Computers, Materials & Continua
DOI: 10.32604/cmc.2023.030789
Article

Tech Science Press

Cancellable Multi-Biometric Feature Veins Template Generation Based on SHA-3 Hashing

Salwa M. Serag Eldin[1],[*], Ahmed Sedik[2], Sultan S. Alshamrani[3] and Ahmed M. Ayoup[4]

[1]Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
[2]Department of Robotics and Intelligent Machine, Faculty of Artificial Intelligent, Kafrelsheikh University, Egypt
[3]Department of Information Technology, College of Computer and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
[4]Department of Electrical Communications Engineering, Faculty of Engineering, Minia University, Minia, 61111, Egypt
*Corresponding Author: Salwa M. Serag Eldin. Email: salwa.serageldin@gmail.com

Received: 01 April 2022; Accepted: 12 June 2022

Abstract: In this paper, a novel cancellable biometrics technique called Multi-Biometric-Feature-Hashing (MBFH) is proposed. The MBFH strategy is utilized to actualize a single direction (non-invertibility) biometric shape. MBFH is a typical model security conspire that is distinguished in the utilization of this protection insurance framework in numerous sorts of biometric feature strategies (retina, palm print, Hand Dorsum, fingerprint). A more robust and accurate multilingual biological structure in expressing human loneliness requires a different format to record clients with inseparable comparisons from individual biographical sources. This may raise worries about their utilization and security when these spread out designs are subverted as everybody is acknowledged for another biometric attribute.The proposed structure comprises of four sections: input multi-biometric acquisition, feature extraction, Multi-Exposure Fusion (MEF) and secure hashing calculation (SHA-3). Multimodal biometrics systems that are more powerful and precise in human-unmistakable evidence require various configurations to store a comparative customer that can be contrasted with biometric wellsprings of people. Disparate top words, biometrics graphs can't be denied and change to another request for positive Identifications (IDs) while settling. Cancellable biometrics is may be the special procedure used to recognize this issue.

Keywords: Feature extraction; multi-biometrics; SHA-3; MEF

1 Introduction

The security and privacy concerns of the cancellable biometric technique can be improved and evaluated depending on the non-invertibility technique. It is a technique related to the complexity of recovering an original biometric feature in relation to a secure erasable pattern [1]. The non-invertibility of the transformation determines the protection of the template schemes based on the transformation of the characteristics of the biometric input. Therefore, it is very important to propose an irreversibility measure that estimates the probability that the opponent cannot match the original template with respect to the transformed pattern.

Biohashing is one of the biometric security system transformation methods that utilises the factor to transform a user key or password. The key must be stored securely, or the user must remember the authentication password. Using a transformation approach to reverse the order or position of the biometric, this non-reversible technique is crucial for authentication as it strengthens the security of the biometric template space. Progress in biohashing is depicted in Fig. 1. It can be broken down as follows:

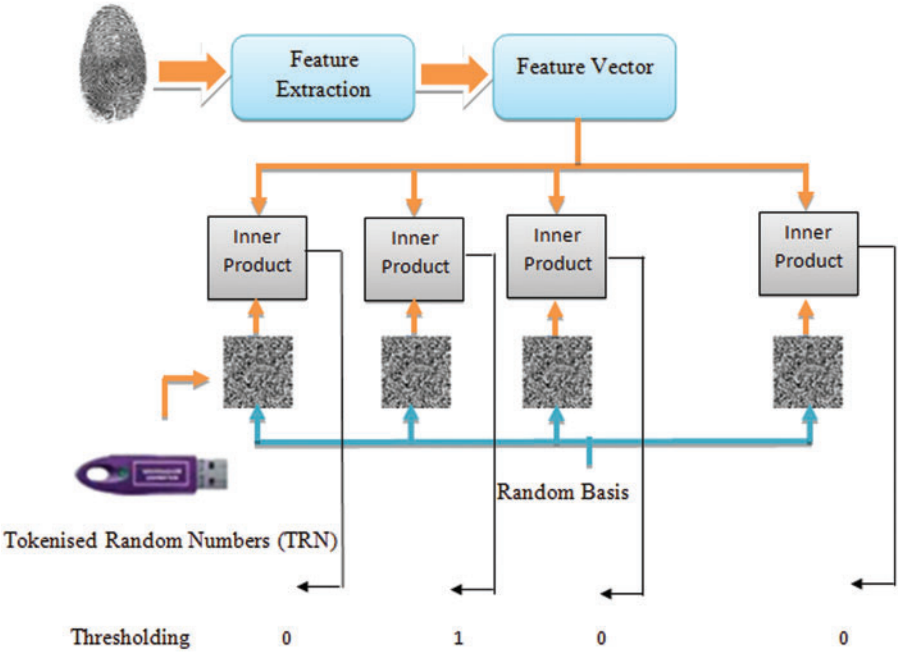


Figure 1: The process of tokenised random number (TRN) [1]

First, the fingerprint is transformed and the fingerprint features are extracted. Feature vectors contain various features of the attached fingerprint that are used to generate hash code. The system then supplies the Tokenized Random Number (TRN). The provided TRN is combined with the obtained feature vectors that form the fingerprint. The inner product that led to the combination is nothing more than a hash code generated for the supplied fingerprint and the token's random number.

The goal of this paper is to generate a cancellable biometric using hashing techniques in which the imposter cannot restore the original biometric from the deformed version or the opponent can be revoking the deformedion that is stored in databased.

This article is divided into six parts. The first part introduces cancellable biometrics based on hashing generation, the second part introduces the related work of different articles in biohashing cancellable biometric. In the third part, we explain the proposed algorithm and the authentication strategy. The fourth part introduces the simulation results and discussion. Finally, the work is concluded and future work is suggested.

2 Related Work

This section summarises the most current and noteworthy related work. Connie et al. [2] proposed novel cancellable biometric methodologies, known as palm hashing, to mitigate the attack points on cancellable biometric registration. The suggested method analyses palm print designs containing several pseudo-random keys to generate a unique code known as a palm hash. The Palm hash code can be utilised in traditional verification methods such as tokens and smart cards.

Pang et al., [3] proposed in this paper a cancellable fingerprint verification framework that was specifically expected to face the shortages of the current authorization biometric system. The proposed technique, geometric and pseudo-Zernike minutes are used as feature extractors to transform the palmprint biometric into a low-dimensional representation with moderate parts.

Jin et al., [4] proposed a new approach to ensure that the cryptographic private key is official and can be recovered from unique fingerprint data using Biohash, ReedSolomon Code (RSC) and the point of secrets exchange agreement. Cheung et al., [5] suggested a secure non-invertiable cancellable biometric . To make sure about security, cancellable biometrics is in a perfect world to be non-invertible with the ultimate objective that no original data can be recovered from the cancellable biometrics design, which is taken care of in databases for singular ID/check. One way to deal with achieve the non-certainty is utilizing non-invertible changes. Starting late some new cancellable biometric approaches are proposed reliant on Bio Hashing. Those strategies are utilizing non-invertible changes to achieve cancellable biometrics and in this manner, non-certainty is furthermore accomplished.

