

Computational Wrist-Print Biometric Identification System Using Discrete Cosine Transform

Kennedy Chinedu Okafor[1,2(✉)] and Omowunmi Mary Longe[2]

[1] Mechatronics Engineering, Federal University of Technology, Owerri, Nigeria
kennedy.okafor@futo.edu.ng
[2] Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg, South Africa
omowunmil@uj.ac.za

Abstract. Biometric Wrist Authentication (BWA) is one of the best-known authentication schemes in many access control systems. The use of fingerprint biometrics as humans attempt to communicate with robots/machines, and their physical environments have inherent setbacks. However, various efforts have been proposed to fix the limitations. Most biometric efforts suffer from lack of computational derivatives and do not support optimal image compression. Motivated by these concerns, the goal of this paper is fivefold. First, we proposed BWA using Discrete Cosine Transform (DCT) to compress palm print images and develop Wrist-Print Biometric Identification System (WPBIS). Second, we developed a process model for DCT and characterized it for wrist templates considering both original and decoded images. Third, Bits per pixel (Bpp) and Compression ratio (Cr) for a wrist template/bioscript are used as metrics for evaluation. Fourth, after adopting various timestamps, we observed that the image template Bpp yielded 1.256 Bpp and compression of 63.26% based on DCT. Fifth, we showed a typical experimental scenario with a digital signal processor feeding images with DCT. Identification and verification of various wrist-prints (test-point samples) are equally carried out. From the results, WPBIS DCT offered higher image intensity compared with Wavelet transform.

Keywords: Computational science · Biometric access control · Digital signal processor · Human-Computer Interface (HCI)

1 Introduction

1.1 Background

Wearable technology has come a long way in the last two decades, thanks to significant advances in bio-physical signal processing and applications. In recent years, bioelectrical signals like the electrocardiogram (ECG), electromyogram (EMG), and electroencephalogram (EEG) have grown in popularity for Wrist-Human-Computer Interfacing (HCI) [1]. EMG devices, in particular, can detect electrical currents produced

© Springer Nature Switzerland AG 2021
O. Gervasi et al. (Eds.): ICCSA 2021, LNCS 12955, pp. 460–475, 2021.
https://doi.org/10.1007/978-3-030-87007-2_33

in muscles during movement [2] and use this data to control actuation systems. This is critical for engaging with wrist-powered devices such as Optitrack gloves [3], physical exercise equipment such as datalite [4], and controlling robotic devices or "bionic" praxes.

Wrists are being used in personal identification and authentication to provide accurate and reliable recognition. Wrist print authentication is a safe, effective, and private method of authentication. The rise of terrorism and other forms of illegal activities such as e-commerce fraud has piqued interest in more efficient and effective methods of determining a person's identity.

In mission-critical access control systems, biometric initiatives that will improve security ideology are always sought. Various integrations and algorithms have been proposed in the past works with a little contribution to wrist print-based biometric identification systems [5]. With rising demands for automatic personal identification, biometric authentication has gotten a lot of attention in the last decade [5]. Palmprint identification/recognition is among the most reliable biometric schemes available today [6].

To date, biometric is very useful in areas of forensic and commercial applications such as the banking sector, voting systems, and other image recognition systems. These leverage schemes like biometric encryption [7], bio-cryptography [8], fuzzy vaults [9]. Yet no work in the literature has dealt with Biometric Wrist Authentication (BWA) based on Discrete Cosine Transform (DCT) for image compression.

In general, a biometric is data about a person that can be used to establish that person's identity. DNA, ear form, ears, fingerprints, hand geometry, irises, keystroke pattern on a keyboard, signature, and voice are some of the biometrics currently being researched [10]. While each biometric has established merits and demerits, all biometrics must have the following four characteristics including accuracy, universality, uniqueness-, and invariance [11]. Some biometrics (faces, speech, signature, keystrokes, and ears) can be obtained without a person's knowledge, while others (fingerprints and hand geometry) require a person's cooperation, and others (irises and DNA) have yet to be determined [12]. This distinction is critical for a variety of applications. Remote surveillance and monitoring (border crossings and airport security) are potential applications for non-intrusive biometrics, while access control and checking electronic commerce transactions are potential applications for cooperative biometrics [13]. Faces, fingerprints, irises, and ears are all image-based, and implementing them necessitates image processing, pattern recognition, and computer vision techniques [12]. Hand geometry, keystrokes, signatures, and expression are all part of the signal processing and pattern matching/recognition domains. Multiple biometrics have been combinedly used in recent efforts [14, 15]. The essence of this work is to exploit cooperative biometrics with a shift to wrist prints.

1.2 Motivation

There are several identified constraints regarding the operability of the fingerprint method of identification. First, the inability for people with some forms of physiological defects, (as regards the fingers), to effectively use such systems. Some of these physiological defects could be congenital deformation of the fingers, loss of all fingers due to an accident, and severe damage to the fingers' skin due to leprosy. Second, the fingertips are used for virtually all daily activities and therefore are exposed to a greater number of risks, unlike the wrists.

