Multimedia Tools and Applications (2024) 83:74785–74812
https://doi.org/10.1007/s11042-023-16479-3

Implementation of quaternion mathematics for biometric security

Fatma Khallaf[1,2] · **Walid El-Shafai**[1,3] · **El-Sayed M. El-Rabaie**[1] · **Mahmoud Nasr**[4,5] · **Mohammed Essam**[6] · **E. S. Shoukralla**[4] · **Saied M. Abd El-atty**[1] · **Fathi E. Abd El-Samie**[1,7]

Received: 1 November 2022 / Revised: 30 July 2023 / Accepted: 8 August 2023 /
Published online: 12 February 2024

Abstract

Cancellable biometrics is an important trend in biometric security systems, allowing for intentional distortions or variations in the original biometric data to be used for authentication, while preserving privacy of users and security of the original data. This paper presents two cancellable biometric recognition algorithms based on quaternion mathematics. The first algorithm depends on the Fractional Fourier transform (FRFT) with quaternion mathematics to induce intentional distortions in biometric data, while the second algorithm relies on quaternion rotation to achieve the desired level of distortion. Both algorithms are evaluated using Equal Error Rate (EER) and Area under Receiver Operating Characteristic curve (AROC). The simulation results indicate that both algorithms achieve EER values close to 0 and AROC values close to 1, demonstrating their effectiveness and reliability for cancellable biometric recognition. The proposed cancellable biometric recognition algorithms are intended to preserve privacy of users and security of biometric data, while maintaining high levels of accuracy and performance. The use of quaternion mathematics allows for intentional distortions to be introduced in a controlled and secure manner, ensuring that the original biometric data remains protected from either hacking or unauthorized access. In conclusion, the proposed cancellable biometric recognition algorithms based on quaternion mathematics are reliable and effective solutions for biometric security, providing both security and privacy preservation within the biometric authentication process.

Keywords Cancellable biometrics · Security systems · Optical encryption · Face recognition · Quaternion mathematics · FRFT

1 Introduction

As a result of the huge technological development and progress in penetrating personal accounts and attacks, there was a need to develop several techniques to increase the security level during the authentication process for users and guarantee that the personal accounts are far from spoofing and forgery. Authentication systems based on biometrics

Extended author information available on the last page of the article for identifying personal data were implemented. Biometric traits are often divided into behavioral and physiological modalities. The physiological biometric modalities include fingerprint, ear shape, face, iris, hand geometry, vein, and retina [2]. Face recognition depends on the spatial geometry of the face -its size, shape, and structure- as criteria to identify individuals. Moreover, face recognition is one of the preferred methods of recognizing individuals. Pigmented portion of the attention is to the iris that remains the same throughout life. The physical characteristics of the hand, such as its length, width, size, finger shape, and spacing between fingers, are determined through hand geometry recognition.

Figure 1 illustrates how behavioral modalities like signature, voice, gait, and keystroke reflect human behavior. A dynamic signature, which represents the writing speed, direction, pressure, and time to completion, can be used to identify persons due to their distinctive writing styles. A singular writing style of an individual helps to identify him according to the dynamic signature that corresponds to the speed, the direction of writing, the pressure applied while writing, and the time taken to end the signature. The dynamics of a keystroke reflect the speed, pressure, and time it takes to type a certain word.

Although biometric identification systems can provide better solutions than systems depending on passwords or tokens in the identification process, there is still a critical problem, as traditional biometric authentication systems may be subject to fraud or reproducibility [4]. For example, fingerprint biometrics can be reproduced by gummy fingers through the use of gelatin-based candy to hold and save the original fingerprints of users. Also, face biometric images can be stolen, and so on, for many other

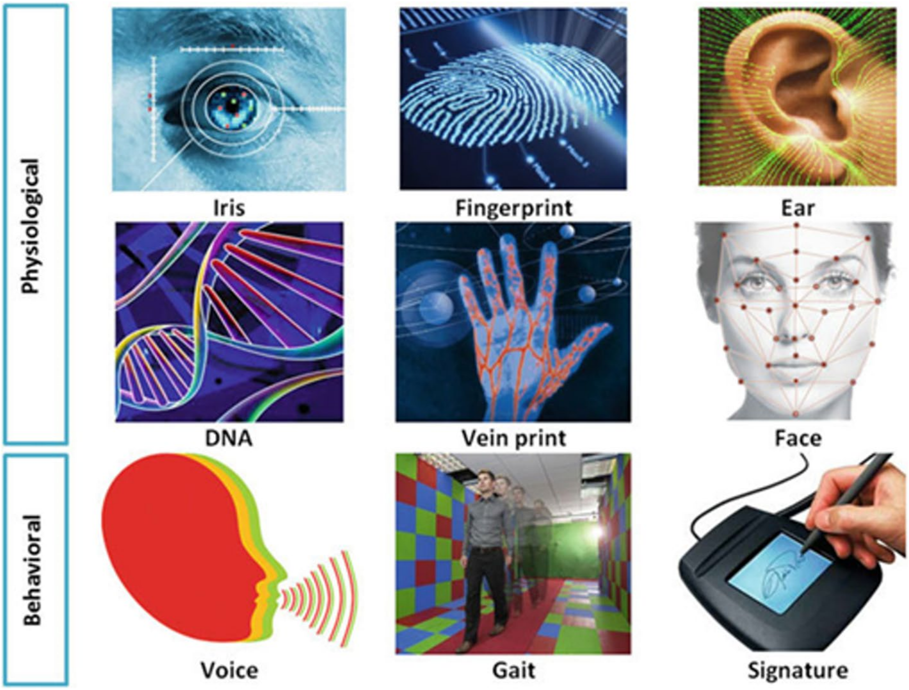


Fig. 1 Types of biometrics [2]

biometrics. Once the original biometric trait is stolen or hacked, there is nothing one can do to secure his/her biometric trait again, and it will be lost forever.

The solution for building robust and secure authentication systems is to use cancellable biometrics. Cancellable biometrics means intentionally distorted or encrypted versions of the original biometrics that can be used for the authentication process. The objective of using cancellable biometrics is to keep the original ones away from utilization and hence hacking attempts, while keeping the ability to discriminate between users. Hence, it is required in a cancellable biometric system to use either non-invertible transforms, distortion functions or strong encryption algorithms to generate the cancellable biometric templates.

To avoid hacking of the stored biometrics of persons, many researchers have developed approaches to guarantee high security levels of original templates by generating highly-distorted or encrypted biometrics to be stored in databases instead of the original ones [7]. However, in the case that the transformed or encrypted templates are hacked, it should be difficult to reconstruct the original data.

There are important requirements that should be satisfied for any proposed approach to achieve high protection levels for original biometric templates stored in a database. These requirements include security, discriminability, and ability to cancel templates and replace them. Security means ensuring that the original biometric templates cannot be reconstructed using the modified ones. Discriminability means the ability to keep the original features without any degradation. Finally, there should be an ability for generating other distorted templates for the authentication process in case the original templates have been attacked or stolen [5, 10, 11, 14].

With the development of mathematics over decades, the branch of quaternion mathematics has evolved as a solution to several complex problems. Quaternion mathematics is based on complex numbers that comprise one real part and three complex parts. Quaternion mathematics was introduced to solve the rotation problems of dynamic systems. This trend has come soon to all branches of science. It found applications in signal and image processing, such as adaptive filtering, image encryption, and 3-D graphics [1].

Cancellable biometrics is an improved way towards more secure biometric systems. This study presents a novel approach for building cancellable biometric systems. The quaternions are used to represent color images acquired as biometrics. The three complex parts of the quaternion used in this paper represent the color image components, while the real part is kept to zero. Quaternion mathematical operations are developed to generate intentionally-distorted versions of the biometrics to be used for identification instead of the original biometrics. The intended distortion effect resembles the encryption effect, as it masks the details of the original biometric images. This trend of using alternatives for original biometrics is known as cancellable biometrics. Its major objective is to save the original biometrics from being hacked if they are used in biometric databases. Two algorithms are presented in this paper for the generation of cancellable biometrics. The first one depends on the utilization of FRFT with quaternion mathematics. The second one depends on the rotation process with Fast Fourier Transform (FFT). Evaluation metrics utilized to assess the proposed algorithms are also presented.

The most important contributions of this paper are introduced as follows:

- Securing the face recognition process through the utilization of quaternion mathematics.
- Generating cancellable face templates from original face images to be utilized instead of the original faces in biometric databases.

- Adopting a statistical framework for the classification process based on the correlation estimates to remove the need to retrieve the original biometrics in the verification process.
- Evaluating the suggested framework performance using several security criteria.
- Proposal of two algorithms based on quaternion mathematics for generating cancellable biometric data from color images.
- Ability of these algorithms to induce intentional distortions in biometric templates in a controlled and secure manner, while maintaining high levels of accuracy and performance for cancellable biometric recognition.
- Utilization of quaternion mathematics for ensuring that the original biometric data remains protected from hacking and unauthorized access, preserving the privacy of users and the security of biometric data.
- Evaluation of both proposed algorithms using EER and ROC curves in the cancellable biometric recognition framework, with simulation results indicating their effectiveness and reliability.
- Investigation of the cancellable biometric algorithms based on quaternion mathematics as reliable and effective solutions for biometric authentication.

The remainder of the paper is structured accordingly. The preliminaries of related work are presented in Section 2. Section 3 includes the proposed algorithms using quaternion mathematics for biometric security. Also, the discussion and comparison of algorithms are given in Section 4. Finally, Section 5 introduces the concluding remarks and future directions for research.

2 Preliminaries of related work

2.1 Biometrics brief history

Biometrics is the study of human metrics, and it has a long history that dates to prehistoric times. Biometric recognition is an old concept and method of identifying individuals based on their physical or behavioral characteristics. Instead of using conventional methods to identify people, biometric traits offer greater security and are more appropriate. In addition, biometric recognition can either support or replace existing techniques in several applications. The objective of this paper is to provide a detailed analysis and comparison of novel biometric recognition methods with those currently in use. Face recognition is an example of the oldest and most fundamental biometric recognition techniques, as faces have been used to differentiate between known and unknown individuals since the start of civilization [6, 8, 9]. Table 1 allows us to examine some of the most significant historical turning points in the evolution of biometrics [16, 20, 24, 37].

