; the obtained results of Average hashing are depicted in Table 9, Table 10 shows the obtained results based on Difference Hash (D-Hash) algorithm, and Table 11 introduces the obtained results of Perceptual Hashing algorithm. The aforementioned algorithms are implemented for hashing the left iris, right iris, and fingerprints.

Table 9 to Table 11 demonstrate that the results obtained using the perceptual hashing family, compared to the SHA family, are more effective in terms of storage requirements for hashed values and the length of the hashed value for each image. The perceptual hash algorithm is known for its capability to generate compact hash values while maintaining the image's identity.

Table 12 provides the average elapsed time for hashing a set of 30 images using the SHA family. The average length of the images is 2426.128 kb, and the average elapsed time for hashing by using SHA-1 is 0.010052284 milliseconds, SHA-256 is 0.019374531 milliseconds, SHA-512 is 0.013015589 milliseconds, SHA3-256 is 0.014943124 milliseconds, and SHA3-512 is 0.025271023 milliseconds.

This information can be useful in determining the most efficient algorithm for a particular application based on the desired level of security and performance.

**Table 8. Hashed value for SHA3-512 algorithm**

| # | Left iris hash | Right iris hash | Fingerprint hash |
|---|---|---|---|
| **1** | 55249b3369e98d68736982d8f1450799ca197bc5b008b5b535d4d203dd9ba6cccd5c11b466e51233529f1f286ed84adc8b1cb3cb2aa4962fcee15d7b89155100 | 0132a0afffcfc76408d639d65f580f76b28f93fca40b999b3538d2bb9e32887dc8efaedb9998c3e22e59a12dc3b6e15183e9dc5a39d6756bdcdee22fbd2f733c | 9678123706708f1a1b0439dec7a1cd43171dfba068b43e261f708328b3f93102b5a6c9fab71ad014dc21920eb85704a0cd89f4156b6ba9473f5a52fc34db4658 |
| **2** | f903c6debcbc135cb9640e58f7ccce30b9f398ad2933c21cbbe74c975294f98d9be702933ca027dae9bba90023680d870abd36130db0388f5282e2b0bebfae31 | 8dc4ff36d8c20963b149a594581a8728ddf248b6a2f199565fec38e0cb8f4c8762b0ee1d7de84467cf0c7a948946687b0dcd1e1ab215228635bb1bce19db8b2c | 1c776d2c82abe0ce7553748d3ed290f08b47d0b7223030700e7279b1f0c3d00b422b36b2ea1af81dd4a45b5c7a37ad126cb3a204d56b1df481ff72de6780ab89 |
| **3** | 611eaa89d8438f639546a5ff6b1c35417600dd8034052331ee9729d9e2ef9fcbf2634e3e085946f062550748de47476549ddd70aea2e20d32f11005954f97f43 | de244de2d5f271affe633e0203e0ade1225c7ce7a312ceb6ae2d508b08d70db41b31c5117a8ce3204abc5c603f7abeeb8dbba15e9ee3e7a904618cd8c2a3f90e | 73d6f3bd2049ac149fb258f51eaa20f840be056412458619887a1baf25e86663a3d65d4660a4f980f6ece4d5eb0539337ec9b770dae4b1e0caa7382df3a44779 |
| **4** | 41c1b3b8c380eab737dba62e429f9681b0a3342827380cfbe33b44e117d8fc415b67441e6e30ca526dae2a44bdb25ea6942fecbee1316165dff6b0b3b7c0a8c5 | a8268ed587bf0d9d298e173224fdf3d48c52438c76e8f02db85c15eaa3867d09ae408f5d459b2b3f75732fd5ae1b0be2debca6632b85ab47afff4242a15e210e | 445de43cc0500de37d2b921da51ef74e04d8a5c974336ec410d2162343e82260f5716d19492bdc3531cd8baf02c2d580b2e84cd2d1b13d40428384211cf280dd |
| **5** | ed3fee35f64ffd37d50875d2e9296cb38ae5c874a965de8df7db83620cd83e3f60eec30a6fe8b21f8fc1af9e9aab398b6355131489e39fbf4e226ae87d55b06d | 511d7f9eaf9c1fae828fb8ca8ad1a2437b1dbffe015d912cf3d4fb87cc54cd7988cd5d8be9e25ba1e0a1530e9f742b17d732054a1668ca19bb3fa6c51f9c3707 | 1ebe92892ba18dccaae865ccce3be729a4377edb3a79c702ec7f4f9b38880fd3171d2a3e38964ae6918f0d38897b0d96fccd3b178b0d7e165964c35b02784276 |