Third, another serious drawback is the secretion of excess oil and/or sweat on the hand surface which inhibits adequate fingerprint capture by the sensor devices. Fourth, medical experts have raised serious concerns on the possibility of contracting a wide range of infections through the use of public fingerprint identification systems. Also, investigations have shown that a typical public fingerprint identification system is as dirty as a typical public toilet.

In this paper, we built WPBIS which leverages DCT for image compression. This can serve a wider category of people irrespective of the condition of their fingers. This eliminates the problems associated with oily/sweaty hands. In addition, due to the physiology of the wrists which makes it more hygienic than the fingers; it would tackle the numerous health concerns people have with using a public-deployed fingerprint-based biometric identification system. The sensor array captures an analog image of the wrist placed on the wrist-print module and sends this image to an ADC that converts this analog image into a digital equivalent code. This then represents the numerical characterization of the wrist-print features. Sample-data code from the wrist-print module is transmitted to the DSP controller for matching against several of such codes previously enrolled and stored in the memory. When there is a mismatch detected by the software agent in the DSP controller, an indication signal notification is generated while denying access and vice versa. Hence, the art of computational science is very apt for DCT.

1.3 Contribution and Article Organization

This paper develops WPBIS using the DCT algorithms while deploying it in an access control system. The specific sub-objectives of this research include:

1. To develop a DCT model that satisfies the requirement of image compression for the identification and verification contexts
2. To develop a WPBIS process model using Bit per pixel and Compression ratio as key evaluation metrics for the data acquisition system.
3. To develop conceptual models while formulating representative lock diagrams for the enrollment and identification procedures in WPBIS
4. To implement the WPBIS DCT algorithm using a software agent in a DSP controller for access control.

2 Literature Review

This section focused on biometric systems, approaches, and modes of operations while presenting gaps. Recall that [1] discussed two general approaches to verify or identify individuals:

- Once-and-for-all: the person is confirmed once and for all time. Until access to the system is granted, specific requirements may be defined to ensure correct and reliable access. However, since access is never re-verified, unauthorized use by someone other than the approved user is a possibility.
- On-going: verification/identification is repeated regularly. This eliminates the possibility of unauthorized use, but it may reduce verification accuracy by necessitating repeated repetition of verification exercises. In Sect. 2.1, related works are discussed.

2.1 Biometric Systems

This is referred to as an image-pattern identification/recognition model that extracts information from biophysical signals to identify individuals or groups [15]. Biometric systems such as Fingerprint [16], facial imaging [17], speech-notes [18], iris-identity [19], ECG [20, 21], EMG [22], and EEG) [23] are very common in most deployments. Each has a unique mix of weakness, ease of use, obtrusiveness, and complexity. There are two modes of operation in such biometric systems include verification: and identification [24]. In terms of authentication or image verification, different schemes have been explored to date. User scanning with complex image-data processing was required for biometric entities in [17, 18], and [19]. These, on the other hand, are not bio-signals in the traditional sense. Two two-factor authentication and multi-channel EMG signals for hand-trajectory are still popular schemes for verifying a person's identity. In some cases, keystroke dynamics when typing a password, as well as related EMG signaling are explored. Face, fingerprints, hand gestures, and speech are widely used for identification in literature. ECG analysis is widely used in bio-signals, but there has been little research on Wrist-Print Biometric Identification System for individual recognition [2]. Existing efforts appear to focus on one-time biometric identification/ verification with constrained controlled signals for image extraction. However, the use of biometric wrist authentication/identification schemes in a continuous image capturing system with optimal compression ratio is novel in access control systems.

2.2 Why Discrete Cosine Transform (DCT) for Image Compression

Existing works have not fully explored the potential of image compression using the DCT, especially in the context of a wrist print-based biometric identification system. DCT is a signal-to-elementary-frequency-component conversion technique that is commonly used in image compression. The major benefits include:

1. The existence of a well-defined pattern of data points summation at various frequencies, which is ideal for image compression.
2. High efficiency for image compression since fewer functions are required to estimate wrist signals.
3. Approximately twice as long as DFTs logic operation on real-datasets with even symmetry only.

3 System Formulation and Design Architecture

In this section, the computational perspectives on WPBIS are briefly established. Given an access control scenario case K, it is expected that writs samples $\{f_0{}^1\ (x), f_0{}^2\ (x)\ldots, f_0{}^{\mathrm{T}}\ (x)\}$ extracted from a base Client BC during enrollment, and verification, Assuming DCT $c_0{}^T(x)$ is derived by getting the Fourier to transform of $f_0{}^{\mathrm{T}}\ (x)$ i.e. $f_0{}^{\mathrm{T}}\ (u)$ and the complex conjugate of $H(\mathrm{u})$ which is the output pattern. $c_0{}^{\mathrm{T}}\ (x)$ should be bound with an N-bit randomly generated key with a linking algorithm and stored in a lookup table K. The authentication scheme can combine the wrist biometric images viz: $\{f_1{}^1\ (x), f_1{}^2\ (x)\ldots, f_1{}^{\mathrm{T}}\ (x)\}$ with $H_{stored(u)}$ to produce an output pattern $c_1{}^{\mathrm{T}}\ (x)$ with the aid of the lookup table L to retrieve N-bits as shown in Fig. 1. Figure 2 shows the wrist palm biometric key retrieval process. The major difficulty in designing this model lies in the process of fusing wrist biometrics with a transparent sensor. In Wrist palm biometrics, no two wrist samples collected from the same base client are the same. In this study, the steps involved in the enrollment and verification are explained in Sect. 3.1.