The main advantage of biometrics is uniqueness. The idea of biometric recognition depends on feature extraction from biometric images, and then features are classified, efficiently. Unfortunately, with the advances in hacking technology, it has become easy for intruders to acquire biometrics or features saved in databases for all persons. If these biometrics or features are illegally captured, they would be destroyed, permanently. Hence, cancellable biometrics must be developed to protect original biometrics from hacking. Cancellable biometrics can be built with encryption schemes or non-invertible transformations to induce the intended distortion of biometrics. Encryption schemes need certain algorithm steps and keys. The original biometrics can be recovered if the decryption is possible and the key is known. On the other hand,

Table 1 Timeline of biometrics

Timeline	Summary	Timeline	Summary
1858	This was Sir William Herschel. The first standardized hand imaging system was created by the Indian civil service.	1996	Commencement of the MST-hosted annual speaker evaluations.
1870	Alphonse Benillon developed “BeniHemp” or anthropometries, to identify individuals using body measurements, physical descriptions, and images.	1997	NSA published the first commercial version, which is the generic biometric interpretability standard.
1892	A fingerprint classification scheme based on details was created by Sir Francis Gallon and is still used to classify individuals.	1998	The FBI launched the Combined DNA Index System (CODIS), which allows users to browse, search, and retrieve DNA forensic data, digitally.
1894	The Tragedy of Pudd’nhead Wilson introduced the idea of a fingerprint identification database.	1999	A comparison of biometrics and machine-readable travel documents has begun.
1896	Sir Edward Henry developed a fingerprint classification system. The General Inspector of Bengal Police for many years, and the FBI have used it.		Major IAFIS components for the FBI have started working,
1903	Fingerprints were utilized by the New York State Prison system to identify criminals.	2000	The First Face Recognition Vendor Test (FRVT 2000) was held.
	Since the measures between two individuals were insufficient, the Benillon system collapsed.		First research paper on vascular patterns for recognition was published.
1907	Hungarians developed the Palm System, which was used in criminal matters.		West Virginia University (WVU) and the FBI launched a biometrics degree program.
1921	Fingaprira analysis department was founded by the FBI.	2001	Fax recognition technology was deployed at the Super Bowl in Tampa, Florida.
1936	Phillainvinisi Frank Burch proposed his pattern for identification purposes.	2002	A biometric standards committee for the International for Standardization Organization (ISO) was established.
1960	Woodrow W. Bledsoe developed the first semi-automated face recognition system.		Formation of Nil Technical Committee on Biometrics.
	A Swedish professor, Gunnar Fent, created the first model of acoustic speech production.		The Identification Service has received a paper on the Integrated Automated Fingerprint Identification System (IAFIS) using palm print technology.
1966	Hughes published a research paper on fingerpaint automation.	2003	The International Civil Aviation Organization (ICAO) adopted a framework for the incorporation of biometrics into machine-readable travel documents.
	Noah America Aviation launched the initial study on automated signature recognition.		European Biometrics Forum was established.

Table 1 (continued)

Timeline	Summary	Timeline	Summary
1969	The FBI attempted to recognize fingerprints, automatically, using NIST recognition framework.	2004	The United States Visitor and Immigrant Status Technology (US-V1SIT) moved into operation.
1970	Face recognition was developed by Goldstein, Hamron, and Lesk for additional automation.		To detect and identify rational security threats, the US Department of Defense (DoD) developed the Automated Biometric Identification System (ABIS).
	The behavioral components of speech were initially modelled by Dr. Joseph Perkell.		For all contractors and employees of the government, Homeland Security Presidential Directive No. 12 (IISPD.12) was issued by President Bush and all employees were forced to have personal identity cards.
1974	First commercial hand geometry system became available.		In Connecticut, Rhode Island, and California, the first state-wide automated palm print databases were established.
1976	The FBI and NIST collaborated to develop the Fim Automated Fingerprint, which uses sensors for extracting minute details.		Face Recognition Grand Challenge (FRGC) started creating algorithms to enhance certain face recognition applications of interest.
	The US Air Force and the MITRE Corporation evaluated the first speaker recognition prototype created by Texas Instruments.	2005	The iris recognition patent from the US has expired.
1977	Patent rights to collect dynamic signature data were granted to Veripen.lnc.		The Intelligence Technology Innovation Center (ITIC) announced the prototype for iris on the move at the biometrics consortium conference.
1980	The NIST Speech Group was founded to promote the use of speech processing techniques.	2006	USA and EU issued biometric passports.
1983	According to a theory put forth by ophthalmologists, Leonard Flom and Araan Safier, there are no two irises that are identical.	2008	The FBI and DoD began developing biometric databases with fingerprint, iris, face, and palm print data.
1984	A patent was granted to David Sidlauskas for a hand identification system.		Hungarian NPP deployed Hand Geometry Identification (HGI).
1986	The exchange of fingerprint minutiae data standard was published by NIST and ANSI. It is the first version of the existing fingerprint interchange standards.	2009	Hungary issued biometrics passports.
	Drs. Leonard Flom and Aran Safrr received a patent indicating that the iris can be used for identification.	2009	Hitachi developed finger vein scanner.
1987	Eigenfaces, a technology for face identification created by Kirby and Sirovich, was used.	2010	The US national security apparatus unified biometrics for identifying terrorists.

Table 1 (continued)

Timeline	Summary	Timeline	Summary
1988	First semi-automated facial recognition system deployment.	2011	Osama bin Laden's body was identified using biometrics by combining facial recognition with DNA.
1991	Facial detection was introduced by Turk and Pentland for accurate tuna face identification.		India deployed mass Iris Recognition System (IRS).
1992	The biometric consortium was founded by the National Security Agency of the US government.	2013	Apple Inc. created and released Touch ID, a fingerprint-based security feature that is accessible on all iPhone and iPad models.
1993	The Face Recognition Technology (FERET) initiative was started by the Defense Advanced Research Products Agency (DARPA).	2014	Hungarian Stadium displayed a vein scanner.
1994	Dr. John Daugman has a patent for his first algorithm for iris recognition.	2016	Hungary deployed biometric personal ID cards.
	There was a competition for the Integrated Automated Fingerprint Identification System (IAFIS).		There was a Windows Hello option. With simply a glance (face) or a touch (fingerprint), which is enterprise-grade security without the need to fill in a password, users were able to sign into Windows 10 in a more private manner.
	Hungarian company was benchmarked for Palm System.	2017	Researchers have created a way to use wearable device technology, such as smart watches and activity trackers, to authenticate handwritten signatures.
	Biometrics were implemented by the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS).		A wearable device secured by wrist vein patterns that may be used for access control, ticketing, ID management, environmental personalization, and more was presented.
1995	The iris prototype was a commonly available product.		The new field of technology, namely Internet of Things (IoT), was introduced. It has significant potential for biometrics at work, home, and vehicles.
1996	The committee of the Olympic Games in Atlanta used hand geometry.		With Akira voice recognition platform, smart speaker devices like Amazon Echo and Google offered a chance to connect voice biometrics, voice control, and speech recognition.
			Jaguar Land Rover has patented a Monistic system that uses a combination of facial and gait recognition to let car owners access the door. Other automakers tested various models with sensors built into door handles, key fobs, steering wheels, and mains-raw.

non-invertible transformations do not allow original biometrics to be recovered, but they are not efficient enough to induce the encryption effect. Hence, in this paper, we will depend on quaternion mathematics in developing biometric hiding schemes to be valid for cancellable biometric applications. The biometric hiding process is an encryption-like process.

2.1.1 Specifications of biometric structures

All biometrics have advantages and disadvantages in the identification process, as it is challenging to directly compare two things. Several comparison criteria have been established by researchers as follows [3]:

- ***Uniqueness:*** Everyone needs to have special characteristics. This signifies distinct informational content.
- ***Permanence:*** The biometric trait should be long-lasting and sufficiently stable.
- ***Performance:*** Accuracy, speed, and security of the whole system should be high.
- ***Circumvention:*** The act of cheating someone should be eliminated.
- ***Computational time:*** The speed at which two templates may be created and checked for identification should be high, since each record in the database must be compared to the user's biometric information.
- ***Accuracy:*** It is a measure of how well the system performs in the environment.

2.1.2 Functionality of the biometric system

The two fundamental phases of all biometric-based authentication systems are enrollment and authentication. Each phase has four main steps: biometric data acquisition, preprocessing, feature extraction, and template generation [7]. A user is registered with the acquired biometric data during the enrolment phase. On the other hand, the user is identified during the authentication phase by comparing the current biometric features with previously-saved biometric features. This is done using threshold values. A block diagram of the biometric verification system is shown in Fig. 2.

Biometric data acquisition: Several sensors are used to obtain the biometric features. For example, fingerprints and hand geometry are collected using sensors; face images are captured using traditional or video cameras; a walking surface captures gait; infrared cameras collect iris and retina scannings; keystrokes are acquired by a keyboard or writing pad; and Electroencephalography (EEG) signals are captured by electrodes placed over the scalp.

Pre-processing: In this step, the collected biometric data is pre-processed to discard noise and improve the signal or image quality for further processes.

Feature extraction and template generation: The most distinguishing features are extracted from the biometric data to identify or verify a person. For various biometric modalities, there are distinct feature extraction methods. In order to make the retrieved features clearly legible and comparable during the matching process, they are converted into templates. The templates can either take the form of numeric values or images [12].