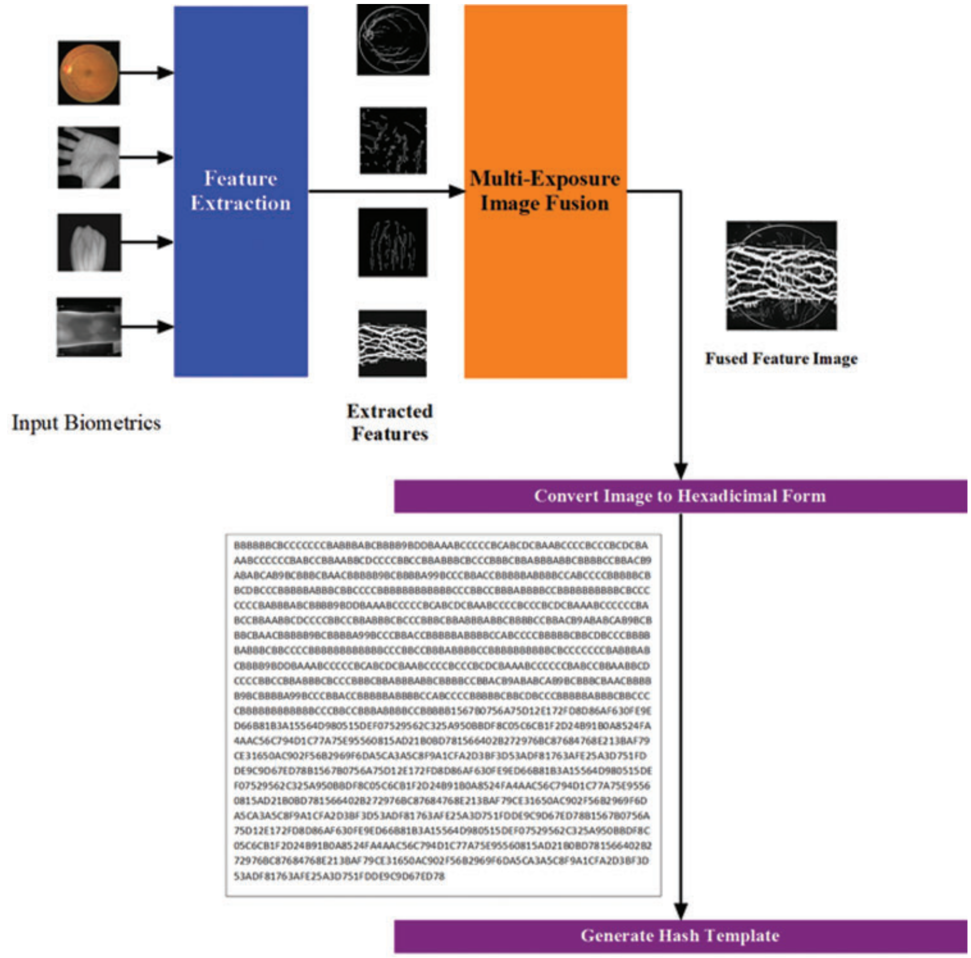
Lumini et al., [6] proposed a couple of plans to improve the base Bio Hashing way to deal with keep up an uncommonly low comparable botch rate when nobody takes the Hash key, and to show up at incredible execution moreover when an "impostor" takes the Hash key.

Sunil Gaddam et al., [7] propels another technique for the ensured accumulating of extraordinary imprint design by delivering Made secure with a set of functions and keys for cryptographic systems used to encrypt or decrypt data with guidance on erasable biometrics traits.. In this article, the reaseacher designed a system to extract cancellable key from exceptional biometrict to beat these issues. The flexibility and immobility of cryptography is updated through the misuse of erasable biometrics.

Chang proposed [8] an alternative method for ensuring about-face biometric data using a single heading change from which unique face images cannot be reconstructed. Using Radon's modified biometric face features and unpredictable multispace projection, a secure, reusable design is constructed. Using an image-based calculation of facts, services in altered formats are compared without the need for further alteration. Takahashi et al. [9] proposed an additional method for generating cancellable novel imprint designs with clear security based on the striking chip organising computation for finger impression confirmation and relationship invariant discretionary filtering for transforming formats.

3 The Proposed Cancellable Multi-Hashing Feature Veins Generating Template

The proposed secure multiple-hashing feature vein creates a pattern scheme based on the reversible SHA-3 technique. The multi-biometric system first captures a sample of a vein and then works through a feature extraction process. The sample is then converted to a biometric feature using some kind of math function. The biological model will provide effective representation and a high classification of attributes that can be compared to other forms identification. Most biological systems allow two modes of operation. The enrollment mode to add templates to the database and the authentication mode that created the template for a person are searched in the pre-written templates database. The proposed technique is performed in six stages. Fig. 2 shows the enrollment scheme of the proposed cancellable of multi-hashing feature veins generating template. The algorithm steps can be explained as follows:



```
BBBBBBCBCCCCCCCBABBBABCBBBB9BDDBAAABCCCCCBCABCDCBAABCCCCBCCCBCDCBA
AABCCCCCCBABCCBBAABBCDCCCCBBCCBBABBBCBCCCBBBCBBABBBABBCBBBBCCBBACB9
ABABCAB9BCBBBCBAACBBBBB9BCBBBBA99BCCCBBACCBBBBBABBBBCCABCCCCBBBBBCB
BCDBCCCBBBBBABBBCBBCCCCBBBBBBBBBBBBBCCCBBCCBBBABBBBCCBBBBBBBBBBCBCCC
CCCCBABBBABCBBBB9BDDBAAABCCCCCBCABCDCBAABCCCCBCCCBCDCBAAABCCCCCCBA
BCCBBAABBCDCCCCBBCCBBABBBCBCCCBBBCBBABBBABBCBBBBCCBBACB9ABABCAB9BCB
BBCBAACBBBBB9BCBBBBA99BCCCBBACCBBBBBABBBBCCABCCCCBBBBBCBBCDBCCCBBBB
BABBBCBBCCCCBBBBBBBBBBBBBCCCBBCCBBBABBBBCCBBBBBBBBBBCBCCCCCCCBABBBAB
CBBBB9BDDBAAABCCCCCBCABCDCBAABCCCCBCCCBCDCBAAABCCCCCCBABCCBBAABBCD
CCCCBBCCBBABBBCBCCCBBBCBBABBBABBCBBBBCCBBACB9ABABCAB9BCBBBCBAACBBBB
B9BCBBBBA99BCCCBBACCBBBBBABBBBCCABCCCCBBBBBCBBCDBCCCBBBBBABBBCBBCCC
CBBBBBBBBBBBBBCCCBBCCBBBABBBBCCBBBBB1567B0756A75D12E172FD8D86AF630FE9E
D66B81B3A15564D980515DEF07529562C325A950BBDF8C05C6CB1F2D24B91B0A8524FA
4AAC56C794D1C77A75E95560815AD21B0BD781566402B272976BC87684768E213BAF79
CE31650AC902F56B2969F6DA5CA3A5C8F9A1CFA2D3BF3D53ADF81763AFE25A3D751FD
DE9C9D67ED78B1567B0756A75D12E172FD8D86AF630FE9ED66B81B3A15564D980515DE
F07529562C325A950BBDF8C05C6CB1F2D24B91B0A8524FA4AAC56C794D1C77A75E9556
0815AD21B0BD781566402B272976BC87684768E213BAF79CE31650AC902F56B2969F6D
A5CA3A5C8F9A1CFA2D3BF3D53ADF81763AFE25A3D751FDDE9C9D67ED78B1567B0756A
75D12E172FD8D86AF630FE9ED66B81B3A15564D980515DEF07529562C325A950BBDF8C
05C6CB1F2D24B91B0A8524FA4AAC56C794D1C77A75E95560815AD21B0BD781566402B2
72976BC87684768E213BAF79CE31650AC902F56B2969F6DA5CA3A5C8F9A1CFA2D3BF3D
53ADF81763AFE25A3D751FDDE9C9D67ED78
```

```
SHA-224  EF9ABE5A7436BB44FD96B63F8309C11BC6A67C66906762AB2FDC2877
SHA-256  7AC8876F5A2BB5C5E33BCAFCF74A1A0C7D32EC7AC2C895914FF4C9EF5E075777
SHA-384  8E978AA3BB5363F8F885581B3F81C8F66819F3118AEB6791D48CC72D295C29F8BFB385E81B1D72E6B691EEAF1546B31C
SHA-512  671C52D211E0605C0D990FE26C67500A2CB865FE9F18260DF684EA7309DD15FDF9D472E1D23760CF88258B44A5855AB6889B54676C0A6F6917BD4F6CCDD84309
```