**Table 9. Hashed value for average hash algorithm**

| # | Left iris hash | Right iris hash | Fingerprint hash |
|---|---|---|---|
| **1** | fefee0c0c0e0f8fe | 3f7f67c181c1f77e | f7e3c1c1c1e3e3ff |
| **2** | feffc180c0c0fcfe | ffdf030101c1ffff | c3c3c383c3c3c3ff |
| **3** | feffe0c0e0e0f8fe | fffff3818080f8ff | ffe3e3c1c1c1c1c3 |
| **4** | ffe1c0c0e0e0fcfe | f0c68303c3c3ffff | e7878383838383c7 |
| **5** | fcfcc0c080e0fcfc | f8fcc28001c1ffff | c1c1c1c1c1e3e3e7 |

**Table 10. Hashed value for difference hash algorithm**

| # | Left iris hash | Right iris hash | Fingerprint hash |
|---|---|---|---|
| **1** | 1f3f78f0f0f0fb3f | 070f3178f878190f | 3870707070603818 |
| **2** | 3f7ff0f0f0b3ff7f | 0fe1f0f070701e1f | f0f0f0f0f8f0e870 |
| **3** | 0f1ff9f0f0f9ffdf | 1f1d78f8f8b89c0f | 3878787870707460 |
| **4** | 0bfcf2f2f2b3ff9f | 3ef3e060e064bc3e | e1f1f1e9f1f1f1f1 |
| **5** | 7ffff9f4b2fe7e7f | 1f7ff1f0b0f0fe3e | 7878787878787830 |

**Table 11. Hashed value for perceptual hash algorithm**

| # | Left iris hash | Right iris hash | Fingerprint hash |
|---|---|---|---|
| **1** | f1c7c79c24319893 | e1129e25389b3367 | bfc0c04f2f3c3c90 |
| **2** | f1e5cf986c309898 | b038c36334c79b66 | b827c7f859d808c6 |
| **3** | e18c9c3465929af3 | e3969c67259a9823 | fa85853b1f6a7081 |
| **4** | bd81c02f67368e98 | b0fccbc067619986 | ff7b80e04c813396 |
| **5** | b082cecc3c7199d9 | a1f69e4622cc9999 | aed1c92752282b1f |

**Table 12. Average elapsed time (millisecond) of SHA-1, SHA-256, SHA-512, SHA3-256, and SHA3-512 algorithms**

| Input Size (KB) | SHA1 | SHA-256 | SHA-512 | SHA3-256 | SHA3-512 |
|---|---|---|---|---|---|
| 2426.128 | 0.010052284 | 0.019374531 | 0.013015589 | 0.014943124 | 0.025271023 |

**Table 13. Average elapsed time (millisecond) of perceptual algorithms**

| Input Size (KB) | Perceptual hash | Average hash | Difference hash |
|---|---|---|---|
| 2426.128 | 0.166455189 | 0.068173806 | 0.077802579 |

