

# Generating a Cancellable Fingerprint using Matrices Operations and Its Fingerprint Processing Requirements

Riki Mukhaiyar<sup>1</sup>

<sup>1</sup> ISPAI Research Group, Universitas Negeri Padang, Padang, Indonesia

Correspondence: Riki Mukhaiyar. E-mail: riki.mukhaiyar@yahoo.co.uk

Received: February 13, 2018

Accepted: April 19, 2018

Online Published: May 28, 2018

doi:10.5539/ass.v14n6p1

URL: <https://doi.org/10.5539/ass.v14n6p1>

## Abstract

Cancellable fingerprint uses transformed or intentionally distorted biometric data instead of the original biometric data for identifying person. When a set of biometric data is found to be compromised, they can be discarded, and a new set of biometric data can be regenerated. This initial principal is identical with a non-invertible concept in matrices operations. In matrix domain, a matrix cannot be transformed into its original form if it meets several requirements such as non-square form matrix, consist of one zero row/column, and no row as multiple of another row. These conditions can be acquired by implementing three matrix operations using Kronecker Product (KP) operation, Elementary Row Operation (ERO), and Inverse Matrix (INV) operation. KP is useful to produce a non-square form matrix, to enlarge the size of matrix, to distinguish and disguise the element of matrix by multiplying each of elements of the matrix with a particular matrix. ERO can be defined as multiplication and addition force to matrix rows. INV is utilized to transform one matrix to another one with a different element or form as a reciprocal matrix of the original. These three matrix operations should be implemented together in generating the cancellable feature to robust image. So, if once three conditions are met by imposter, it is impossible to find the original image of the fingerprint. The initial aim of these operations is to camouflage the original look of the fingerprint feature into an abstract-look to deceive an un-authorized personal using the fingerprint irresponsibly. In this research, several fingerprint processing steps such as fingerprint pre-processing, core-point identification, region of interest, minutiae extration, etc; are determined to improve the quality of the cancellable feature. Three different databases i.e. FVC2002, FVC2004, and BRC are utilized in this work.

**Keywords:** cancellable biometric, fingerprint processing steps, elementary row operation, Kronecker product operation, inverse matrix operation

## 1. Introduction

Cancellable biometrics has been a challenging but essential approach to protect the privacy of biometric. The biometric trait of a person cannot be easily replaced. Once a biometrics is compromised, it would mean the loss of a user's identity forever (Schneir, 1999. p. 1). The proper cancellable biometric system has to have these criterion; distinctive, reusable, unidirectional transformation, and performance.

Cancellable biometrics offers a solution for preserving user privacy since the user's true biometric is never reveal in the authentication process. It ensures that template protection is achieved at the feature level with the assistance of the auxiliary data/non-invertible transforms. On the other hand, cancellable biometrics has certain limitations that need to be taken into account. For non-invertible transforms, non-invertible enhances the security of the template space by employing a transformation process to reset the order or position of the feature set. However, this weakens the discriminatory power (performance) of the transformed features due to the enlargement of intra-class variation in the biometrics. In this content, if performance is the main concern in the design of a biometric system, then the system is expected to be lacking in randomness are required for the design of a secure and unpredictable template space. Hence, it becomes a challenge to design a non-invertible function that satisfies both performance and non-invertible requirements.

These above basic concepts are similar with the idea of inverse matrix and elementary row operation in matrices domain. Biometric image as a digital image definitely can be processed in matrices domain. This means the acquired biometric image can undergo a series of matrices operations such as inverse matrix (INV) operation, elementary row operation (ERO), and Kronecker product (KP) operation. In matrices domain, these three

operations have their own objectives i.e. INV for inverting matrix elements, ERO for changing rows or columns, and KP for enlarging size of the matrix. The combination of these operations can produce a non-invertible matrix.