3.1 System Enrollment and Verification Algorithms

Figure 1 briefly describes the sequence of steps in the enrollment and verification which the WPBIS explores. The enrollment algorithm is broken into three stages; the processing of images, key linking, and identification code creation. The verification algorithm also has three stages namely; image processing, key retrieval, and key validation. The enrollment procedure's goal is to build the user's Wrist Bioscrypt by linking an arbitrary N-bit key to the user's wrist print. A collection of valid Action Client wrist images, a randomly generated phase-only array, $R(u)$, and an N-bit cryptographic key, k_0, are needed for the enrollment process, as shown in Fig. 1. A random number generator is used to generate R(u) (RNG). The key, k_0, could be a previously produced key that is fed into

the Biometric Encryption algorithm, or it could be generated by the RNG. The random phase array, R(u), and the key, k_0, are fully independent of the wrist palm biometric images. This enrollment stage aims to create an output pattern, $c_0(x)$, that will be passed on to stage **En-2**, as well as the stored filter feature, Restored (u). T wrist palm photos, $T = n$, $n > 3$, are obtained from the base using a certain number of times. The images are then subjected to DCT Fourier transforms to convolve their 2D images. After that, the output pattern, $c_0(x)$, is evaluated.

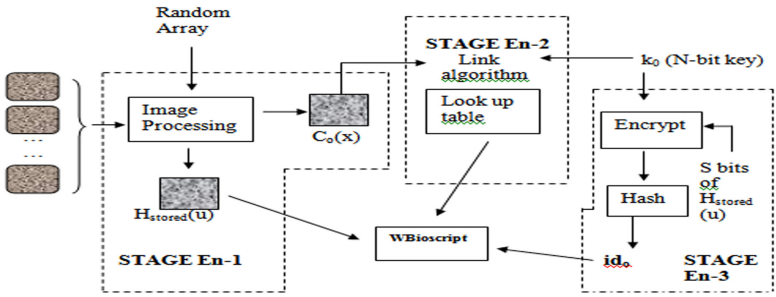


Fig. 1. Wrist palm biometric encryption enrollment process.

The relation algorithm is in charge of connecting the output pattern $c_0(x)$ to an N-bit key k_0. A lookup table will be generated and stored in the wrist Bioscrypt during the linking process for use in key retrieval during verification. The fact that the output pattern obtained during the registration, $c_0(x)$, and the pattern obtained during verification, $c_1(x)$, would differ to some degree is a significant consideration for this method. These variations are attributable to changes in the physical content of the base user's wrist and its location at the image capture device's point of capture, among other things. To account for these variations, some redundancy in the enrollment process is needed. The algorithm I describes the enrollment process.

Algorithm I. DCT Enrollement Process

Inputs: Image templates_Control-CallSchedule for image to *N+1*
History of WPBIS resources, Provisioning and transactional workflow
$\prod \beta 1$ & $\prod \beta 2$// initialValue constant & trendPosteriorValue
pastValueForSubsytems, pastValueForSubsytems

Output: DCT Optimal Scale+ _DES

int i←0;

While i <DCT_monitorCallSchedule d **do**

Begin ( )

En-1: Image Processing on the Wrist

Build two output arrays (product of the two) by combining a set of input wrist print images from the base client (wrist training) with a random (phase) array: *H*stored(u) and $c_0(x)$.

En-2: DCT Wrist Key Connecting

Using the connect algorithm, link a DCT key, k_0, to a pattern, $c_0(x)$.

En-3: Creating a unique identifier

Create a unique identification code, id_0, using the key, k_0.

i ++;

end while

Return

Figure 2 shows the identification process for Wrist Biometric Encryption based on DCT. The idea in Algorithm II is to create a new identification code, id_1, and compare it to id_0 to validate k_1. The verification procedure aims to retrieve the *N*-bit key writ picture for a legitimate user successfully.