**Table 14. SHA Family - Number of success matching and percentage of success for 30 Person**

| Algorithm | 1 Sample | | 2 Sample | | 3 Sample | | 4 Sample | |
|---|---|---|---|---|---|---|---|---|
| | Number of Success | Percentage of Success | Number of Success | Percentage of Success | Number of Success | Percentage of Success | Number of Success | Percentage of Success |
| **SAH1** | 2 | 6.66% | 3 | 10% | 3 | 10% | 2 | 6.66% |
| **SHA-256** | 0 | 0% | 0 | 0% | 1 | 3.33% | 0 | 0% |
| **SHA-512** | 3 | 10% | 2 | 6.66% | 2 | 6.66% | 1 | 3.33% |
| **SHA3-256** | 0 | 0% | 0 | 0% | 0 | 0% | 0 | 0% |
| **SHA3-512** | 0 | 0% | 0 | 0% | 0 | 0% | 0 | 0% |

**Table 15. Perceptual Family - Number of success matching and percentage of success for 30 person**

| Algorithm | 1 Sample | | 2 Sample | | 3 Sample | | 4 Sample | |
|---|---|---|---|---|---|---|---|---|
| | *Number of Success* | *Percentage of Success* | *Number of Success* | *Percentage of Success* | *Number of Success* | *Percentage of Success* | *Number of Success* | *Percentage of Success* |
| **Perceptual hash** | 14 | 46.66% | 16 | 53.33% | 18 | 60% | 25 | 83.33% |
| **Average hash** | 12 | 40% | 19 | 63.33% | 21 | 70% | 20 | 66.66% |
| **Difference hash** | 16 | 53.33% | 19 | 63.33% | 23 | 76.66% | 25 | 83.33% |

The SHA-1 algorithm gives the best average elapsed time, with a value of 0.010052284 milliseconds, whereas the SHA3-512 algorithm demonstrates the worst average elapsed time at 0.025271023 milliseconds. This data can be valuable when selecting the most efficient algorithm for a specific application, considering the desired level of security and performance. It is widely recognized that SHA3-512 is considered more secure than other SHA algorithms.

On the other hand, Table 13 shows the average elapsed time of the perceptual, average and difference hashing algorithms. It is clear from the table that the perceptual hashing algorithm takes the longest time, at 0.166455189 milliseconds, while the average and difference hashing algorithms take slightly less time at 0.068173806 and 0.077802579 milliseconds, respectively. This data provides valuable information for choosing the most efficient algorithm for a particular application.

The second phase, the verification phase, is tested using an authorized person and an unauthorized person; the authentication system succeeds in verifying process. Table 14 illustrates the obtained results from the verification phase of the authentication system based on the SHA family.

Table 14 presents the results for the SHA family of algorithms, revealing that the number of successful matches was relatively low, with the highest percentage of success being 10% for SHA-1 when using three samples for each person. The results for SHA-512 have the best matching in the case of 1 sample and then oscillate for 2, 3 and 4 samples, respectively.

The results for SHA-256 have zero matches when using one or two samples and a slight increase in matches when using three samples but then decrease again when using four samples. SHA3-512 and SHA3-256 had no successful matches throughout all the trials. These results indicate that using the SHA family of algorithms alone may not be sufficient for achieving accurate and reliable biometric authentication.

The obtained results from the implementation of perceptual hashing algorithms are included in Table 15. The obtained results in Table 15 show the verification phase of the authentication system for the Perceptual hash family. The matching process results for the Perceptual Hash algorithm show a significant number of successful matches as the number of samples stored for each person increases. With 14 matches for 1 sample, 16 matches for 2 samples, 18 matches for 3 samples, and 25 matches for 4 samples, it can be seen that the Perceptual Hash algorithm is more effective when more samples are used.

On the other hand, the Average Hash algorithm is not as stable, with 12 matches for 1 sample, 19 matches for 2 samples, 21 matches for 3 samples, and 20 matches for 4 samples. The Difference Hash algorithm, however, performed similarly to the Perceptual Hash algorithm with 16 matches for 1 sample, 19 matches for 2 samples, 23 matches for 3 samples, and 25 matches for 4 samples.

Overall, the Perceptual Hash and Difference Hash algorithms had a matching rate of 83.33%, which is considered very high.