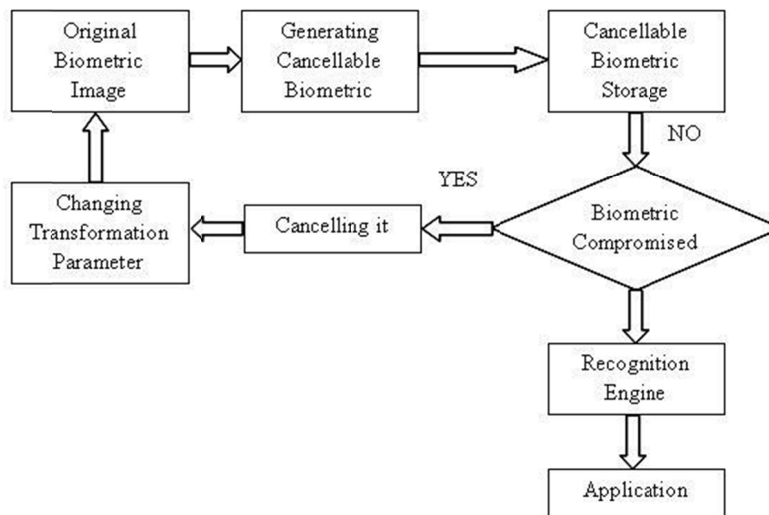


Figure 1. Re-Issuing Procedure

This research aims to develop a cancellable template for fingerprint feature, such as minutiae, based on the similarity between a non-inverted needed of the fingerprint template in cancellable system and a non-inversed matrix in matrices operations. A template can be categorized as a cancellable template when it is non-invertible to the original image. By similar token, matrices cannot be inverted when the following three conditions are met. Firstly, there is at least one zero row. Next, there is a row that is a multiple of another row. Finally, the matrix form is not a square.

The implementation of these matrices operations into a fingerprint image requires several conditions such as clarity and square form of the input image. Working in matrix domain means that every element of matrix/image should be determined to avoid miscalculation in process. Value of each element has to be “true” as a representative of the original condition of the image/matrix. True means that the amount of each element is free from unqualified thing as known as noise. Therefore, in this research, several fingerprint processing steps are demanded to support the system to obtain a fingerprint input with better quality to ensure that no feature information of the fingerprint is missed.

## 2. Related Works

The security requirement in authentication system based on biometric technology has to be the benchmark mainstay of the system as its characteristic will be permanently associated with the eligible user and cannot be cancelled or withdrawn whenever it is used inappropriately. Since someone’s biometric characteristic cannot be easily replaced, the impost data will be lost. As the result, there is a possibility that the user will lose all the access to the application using those biometric data. In order to overcome this possibility, the susceptibility of biometric system needs to be systematically identified and recognized (Bolle, Connell, & Ratha, 2002. pp. 2727-2738; Schneier, 1999, p. 1). Thus, protecting biometric information become the main concern as well as main challenge to all researchers in this field.

Cancellable biometric is a concept where its biometric template is protected by combining both security system and replacement feature into the biometric system. The main idea of this system is that cancellable biometric transforming and changing all images and features of biometric before continuing to matching process, yet maintaining the natural characteristic of its cancellable scheme. The proper cancellable biometric system has to have these criterion; distinctive, reusable, unidirectional transformation, and performance (Maltoni, Maio, Jain, & Prabhakar, 2003).

The transformation process implemented in various biometric technologies has several functions such as, face identification ((Boult, 2006, pp. 560-566; Ross & Govindrajana, 2005, pp. 196-204; Li & Jain, 2004; Cardinaux, Sanderson, & Bengio, 2006, pp. 361-373), signature identification (Campisi, Maiorana, & Neri, 2008; Bhattacharyya, Bandopadhyaya, Das, Ganguly, & Mukherjee, 2008, pp. 181-185), iris identification (Kanade, Petrovska-Delacretaz, & Dorizzi, 2009, pp. 120-127; Ganorkar & Ghatol, 2007, pp. 91-96; Wayman, Jain,