Figure 2: The enrollment scheme of the proposed cancellable multi-hashing feature veins generating template

Step 1: Feature Extraction

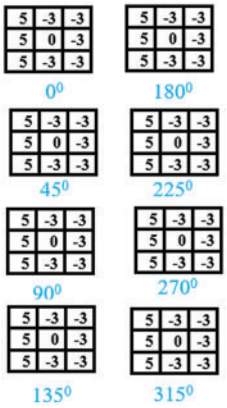
Attribution is done behind the palm and dorsal of the hand using 3 steps. The first step is to convert the caption image to a grayscale image. The second is to apply a medium filter to remove noise. In addition, the third stage is based on image enhancement Contrast Limited Adaptive Histogram Equalization (CLAHE) technique. Adaptive Histogram Smoothing (AHE) is a local technique that calculates multiple histograms for different parts of a biometric. These histograms are individually aligned and then merged to distribute the recovery value of the biometric. In the homogeneous areas of the image, she tends to increase contrast because the histogram is concentrated in these areas (there are very few different grays). Contrast Limited AHE [10] limits contrast enhancement to reduce the issue of size enhancement.

CLAHE successfully is used as an easy way to improve contrast and vascular image quality. The fourth is done to make the average filter on the enhanced image much smoother. Alternatively, the next step is based on the implementation of an adaptive bracket to clean the biometric strands in black. Then image-enhancing techniques apply to the resulting image to clearly visualize the veins.

Soft tissue that attaches to the inside of the eye, the retina is a multilayered structure connected by synapses. On the nasal side of the optical disc's centre, the central retinal vein and artery appear adjacent [10]. Information regarding vessel structure can facilitate severity classification and serve as a marker during segment surgery. The RGB values for the image's distinguishing characteristics are provided below. The primary objective of this research is to accurately harvest blood vessels and to replace existing vessel harvesting procedures. In the initial step of edge enhancement, the Red Green Blue (RGB) retinal image illuminates the edges. In addition to preparing the blood vessel margins, the histogram must be filtered and smoothed for irregular noise and low intensity after the conversion to retinal grayscale. Due to edge enhancements, multiple tiny objects are produced after binarization. Again, it is necessary to eradicate the papilla from the vascular image by removing the papilla from the papilla. The steps are described in detail below.

1. Edge Enhancement

The Kirsch colour photograph layout [11] In order to detect blood vessels in retinal images, the Kirsch template is utilised. Fig. 3 demonstrates the automated rotation of the Kirsch techniques. The Kirsch operator is one of the discrete forms of first-order derivatives used for edge detection and enhancement. The operator uses eight templates that are gradually rotated by 45 degrees to detect the edges. At each pixel, the gradient is produced by convolving the image with eight impulse response template matrices. This produces the gradient in multiple directions. The final gradient is the sum of the raised edges when all RGB channel directions are evaluated instead of just one. Fig. 4 depicts a number of enlarged photos of steering.



$$\begin{array}{|c|c|c|}\hline 5 & -3 & -3 \\ \hline 5 & 0 & -3 \\ \hline 5 & -3 & -3 \\ \hline \end{array}$$

0^0

$$\begin{array}{|c|c|c|}\hline 5 & -3 & -3 \\ \hline 5 & 0 & -3 \\ \hline 5 & -3 & -3 \\ \hline \end{array}$$

180^0

$$\begin{array}{|c|c|c|}\hline 5 & -3 & -3 \\ \hline 5 & 0 & -3 \\ \hline 5 & -3 & -3 \\ \hline \end{array}$$

45^0

$$\begin{array}{|c|c|c|}\hline 5 & -3 & -3 \\ \hline 5 & 0 & -3 \\ \hline 5 & -3 & -3 \\ \hline \end{array}$$

225^0

$$\begin{array}{|c|c|c|}\hline 5 & -3 & -3 \\ \hline 5 & 0 & -3 \\ \hline 5 & -3 & -3 \\ \hline \end{array}$$

90^0

$$\begin{array}{|c|c|c|}\hline 5 & -3 & -3 \\ \hline 5 & 0 & -3 \\ \hline 5 & -3 & -3 \\ \hline \end{array}$$

270^0

$$\begin{array}{|c|c|c|}\hline 5 & -3 & -3 \\ \hline 5 & 0 & -3 \\ \hline 5 & -3 & -3 \\ \hline \end{array}$$

135^0

$$\begin{array}{|c|c|c|}\hline 5 & -3 & -3 \\ \hline 5 & 0 & -3 \\ \hline 5 & -3 & -3 \\ \hline \end{array}$$

315^0

Figure 3: Array of kirsch's template [11]

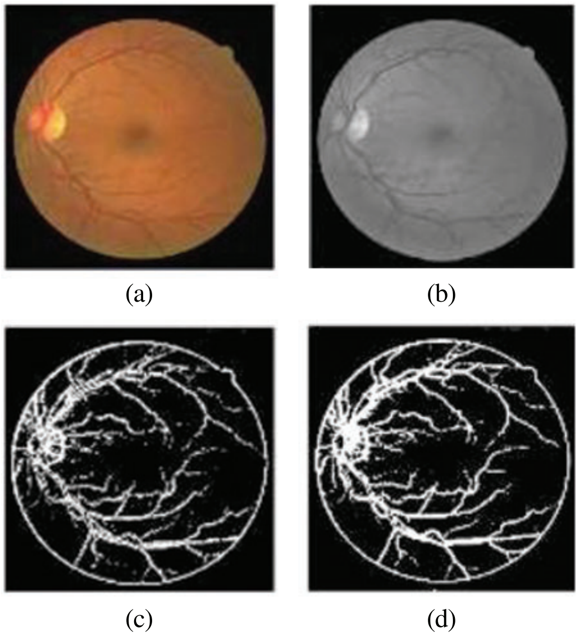


Figure 4: (a) Input retinal image, (b) Green channel image, (c) detected retinal vessels and (d) Image after closing [11]

2. Gray-Scale Conversion and Medium Filtering

Using Eq., we convert the edge-enhanced RGB image to its grayscale image (1). To convert an RGB image to grey, the red, green, and blue values must be calculated according to the intensity of the gamma-extended linear encoding. If the grayscale output is I and the red, green, and blue components are R, G, and B, then the grayscale output is I.

$$I = 0.33R + 0.5G + 0.166B \tag{1}$$

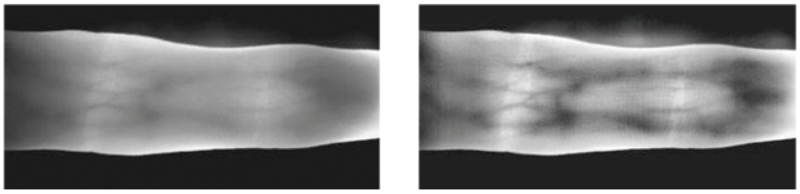
where the intensities between the lines (in this case, the vein) are the background. The finger is treated as a similar electrical sample. For example, the left index finger is compared to the middle finger of the right hand. Two database performance experiments are performed: one with adaptive histogram smoothing and one without it-a step before processing. The procedure this step is performed by default using MATLAB's adapthisteq function. The effect of the histogram equation applied to the vascular model image can be seen in Fig. 5 Binary masks are used to ensure that only the regions of the image with fingers are compared to each other [12]. These algorithms were applied in our compiled dataset and into the V4 finger vein database of Peking University. The performance of the algorithm is measured according to the Equal Error Rate (EER) [13].