## 6. Conclusion

The multi-biometric authentication model was successfully implemented and tested, combining fingerprint, left iris, and right iris. The implementation results revealed that the SHA family of algorithms, particularly SHA-1 and SHA-512, yielded the highest number of successful matches compared to other algorithms, such as SHA-256, SHA3-256, and SHA3-512. However, it was found that the SHA hashed algorithm family is not ideal for multi-biometric authentication.

On the other hand, the utilization of perceptual hashing algorithms, including Perceptual Hash and Difference Hash, resulted in the highest number of successful matches, achieving a maximum of 25 out of 30 matched individuals when using 4 samples per person. The study also demonstrated that increasing the number of samples per person improved the accuracy of the authentication system, with the highest accuracy achieved using 4 samples per person. Nonetheless, further improvements can be made to the proposed model by implementing more advanced and sophisticated image hashing and matching algorithms. Additionally, incorporating additional biometric modalities can enhance the accuracy and security of the model.

The proposed model holds potential applications in various fields, such as security systems, access control, and personal identification. By enhancing the performance of the biometric system while ensuring user privacy, the proposed model presented a promising solution for multi-biometric authentication.

## References


[1] Maria Papathanasaki, Maglaras Leandros, and Nick Ayres, “Modern Authentication Methods: A Comprehensive Survey,” *AI, Computer Science and Robotics Technology*, pp. 1-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] R. Neha, and P. Monica, “A Review of Advancement in Multimodal Biometrics System,” *International Journal of Scientific & Engineering Research*, vol. 7, no. 12, pp. 241-248, 2016. [Google Scholar] [Publisher Link]

[3] B. Miller, "Everything you need to Know about Biometric Identification,” Personal Identification News 1988 Biometric Industry Directory, Washington DC: Warfel& Miller Inc., Washington DC, 1988.

[4] James L. Wayman, “*National Biometric Test Center Collected Works 1997–2000,”* San Jose State University, 2000. [Google Scholar] [Publisher Link]

[5] Bart Preneel, René Govaerts, and Joos Vandewalle, “Cryptographic Hash Functions: An Overview,” *Proceedings of the 6th International Computer Security and Virus Conference*, vol. 19, 1993. [Google Scholar] [Publisher Link]

[6] Rui Zhang, and Zheng Yan, “A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification,” *IEEE Access*, vol. 7, pp. 5994-6009, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[7] Atul N. Kataria et al., “A Survey of Automated Biometric Authentication Techniques,” *Nirma University International Conference on Engineering, IEEE*, pp. 1-6, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[8] Anil K. Jain, Arun Ross, and Salil Prabhakar, “An Introduction to Biometric Recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[9] Dapeng Zhang, and Wei Shu, “Two Novel Characteristics in Palmprint Verification: Datum Point Invariance and Line Feature Matching,” *Pattern Recognition*, vol. 32, no. 4, pp. 691-702, 1999. [CrossRef] [Google Scholar] [Publisher Link]

[10] Delac Kresimir, and Mislav Grgic, “A Survey of Biometric Recognition Methods,” *Proceedings Elmar-2004, 46th International Symposium on Electronics in Marine, IEEE*, pp. 184-193, 2004. [Google Scholar] [Publisher Link]

[11] Alfred Victor Iannarelli, *Ear Identification*, Paramont Publishing Company, 1989 [Publisher Link]

[12] Mark Burge, and Wilhelm Burger, “Ear Biometrics in Computer Vision,” *Proceedings 15th International Conference on Pattern Recognition*, vol. 2, pp. 822-826, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[13] AlMahafzah, Harbi, and Maen Zaid Al Rwashdeh, “A Survey of Multibiometric Systems,” *arXiv preprint, Computer Vision and Pattern Recognition*, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[14] Mohamed Deriche, “Trends and Challenges in Mono and Multi Biometrics,” *First Workshops on Image Processing Theory, Tools and Applications, IEEE*, pp. 1-9, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[15] M. S. Ahuja, and S. Chabbra, "A Survey of Multimodal Biometrics," *International Journal of Computer Science and its Application*s, vol. 1, no. pp. 157-160, 2011.