Maltoni, & Maio, 2005; Daugman, 2003, pp. 279-291), voice identification (Xu & Cheng, 2008, pp. 263-266; Furui, 1997, pp. 856-872), etc. Many recent literatures state that fingerprint is one of the technologies that are mostly discussed about protection method toward its biometric template (Ratha, Chikkerur, Connell, & Bolle, 2007, pp. 561-572; Mukhaiyar, 2014, pp. 163-166; Lee & Kim, 2010; Lee, Choi, Toh, Lee, & Kim, 2007, pp. 980-992; Farooq, Bolle, Jea, & Ratha, 2007). One of the literatures is as reported in (Ratha, Chikkerur, Connell, & Bolle, 2007, pp. 561-572). In his research, the writer proposed three types of transformation to be implemented in fingerprint images; Cartesian transformation, polar transformation, and image folding.

The first two transformations have a disadvantage in boundary issue. If the original minutiae point is out from its boundary and then divide the area of the feature as the result of minor distortion of image alignment, or if the original fingerprint image is damaged, then the transformation version of minutiae points will be placed on far from where it is supposed to be. Meanwhile, the third method relates to the functional use of smoothing local value to flipping through the space of fingerprint feature. In (Lee, Choi, Toh, Lee, & Kim, 2007, pp. 980-992), Local smoothing function is used to create cancellable fingerprint template by maintaining the original geometric connection (rotation and movement) between the registered template and the questionable template after transformation process is conducted. Therefore, the template transformation result can be used to identify a person without requesting the alignment of image fingerprint used as an input.

However, this analysis security method is yet sufficient enough as a protection over a biometric data. As an example, an impostor might narrow down the candidate owners of the original minutiae design based on the limitation in orientation continuity of minutiae feature and local smoothing process of transformation function. The result of this action can be seen in research report (Ratha, Chikkerur, Connell, & Bolle, 2007, pp. 561-572). Several investigations had been conducted regarding to this issue. For instance, in (Farooq, Bolle, Jea, & Ratha, 2007), the writer presented the conversion of a fingerprint into a binary-string area based on its minutiae series. The representations of binary numbers are transformed into an anonymous representation using a unique personal key. According to the writer, not only that the offering transformation cannot possibly be inverted, but also when it is being misused by someone else, then the template will disappear and can be renewed by entering different key of information. One of the advantages of this representation is that the existed methods like bio-hashing could be implemented.

In (Chikkerur, Ratha, Connell, & Bolle, 2008, pp. 1-6), a secure method to produce a template of cancellable fingerprint is introduced. This method is extracting local image of fingerprint filled with minutia into small pieces and then transforming them into projection matrices without changing the space between each minutia in those small pieces. However, the disadvantage of this method is the poor accuracy in the container of transformation results. In the same year, an author (Bringer, Chabanne, & Kindarji, 2008, pp. 43-51) had presenting an idea in constructing cancellable biometric system and secure sketches in order to protect the privacy of biometric template while supervising the matching process between the protected data and referenced data. The standard process in cancellable biometric is to perform a transformation to create an unchangeable image and to produce a matching process for those transformed images. This research showed that the use of correction system on the sketches that secured from cancellable biometric system resulting a system that supervising the proper matching process.

In (Yang, Busch, Derawi, Bours, & Gafurov, 2009, pp. 490-499), geometric transformation system of minutiae position is proposed to create template of cancellable fingerprints which is useful in alignment process. In order to create template of cancellable fingerprint, a supervising parameter over the encryption of minutiae features is conducted in the surrounding area of minutiae. Then, all the encrypted minutiae will be superimposed to form a protected template. The parameters to control the minutiae encryption are created from the arranged minutiae geometric. Compared with the parameters where the algorithms of cancellable templates use the information of minutiae that have to be encrypted, this minutiae encryption can guaranty the solidity of non-inevitability concept.