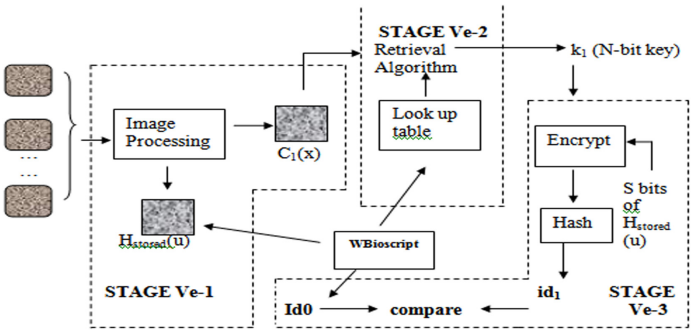


Fig. 2. Identification process for wrist biometric encryption

To retrieve and verify the validity of an N-bit key, a collection of wrist biometric images is obtained from the Action Client and combined with *H*stored(u), the lookup table, and id_0., from Bioscrypt. This key will be passed on to the final output stage if it is found to be right. Wrist print images *T* are obtained from the base client, just as they were during registration. The images are subjected to DCT Fourier transformations, and the results are saved. The output pattern, $c_1(x)$, is evaluated using *H*stored(u) retrieved from

the wrist Bioscrypt. The cryptographic key will be retrieved using the $c_1(x)$ authentication pattern. In this case, the similarity of $c_1(x)$ and $c_0(x)$ performance patterns have an important impact on *t.* Algorithm II simplifies the procedure.

Algorithm II. DCT Key retrival and Validation Process

Inputs: Image Bioscrypt _Control-featureSchedule for image to $N+1$; id_1, id_0
History of WPBIS resources, Provisioning and transactional workflow
$\prod \beta 1$ & $\prod \beta 2$// initialValue constant & trendPosteriorValue
pastValueForSubsytems, pastValueForSubsytems

Output: DCT Optimal Scale+ _DES

int $i \leftarrow 0$;

While $i <$ DCT_monitorCallScheduled **do**

Ve-1: Image Processing,

To create an output pattern, c_1, combine Hstored(u) from the Wrist Bioscrypt with a new set of input wrist images from the base client (also trained) (x).

Ve-2: Key Retrieval

Using the retrieval algorithm, extract a key, k_1, from $c_1(x)$.

Ve-3: Key Validation

The retrieval algorithm is in charge of extracting a key from the c_0 verification output pattern (x).

To retrieve an N-bit key that was connected with $c_0(x)$ using the connection algorithm, the steps outlined below are valid.

Start now ( )

1. Take the central part of $c_1(x)$ and extract it (a $N*N$ matrix).
2. To construct a verification prototype, concatenate the actual and imaginary bits, as in **En-2** enrollment level. Binarize each value to construct a binarized verification template, as in **En-2** (the equivalent of the binarized enrollment template).
3. Using the lookup table, extract the key's necessary constituent bits from the binarized verification template. Define k_1 as a vector with N elements. Sum the L bits of the binarized verification template whose indices are defined by the nth column of the lookup table for the nth element of k_1. If the number of these bits is greater than $L/2$, the nth element of k_1 is set to 1, otherwise, it is set to 0.
4. Check the validity of the key you just got. The verification stage **Ve-3** process is defined in the following section.
5. Release k_1 into the device if it is discovered to be the correct key.
6. Return to $c_1(x)$ and remove the center portion of $c_1(x)$ t if k_1 is found to be wrong.
7. Repeat steps 2 to 5 of the retrieval algorithm for all portions of $c_1(x)$ that are one pixel offset from the center, then two-pixel offsets, and so on, up to approximately sixteen-pixel offsets.
8. Stop the algorithm and release k_1 if the key retrieved is found to be correct at any point.
9. Release an "identification failed" message if the key is found to be incorrect for all pixel offsets.

i ++;

end while

Return

The key retrieval construct in step 5 is needed to account for relative translations of the Action Client's input fingerprints at both biometric enrollment and its controlled verification. The legitimate user is granted access to the door security after the identification stage, which involves the key retrieval algorithm is completed. After the base client

writs are captured for verification, this wrist Bioscript is automatically erased from the DSP controller memory, so even if the base client presents for the second time, this will not be recognized as a legitimate base client. The WPBIS ensures that only one person has access to information and that vulnerabilities are kept to a bare minimum. Wrist palm biometric key binding and Wrist palm biometric key retrieval are the core of the WPBIS design.

3.2 DCT Transform and Compression

DCT algorithm is applied in palmprint image compression to develop WPBIS. To maximize the benefits, this was optimized for door access control in a security-sensitive domain. A process model for DCT is characterized as a wrist template for both the original image and decoded image. Figure 3 shows the WPBIS principles behind image compression:

i. Redundancy elimination, which helps to eliminate repetition from the signal source.
ii. Irrelevancy reduction—this omits portions of the signal that the signal receiver would not hear.
iii. Layered pattern recognition and good protection.

As shown in Fig. 3, there are three major sub-routines introduced when considering WPBIS namely Intelligent (i.e. identification analysis), serial communication, and control sub-routines. A DSP-based agent was used to create interrupt capability for the entire BWAS. Hence, it can suspend whatever action is executing whenever events of higher priority occur and attend to that event after which it goes back to what it was doing. It runs at the external clock speed of 24 MHz. With this, any identification can be analyzed within milliseconds. The structure of WPBIS is fully powered by intelligent computational algorithms controlling the wrist biometric end-to-end processes. The inputs to the system are captured with wrist prints from the sensors. Similarly, feedback is obtained from output actuators. The output devices include the buzzer alarm; dashboard display, drive mechanism, and electric motor. The software implementation is divided into three levels: the intelligent identification analysis sub-routine, serial communication sub-routine, and access control sub-routine in the WPBIS-DSP running DCT.