Matching: Here, the stored biometric templates are compared to the input query biometric template. Typically, distance metrics like Euclidean distance, Hamming distance, and pixel

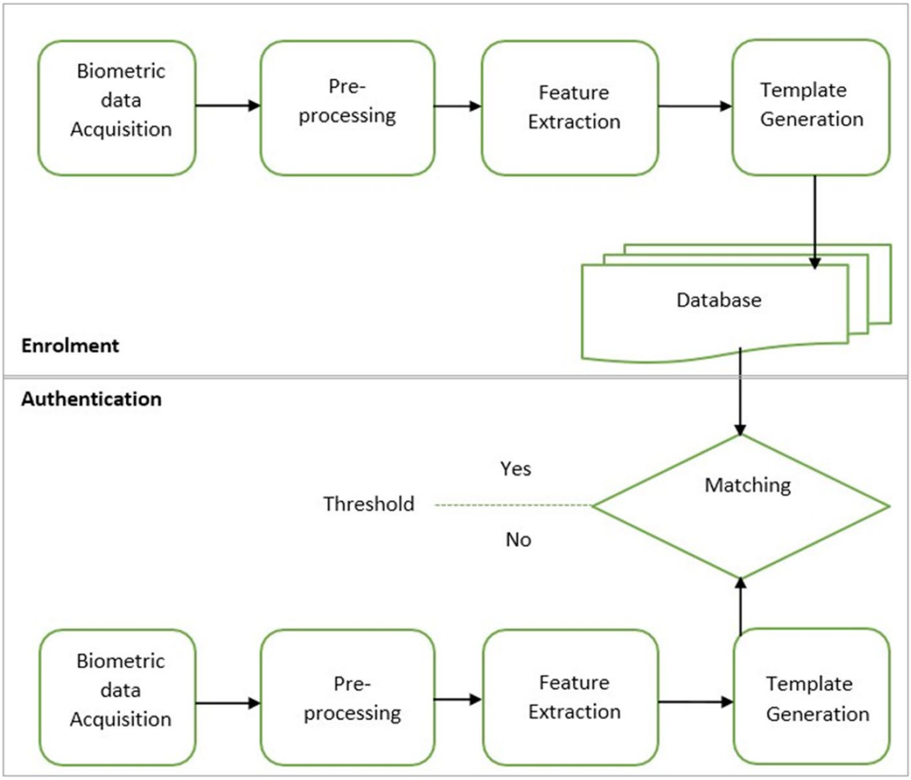


Fig. 2 Block diagram of the biometric verification system

counts are used for matching. Learning-based classifiers have become more and more popular recently to differentiate between authorized and unauthorized individuals. A matching score is determined by finding the similarity level between the current and stored biometric templates. The authenticity of a person is determined based on the similarity measure.

2.1.3 Cancellable face recognition

Cancellable biometric authentication is a template-based authentication mechanism, wherein the initial biometric pattern is purposefully altered in order to be associated with the authentication scheme. The original face pattern is not saved. Instead, a deformed version of the face template is used. As a result, cancellable face authentication offers higher security compared to password or token-based authentication methods. Cancellable face identification depends on recognizing encrypted or deformed facial characteristics of individuals [15, 40].

2.2 Quaternion mathematics

The quaternions constitute a specific system of complex numbers in three-dimensional (3-D) space, which is usually used to represent rotations. The quaternion could be expressed as a vector in the 3-D space plus a scalar quantity. Thus, quaternions are illustrated in the form $p=\alpha+ai+bj+ck$, where α, a, b, c are real numbers, and i, j, k are the fundamental quaternion basis vectors. Algebraic operations on quaternions are somewhat, and not in all respect, like algebraic operations on vectors. For example, the basic rules for multiplication of similar fundamental units are the same as those of the scalar product of vectors, while multiplication of different fundamental units is the same as the vectors' cross product. Table 2 summarizes the notations that are used in this paper.

William Rowan Hamilton, an Irish mathematician, developed quaternions in 1843. The use of quaternions to describe 3-D rotations is one of the most well-known uses of Hamilton's Algebra. In fact, due to the requirement of real-time calculations, quaternions, and rotations are strongly interconnected [23], and their application has become essential in

Table 2 Table of notations

Variable	Definition
α, a, b, c	Real numbers
i, j,k	Fundamental quaternion basis vectors
p	Quaternion
$\mu_{2\,,}\mu_1$	Means of the two distributions
σ_1^2, σ_2^2	Standard deviations
d	Decidability index
RGB	Red, Green, and Blue components
R	Component on the i-axis
G	Component on the j-axis
B	Component on the k- axis
q_{face}	Original color face image quaternion
q_{mask}	User-specific mask image quaternion
q_{output}	Quaternion multiplication of q_{face} and q_{mask}
q_{final}	Inverse quaternion process output
(t, w)	Original coordinates
(u, v)	Rotation coordinates
k_α, k_β	1- D FRFT kernels
$R^\alpha = X^\alpha$	FRFT of a function x with an angle α
n, m	Dimensions of the 2-D signal
p, q	Frequency variables
F^0	Zero rotation
F^a	Transformation from coordinates (t, w)
α, β	Order of 2D FRFT
$k_{\alpha,\beta}(p, q, m, n) = k_\alpha \otimes k_\beta$	2-D fractional transform kernel
$F^{\pi/2}$	Fourier transform operator
F^{π}	Time reverse operator
$F^{3\pi/2}$	Inverse Fourier transform operator
$F^{2\pi}$	2π rotation operator

many contemporary technologies. As a result of quaternion analysis [27], quaternions are now acknowledged as potent modeling and problem-solving tools in both theoretical and applied mathematics. Due to the increasing interest in quaternions and their applications in almost all applied sciences, several software applications have been developed to perform calculations in algebra with real quaternions.

Complex numbers are an expansion of real numbers, and the quaternions are a four-dimensional (4-D) extension of the complex number system. Quaternion algebra is commonly used to describe body rotation in a 3-D space. Although Euler angle sequences are relatively easy to understand and they represent a traditional way to interpret rotations, quaternions have an important advantage. A condition known as Gimbal Lock (singularity) takes place when two axes align, and the degree of flexibility is destroyed while employing Euler angle sequences. Singularity is avoided, when quaternions are used. Also, quaternions provide a smooth rotation for a rigid body.

In the proposed algorithms, we represent the input color images with quaternions and use the rotation properties of quaternions to generate cancellable biometrics. Usually, the geometry of quaternions is understood in terms of rotations, as illustrated in Figs. 3 and 4.

2.2.1 Advantages of quaternions

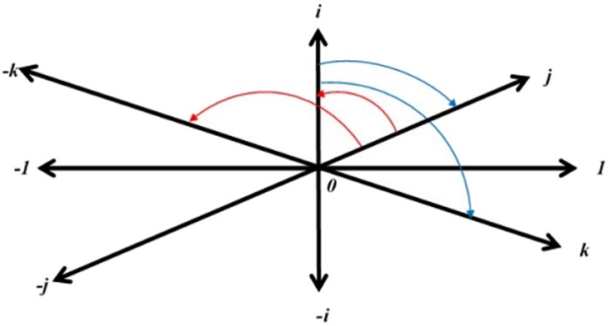
- Faster multiplication algorithms to combine successive rotations than using rotation matrices.
- Ease to normalize compared to rotation matrices.
- Interpolation and mathematical stability – suitability for statistics.

2.2.2 Applications of quaternions

Quaternion models have been used to represent and study every level of nature (in the sense of scale and complexity).

- Aerospace Guidance and Orientations.
- Computer Graphics and Computer Animation.
- Signal/Image Processing.
- Color Hues and Distortion.
- DNA, Matrix Genetics, and Music.
- Organic Chemistry and Chiral Tetrahedral Molecules.

Fig. 3 Graphical representation of quaternion unit product as a 90° rotation in 4-D space. This shows the non-commutative nature of the quaternion



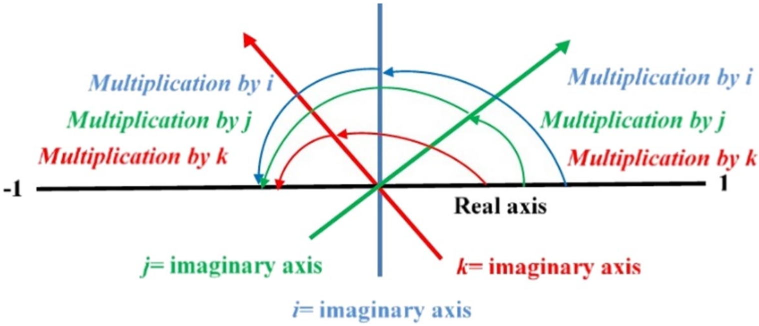


Fig. 4 Quaternion rotations through the complex plane

- Ownership, Entanglement, and Coordination.
- Quantum Mechanics.

One of our main contributions in this paper is a novel cancellable face recognition system based on quaternion mathematics. The main concept behind it is to mask the features of faces before using them for face recognition. The purpose of this procedure is to protect user privacy during the creation of the biometric database and the biometric verification process. If the database is compromised, it is possible to change the biometric templates that have been previously saved. In this process, color face images are represented in quaternion format. Then, other masking images are generated in quaternion format also. The cancellable templates are created by first applying quaternion multiplication and then quaternion inverse. Performance analysis of the proposed algorithms reveal low EER and a significant area under the ROC curve, which are the necessary conditions for a successful cancellable biometric recognition system [21, 33].

2.3 Metrics for performance evaluation

The most agreed performance indicators are the False Acceptance Rate (FAR), False Rejection Rate (FRR), EER, ROC, and decidability (*d*) [17, 22, 25, 31, 35, 36, 38]. These metrics are discussed in detail as follows.

- **False Acceptance Rate (FAR):** It describes a scenario in which a biometric authentication device accepts an unauthorized person as an authenticated user. It refers to the proportion of falsely-accepted unauthorized users. It can be calculated using the following equation:

$$FAR = \frac{Number\ of\ accepted\ unauthorized\ users}{Total\ number\ of\ unauthorized\ accesses} \times 100 \tag{1}$$

For example, if a system has an FAR of 0.1%, this means that for every 1000 authentication attempts, one imposter is falsely accepted as a legitimate user. The FAR is an important metric for evaluating the effectiveness and security of biometric authentication systems. A low FAR indicates that the system is more reliable and less likely to allow unauthorized access. However, it is important to note that a low FAR may come at the cost of a high FRR, which gives the rate at which the system rejects valid users. In summary, the FAR is a measure of the likelihood that a biometric authentication system will incorrectly accept an imposter as an authorized user, and it is an important metric for assessing the security and effectiveness of such systems.