### **3. Cancellable Supporting Elements**

As aforementioned previously, several fingerprint processing steps are required in this research to obtain an appropriate fingerprint image as input of the cancellable system i.e. fingerprint pre-processing (Maltoni, Maio, Jain, & Prabhakar, 2003), core-point identification (Cappelli, Lumini, Maio, & Maltoni, 1999, pp. 402-421; Mukhaiyar, 2017, pp. 146-150; Jain, Prabhakar, Hong, & Pankanti, 2000, pp. 846-859), Region of Interest (RoI) (Mukhaiyar, 2017, pp. 146-150), fingerprint classification (Bolle, Connell, & Ratha, 2002, pp. 2727-2738; Nillson & Bigun, 2003, pp. 2135-2144; Mukhaiyar, 2017, pp. 118-123), minutiae extraction (Amengual, Juan, Prez, Prat, Sez, & Vilar, 1997, pp. 871-875; Kasaei, Deriche, & Boashash, 1997, pp. 303-306), and fingerprint

authentication (Cardinaux, Sanderson, & Bengio, 2006, pp. 361-373), signature identification (Campisi, Maiorana, & Neri, 2008). Pre-processing step is required to provide a better quality fingerprint as an input for cancellable fingerprint algorithm. This stage can minimize the possibility of obtaining false-feature information caused by noises, scars, unclear ridges/valleys, etc. Core-point is needed as a reference point to select a certain region for fingerprint input. Moreover, core-point is also utilized as an important requirement in classification step. Lastly, minutiae extraction is used as one of the input of the cancellable system.

Producing a cancellable fingerprint using matrices operations demands a square form image as an input. Since mostly fingerprint recognition images are not square form, Region of Interest step is appropriate to be implemented. Still, this stage is able to omit a useless part of fingerprint so that only a true feature extracted in feature extraction process.

Fingerprint classification aims to split fingerprints in database into a different type based on its pattern combination. This step is required in this research because by classifying the fingerprint either a registered or verified one, time consuming problem in authentication process could be solved. Moreover, fingerprint classification can confidentially gain accuracy to recognize an authenticity of fingerprint.

In this research, the possibility to establish a cancellable fingerprint except by using an enhanced fingerprint image like minutiae extraction is determined as well. The reason is because naturally minutiae by naked eyes not showing as a fingerprint anymore. It just looks like scattered figured points. However, implementing an improved minutiae extraction approach is needed to omit false-recorded information for fingerprint recognition.

**4. Matrices Operations**

The main aim in generating cancellable biometric is producing a reliable revocable biometric template. Cancellable biometric is needed to preserve information of an authorized person from an impostor. One way is by randomizing the original biometric feature to generate a vague image. In this research, the disguising process is obtained using three matrices operations: Elementary Row Operation (ERO), Kronecker Product (KP) operation, and inverse matrix operation.

This idea is to deliver as one of the cancellable biometric approaches because using ERO, KP, and inverse operations can verily give us a lot of alternatives to randomize the original image as long as it is able to satisfy three requirements of non-inverted matrices. First of all, at least one row or column of the original matrix should be zero (0) value. Secondly, the original matrix must be modified into non-square matrix form. And the last is to make sure that none of each row is a multiple of another row.

Furthermore, the use of Kronecker/Tensor Product is based on due that are needed a large, non-inverted and totally different cancellable biometric image than the original biometric image.

*4.1 Elementary Row Operation (ERO)*

Generally, Elementary Row Operation, ERO, can be defined as multiplication and addition force to matrix rows. The three operations corresponding to the operations on rows of ERO are multiply a row through by a nonzero constant, interchange two rows, and add a multiple of one row to another row (Anton & Rorres, 2005).