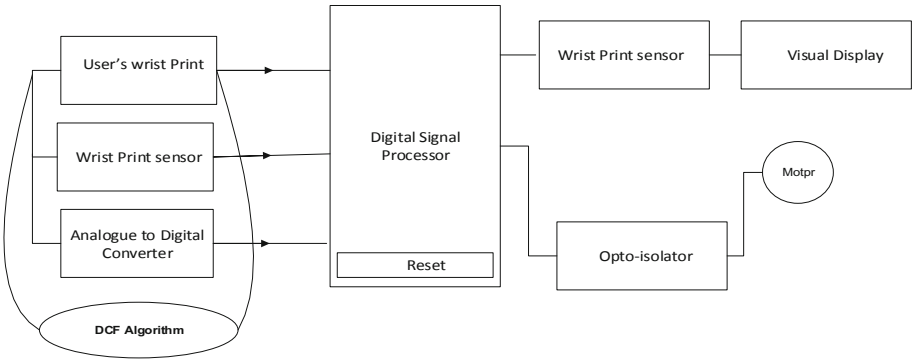


Fig. 3. Wrist-print biometric identification system (WPBIS)

3.3 WPBIS Model Integration

Figure 4 depicts that the Palm print WPBIS is made up of four subsystems, which are scanner, pre-processing, feature extraction, and matcher. The palm print scanner in the device collects photographs. Pre-processing involves setting up a coordinate scheme to align the palm print images and segmenting a portion of the image for feature extraction. Feature extraction is the method of extracting useful features from a palmprint that has already been processed. The authentic imagery is evaluated by the Matcher software. Image acquisition, pre-processing, feature extraction, and matching are the four stages in the palm print recognition scheme.

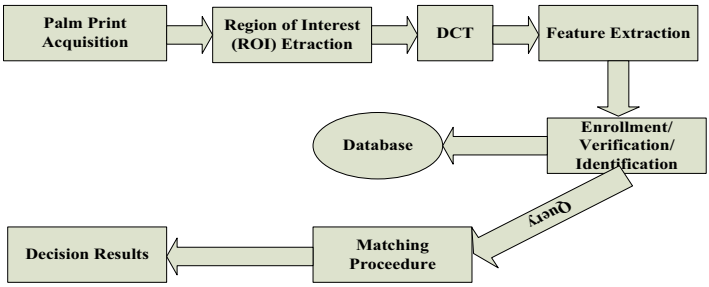


Fig. 4. General block diagram of WPBIS

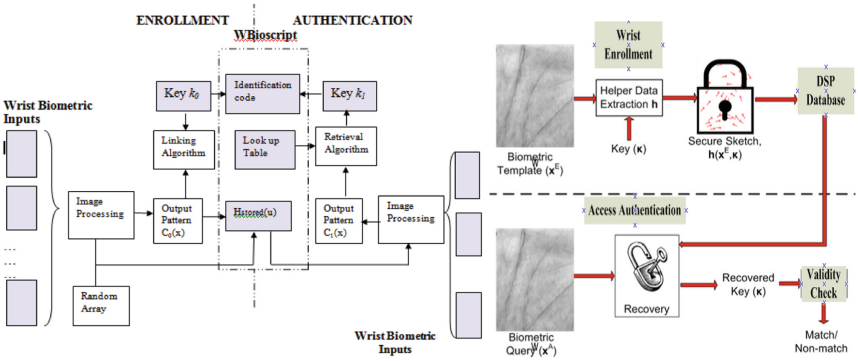
Figure 4 depicts the system diagram of the palm-print identification device. The major elements of the WPBIS are divided into four sub-sections:

i. Image capturing
During this process, various types of digital cameras are used to capture images of palm prints. The accuracy of the acquired image can be blurred or noisy, which reduces the image's quality and directly affects the output rate of the palm print recognition system.
ii. Pre-processing
Pre-processing is applied to the image after the data or image of the palm print has been captured. When noise is present in a captured image, it can be removed using filters during the processing step.
iii. Extraction of Characteristics
Pre-processing follows feature extraction. Principal lines, orientation area, minutiae, density map, texture, singular points, and other palm features are extracted during the feature extraction process.
iv. Compatibility
The feature extraction process is followed by the matching phase. The degree of similarity between the recognition template and the master template is determined by feature matching. This is done in a variety of ways. As shown in Fig. 4, individual input is matched with templates stored in the database. The system is optimized for efficient access control application integration addresses interface scalability, efficient control behavior, and in-depth security.

For efficiency in image compression in the access control template storage, an efficient interconnection of WPBIS must provide higher scalability and flexibility at large. The key goals considered in the WPBIS model, viz: maintain high throughput, low latency, rapid convergence, and scalable networks with low administrative overhead. If the input image is captured by a low-cost sensor, the DCT device performs a preprocessing procedure to reduce the blur effect that is common in the input image. Let's discuss the system characterization regarding the linking and digital key retrieval in Fig. 5a and 5b.