- **False Rejection Rate (FRR):** It describes a scenario in which a legitimate individual is identified as being unauthenticated by the biometric authentication device. It refers to the proportion of valid users, who were mistakenly rejected. It is calculated as:

$$FRR = \frac{Number\ of\ rejected\ legitimate\ users}{Total\ number\ of\ legitimate\ accesses} \times 100 \tag{2}$$

For example, if a system has an FRR of 1%, this means that for every 100 authentication attempts by authorized users, one legitimate user is falsely rejected as an imposter. The FRR is an important metric for evaluating the effectiveness and usability of biometric authentication systems. A low FRR indicates that the system is more accurate and less likely to deny access to legitimate users. However, a low FRR may come at the cost of a high FAR, which measures the rate at which the system accepts imposters. In summary, the FRR is a measure of the likelihood that a biometric authentication system will incorrectly reject an authorized user as an imposter, and it is an important metric for assessing the usability and effectiveness of such systems.

- **Equal Error Rate (EER) or Crossover Error Rate (CER):** It is a statistical metric used to evaluate the performance of biometric authentication systems. It is the error rate at which FAR and FRR are equal. The lower the EER, the more accuracy and dependability the biometric authentication system has. Generally, EER can be approximated by:

$$\mathrm{EER} = \frac{(\mathrm{FAR} + \mathrm{FRR})}{2} \tag{3}$$

It is also calculated from the ROC curve, which gives the True Positive Rate (TPR) versus the False Positive Rate (FPR) for varying decision thresholds. A lower EER implies lower FAR and FRR. Hence, EER and system performance are inversely related, which means that a lower EER value indicates better recognition performance, as it means that the system is equally good at detecting both genuine users and imposters. Moreover, it is a useful metric for evaluating the overall accuracy and usability of biometric authentication systems.

- **Failure To Enrollment (FTE):** It is the rate of incorrect attempts to generate a template from an input. It is often determined by a minimum of three attempts and can be described as the probability that users may try to enroll themselves but be unsuccessful. Inputs of poor quality are the main factor for this. This may occur for various reasons, such as poor-quality biometric samples, system errors, or user-related issues such as lack of cooperation or physical disabilities. FTE is an important performance metric for biometric systems, as it directly affects the system ability to accurately recognize enrolled users during subsequent authentication attempts. High FTE rates may lead to lower system accuracy and decreased user acceptance, while low FTE rates indicate a robust and reliable biometric system.
- **Failure to Capture Rate (FCR):** This is the probability that an autonomous system may not identify an appropriately-presented biometric input. It is a metric used to evaluate the performance of a biometric system in capturing the biometric trait of an enrolled user during the authentication process. FCR gives the frequency with which the system cannot identify a legitimate user biometric trait during an authentication attempt. This can occur

for various reasons, such as low quality of biometric samples, system errors, or user-related issues, such as physical disabilities or changes in the biometric traits. FCR is an important performance metric for biometric systems, as it directly reflects their ability to authenticate enrolled users, accurately. A high FCR may lead to increased false rejection rates, decreased user acceptance, and reduced system effectiveness, while a low FCR indicates a robust and reliable biometric system.

- **Receiver Operating Characteristic (ROC) Curve:** It is a graphical representation of the performance of a binary classification system. It shows the TPR on the *y*-axis against the FPR on the *x*-axis at different threshold settings. TPR represents the proportion of true positive instances, correctly identified as positive, out of all actual positive instances, while FPR represents the proportion of false positive instances, incorrectly identified as positive, out of all actual negative instances.

  The ROC curve allows us to visualize the trade-off between the TPR and FPR at different decision thresholds and evaluate the biometric system performance by calculating the Area Under the Curve (AUC). For example, a perfect classification system would have an AUC of 1, while a random-guess classifier would have an AUC of 0.5. The AUC is widely used as a performance metric for biometric recognition systems.

  Based on TPR and FPR, the ROC curve is produced. TPR and TNR are both referred to as sensitivity and specificity, respectively. The FPR gives the probability of incorrectly accepting an imposter pattern as a genuine pattern, while the FRR gives the probability of incorrectly refusing a user as an imposter. Equations (4) and (5) are used to measure the matching performance using negative and positive predictive values (NPV and PPV).

$$PPV = \frac{Number\ of\ \ true\ positives}{Number\ of\ \ true\ positives + Number\ of\ \ false\ \ positives} \tag{4}$$

$$NPV = \frac{Number\ of\ true\ negatives}{Number\ of\ true\ negatives + Number\ of\ false\ negatives} \tag{5}$$

- **Decidability Index (*d*)**: The decidability index is used when there are two choices, such as genuine users and imposters, in the case of template recognition. It is a measure of how different the two inter-class and intra-class distinctions are. The condition we need is that the two distributions do not overlap. The difference, which is a realistic case, results in false rejection and acceptance errors. Therefore, the value of *d* needs to be as high as possible. The value of *d* is defined in the eq. (6):

$$d = \frac{|\ \mu_1 - \mu_2\ |}{\sqrt{\left(\sigma_1^2 + \sigma_2^2\right)/2}} \tag{6}$$

where μ_1 and μ_2 are the means of the two distributions, and σ_1^2 and σ_2^2 are their standard deviations. The value of *d* ranges from 0 to infinity, with larger values indicating better discriminability between genuine users an impostors. The value of 0 indicates that the system is unable to distinguish between genuine users an impostors. In summary, the higher the decidability value, the better the system ability to discriminate between genuine users and impostors is.

3 Proposed algorithms

The primary objective of this study is to use quaternion mathematics to secure the face recognition process. Hence, cancellable face templates are generated from original face images to be utilized instead of the original faces in biometric databases. For generating a secured cancellable biometric template, quaternion mathematics is applied. The quaternions have advantages over other representations. An image can be represented as shown in Fig. 5, by extracting the Red, Green, and Blue (RGB) components of the image [13, 32, 39], and then letting the scalar part to be "0", and the vector components to be the RGB components of the image as follows:

$$q = 0 + Ri + Gj + Bk \tag{7}$$

After representing the image by quaternion mathematics, the proposed algorithms can be applied using quaternion algebra. Then, we use quaternions to extract secure templates from the original input biometric images with different algorithms.

Figure 6 illustrates how the suggested cancellable face recognition system generates distorted templates from the original color faces by multiplying quaternions with an auxiliary image. This figure clarifies that the RGB components of the original color face image have been merged into a quaternion. These components are represented in the quaternion formula by setting the *R* component on the *i*-axis, the *G* component on the *j*-axis, and the *B* component on the *k*-axis. The assumed scalar part is equal to zero. Thus,

$$q_{face} = 0 + R_1 i + G_1 j + B_1 k \tag{8}$$

In addition, a user-specific mask image is used and represented as another quaternion. By using this user-specific mask image, the proposed cancellable biometric system can achieve high security of data and privacy of users. The mask image can be customized and kept secret for each user, preventing unauthorized access or hacking. The use of quaternion mathematics also enables the mask image to be applied precisely and controlled, ensuring that the resulting transformed data can be used for accurate and reliable authentication.

$$q_{mask} = 0 + R_2 i + G_2 j + B_2 k \tag{9}$$

After that, quaternion multiplication is implemented as follows,

$$q_{output} = q_{face} \otimes q_{mask} \tag{10}$$

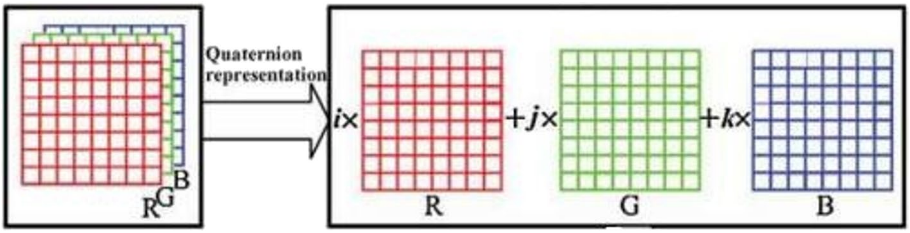


Fig. 5 Quaternion representation for images

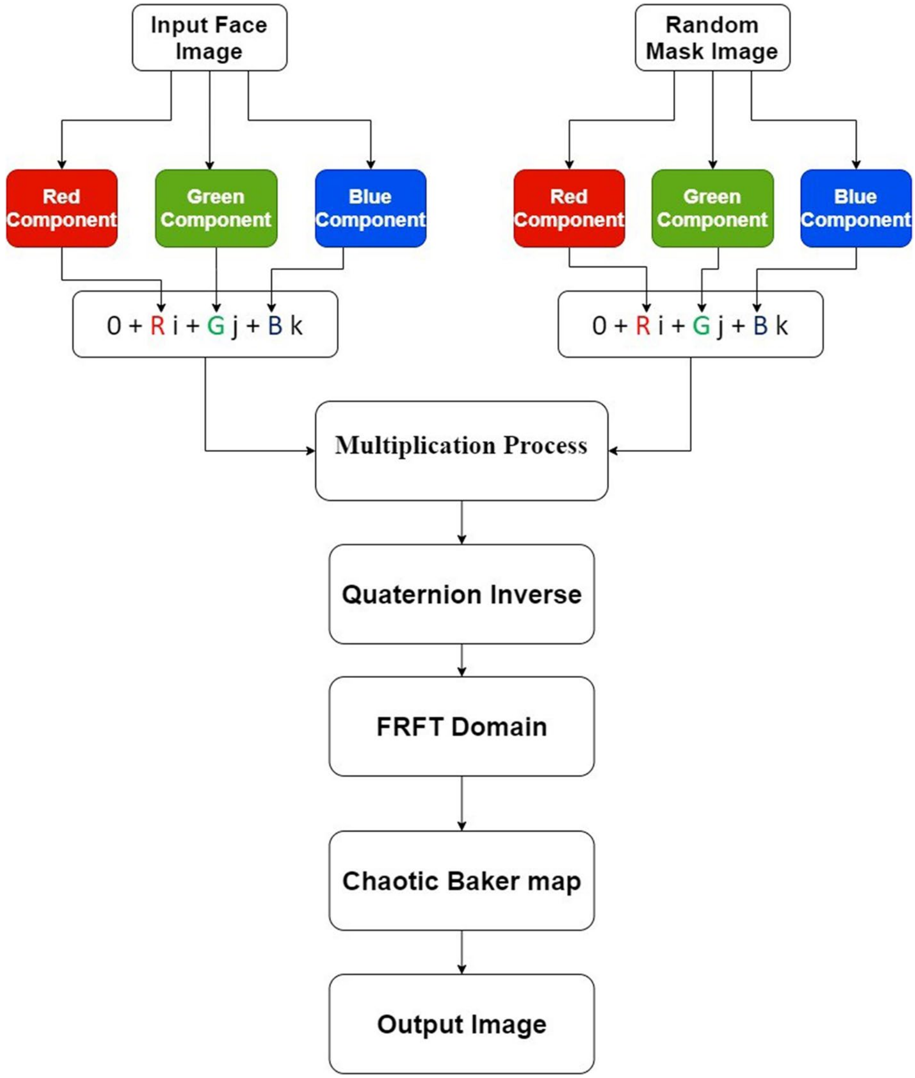


Fig. 6 Block diagram for generating cancellable biometric templates using quaternion mathematics and 2-D FRFT