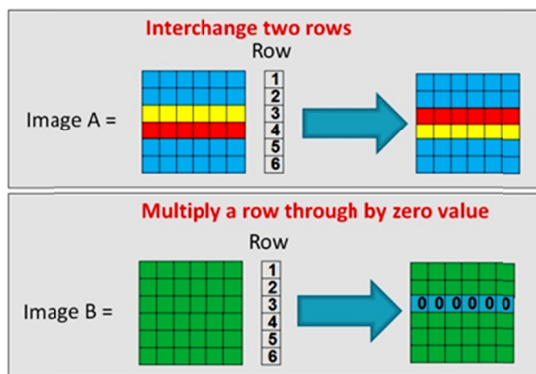


Figure 2. Illustration of the Operation of ERO

*4.2 Kronecker Product Operation (KP)*

In (Laub, 2005, pp. 139-142), the definition of Kronecker Product or Tensor Product can be obtained as follows. Let  $A \in \mathbb{R}^{m \times n}$ ,  $B \in \mathbb{R}^{p \times q}$ . Then the Kronecker Product of A and B is defined as the matrix

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix} \in \mathbb{R}^{mp \times nq} \tag{1}$$

Obviously, the same definition holds if  $A$  and  $B$  are complex-valued matrices.

There are two advantages that are able to be obtained using this operation. First of all, it is obviously able to change the value of each element of the original matrix. And secondly, as if  $B$  is any kind of matrix's form, it is mean that a new larger matrix can be generated in any form of matrix.

### 4.3 Inverse Matrix Operation (INV)

In matrices domain, whether a given  $n \times n$ (square) matrix  $A$  has a multiplication inverse matrix (that is, a matrix  $A^{-1}$  such that  $AA^{-1} = I_n$ ) is going to be considered. Interestingly, not all square matrices have multiplicative inverses, but most do. These inverses can be found by examining some properties of multiplicative inverses and illustrating methods for finding when these exist.

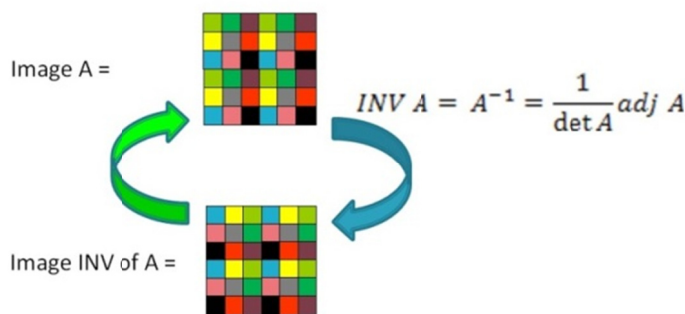


Figure 3. Illustration of the Inverse Operation

## 5. Cancellable Fingerprint Method

### 5.1 Basic Concept

A feature can be categorized as a cancellable feature when it is non-invertible to the original image. The same thing applies to matrices. The matrices cannot be inverted when satisfying three situations. Firstly, there is one zero row at least. Next, there is a row that is a multiple of another row. And lastly, the matrix form is not a square.

Related to the first requirement, it can be achieved by using Elementary Row Operation (ERO) where a selected row is multiplied by zero. For the second requirement, since in image system it is rare to find a row which is a multiple of another row, hence by using ERO this condition can be created. Furthermore, to ensure the obtained cancellable matrix is completely masked and able to meet the last requirement of non-invertible matrix, each element of the transformed matrix is multiplied by an arbitrary matrix/element using the Kronecker Product operation. By using this process, the outcome is a matrix that has more numerous elements and an adjustable matrix form (whether rectangle or square matrix).

Since the proposed method deals with matrices, there should be no noise in the system because the existence of noise may add specific information to the biometric feature. Related to cancellable biometric, since the end of this system is authentication process, even a very little noise will affect the quality of cancellable feature significantly and will certainly resulting low precision in verification later on. Thus, the early process to be done toward the result of established fingerprint is the enhancement step. The enhanced fingerprint will provide a feature with the precise value of fingerprint information so that when it is extracted to domain matrices, there will be no unnecessary values that go into it. After the fingerprint enhancement step, the cancellable input image will subject to several matrices transformations. To simplify the next appellation, we name it as matrix  $A$ .