In this study, a Convolutional Neural Network-based method for finger vein feature extraction was implemented (CNN). This technique is based on the architecture of Ronneberger et al U-net. The community consists of a component for coding and a component for interpretation. The encoding design consists of units of two convolution layers, each followed by a rectification layer (ReLU) and a 2 2 downsampling layer (Pooling) with a stride of 2. Feature channels are repeated at every step of downsampling.

The related interpretation structure consists of 2 2-layer upsampling building blocks that halve the fold range of function channels, a concatenation operator with the function map truncated by the coding unit, and 3 3 convolutions, each accompanied by a ReLU. In the last layer, the problem function vectors are mapped to the preferred section region using an 11 convolution. The force characteristic is computed using a softmax operation on the final function map in conjunction with the transverse entropy loss characteristic. The cross-entropy penalises the softmax deviation (M(x)(x)) from one (1.00) at each point in the following manner:

$$\varepsilon = \sum_{k=1} \log \left(M\lambda \left(\mathrm{x} \right) \left(x \right) \right) \tag{2}$$

where $\lambda : \Omega \rightarrow \{1, \ldots, \mathrm{K}\}$ is the real label of every pixel, at the placement $\mathrm{x} \in \Omega$, with $\Omega \subset \mathrm{Z2}$. The network soft-max layer generates the very last segmentation as a chance map, whose pixel values mirror the chance of a selected pixel belonging to a vein or not. The community has a huge range of function channels, which permit it to propagate context facts to better decision layers, and gives stop-to-stop education with ca onfined range of education samples. The community implementation turned into realised withinside the Tensor Flow approach with the use of the Keras library.



(a) Authenticate Biometric (b) Adaptive Histogram Equalisation

Figure 5: Consequence of adaptive equalization of the histogram [12]

Step 2: Image Fusion Technique

Multiple Exposure Synthesis (MEF) techniques employed nowadays are based on weighted fusion [14–17]. By establishing the weight of each pixel depending on its intensity, the principal concept of the weight combination is created. This mass is computed as:

$$\mathrm{I}_{\mathrm{fused}} \left(\mathrm{x}, \mathrm{y} \right) = \sum\nolimits_{n=1}^{N} . W_n \ \left(x, y \right) I_n \ \left(x, y \right) \tag{3}$$

where N is the number of images in a multiple exposure image set. In(x;y) is the pixel intensity of the nth image in the set and Wn(x;y) denotes the weight representing the importance of the pixel In(x;y). In this document we normalize the pixel intensity in the range from [0, 1]. The final weight for each image is calculated by combining two weights with normalization as

$$W_n \left(x, y \right) = \frac{W_{1,n} \left(x, y \right)^{p1} \ \times \ W_{2,n} \left(x, y \right)^{p2}}{\sum\nolimits_{n=1}^{N} . W_{1,n} \left(x, y \right)^{p1} \ \times \ W_{2,n} \left(x, y \right)^{p2} + \epsilon} \tag{4}$$

where p1, p2 > 0 are parameters that determine which of them to define.However, we set these parameters in the same way (p1 = p2 = 1). Using the weights obtained above, we can combine the figure according to the Eq. (3) However, this method tends to give an unnatural picture for these works as the weight values tend to be unstable and noisy. Then we apply Eq. (4). With high resolution using the resolution pyramid image contained in [14]. MEF is processed in each

pyramid and the final result is synthesized.

Step 3: The Trusted Hash Algorithm

On August 5, 2015, the National Institute of Standards and Technology (NIST) announced the Secure Hash Algorithm (SHA3). It is the family's most temperamental algorithm. [17,18] SHA3 is a subset of the larger cryptographic family Keccak. Guido Bertoni, Joan Daemen, Michal Peeters, and Gilles Van Assche are responsible for the design of Radio Gatn. Keccak implements a novel technique called sponge construction. The architecture of the sponge is dependent on a number of random functions or random permissions and allows for the entrance of data ("absorb" in the term sponge) and the quantity to release ("squeeze"). The data, which works as a generator of random numbers, takes into account all previous inputs. This leads to exceptional adaptability. NIST has no current plans to remove SHA2 from the new safe hash standard. SHA3 is intended to be directly interchangeable with SHA2 in the current application, if required, and to strengthen the robustness of the overall hash algorithm toolkit [19]. The construction of a sponge is shown at Fig. 6.

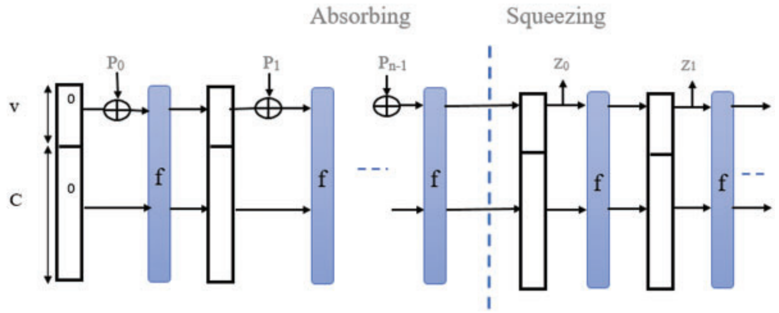


Figure 6: Construction of a sponge for the functions of the hash

SHA-3 uses a structure like a sponge [20] in which data is "absorbed" and then "squeezed" to get a result. During the validation step, the XOR message blocks are transferred to a server state, which is then fully communicated via the system function f. Throughout the duration of compression, the output log is alternately read from the same sub-state and transition state f. The output log is alternately read from the same sub-state and the transition state f throughout "compression." The portion of the state that is written and read is known as the "rate" (R symbol), but the size of the section that is not entered by the input/output is known as the "capacity" (denoted R). Capacity determines the security of the scheme. The highest level of protection is 12 power.

Taking into account the input bit string N, the padding function pad, and the permutation function f operating on b-width, velocity r, and output-length d-bit blocks, we have the capacity c = b-r and the sponge structure z = sponge [f, pad, r] (N, d), obtaining a string Z of length d along length d, works as follows: [21,22]

- Insert the N input using the pad function to create a softened bit string P of length (so that n = Len (p)/r is an integer).
- Divide P n into successive r-bit bits $P_0 \ldots P_{n-1}$
- Initialize state S on line b with zero 40 bits
- Assimilate input state: for every block Pi:
- Extend Pi c at the end with a string of zero bits to obtain the length b
- XOR that with S
- The result must apply a block permutation f to obtain a new state S
- Initialize Z as an empty string
- And the length Z is less than d:
- Add the first S bits to Z

- If Z is still less than d bits, use f S to get a new state S
- Shorten Z to d bits

SHA-3 state b = 5 5 w = 5 5 64 = 1600 bits in total. Cookies are defined for word lengths of up to 1 bit (25 bits in total). In reality, intermediate state values (from w = 8, 200 bits to w = 32, 800 bits) can be employed for straightforward application [23–25]. For SHA-3–224, SHA-3–256, SHA-3–384, and SHA-3–512 instances, r is larger than d, therefore no further block permutations are required at the squeezing point; the intended hash is the crucial bit of state. Keccak-f [1600] is a substitution for SHA-3's block transformation. that uses XOR, AN, and NET operations and is easy to perform on both software and hardware. It is defined for the size of any two words, $w = 2\ell$ bits. The main definition of SHA-3 uses 64-bit words, $\ell = 6$. The state can be thought of as an array of $5 \times 5 \times w$ bits. Let be the [i] [j] [k] be bit $(5i + j) \times w + k$ of the input., $\ell = 6$. The state can be viewed as an array of $5 \times 5 \times w$ bits. Let [i][j][k] be the $(5i + j) \times w + k$ bit of the input, with smaller integers and larger subscripts. namely.I select rows, columns, j and bits. Index arithmetic is applied for the first two dimensions modulo 5 and for the third dimension modulo w. SHA3 security is not vulnerable to the length extension attack:

SHA2 attacks divide the data into fundamental blocks and provide identical results for each block's output function. In addition, the entire message's output represents the current result once all blocks have been processed.