Quaternion multiplication is important in many applications, such as computer graphics, robotics, and control theory. It enables the representation and manipulation of complex rotations and orientations in three-dimensional space, which is crucial for many engineering and scientific problems.

An inverse quaternion process is implemented as follows,

$$q_{final} = q_{output}^{-1} \tag{11}$$

The inverse of a quaternion is an important operation in many applications that involve rotations and orientations, such as robotics, computer graphics, and physics. It allows to undo a rotation or orientation that has been applied to a vector, which is useful for many engineering and scientific problems. The cancellable template, in this case, is a gray-scale image generated from the quaternion inverse.

Two algorithms are provided in this section for cancellable face recognition. The first one depends on the utilization of FRFT with quaternion mathematics. The second one depends on the utilization of other auxiliary tools, including rotation and FFT with quaternion mathematics, to generate the cancellable templates. A statistical framework is adopted for the classification process based on correlation estimation to eliminate the need for recovering the original templates in the verification process.

3.1 Algorithm based on FRFT and quaternion mathematics

The first cancellable biometric recognition algorithm has a layer of encryption. This layer is represented by chaotic encryption in the FRFT domain. The FRFT adds a degree of freedom through the selection of the rotation angle. In addition, Baker map adds a degree of permutation to enhance the security level of biometrics. The Baker map and the Arnold's cat map are two-dimensional chaotic maps that operate on points within a unit square. The employed Baker map expression that is used in the proposed work is illustrated with more details in [19, 26, 28–30]. The Baker map is a key component of the proposed algorithms based on quaternion mathematics for generating cancellable biometric data. The Baker map is used in our work for its chaotic behavior and sensitivity to initial conditions, making it suitable for introducing intentional distortions or variations in the biometric data. In our proposed algorithms, the Baker map is utilized along with quaternion mathematics to induce intentional distortions in color images, thus generating cancellable biometric templates, while preserving privacy of users and security of the original data.

The 1-D FRFT kernel is a mathematical function that transforms a time-domain signal into the fractional Fourier domain. The FRFT is a generalization of the Fourier transform, which allows for variable rotation of the frequency axis in the time-frequency plane. The 1-D FRFT kernel is given by [18, 34]:

$$k_\alpha(t,u) = \begin{cases} \sqrt{\frac{1-j\cot\alpha}{2\pi}}\exp\left(j\frac{t^2-u^2}{2}\cot\alpha - j\frac{tu}{\sin\alpha}\right), & if\ \alpha \neq n\pi \\ \delta(u-t) & if\ \alpha = n\pi \\ \delta(u+t) & if\ \alpha = (2n+1)\pi \end{cases} \tag{12}$$

The FRFT of a function x with an angle α, and with t and u as the time and frequency variables, respectively , is given as:

$$X_\alpha(u) = \int_{-\infty}^{\infty} x(t)k_\alpha(t,u)dt \tag{13}$$

The 1-D FRFT is an important tool in signal processing, particularly in applications that involve non-stationary or time-varying signals. It is used in a variety of fields, including image and video processing, communications, and biomedical signal analysis. Figure 6 shows the block diagram for generating the cancellable biometric templates using quaternion multiplication and 2-D FRFT.

Equations (12) and (13) can be used to obtain,

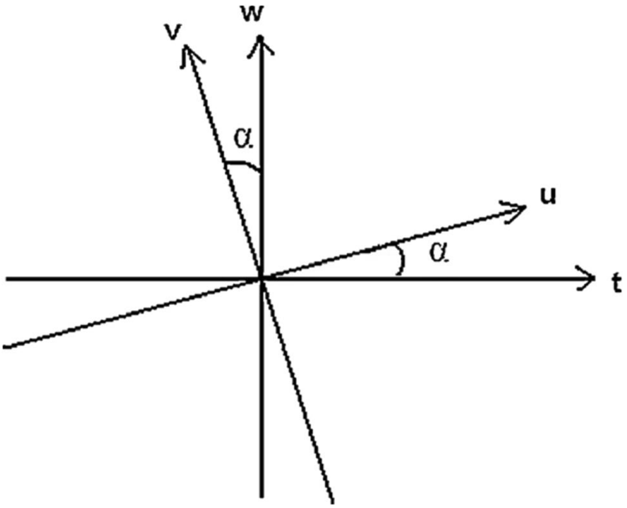


Fig. 7 The original coordinates (t, w) rotate to coordinates (u, v) with angle α in the time-frequency plane

$$f_a(u) = f^a\left[f(x)\right] = C_\alpha \int f(x)\exp\left[i\pi\frac{u^2+x^2}{tan\alpha} - 2i\pi\frac{ux}{sin\alpha}\right]dx \tag{14}$$

where $\alpha = \frac{a\pi}{2}$ and $C_\alpha = \frac{\exp-\left[i\left(\frac{\pi\sin(\sin(\alpha))}{4} - \frac{\alpha}{2}\right)\right]}{|\sin\alpha|^{1/2.}}$

Thus, as shown in Fig. 7, F^a denotes the transformation from coordinates (t, w) in the counter-clockwise direction to coordinates (u, v) with an angle α. Here, F^0 means zero rotation.

$F^{\pi/2}$ means Fourier Transform (FT) operator, F^π means time reverse operator, $F^{3\pi/2}$ means inverse FT operator, $F^{2\pi}$ means 2π rotation operator, and $F^\beta F^\alpha = F^{\beta+\alpha}$.

For image processing, the forward and inverse 2-D FRFT of an image is used and they are computed as:

$$F_{\alpha,\beta}(m,n) = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} f(p,q)k_{\alpha,\beta}(p,q,m,n) \tag{15}$$

$$f_{\alpha,\beta}(p,q) = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} F_{\alpha,\beta}(m,n)k_{-\alpha,-\beta}(p,q,m,n) \tag{16}$$

where (α,β) is the order of 2D FRFT. $k_{\alpha,\,\beta}(p,q,m,n) = k_\alpha \otimes k_\beta$ is the transform kernel, k_α, and k_β are the 1-D FRFT kernels. The 2-D FRFT is an extension of the 1-D FRFT to two dimensions. It can be defined as the repeated application of the 1-D FRFT along the two dimensions of a 2-D signal. The inverse 2-D FRFT can be obtained by applying the forward 2-D FRFT with negative values of (α,β). The 2-D FRFT is widely used in various image processing applications, such as image compression, filtering, and edge detection. It allows for analyzing image components at different orientations and frequencies, making it a powerful tool for image processing.

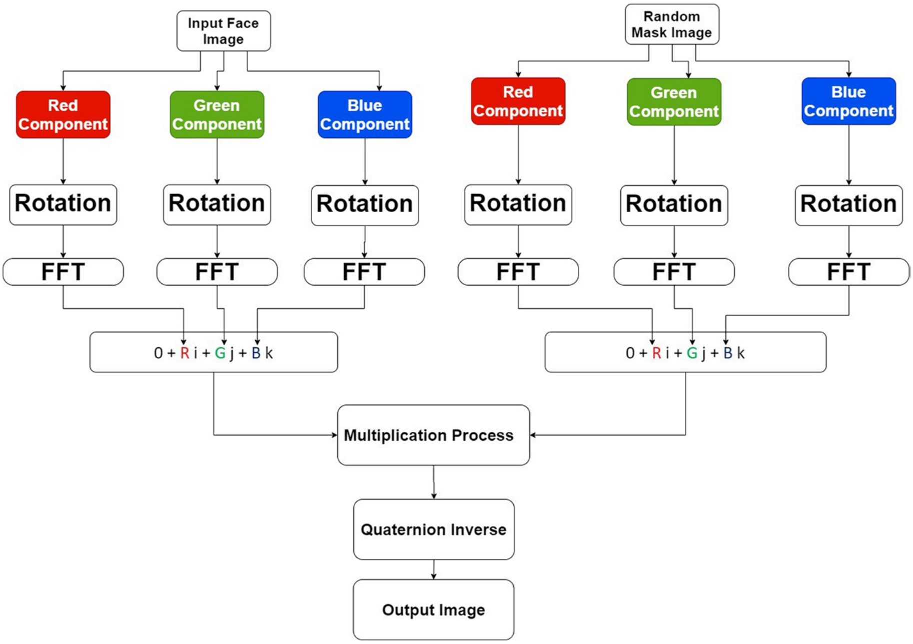


Fig. 8 Block diagram for generating cancellable biometric templates using FFT and rotation

3.2 Algorithm based on quaternion mathematics and rotation

The second proposed cancellable biometric recognition algorithm depends on the addition of a rotation step to be performed on the separate components of the color images. After that, the FFT is estimated for each component. Finally, quaternion processing is implemented. Figure 8 shows the block diagram for generating the encrypted templates using FFT and rotation. The rotation allows more distortion of the original biometric templates prior to the FFT. After that, the quaternion operations are performed to generate the cancellable biometric templates.