4 System Characterization

In this section, a brief description of the WPBIS algorithms is given. The WPBIS algorithm's goal is to use a biometric image compression algorithm on the DSP controller to give an interface for linking and retrieving digital image keys. This wrist-biometric image depicts a 2D palmprint image that was captured as a device input component. The digital key that results is then used as a binding key as shown in Fig. 5a and 5b. It describes the WPBIS security model designed to allow an image from an enrolled base client (that differs significantly from the original) to decode the full correct image template stored in the DSP. Also, an image from another individual must be distinct from others, even if it is just slightly different from the enrolled image.



a) Linking algorithm b) Retrieval digital key

Fig. 5. Enrollment and verification in wrist biometrically encrypted system

4.1 Modeling Assumptions

The WPBIS was presumed to fit into use case door access control systems (security sense only) for this study, as shown in Fig. 5. During the enrollment exercise, we conclude that several wrist samples F_0 are obtained and encrypted. The wrist samples obtained from base clients during the enrollment or registration process are processed and then bound with randomly generated strings of number N_k is a Biometric Key Binding (BKB) algorithm in DCT so that the randomly generated string N_k can be retrieved on the representation of the same wrist sample F_1 of which F_1F_0'. The interface connection used between the various door access point modules *pm1, pm2,…., pmn* in this protection and privacy dependent algorithm for the WPBIS is mapped to the DSP-based controller

where encrypted writs templates E_n is processed. During and after the access control processes, this DCT connection model provides a stable mapping mechanism between the various endpoints in the model.

For wrist biometric input signals in matrix form, an image compression model using the discrete cosine transform (DCT) was developed and implemented. The DCT is a technique for translating signals into elementary frequency components. This is required for biometric image footprint data to have enough storage space, a wide transmission bandwidth, and a longer transmission time. By spinning the frequencies of the different images before capturing them, a high level of encryption against any hacking attempt is ensured. This is to ensure that anyone who does not have the necessary knowledge of the number of spectra and their distributions in the spectral plane will be unable to decrypt this data. The shape of the spectra obtained with the DCT is very distinctive and easily observable even when the image spectrum is not rotated. This is very vital at the feature extraction and verification stages.

Following the application of the DCT method and the transmission of compressed and encrypted data, the images are extracted after reception by following the key steps of the transmission method, but in the opposite direction. To obtain the original images, the obtained image is multiplied by the inverse of random mask or the inverse wrist print spectrum considering the legitimate individual. Afterwards, numerous rotations is then activated in the opposite direction. Finally, the DCT is inversed as appropriate. These processes are used to drive the input sensor capture of the WPBIS in Fig. 5a and 5b. WPBIS Biosensor Integration.

In this Section, HyperTerminal implementation for Algorithm III and IV is presented. Algorithm III is used to connect the Biosensor to the terminal process for system setup and initialization.

Algorithm III. Biometric Sensor Connect to HyperTerminal Process

Inputs: Biometric sensor module
History of biometric sensor module and transactional workflow
$\prod \beta 1$ & $\prod \beta 2$// initial parameters
Output: DCT Optimal Scale+ _DES
int i←0;
While i <DCT_monitorCallSchedule d **do**
Begin ( )
1. Connect the biometric sensor module to smart agent.
2. Call hyper terminal in windows ( );
3. Call project name ( );
4. Select modem from pop-up ( )
5. Select the com port to which the biometric sensor is attached from the "connect using" drop-down menu.
6. Set the Baud rate to 9600.
None = parity
Flow control = Hardware Data bits = 8 Stop bits = 1
Activate ( );
8. Set the module's serial speed to automatic.
9. Call display dashboard ()
End procedure ( )
i ++;
end while
Return

Now, from Algorithm IV, the DSP controller was optimized based on the following desirable features: multi-level programming, fast response time, 32 input/output ports availability, serial communication capability, substantial memory space (4k), and low power consumption.

Algorithm IV. Biometric Sensor Port Connection with AT Command

Inputs: Biometric sensor module
History of biometric sensor module and transactional workflow
$\prod \beta 1$ & $\prod \beta 2$// initial parameters

Output: DCT Optimal Scale+ _DES

int i←0;

While i <DCT_monitorCallSchedule d **do**

Begin ( )

Begin ( )

1. Connect the serial port of the controller to that of the biometric sensor module.
2. Send the command "AT' to the sensor module.
3. Receive 'AT OK' from the sensor module.
4. Send 'AT+CMGF=1' to the sensor module.
5. Receive "AT+CMGF=1' OK' from the sensor module.
6. Send 'AT+CMGF=" digital code of a user"
7. Receive 'AT+CMGF=" digital code of a user",>
8. Send the message
9. Send the ASCII value of control *z*
10. Receive + CMGS: memory storage of the user message sent
11. Set up controller emulator
12. Write the equivalent PDL to send/receive to and from the sensor module
13. Display the result on the display dashboard.