The internal state of the sponge construct exceeds the hash function's output. Therefore, it is pointless to generate a block without the majority of the state, as the complete state is necessary to continue with the digest.

4 Authentication Strategy

The proposed authentication system technique takes the biometric authentication system's risk model into account. During the initial enrollment phase, the operator gathered a large number of biometric user attributes. Several processes are then done to obtain biometric features based on the discovered biological traits, and a combined technique for obtaining photographs is established. The operator can choose the output size SHA-3 to generate a message digest for each user who has been authenticated. Using the authentication method, multi-gauge tokens are extracted from the incoming user in order to determine the tokens the user has received. The process of blending is used to extract the merged image. The operator utilised the chosen hash variation. In the registration technique, when constructing a message summary as seen in Fig. 7, the message generated corresponds to the message summary recorded in the summary database; if it matches, the user becomes a genius, and if it does not, the incoming person becomes a fraud.

5 Simulation Results

This work presents a cancellable multi-biometric approach based on picture fusion and hashing techniques. The fundamental concept is to produce text-hash templates that represent the original biometric photos. The proposed technique is implemented on images of the retina, finger veins, palm, and dorsal vein. In addition, pairwise evaluation metrics such as hamming, spearman, and Jaccard pairwise distances have been applied. Text templates are created using SHA-224, SHA-256, SHA-384, and SHA-512. Each image in Fig. 8 depicts the visual representation of each hashing algorithm. Tab. 1 also displays the hexadecimal hash text for each hashing algorithm. Moreover, each algorithm generates a hash of a particular length, SHA-224 with 56 characters, SHA-256 with 64, SHA-384 with 96, and SHA-512 with 128, see Tab. 2. Statistical criteria are used to evaluate the generated hashes in order to ensure that the proposed model provides a unique text template for each user.

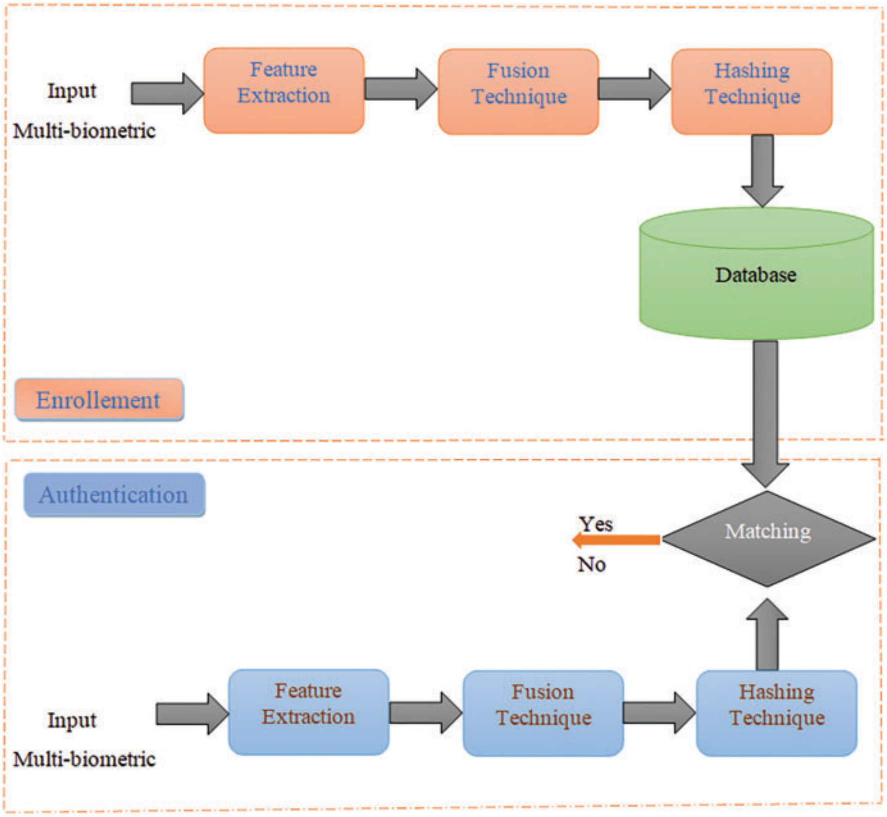


Figure 7: Block diagram of the proposed authentication technique

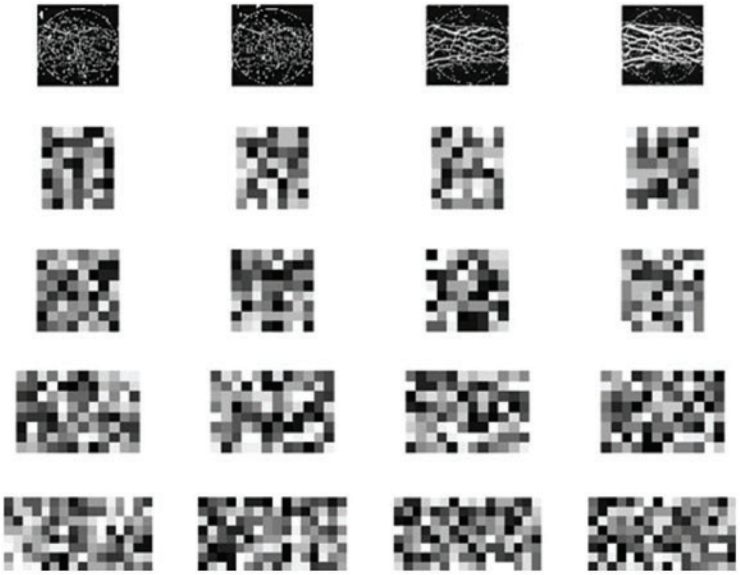
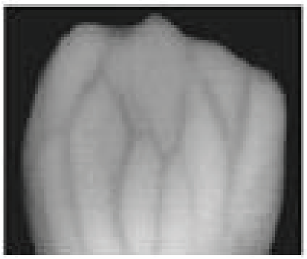
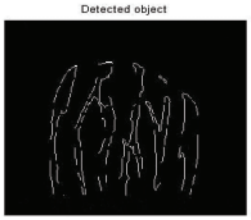
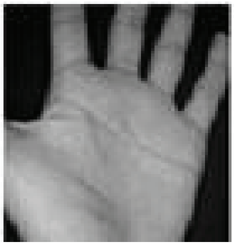
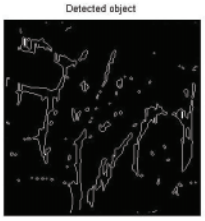
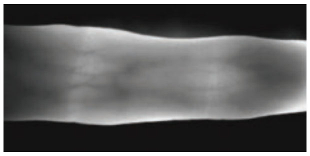
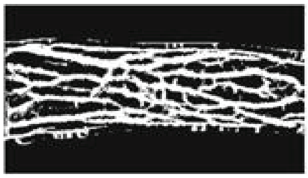
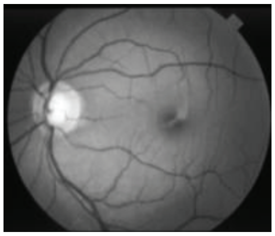
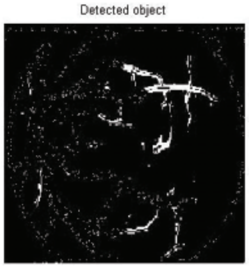