Meanwhile, the acquired fingerprint image is in matrices domain, we next discuss how to build the system of cancellable biometrics using matrix  $A$  as an input. Firstly, matrix  $A$  will be inversed as the first step to disguise the real feature. This idea is tentatively, because it will be considered whether directly inverting matrix  $A$  is an effective way or, on the other hand, inverting matrix  $A$  after another matrix operation. The next step will be applying the Elementary Row Operation (ERO) to matrix  $A$  to obtain zero-value row or to apply Kronecker

Product (KP) operation. In this research, it will be analysed of how much zero rows needed to achieve the requirement of maximum non-invertible. Besides the use of ERO to obtain zero rows, another thing to be considered in this research is the use of ERO to create rows that are the multiple of the other rows.

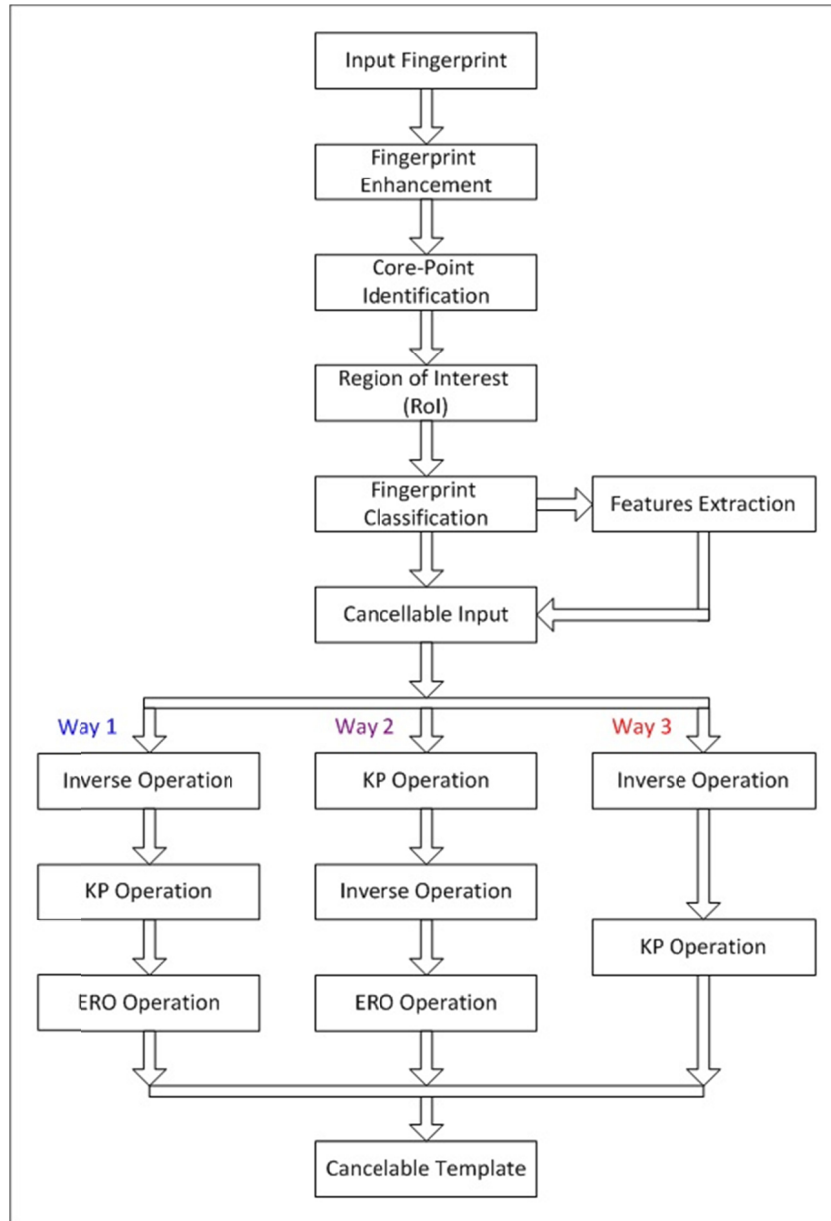


Figure 4. Steps Flow Chart

In case of the ERO as the step taken, matrix A that has been imposed ERO operation; we name it as matrix K; that will go through KP operation to produce KP matrix which every initial element is unrecognizable. Let us name it as matrix M. In this KP operation, matrix K will be multiplied by tensor factor that can be in a form of matrix or integer with constant value. Let name it as B. The form and the value of factor B will be one of the analysis materials in this research. For example, if factor B is matrix B, then the value can be taken from