4 Simulation results and comparison

This section presents the simulation results of the two cancellable biometric recognition algorithms. The simulation experiments are carried out using MATLAB 2020b on Windows 10 64-bit operating system with an Intel® Core™i7-7700HQ CPU @2.80GHz with 16 GB RAM.

Several face images were collected from different datasets, including:

1. BIDA Lab.
2. The IARPA Janus Benchmark A (IJB-A).
3. The Peking Finger Vein Recognition Dataset.

In our simulation scenarios, we considered 400 face images and generated cancellable templates for each one. Both genuine and imposter correlation scores were generated,

Table 3 Different FRFT angles

Angles	M1	M2	M3	M4	M5
(x, y)	(30,20)	(30,30)	(40,50)	(40,40)	(43,64)
Angles	M6	M7	M8	M9	M10
(x, y)	(20,31)	(22,37)	(78,83)	(45,45)	(0,10)
Angles	M11	M12	M13	M14	M15
(x, y)	(0,22)	(0,35)	(0,40)	(0,73)	(0,95)
Angles	M16	M17	M18	M19	M20
(x, y)	(20,0)	(34,0)	(46,0)	(60,0)	(82,0)

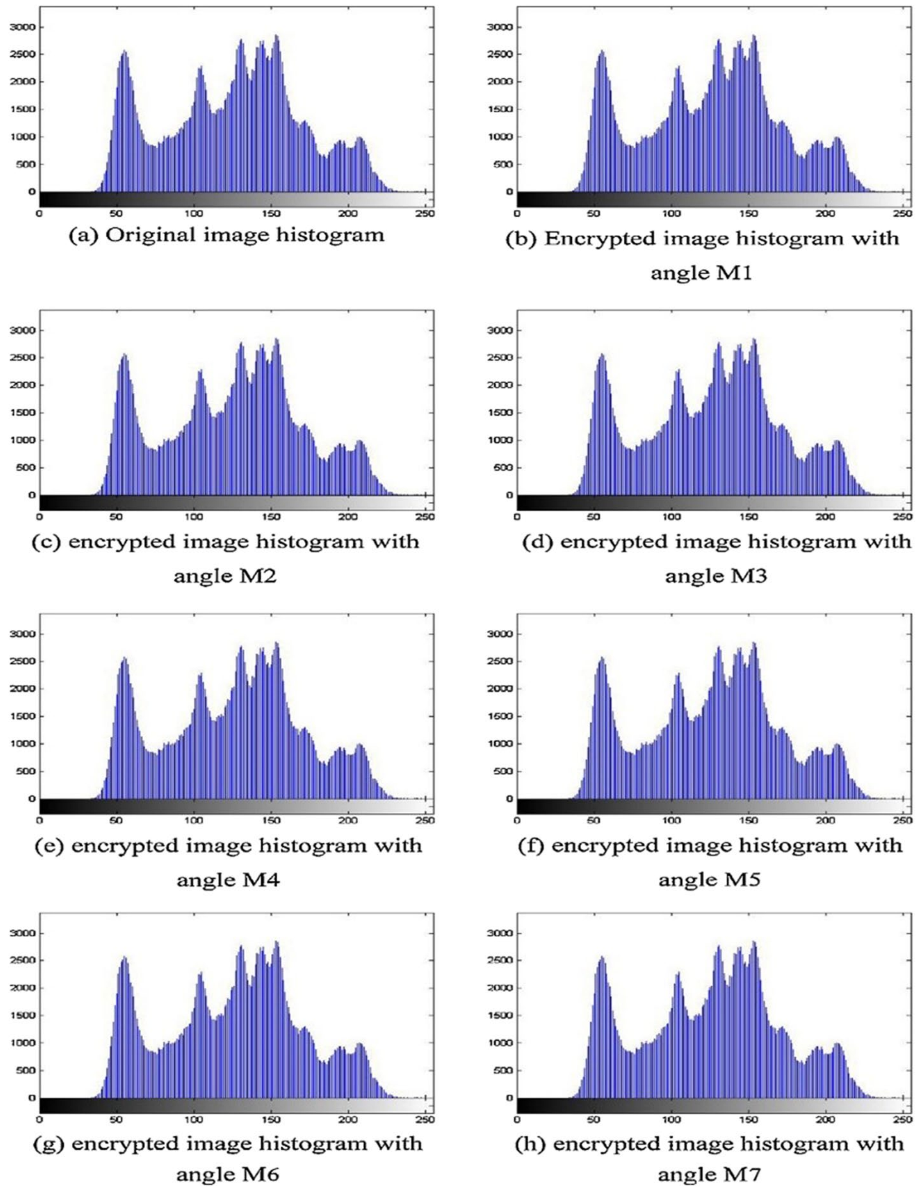
and Probability Density Functions (PDFs) for both cases were estimated. The intersection point of these PDFs is used to determine the EER. In addition, ROC curves were estimated, and AROC values were also evaluated. Low EER and high AROC values reflect the efficiency of the cancellable biometric system.

4.1 Results of the algorithm based on FRFT and quaternion mathematics

The chaotic Baker map encryption method is used multiple times with various FRFT angles to examine the impact of the angle of rotation. Table 3 shows the utilization of twenty different rotation angles with the chaotic Baker map encryption to examine the impact of these angles. The table shows the EER and AROC values obtained by applying the proposed algorithm with the chaotic Baker map encryption method using different FRFT angles. The angles used range from 0 to 180 degrees in increments of 10 degrees. The table shows that the EER and AROC values vary slightly depending on the angle used, with some angles showing slightly better performance than others. Overall, the proposed algorithm with the chaotic Baker map encryption method shows consistent and reliable performance across all tested angles, indicating its effectiveness for biometric security applications.

Figure 9 displays chaotic Baker-map-based masked image histograms using various FRFT angles. Since this map simply scrambles the original images, the histograms are identical to those of the original images. As shown, the histogram analysis of the masked images in this case is unaffected by the angles. The figure reveals the impact of using various FRFT angles in the masking process of biometric data using the chaotic Baker map method. It displays histograms of the masked images using different angles. The histograms of the masked images are not affected by the various angles used in the masking process. This implies that the proposed algorithm is robust and reliable, since the same level of security can be achieved regardless of the angle used in the masking process.

Table 4 illustrates the quality metrics of the proposed cancellable biometric recognition algorithm based on FRFT and chaotic Baker map. The rotation angles of (45, 45) give the best performance of the cancellable biometric algorithm. Based on the results in Table 4, the proposed cancellable biometric recognition algorithm using FRFT and chaotic Baker map achieves high performance in terms of quality metrics such as EER and AROC. Notably, the rotation angles of (45, 45) give the best performance of the algorithm, which indicates that the specific combination of quaternion rotation and FRFT can effectively induce intentional distortions and achieve high recognition accuracy. These results demonstrate the effectiveness of the proposed algorithm in



(a) Original image histogram

(b) Encrypted image histogram with angle M1

(c) encrypted image histogram with angle M2

(d) encrypted image histogram with angle M3

(e) encrypted image histogram with angle M4

(f) encrypted image histogram with angle M5

(g) encrypted image histogram with angle M6

(h) encrypted image histogram with angle M7

Fig. 9 Histograms of the masked image using the chaotic Baker map and different FRFT angles

generating cancellable biometrics and maintaining the security of the original biometric data and the privacy of users.

Table 4 Performance evaluation metrics of the cancellable biometric algorithm based on FRFT and quaternion mathematics

Angle of FRFT	Without Noise		Noise Variance (0.01)		Noise Variance (0.03)		Noise Variance (0.06)	
	AROC	EER	AROC	EER	AROC	EER	AROC	EER
M1 (30,20)	0.9693	0.075	0.9638	0.077	0.9456	0.0785	0.9050	0.0793
M2 (30,30)	0.9693	0.074	0.9638	0.076	0.9457	0.0784	0.9050	0.0792
M3 (40,50)	0.9693	0.073	0.9637	0.076	0.9457	0.077	0.9053	0.078
M4 (40,40)	0.9692	0.074	0.9638	0.077	0.9455	0.078	0.9049	0.079
M5 (43,64)	0.9693	0.075	0.9639	0.075	0.9455	0.076	0.9048	0.077
M6 (20,31)	0.9596	0.077	0.9538	0.078	0.9356	0.079	0.8955	0.08
M7 (22,37)	0.9595	0.08	0.9537	0.081	0.9355	0.082	0.8956	0.085
M8 (78,83)	0.9594	0.081	0.9538	0.081	0.9354	0.083	0.8955	0.084
M9 (45,45)	0.9895	0.007	0.9736	0.008	0.9728	0.0082	0.9720	0.0088
M10 (0,10)	0.9499	0.075	0.9439	0.077	0.9354	0.079	0.8953	0.08
M11 (0,22)	0.9496	0.074	0.9438	0.075	0.9256	0.076	0.8856	0.078
M12 (0,35)	0.9495	0.073	0.9437	0.075	0.9255	0.076	0.8855	0.079
M13 (0,40)	0.9495	0.075	0.9436	0.076	0.9254	0.078	0.8854	0.08
M14 (0,73)	0.9494	0.078	0.9436	0.079	0.9254	0.08	0.8854	0.083
M15 (0,95)	0.9495	0.078	0.9437	0.079	0.9253	0.081	0.8853	0.083
M16 (20,0)	0.9494	0.077	0.9435	0.078	0.9156	0.079	0.8757	0.081
M17 (34,0)	0.9396	0.074	0.9338	0.075	0.9156	0.077	0.8756	0.079
M18 (46,0)	0.9395	0.074	0.9337	0.075	0.9155	0.077	0.8755	0.08
M19 (60,0)	0.9394	0.073	0.9336	0.074	0.9153	0.078	0.8754	0.079
M20 (84,0)	0.9395	0.073	0.9336	0.074	0.9154	0.077	0.8753	0.079

4.2 Results of the algorithm based on quaternion mathematics and rotation

Several simulation results have been obtained for the proposed cancellable biometric algorithm based on quaternion mathematics and rotation. Figure 10 shows samples of the output masked face templates. The current study presents several images showing the original face templates and their corresponding masked face templates produced by the proposed algorithm. These masked templates appear to be heavily distorted versions of the original templates due to the intentional distortions introduced by the algorithm. However, the distortions are controlled, so that the masked templates can still be used for biometric authentication, while preserving privacy of users and security of the original biometric data.