[16] Mahesh Kale, and Shrikant Dhamdhere, “Survey Paper on Different Types of Hashing Algorithm,” *International Journal of Advance Scientific Research Algorithm*, vol. 3, no. 2, pp. 14-16, 2018. [Google Scholar] [Publisher Link]

[17] Ahmed Y. Mahmoud, “A Novel Hash Functions for Data Integrity Based on Affine Hill Cipher and Tensor Product,” *International Journal of Engineering Trends and Technology,* vol. 70, no. 11, pp. 1–9, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Andrea Drmic et al., “Evaluating Robustness of Perceptual Image Hashing Algorithms,” *40th International Convention on Information and Communication Technology, Electronics and Microelectronics, IEEE*, pp. 995-1000, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[19] William Stallings, *Cryptography and Network Security, Principles and Practice*, 8th Edition, Pearson, 2023. [Google Scholar] [Publisher Link]
[20] Zauner Christoph, "*Implementation and Benchmarking of Perceptual Image Hash Functions*," Thesis, Sichere Informations Systeme in Hagenberg, 2010. [Google Scholar] [Publisher Link]
[21] Ann Cavoukian, Alex Stoianov, and Fred Carter, "Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security and Privacy," *Policies and Research in Identity Management,* vol. 261, pp. 55-77, 2008. [CrossRef] [Google Scholar] [Publisher Link]
[22] Abeng Enangha Eyam, and W. Adebisi Adesola, "Application of Hybrid Hash Message Authentication Code Approach in Biometrics Information System Design," *Global Journal of Pure and Applied Sciences,* vol. 18, no. 1, pp. 59-66, 2012. [Google Scholar] [Publisher Link]
[23] Idrus, Syed Zulkarnain Syed et al., "A Review on Authentication Methods," *Australian Journal of Basic and Applied Sciences*, vol. 7, no. 5, pp. 95-107, 2013. [Google Scholar] [Publisher Link]
[24] Bigun Josef et al., "Multimodal Biometric Authentication Using Quality Signals in Mobile Communications," *12th International Conference on Image Analysis and Processing*, pp. 2-11, 2003. [CrossRef] [Google Scholar] [Publisher Link]
[25] Julian Fierrez-Aguilar et al., "Kernel-Based Multimodal Biometric Verification Using Quality Signals," *Biometric Technology for Human Identification*, vol. 5404, 2004. [CrossRef] [Google Scholar] [Publisher Link]
[26] Josef Kittler et al., "Quality Dependent Fusion of Intramodal and Multimodal Biometric Experts," *Biometric Technology for Human Identification*, vol. 6539, 2007. [CrossRef] [Google Scholar] [Publisher Link]
[27] Karthik Nanda Kumar et al., "Likelihood Ratio-Based Biometric Score Fusion," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 30, no. 2, pp. 342-347, 2007. [CrossRef] [Google Scholar] [Publisher Link]
[28] Gatheejathul J. Kubra, and P. Rajesh et al., "Iris Recognition and its Protection Overtone using Cryptographic Hash Function," *SSRG International Journal of Computer Science and Engineering*, vol. 3, no. 5, pp. 1-9, 2016. [CrossRef] [Publisher Link]
[29] Fronthaler Hartwig et al., "Fingerprint Image-Quality Estimation and Its Application to Multi Algorithm Verification," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 2, pp. 331-338, 2008. [CrossRef] [Google Scholar] [Publisher Link]
[30] Yi Chen, Sarat C. Dass, and Anil K. Jain, "Fingerprint Quality Indices for Predicting Authentication Performance," *International Conference on Audio- and Video-Based Biometric Person Authentication*, vol. 3546, pp. 160-170, 2005. [CrossRef] [Google Scholar] [Publisher Link]