i ++;

end while

Return

5 Experimental Study

In this section, MATLAB Simulink [25] image vision was used to realize the validation of the WPBIS process model (image compression). Three main components are introduced. First, functional scanner module is used to carry out enrollment and verification in the system. It has a visual display unit (VDU), which enables users to interact with the door mechanism. This is similar to a Wrist-reader/module used in the acquisition of wrist palm images from end-users for authentication to access control systems. Second, the VDU dashboard provides the end-user with a simple image status of enrollment or verification transactions. Appropriate identity mapping is communicated by the VDU dashboard for listing invalid user/accessor legitimate access. Third, the stable DSP emulator processor is used for processing the DCT and is protected from scores manipulations. By applying Algorithms I to IV, the outcome is the biometric sensor module and the DSP. The experimental system with DCT algorithms sequentially sends messages to the biometric sensor module using a low latency DSP Microcontroller. The biometric sensor interface to the DSP was achieved in the WPBIS. Its output interface comprises: interface display

dashboard to the controller, interface of the buzzer alarm to the controller, and interface of the motor to the controller.

In the process model for less complex writs template, a DSP block sends 8-by-8 submatrices of a wrist image frame to the subsystem for processing. Within this subsystem, the model quantizes each 8-by-8 sub-matrix after applying the DCT. To retrieve the original data, the model uses inverse quantization and inverse DCT in the decoder subsystem. The signal preprocessing module, an optical filter module, and a pattern recognition module are all integrated into the DSP. For the discrimination of eight hand movements, the online DSP controller can provide an 87.5% correct score. For the wrist bloc processing DSP model in WPBIS, this is validated using the Bpp test and compression ratio index for the sampled inputs. Both the original wrist image display and the optimized image display were obtained. As shown in Fig. 6a, the DCT Throughput/Compression ratio for the Wrist Image display is estimated at 93.55% which is very significant. Also, with the application of various timestamps, the sample image template Bpp yielded 1.256 Bpp (minimum) and compression of 63.26% based on the DCT as shown in Fig. 6b. The Wrist DSP model yielded 66.70% and 33.30% wrist image intensities respectively for the proposed DCT and wavelet scheme. DCT uses high throughput compression hits for massive data extraction from bioscript multispectral images efficiently. The main trade-off is observed in the computational system resources needed for DCT processing especially for complex image pixels.

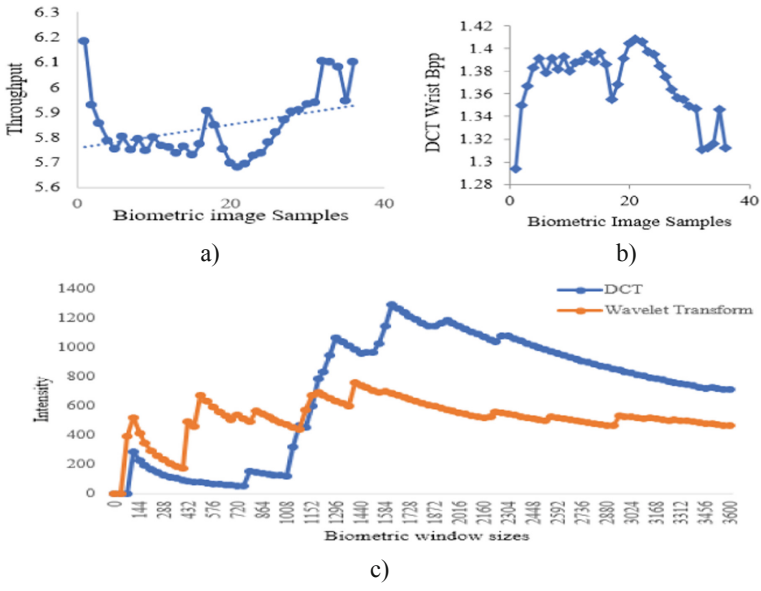


Fig. 6. a) DCT Throughput CR b) DCT Wrist_Bpp test extract c) DCT vs Wavelet intensities.

6 Conclusion

In this paper, Biometric Wrist Authentication (BWA) based on DCT for palmprint image compression is presented as an optimal scheme for image compression. The WPBIS-DCT is an efficient biometric technique considering two main areas: wrist-image extraction and line features from a 2/3D palmprint binary image. The system extracts orientation features and performs two distinct operations. Firstly, the encryption process changes the compressed data in such a way that it is unreadable to an unauthorized agent. Secondly, image compression is achieved involving the reduction of data sizes to be transmitted by removing redundant data. These two procedures are computed using DCT. This non-destructive spectral fusion allows for image compression and encryption concurrently. In summary, the proposed BWA leveraging DCT is useful in biometric access control systems and this has been applied in a DSP block for palmprint image compression. Results of the process model show that the sample (image template) Bpp yield 1.256 Bpp (minimum) and a Cr of 63.26% based on the DCT. Also, the DCT offered more acceptable palmprint image security and can carry more pixels than the wavelet scheme in typical deployment scenarios. Future work would deliver the optimal hardware prototype and machine interfacing with Field programmable gate arrays (FPGAs).