Figure 8: The generated templates represented in image form of the proposed technique

Table 1: Feature extraction input multi-biometric (Palm, Retina, Dorsal hand, Fingerprint)

Input Biometric	Feature Extraction
	
	
	
	

5.1 Image-based Evaluation

The first trend discussed in this paper is the generation of a visual template using biometric image fusion. As seen in Fig. 8, the created templates can be expressed in image form. Tabulator 3 depicts the image-based evaluation. Unified Average Changing Intensity (UACI), Structural Similarity Index

(SSIM), Universal Image Quality (UIQ), Spectral Distribution (SD), Peak Signal to Noise Ratio (PSNR), and Number Pixel Change Rate are used to evaluate the created visual templates (NPCR).

Simulation results indicate that the proposed method obtained a high level of qualitative and quantitative performance prior to image-based evaluation, see Tab. 3. Therefore, the proposed solution can be deemed an effective security technique.

Table 2: The SHA-3 algorithm and variant output size plus rounds [22]

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Rounds	Operations	Security (in bits) Against collision attacks	Capacity against length extension attacks	First published
SHA-3	SHA3-224	224	1600 (5∗5∗64)	1152	24[4]	And,Xor, Rot,Not	112	448	2015
SHA-3	SHA3-256	256	1600 (5∗5∗64)	1088	24[4]	And,Xor, Rot,Not	128	512	2015
SHA-3	SHA3-384	384	1600 (5∗5∗64)	832	24[4]	And,Xor, Rot,Not	192	768	2015
SHA-3	SHA3-512	512	1600 (5∗5∗64)	576	24[4]	And,Xor, Rot,Not	256	1024	2015

Table 3: Image-based evaluation results

Image	Method	NPCR (%)	PSNR (dB)	SSIM	UIQ	SD	UACI
1	SHA-224	99.6567	14.0371	0.0316	0.3805	103.99	40.784
	SHA-256	99.308	13.135	0.0347	0.3438	99.29	38.9431
	SHA-384	99.7253	14.3694	0.0139	0.3692	106.657	41.8263
	SHA-512	99.7429	13.1825	0.0113	0.34	115.3045	45.2174
2	SHA-224	99.7597	13.4709	0.0146	0.3570	111.2071	41.6106
	SHA-256	99.4808	14.6462	0.0205	0.3616	103.7476	40.6837
	SHA-384	99.6056	13.4024	0.014	0.3355	111.4956	43.7238
	SHA-512	99.477	15.1603	0.0175	0.3657	99.8106	39.1414
3	SHA-224	99.8188	14.1610	0.0288	0.379	108.2863	42.4652
	SHA-256	99.4877	14.6369	0.0267	0.3752	101.4454	39.7857
	SHA-384	99.6877	14.4479	0.0203	0.3597	105.6668	41.438
	SHA-512	99.5089	15.7727	0.0205	0.4064	97.4189	38.2035
4	SHA-224	99.6471	16.3405	0.0222	0.46	95.581	37.5739
	SHA-256	99.6738	14.0403	0.0179	0.4297	104.2769	40.2989
	SHA-384	99.6749	15.7818	0.0187	0.4379	97.7577	38.3363
	SHA-512	99.6014	15.7205	0.019	0.4287	98.5231	38.6365

5.2 *Text-based Evaluation*

The other trend of this work is to generate a text templates which are generated to provide another form of cancelable templates. Tab. 4 Shows the generated text templates. In addition, the numerical observations of both hamming, spearman, Jaccard distances for each hashing technique are illustrated in Tab. 5. Furthermore, the statiscal metrics are visualized into curves which are shown in Fig. 9. The statistical analysis reveals that the proposed algorithm achieved average values over 0.9 in both spearman, Jaccard, and hamming distance regarding the pairwise evaluation of the generated text templates.

Table 4: The generated text templates obtained by SHA-224, SHA-256, SHA-384 and SHA-512

ID	Hash technique	Output hash template
1	SHA-224	560D31B8C1898661E4D2DCABC4712455149AAB7E1F8BE3D5C8005065
	SHA-256	819694037C5836A6CA616D889F27189369C9895D9A0E04B9B1216E3B812DB461
	SHA-384	B638412A55263FCBD1F435487F9612B5E1CFD67470695A821565B5FB813E7AE0DBE836A5B98B1B3EE8FD83BAED3B6349
	SHA-512	438AEF8CCC2ADDFF5CECB4AE55D9AA7FBE848C6156391E2A898F7E0014A3259D53A665F395DABA9A95FFE95AEDD2873898FF143CFF93AC8576B961D93E8711C5
2	SHA-224	C6CBECA8D30EB34FF4B55E46262C1DFEBB6AE035BB5369BC16286C1B
	SHA-256	2135AD2AA94480CD846CE8DEC61767A25E0730A0F325F5BAC186ACBF5281D581
	SHA-384	49A7F6BED6BBB7829E90554BF1A64BFEAFD837FE20DE6037D077056D2ACAD0F48AFD11E5A5F14DF05D440FA5443D842E
	SHA-512	05D14A50530DA02B6935520E0BE24211EC42D6FF286609E82D6F7C8506889E6CFB779D630064D00BA4FEFBEE6187CB7E484982035CE59DE415836C844CE8D69A
3	SHA-224	92BBDA2C1AB412D5ED1A7CF953CC3A89E5A55EF5FDBF0CB974BD9453
	SHA-256	0E0DE0D5EE220A85C7495AED80E996014D7B181172410822CB20E4DACB84B12C
	SHA-384	6F02DCE222B18AA852D5A8D958A93E3B24D67FE1D90BC7FEB36201F8D1CB41D3D5710FB78C4F4C68BF30DA6B8F545F4E
	SHA-512	B31F51BD28087814204AAB48CAF23F18E29A095DD45BB57508C25CDFE2080B6DC357B16BE6939A173188F4FFA6BA844FA220CC3F3A19E18724DA78DDECB71766
4	SHA-224	EF9ABE5A7436BB44FD96B63F8309C11BC6A67C66906762AB2FDC2877
	SHA-256	7AC8876F5A2BB5C5E33BCAFCF74A1A0C7D32EC7AC2C895914FF4C9EF5E075777
	SHA-384	8E978AA3BB5363F8F885581B3F81C8F66819F3118AEB6791D48CC72D295C29F8BFB385E81B1D72E6B691EEAF1546B31C
	SHA-512	671C52D211E0605C0D990FE26C67500A2CB865FE9F18260DF684EA7309DD15FDF9D472E1D23760CF88258B44A5855AB6889B54676C0A6F6917BD4F6CCDD84309

Table 5: The numerical observations of both hamming, spearman, Jaccard distances for each hashing technique