Figure 11 shows a) genuine and impostor distributions as Probability of True Distribution (PTD) and the Probability of False Distribution (PFD) and b) the ROC curve for the proposed algorithm. The genuine and impostor distributions can be used to evaluate the performance of the algorithm in terms of correct recognition and rejection of identities.

The PTD refers to the distribution of genuine similarity scores, which is a histogram showing the frequency of similarity scores between genuine pairs of samples. Similarly, the PFD refers to the distribution of impostor similarity scores, which is a histogram showing the frequency of similarity scores between impostor pairs of samples. For the proposed algorithm, Fig. 11 shows the genuine and impostor distributions as PTD and PFD, respectively,

Table 5 Evaluation metrics in terms of EER and AROC for the proposed algorithm based on quaternion mathematics and rotation

Evaluation metrics	Proposed algorithm
EER	0.00006
AROC	0.9999

Table 6 EER and AROC evaluation metrics for the proposed algorithm based on quaternion mathematics and rotation with noise

Noise variance	EER	AROC
0.01	0.00005	0.999
0.03	0.00003	0.995
0.05	0.0009	0.990
0.08	0.00086	0.989

and the ROC curve illustrates the performance of the algorithm in terms of its ability to distinguish between genuine and impostor samples.

The correlation score behavior of the algorithm can be analyzed by examining the overlap between the genuine and impostor distributions. Ideally, the genuine distribution should be shifted to the right and separated from the impostor distribution. This means that the algorithm is able to accurately distinguish between genuine users and impostors. However, if there is significant overlap between the two distributions, the algorithm may have difficulty in distinguishing between genuine users and impostors.

A ROC curve that is close to the upper-left corner of the graph, indicates high TPR and low FPR. A curve that is closer to the diagonal line, on the other hand, would indicate poor performance of the algorithm. A higher AUC indicates better performance, while an AUC of 0.5 indicates that the algorithm is no better than random guessing.

Table 5 shows the evaluation metrics for the proposed cancellable biometric recognition algorithm based on quaternion mathematics and rotation. The low EER and the high AROC indicate the good performance of the algorithm.

To evaluate the performance of the proposed algorithm based on quaternion mathematics and rotation with noise variance levels of 0.01, 0.03, 0.05, and 0.08, we can compute the EER and AROC values for each noise variance level to assess the performance of the system under different levels of noise. Table 6 shows the effect of noise on the performance of the proposed algorithm. Generally, higher levels of noise result in decreased performance levels, as the noise can introduce errors and affect the similarity scores. It is important to note that the achieved AROC values are high enough, which ensures high performance levels even in the presence of noise.

4.3 Result discussion and comparison

It is clear from the obtained results for both cancellable biometric recognition algorithms that they could identify users based on their masked templates. The algorithms are ranked according to the EER and AROC values. Low EER and high AROC values reflect the strength of the algorithm. We compare between he two proposed algorithms. The algorithm based on quaternion mathematics and rotation comes first with EER = 0.00006 and AROC = 0.9999. After that, the algorithm based on FRFT and quaternion mathematics comes second with EER = 0.0007 and AROC = 0.9895 for angles of (45,45). The sensitivity

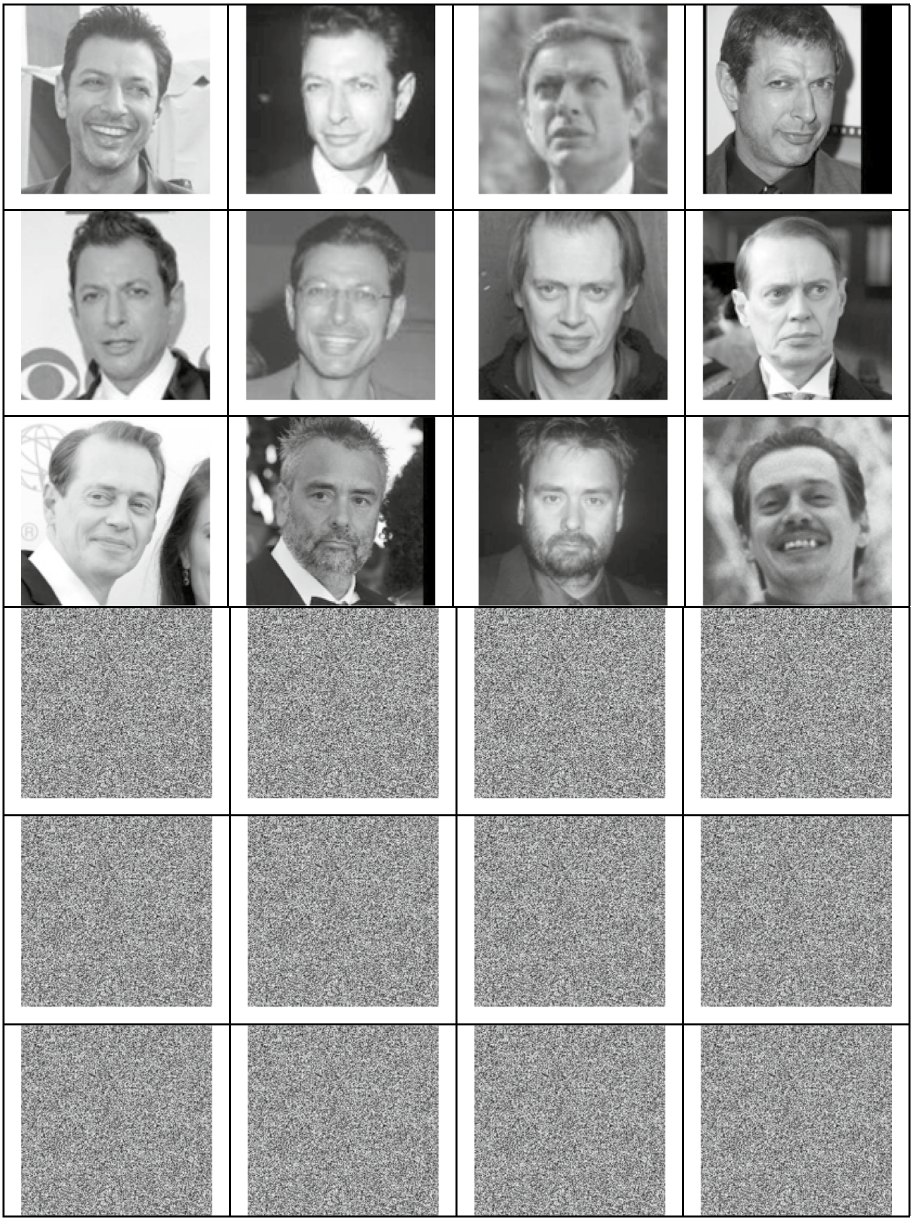
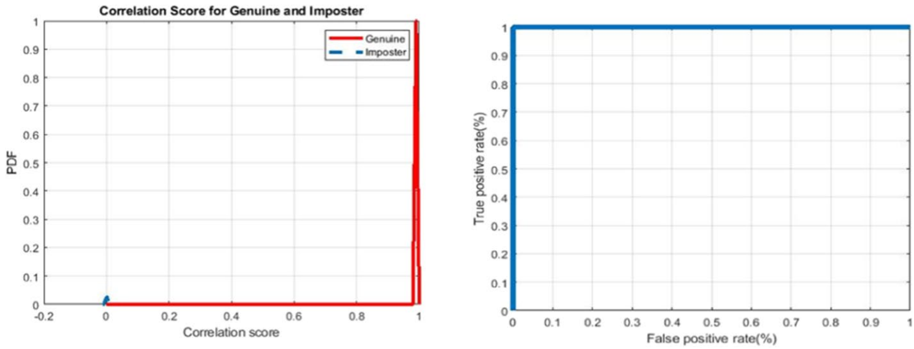


Fig. 10 Samples of original and output masked face templates with the proposed algorithm based on quaternion mathematics and rotation

of both algorithms to the presence of noise has also been investigated. This study reveals that the algorithms based on quaternion mathematics have low noise sensitivity.

The obtained results reflect the ability of quaternion mathematical operations with the help of auxiliary images to generate distorted or encrypted versions of biometric templates, while keeping the ability to discriminate between users. Other supporting operations such as FFT,



a) PTD and PFD distributions b) ROC curve.

Fig. 11 Genuine and impostor distributions for the proposed algorithm based on quaternion mathematics and rotation

FRFT, chaotic encryption, and rotation can help produce more secure templates, while maintaining the discrimination ability.

5 Conclusions and future work

Quaternion mathematics is studied in this paper as a recent development in mathematics. It has been exploited for biometric security applications. The objective was to generate cancellable biometric templates that can be used for user authentication or verification, while keeping the original biometrics secure during hacking attempts. Two algorithms have been presented and evaluated for this purpose. The core of these algorithms is quaternion mathematics with the help of an auxiliary image. Both algorithms managed to achieve high performance even in the presence of noise. Hence, quaternion mathematics is strongly recommended to take place in the future security applications. Briefly, the proposed cancellable biometric algorithms based on quaternion mathematics are significant for the field of biometric security systems for several reasons. First, these algorithms allow intentional distortions or variations in the original biometric data to be used for authentication, while preserving privacy of users and security of the original data. This is a significant improvement over traditional biometric security systems that store and compare biometric data in its original form, leaving it vulnerable to hacking and unauthorized access. Second, the use of quaternion mathematics allows for intentional distortions to be introduced in a controlled and secure manner, ensuring that the original biometric data remains protected from hacking or unauthorized access. Third, the proposed algorithms achieved high recognition performance. For future work, utilization of quaternion mathematics in artificial intelligence, steganography of images with quaternion mathematics, design of filters using quaternion mathematics, and development of algorithms to follow the paths in video sequences captured by drones based on quaternion mathematics will be considered.