[31] Xiufeng Gao et al., "Standardization of Face Image Sample Quality," *Advances in Biometrics: International Conference*, vol. 4642, pp. 242-251, 2007. [CrossRef] [Google Scholar] [Publisher Link]
[32] National Institute of Standards and Technology, Nist Speech Quality Assurance Package 2.3 Documentation," Hashing Algorithms.
[33] Müller Sascha, and Olaf Henniger, "Evaluating the Biometric Sample Quality of Handwritten Signatures," *Advances in Biometrics: International Conference on Biometrics*, vol. 4642, pp. 407-414, 2007. [CrossRef] [Google Scholar] [Publisher Link]
[34] Bengio Samyet al., "Confidence Measures for Multimodal Identity Verification," *Information Fusion*, vol. 3, no. 4, pp. 267-276, 2002. [CrossRef] [Google Scholar] [Publisher Link]
[35] Norman Poh, and SamyBengio, "Improving Fusion with Margin-Derived Confidence in Biometric Authentication Tasks," *International Conference on Audio- and Video-Based Biometric Person Authentication*, vol. 3546, pp. 474-483, 2005. [CrossRef] [Google Scholar] [Publisher Link]
[36] G. Prabhu, and S. Poornima, "Minimize Search Time through Gender Classification from Multimodal Biometrics," *Procedia Computer Science*, vol. 50, pp. 289-294, 2015. [CrossRef] [Google Scholar] [Publisher Link]
[37] Razzak Muhammad Imran, Rubiyah Yusof, and Marzuki Khalid, "Multimodal Face and Finger Veins Biometric Authentication," *Scientific Research and Essays*, vol. 5, no. 17, pp. 2529-2534, 2010. [CrossRef] [Google Scholar] [Publisher Link]
[38] Soltane Mohamed, Noureddine Doghmane, and Noureddine Guersi, "Face and Speech Based Multi-Modal Biometric Authentication," *International Journal of Advanced Science and Technology*, vol. 21, pp. 41-56, 2010. [Google Scholar] [Publisher Link]
[39] Dalka Piotr, and Andrzej Czyzewski, "Human-Computer Interface Based on Visual Lip Movement and Gesture Recognition," *International Journal of Computer Science and Applications*, vol. 7, no. 3, pp. 124-139, 2010. [Google Scholar] [Publisher Link]
[40] A.A. Darwish, R. Abd Elghafar, and A. Fawzi Ali, "Multimodal Face and Ear Images," *Journal of Computer Science*, vol. 5, no. 5, pp. 374-379, 2009. [CrossRef] [Google Scholar] [Publisher Link]
[41] Chander Kant, "Performance Improvement of Biometric System using Multimodal Approach," *International Journal of Innovations & Advancement in Computer Science*, pp. 2347-8616, 2014.
[42] Shigefumi Yamada, Toshio Endoh, and Takashi, "Evaluation of Independence between Palm Vein and Fingerprint for Multimodal Biometrics," *Proceedings of the International Conference of Biometrics Special Interest Group, IEEE*, pp. 1-4, 2012. [Google Scholar] [Publisher Link]
[43] V.D. Mhaske, and A.J. Patankar, "Multimodal Biometrics by Integrating Fingerprint and Palmprint for Security," *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-5, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[44] Vadhera Priyanka, and Bhumika Lall, "Review Paper on Secure Hashing Algorithm and Its Variants," *International Journal of Science and Research*, vol. 3, no. 6, pp. 629-632, 2014. [Google Scholar] [Publisher Link]

[45] Surbhi Aggarwal Gupta, Neha Goyal, and Kirti Aggarwal, "A Review of Comparative Study of MD5 and SHA Security Algorithm," *International Journal of Computer Applications*, vol. 104, no. 14, pp. 1-4, 2014. [Google Scholar] [Publisher Link]

[46] Shah B. Chaitya, and Drashti R. Panchal, "Secured Hash Algorithm-1: Review Paper," International *Journal of Advanced Research in Engineering Technology and Sciences*, vol. 2, pp. 26-30, 2014. [Google Scholar]