Pairs	SHA-224			SHA-256			SHA-384			SHA-512		
	Jaccard	Spearman	Hamming	Jaccard	Spearman	Hamming	Jaccard	Spearman	Hamming	Jaccard	Spearman	Hamming
1, 2	0.9286	1.1095	0.9286	0.9063	0.8499	0.9063	0.9271	1.0525	0.9271	0.9453	0.8731	0.9453
1, 3	0.9643	1.1359	0.9643	0.9375	1.0408	0.9375	0.9479	0.8991	0.9479	0.9219	1.0597	0.9219
1, 4	1	1.1019	1	0.9844	1.0304	0.9844	0.9792	0.8742	0.9792	0.9531	0.9724	0.9531
2, 3	0.9286	1.0915	0.9286	0.9688	0.9059	0.9688	0.9271	1.0075	0.9271	0.9141	0.9912	0.9141
2, 4	0.9286	0.9297	0.9286	0.9375	0.7985	0.9375	0.8854	0.9446	0.8854	0.9063	0.9486	0.9063
3, 4	0.9464	0.999	0.9464	0.9063	0.9063	0.9063	0.9271	1.0231	0.9271	0.9688	1.0191	0.9688
Average	0.9494	1.06125	0.9494	0.9401	0.9219	0.9401	0.9323	0.9668	0.9323	0.9349	0.9773	0.9349

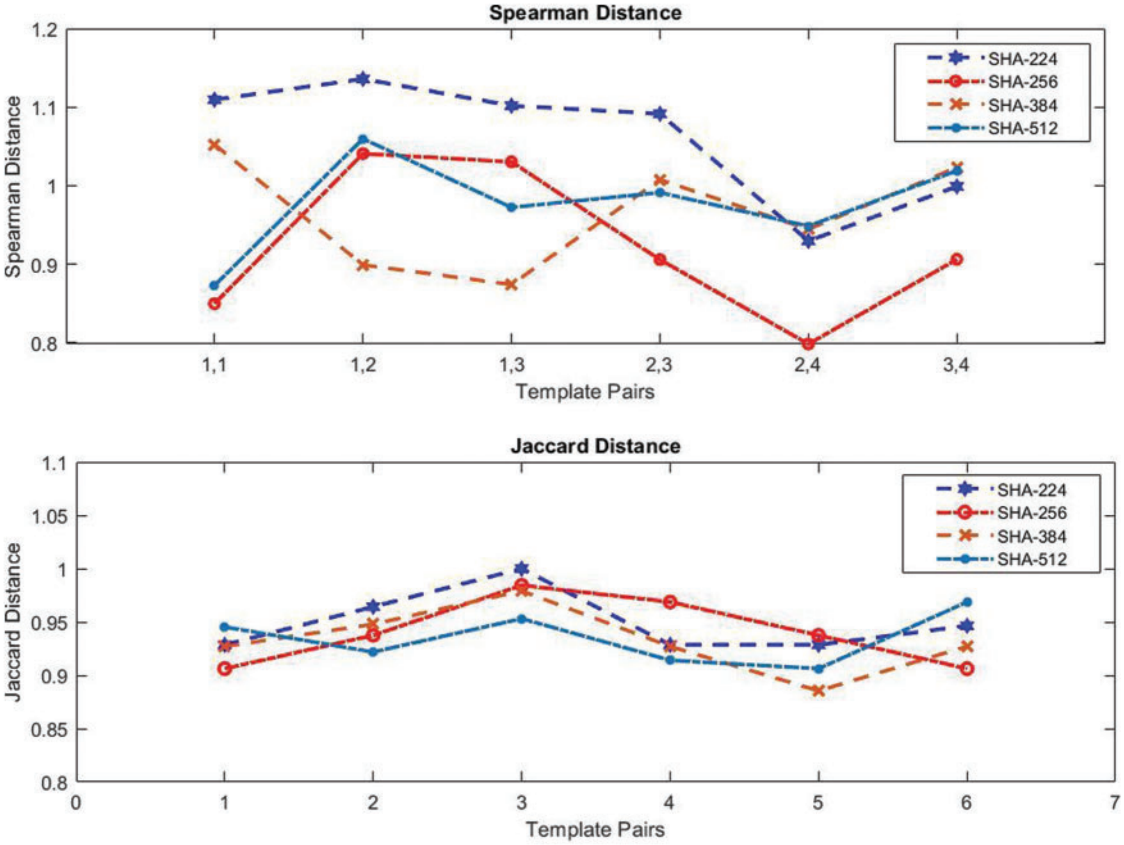


Figure 9: (Continued)

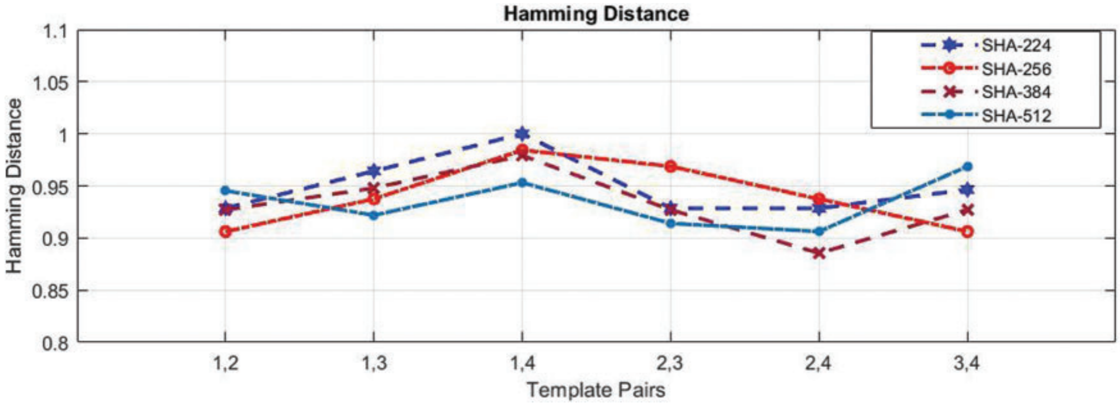


Figure 9: Text-based evaluation using hamming distance, Jaccard and spearman

The proposed method is validated by a brief comparison with the works in the literature. This comparison is carried out in terms of EER, FAR, and FRR as shown in Tab. 6. The proposed SHA-512 method appears an efficient performance where it achieved 0.0041, 0.001, and 0.0018 for EER, FAR, and FRR, respectively. Therefore, itaccomplishedd a superior performance among the proposed methods and the works in the literature as well. So, it can be considered an efficient solution prior to cancelable biometric generation.

Table 6: The proposed method compared to literature works

Cancellable biometrics method	Hash technique	EER	FAR	FRR
Proposed approach	SHA-224	0.0060	0.0011	0.0017
	SHA-256	0.0055	0.0015	0.0023
	SHA-384	0.0049	0.0013	0.0019
	SHA-512	0.0041	0.0010	0.0018
[26]		0.0924	0.0562	0.0257
[27]		0.0178	0.0071	0.0876
[28]		0.0098	0.0104	0.018
[29]		0.1081	0.0927	0.0967
[30]		0.0416	0.1955	0.0489
[31]		0.0859	0.0435	0.0627
[32]		0.0357	0.0985	0.0612
[33]		0.0046	0.0235	0.0929

6 Conclusions and Future Work

In this paper, we suggested a novel mechanismdepends on edge enhancement and material classification for automated extraction to improve the biological algorithm. This article displays that utilizing a bio-hash cancellable biometric, the statistical information comparison obtaobtains lower hamming distance metric.The proposed framework meets the needs of extractable biometrics without sacrificing recognition accuracy compared to the initial comparison of authenticate biometric. The proposed bio-mixing template feature is useful for the security of any biometric data. This paper provides four implementations for the SHA-3 family which provide a higher level of family security than the current SHA-2. The proposed performance is compared in multi-biometric and robust hashing against attacks plus fusion technique compared to other related work in [26–33].