References

1. Raurale, S.A., McAllister, J., Rincón, J.M.D.: EMG biometric systems based on different wrist-hand movements. IEEE Access **9**, 12256–12266 (2021)
2. Kakei, S.: Muscle and movement representations in the primary motor cortex. Science **285**(5436), 2136–2139 (1999)
3. Wearable Manus Gloves, November 2020. https://manus-vr.com/mocap-gloves
4. DataLite Device, November 2020. https://www.biometricsltd.com/datalite
5. Fan, W., Wang, K., Cayre, F., Xiong, Z.: Median filtered image quality enhancement and anti-forensics via variational deconvolution. IEEE Trans. Inf. Forensics Secur. **10**(5), 1076–1091 (2015)
6. Fei, L., Zhang, B., Xu, Y., Tian, C., Rida, I., Zhang, D.: Jointly heterogeneous palmprint discriminant feature learning. IEEE Trans. Neural Netw. Learn. Syst. (2021). Early Access.
7. Bui, F.M., Martin, K., Lu, H., Plataniotis, K.N., Hatzinakos, D.: Fuzzy key binding strategies based on quantization index modulation (QIM) for biometric encryption (BE) applications. IEEE Trans. Inf. Forensics Secur. **5**(1), 118–132 (2010). Early Access
8. Fadil, I., Barmawi, A.M.: Improving bio-cryptography authentication protocol. In: 2015 9th International Conference on Telecommunication Systems Services and Applications (TSSA), pp. 1–6 (2015)
9. Lai, Y.-L., Hwang, J.Y., Jin, Z., Kim, S., Cho, S., Teoh, A.B.J.: Secure secret sharing enabled b-band mini vaults bio-cryptosystem for vectorial biometrics. IEEE Trans. Dependable Secure Comput. **18**(1), 58–71 (2021)
10. Drozdowski, P., Rathgeb, C., Dantcheva, A., Damer, N., Busch, C.: Demographic bias in biometrics: a survey on an emerging challenge. IEEE Transactions on Technology and Society **1**(2), 89–103 (2020)
11. Drozdowski, P., Rathgeb, C., Dantcheva, A., Damer, N., Busch, C.: Demographic bias in biometrics: a survey on an emerging challenge. IEEE Trans. Technol. Soc. **1**(2), 89–103 (2020)

12. Weaver, A.C.: Biometric authentication. Computer **39**(2), 96–97 (2006)
13. Pawar, N., Ingole, D.T., Ingole, M.D.: Normalization method for misaligned face samples in non-cooperative biometrics. In: 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), pp. 330–333 (2017)
14. Luo, Z., Li, J., Zhu, Y.: A deep feature fusion network based on multiple attention mechanisms for joint iris-periocular biometric recognition. IEEE Signal Process. Lett. **28**, 1060–1064 (2021)
15. Edwards, T., Hossain, M.S.: Effectiveness of deep learning on serial fusion based biometric systems. IEEE Trans. Artif. Intell. **2**(1), 28–41 (2021)
16. Zhou, C., Liu, J., Sheng, M., Zheng, Y., Li, J.: Exploiting fingerprint correlation for fingerprint-based indoor localization: a deep learning based approach. IEEE Trans. Vehicul. Technol. (2021). Early Access
17. Yuan, C., Jiao, S., Sun, X., Wu, Q.J.: MFFFLD: a multi-modal feature fusion based fingerprint liveness detection. IEEE Trans. Cogn. Dev. Syst. (2021). Early Access
18. Hsu, J.H., Su, M.H., Wu, C.H., Chen, Y.H.: Speech emotion recognition considering nonverbal vocalization in affective conversations. In: IEEE/ACM Transactions on Audio, Speech, and Language Processing (2021). Early Access
19. Wang, C., Muhammad, J., Wang, Y., He, Z., Sun, Z.: Towards complete and accurate iris segmentation using deep multi-task attention network for non-cooperative iris recognition. IEEE Trans. Info. Forensics Sec. **15**, 2944–2959 (2020)
20. Shi, H., Liu, R., Chen, C., Shu, M., Wang, Y.: ECG baseline estimation and denoising with group sparse regularization. IEEE Access **9** 23595–23607 (2021)
21. Zhang, J., et al.: MLBF-Net: a multi-lead-branch fusion network for multi-class arrhythmia classification using 12-Lead ECG. IEEE J. Trans. Eng. Health Med. **9**, 1–11 (2021). Art no. 1900211
22. Stanley, P.K., et al.: Electromyogram based bot-assistive device for paralyzed people. In: Proceedings IEEE ESCI, pp. 623–626 (2021)
23. Ahmed, M.A., Deyu, Q., Alshemmary, E.N.: Electroencephalogram signal eye blink rejection improvement based on the hybrid stone blind origin separation and particle swarm optimization technique. IEEE Access **8**, 105671–105680 (2020)
24. Shahreza, H.O., Marcel, S.: Towards protecting and enhancing vascular biometric recognition methods via biohashing and deep neural networks. IEEE Trans. Biometr. Behav. Identity Sci. (2021). Early Access
25. Behrens, A., et al.: MATLAB Meets LEGO mindstorms—a freshman introduction course into practical engineering. IEEE Trans. Educ. **53**(2), 306–317 (2010)