[47] Sampada Abhijit Dhole et al., "Multimodal Biometric Identification System using Random Selection of Biometrics," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 10, no. 1, pp. 63-73, 2023. [CrossRef] [Publisher Link]

[48] Viies Vladimir, "*Possible Application of Perceptual Image Hashing*," Master thesis, Tallinn University of Technology, Faculty of Information Technology, Department of Computer Engineering, 2015. [Google Scholar]

[49] Yang Xin, Qiang Zhu, and Kwang-Ting Cheng, "My Finder: Near-Duplicate Detection for Large Image Collections," *Proceedings of the 17th ACM International Conference on Multimedia*, pp. 1013-1014, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[50] Weiss Yair, Antonio Torralba, and Rob Fergus, "Spectral Hashing," *Proceedings of the 21st International Conference on Neural Information Processing Systems*, pp. 1753-1760, 2008. [Google Scholar] [Publisher Link]

[51] Wang Jun, Sanjiv Kumar, and Shih-Fu Chang, "Semi-Supervised Hashing for Scalable Image Retrieval," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pp. 3424-3431, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[52] Chum Ondrej, James Philbin, and Andrew Zisserman, "Near Duplicate Image Detection: Min-hash and TF-IDF weighting," *Proceedings of the British Machine Vision Conference*, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[53] R. Nanmaran et al., "Design and Development of an Improved Multimodal Biometric Authentication System using Machine learning Classifiers," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 10, no. 5, pp. 14-22, 2023. [CrossRef] [Publisher Link]

[54] Liu Wei et al., "Hashing with Graphs," *Proceedings of the 28th International Conference on Machine Learning*, pp. 1-8, 2011. [Google Scholar] [Publisher Link]

[55] Kulis Brian, and Kristen Grauman, "Kernelized Locality-Sensitive Hashing for Scalable Image Search," *IEEE 12th International Conference on Computer Vision*, pp. 2130-2137, 2009. [Google Scholar] [Publisher Link]

[56] Lin Kevin et al., "Deep Learning of Binary Hash Codes for Fast Image Retrieval," *IEEE Conference on Computer Vision and Pattern Recognition Workshop*, pp. 27-35, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[57] Rongkai Xia et al.., "Supervised Hashing for Image Retrieval via Image Representation Learning," *28thAAAI Conference on Artificial Intelligence*, vol. 28, no. 1, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[58] Talreja Veeru et al., "Deep Hashing for Secure Multimodal Biometrics," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1306-1321, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[59] Sutcu Yagiz, Husrev Taha Sencar, and Nasir Memon, "A Secure Biometric Authentication Scheme Based on Robust Hashing," *Proceedings of the 7th Workshop on Multimedia and Security*, pp. 111-116, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[60] Kryszczuk Krzysztof, and Andrzej Drygajlo, "Credence Estimation and Error Prediction in Biometric Identity Verification," *Signal Processing*, vol. 88, no. 4, pp. 916-925, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[61] Pooja Goyal, Sushil Kumar, and Komal Kumar Bhatia, "Hashing and Clustering Based Novelty Detection," *SSRG International Journal of Computer Science and Engineering*, vol. 6, no. 6, pp. 1-9, 2019. [CrossRef] [Publisher Link]

[62] Verma Sandhya, and G.S. Prajapati, "A Survey of Cryptographic Hash Algorithms and Issues," *International Journal of Computer Security & Source Code Analysis*, vol. 1, no. 3, pp. 17-20, 2015. [Google Scholar] [Publisher Link]

[63] Chum Ondrej, Michal Perd'och, and Jiri Matas, "Geometric Min-Hashing: Finding a (thick) Needle in a Haystack," *IEEE Conference on Computer Vision and Pattern Recognition*, pp. 17-24, 2009. [CrossRef] [Google Scholar] [Publisher Link]