Acknowledgements The authors are very grateful to all the institutions given in the affiliation list for performing this research work, successfully. The authors would like to thank Prince Sultan University for their support.

Authors' contributions All authors are equally contributed.

Funding The authors did not receive support from any organization for the submitted work.

Data availability All data are available upon request from the corresponding author.

Declarations

Ethics approval and consent to participate All authors contributed and accepted to submit the current work.

Consent for publication All authors accepted to submit and publish the submitted work.

Competing interests The authors have neither relevant financial nor non-financial interests to disclose.

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

References

1. Abd El-Samie FE, Nassar RM, Safan M, Abdelhamed MA, Khalaf AA, El Banby GM, … El-Shafai W (2021) Efficient implementation of optical scanning holography in cancelable biometrics. Appl Opt 60(13):3659–3667
2. Abou Elazm LA, Ibrahim S, Egila MG, Shawky H, Elsaid MK, El-Shafai W, Abd El-Samie FE (2020) Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption. Multimed Tools Appl 79:14053–14078
3. Al Ali ZT, Al Kababji AM, Shukur MB (2020, December) Transcript Validation System using biometric characteristics. In: 2020 International Conference on Advanced Science and Engineering (ICOASE), IEEE, pp 1–6
4. Alarifi A, Amoon M, Aly MH, El-Shafai W (2020) Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system. IEEE Access 8:221246–221268
5. Algarni AD, El Banby G, Ismail S, El-Shafai W, El-Samie FEA, Soliman F, N. (2020) Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications. Entropy 22(12):1361
6. Ayoup A, Khalaf A, El-Shafai W, Abd El-Samie F, Alraddady F, Eldin S (2022) Cancellable multi-biometric template generation based on arnold cat map and aliasing. CMC-Comput Mater Contin 72(2):3687–3703
7. Badr IS, Radwan AG, El-Rabaie ESM, Said LA, El Banby GM, El-Shafai W, Abd El-Samie FE (2021) Cancellable face recognition based on fractional-order Lorenz chaotic system and Haar wavelet fusion. Digit Signal Process 116:103103
8. Elazm LAA, El-Shafai W, Ibrahim S, Egila MG, Shawkey H, Elsaid MK, … El-Samie FEA (2023) Efficient hardware design of a secure cancellable biometric cryptosystem. Intell Autom Soft Comput 36(1):929–955
9. El-Gazar S, El Shafai W, El Banby GM, Hamed HF, Salama GM, Abd-Elnaby M, Abd El-Samie FE (2022) Cancelable speaker identification system based on optical-like encryption algorithms. Comput Syst Sci Eng 43(1):87–102
10. El-Hameed HAA, Ramadan N, El-Shafai W, Khalaf AA, Ahmed HEH, Elkhamy SE, El-Samie FEA (2021) Cancelable biometric security system based on advanced chaotic maps. Vis Comput:1–17
11. El-Shafai W, Mohamed FAHE, Elkamchouchi HM, Abd-Elnaby M, Elshafee A (2021) Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. IEEE Access 9:77675–77692
12. El-Shafai W, Khallaf F, El-Rabaie ESM, El-Samie FEA (2021) Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. J Ambient Intell Humaniz Comput 12(10):9007–9035
13. El-Shafai W, Khallaf F, El-Rabaie ESM, El-Samie FEA (2022) Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services. J Ambient Intell Humaniz Comput:1–28
14. El-Shafai W, Khallaf F, El-Rabaie ESM, El-Samie A, Fathi E (2022) Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications. Neural Comput & Applic 34:1–25
15. El-Shafai W, Khallaf F, El-Rabaie EM, El-Samie FEA, Almomani I (2023) A multi-stage security solution for medical color images in healthcare applications. Comput Syst Sci Eng 46(3):3599–3618

16. Faragallah OS, Naeem EA, El-Shafai W, Ramadan N, Ahmed HEDH, Elnaby MMA, … El-Samie FEA (2022) Efficient chaotic-Baker-map-based cancelable face recognition. J Ambient Intell Humaniz Comput:1–39
17. Gupta M, Sahai A, Verma S, Agarwal V (2019) Score improvement using backpropagation in biometric recognition system. In: Applications of Artificial Intelligence Techniques in Engineering. Springer, Singapore, pp 377–383
18. Hassanin AAI, Abd El-Samie FE, Mohamed AEH (2021, July) Cancelable biometric system for face recognition based on a regularized restoration model. In 2021 International Conference on Electronic Engineering (ICEEM), IEEE, pp 1–5
19. Hou C, Liu X, Feng S (2020) Quantum image scrambling algorithm based on discrete Baker map. Modern Physics Letters A 35(17):2050145
20. Jain AK, Nandakumar K, Ross A (2016) 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recogn Lett 79:80–105
21. Jia Z, Ng MK, Song GJ (2019) Lanczos method for large-scale quaternion singular value decomposition. Numer Algorithms 82(2):699–717
22. Joshi JC, Nangia SA, Tiwari K, Gupta KK (2019, March) Finger Knuckleprint based personal authentication using siamese network. In 2019 6th international conference on signal processing and integrated networks (SPIN), IEEE, pp 282–286
23. Kameli Donachali A, Jafari H (2020) A decomposition method for solving quaternion differential equations. Int J Appl Comput Math 6(4):1–7
24. Kumar S, Lamba VK, Jangra S (2019) A comprehensive study of periocular biometrics on IRIS recognition. Int J Control Autom 12(5):391–401
25. Kumar KC, Lala A, Vyas R, Sharma M (2020, November) Periocular recognition via effective textural descriptor. In: 2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), IEEE, pp 1–6
26. Liu H, Wang X (2010) Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 59(10):3320–3327
27. Liu Y, Zheng Y, Lu J, Cao J, Rutkowski L (2019) Constrained quaternion-variable convex optimization: a quaternion-valued recurrent neural network approach. IEEE Trans Neural Netw Learn Syst 31(3):1022–1035
28. Liu H, Kadir A, Liu J (2019) Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system. Opt Lasers Eng 122:123–133
29. Liu H, Kadir A, Xu C (2020) Color image encryption with cipher feedback and coupling chaotic map. Int J Bifurc Chaos 30(12):2050173
30. Liu H, Xu Y, Ma C (2020) Chaos-based image hybrid encryption algorithm using key stretching and hash feedback. Optik 216:164925
31. Luo Z, Gu Q, Qi G, Liu S, Zhu Y, Bai Z (2019, November) A robust single-sensor face and iris biometric identification system based on multimodal feature extraction network. In: 2019 IEEE 31st International Conference on Tools with Artificial Intelligence (ICTAI), IEEE, pp 1237–1244
32. Parcollet T, Morchid M, Linarès G (2019, May) Quaternion convolutional neural networks for heterogeneous image processing. In ICASSP 2019–2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, pp 8514–8518
33. Pratap A, Raja R, Alzabut J, Cao J, Rajchakit G, Huang C (2020) Mittag-Leffler stability and adaptive impulsive synchronization of fractional order neural networks in quaternion field. Math Methods Appl Sci 43(10):6223–6253
34. Rajakumar R (2021) Quaternionic short-time fractional Fourier transform. Int J Appl Comput Math 7(3):1–13
35. Rajalakshmi M, Annapurani Panaiyappan K (2022) A multimodal architecture using Adapt-HKFCT segmentation and feature-based chaos integrated deep neural networks (Chaos-DNN-SPOA) for contactless biometricpalm vein recognition system. Int J Intell Syst 37(3):1846–1879
36. Rajasekar V, Premalatha J, Sathya K (2021) Cancelable Iris template for secure authentication based on random projection and double random phase encoding. Peer-to-Peer Netw Appl 14(2):747–762
37. Roopkumar R (2020) Quaternionic fractional fourier transform for boehmians. Ukr Math J 72(6):942–952
38. Singh BK, Kumar R, Kishore RR (2021) A biometric system design using finger knuckle biological trait. Multimed Tools Appl:1–18
39. Soliman NF, Algarni AD, El-Shafai W, Abd El-Samie FE, El Banby GM (2021) An efficient GCD-based cancelable biometric algorithm for single and multiple biometrics. CMC-Comput Mater Contin 69(2):1571–1595
40. Tran QN, Turnbull BP, Hu J (2021) Biometrics and privacy-preservation: How do they evolve? IEEE Open J Comput Soc 2:179–191

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Fatma Khallaf[1,2] · Walid El-Shafai[1,3] · El-Sayed M. El-Rabaie[1] · Mahmoud Nasr[4,5] · Mohammed Essam[6] · E. S. Shoukralla[4] · Saied M. Abd El-atty[1] · Fathi E. Abd El-Samie[1,7]

✉ Fatma Khallaf
fatma.khallaf@acu.edu.eg

Walid El-Shafai
eng.waled.elshafai@gmail.com; walid.elshafai@el-eng.menofia.edu.eg

El-Sayed M. El-Rabaie
srabie1@yahoo.com

Mahmoud Nasr
nasr@agh.edu.pl

Mohammed Essam
mohamed.essam@fue.edu.eg

E. S. Shoukralla
shoukrala@hotmail.com

Saied M. Abd El-atty
sabdelatty@el-eng.menofia.edu.eg

Fathi E. Abd El-Samie
feabdelhamid@pnu.edu.sa; fathi_sayed@yahoo.com

[1] Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[2] Department of Electrical Engineering, Faculty of Engineering, Ahram Canadian University, 6th October City, Giza, Egypt

[3] Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia

[4] Department of Biomedical Engineering, AGH University of Krakow, 30-059 Krakow, Poland

[5] Engineering Mathematics and Physics Department, Faculty of Engineering and Technology, Future University in Egypt, 11835 New Cairo, Egypt

[6] Biomedical Engineering Department, Future university, Cairo, Egypt

[7] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, P.O. Box 84428, 11671, Saudi Arabia