The future work addresses two trends which treats the remaining shortages of the hash index. The first trend, the approach is apply to a resizable and unordered biometric. The second trend include the integration of biometric encryption cancellable , where the key can be embeded with the privacy policy structure for safety analysis. Investigating the adaptability of this framework for adding white Gaussian noise would be undertaken as a future extension of this work.

Acknowledgement: The authors thank the researchers of Taif University for their support. Taif University Researchers supporting Project number (TURSP-2020/215), Taif University, Taif, Saudi Arabia.

Funding Statement: This research was supported by Taif University Researchers Supporting Project Number (TURSP-2020/215), Taif University, Taif, Saudi Arabia (www.tu.edu.sa).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Sutcu, H. Sencar and N. Memon, "A secure biometric authentication scheme based on robust hashing," in *Proc of the 7th Workshop on Multimedia and Security*, New York, USA, pp. 111–116, 2005.

[2] T. Connie, A. Teoh, M. Goh and D. Ngo, "Palmhashing: A novel approach for cancellable biometrics," *Information Processing Letters*, vol. 93, no. 1, pp. 1–5, 2005.

[3] Y. Pang, A. Teoh and D. Ngo, "Palmprint based cancellable biometric authentication system," *International Journal of Signal Processing*, vol. 1, no. 2, pp. 98–104, 2004.

[4] A. Jin, D. Ling and A. Goh, "Biohashing: Two-factor authentication featuring fingerprint data and tokenized random number," *Pattern Recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[5] K. Cheung, A. Kong, J. You and D. Zhang, "An analysis on invertibility of cancellable biometrics based on BioHashing," *In CISST*, vol. 2005, pp. 40–45, 2005.

[6] A. Lumini and L. Nanni, "An improved biohashing for human authentication," *Pattern Recognition*, vol. 40, no. 3, pp. 1057–1065, 2007.

[7] S. Gaddam and M. Lal, "Efficient cancellable biometric Key generation scheme for cryptography," *IJ Network Security*, vol. 11, no. 2, pp. 61–69, 2010.

[8] Y. Chang, Z. Wende and T. Chen, "Biometrics-based cryptographic key generation," in *Proc. IEEE Int. Conf. on Multimedia and Expo*, Baltimore, MD, USA, vol. 3, pp. 2203–2206, 2004.

[9] K. Takahashi and S. Hitachi, "Generating provably secure cancellable fingerprint templates based on correlation-invariant random filtering," in *Proc. IEEE 3rd Int. Conf. on Biometrics: Theory, Applications, and Systems*, IEEE, Alghero, Italy, pp. 1–6, 2009.

[10] K. Zuiderveld, "Contrast limited adaptive histogram equalization," *Graphics Gems*, Academic Press, pp. 474–485, 1994.

[11] D. Onkaew, R. Turior, B. Uyyanonvara, N. Akinori and C. Sinthanayothin, "Automatic vessel extraction with combined bottom-hat and match-filter," in *Int. Conf. Information and Communication Technology for Embedded Systems (ICICTES)*, Nakhonpathom,Thailand, pp. 101–105, 2011.

[12] A. Uhl, C. Busch, S. Marcel and R. Veldhuis, "Handbook of vascular biometrics," *Springer Nature*, pp. 533, 2020.

[13] Peking University (2013) "PKU finger vein database," http://rate.pku.edu.cn.
[14] S. Lee, J. Park and N. Cho, "A multi-exposure image fusion based on the adaptive weights reflecting the relative pixel intensity and global gradient," in *Proc. 25th IEEE Int. Conf. on Image Processing (ICIP)*, Athens, Greece, pp. 1737–1741, 2018.
[15] N.SHA,(3), "Cryptographic hash standard," Dostopno na: https://www.nist.gov/news-events/news/2015/08/nistreleases-sha-3-cryptographic-hash-standard, August 05, 2015.
[16] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar *et al.,* "Advances in quantum cryptography. advances in optics and photonics," vol. 12, no. 4, pp. 1012–1236, 2020.
[17] C. Boutin, "NIST selects winner of Secure Hash Algorithm (SHA-3) Competition," vol. 2. *Press Release*, October, 2012.
[18] G. Bertoni, J. Daemen, M. Peeters and G. van Assche, "Sponge functions," in *Ecrypt Hash Workshop*, 2007. http://www.csrc.nist.gov/pki/HashWorkshop/Public_Comments/2007_May.html.
[19] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche and R. Van Keer, "CAESAR submission: Ketje v2," in *CAESAR First Round Submission*, March 2014. https://keccak.team/ketje.html.
[20] R. Kayser, "Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA-3) family," *Federal Register*, vol. 72, no. 212, pp. 62, 2007.
[21] Shu-jen Chang, Ray Perlner, William E. Burr, Meltem Sönmez Turan, John M. Kelsey, Souradyuti Paul and Lawrence E. Bassham, "Third-round report of the SHA-3 cryptographic hash algorithm competition," *NIST Interag. Rep.*, 7896*,* 2012.
[22] R. Fuksis, A. Kadikis and M. Greitans, "Biohashing and fusion of palmprint and palm vein biometric data," in *Proc. Int. Conf. on Hand-Based Biometrics*, Orlando, FL, USA, pp. 1–6, IEEE, 2011.
[23] A. Sardar, S. Umer, C. Pero and M. Nappi, "A novel cancellable FaceHashing technique based on non-invertible transformation with encryption and decryption template," *IEEE Access*, vol. 8, pp. 105263–105277, 2020.
[24] R. Belguechi, E. Cherrier and C. Rosenberger, "Texture based fingerprint biohashing: Attacks and robustness," in *Proc. 5th IAPR Int. Conf. on Biometrics (ICB)*, IEEE, New Dehli, India, pp. 196–201, 2012.
[25] R. Soliman, G. El Banby, A. Algarni, D. M. Elsheikhand, F. El-Samie *et al.,*"Double random phase encoding for cancellable face and iris recognition," *Applied. Optics*, vol. 57, pp. 10305–10316. 2018.
[26] R. Soliman, M. Amin and F. El-Samie, "A modified cancellable biometrics scheme using random projection," *Annals of Data Science*, vol. 6, pp. 223–236, 2018.
[27] A. Algarni, G. El Barnby, N. Soliman, F. El-Samie and A. Iliyasu, "Efficient implementation of homomorphic and fuzzy transforms in random-projection encryption frameworks for cancellable face recognition," *Electronics*, vol. 9, pp. 1046, 2020.
[28] E. B. Tarif, S. Wibowo, S. Wasimi and A. Tareef, "A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system," *Multimedia Tools Application*, vol. 77, no. 2, pp. 2485–2503, 2019.
[29] S. Sree and N. Radha, "Cancellable multimodal biometric user authentication system with fuzzy vault," in *Proc. of the 2016 Int. Conf. on Computer Communication and Informatics (ICCCI)*, Coilmbatore, India, pp. 1–6, 7–9, 2016.
[30] T. Dang, K. Truong, T. Le and H. Truong, "Cancellable fuzzy vault with periodic transformation for biometric template protection," *IET Biometrics*, vol. 5, pp. 229–235, 2016.
[31] P. Kumar, J. Joseph and K. Singh, "Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator," *Applied. Optics*, vol. 50, pp. 1805–1811, 2011.
[32] P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, pp. 767–769, 1995. [CrossRef].
[33] F. Dubost, G. Bortsova, H. Adams, A. Ikram, W. Niessen *et al.,*"GP-Unet: Lesion detection from weak labels with a 3D regression network," in *Proc, Int. Conf. on Medical Image Computing and Computer-Assisted Intervention*, Singapore, Springer, Cham, pp. 214–221, September 2017.