the numbers given by a person who have registered his biometrics when he registered himself as an authentic person of a biometric whose the cancellable feature is being built. In this research, the steps of using ERO and KP will be analysed as well, whether the use of ERO in the beginning and KP afterwards is better, or vice versa. The result of the process above will be a cancellable matrix of matrix A, and be namely as matrix C which is as a cancellable template.

To secure the original input, this algorithm should be executed using one way transform concept. Hence,

identification attempt by imposter can be eluded because the system does not provide a looping process. The following figure illustrates the concept used in this research.

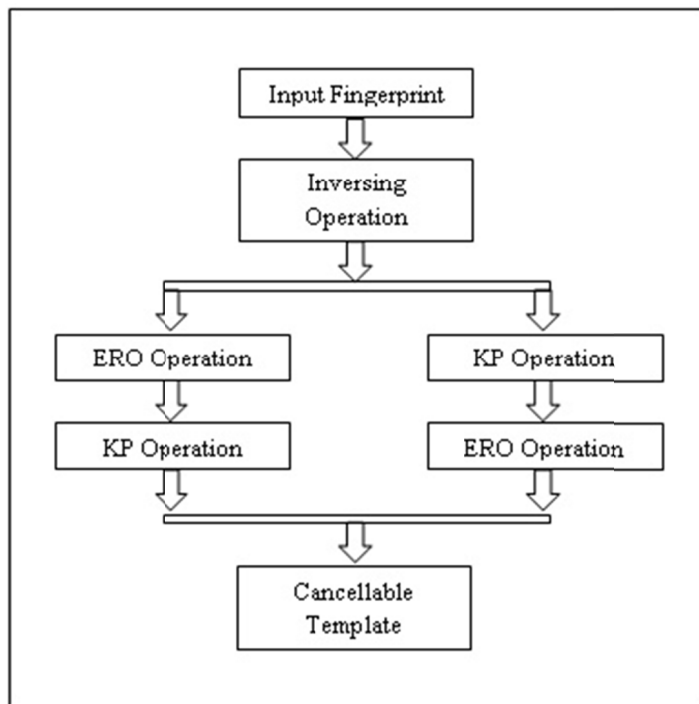


Figure 5. Cancellable System Flow Chart

These aforementioned processes can be illustrated as following mathematical steps. Let say that the original input matrix is A which a three-by-three matrix is. As said before that the first alternative step that is going to do is to inverse the original matrix to camouflage it. Let say it as

$$A^{-1} = \frac{1}{|A|}adj. \tag{2}$$

Supposing  $A = \begin{bmatrix} 2 & 5 & 7 \\ 3 & 2 & 0 \\ 8 & 9 & 6 \end{bmatrix}$ ,

where  $|A| = 11$ , and

$$adjA = \begin{bmatrix} 12 & 33 & 11 \\ -18 & -44 & 21 \\ 11 & 22 & -11 \end{bmatrix},$$

that,

$$A^{-1} = \begin{bmatrix} \frac{12}{11} & 3 & -\frac{14}{11} \\ -\frac{18}{11} & -4 & \frac{21}{11} \\ 1 & 2 & -1 \end{bmatrix}$$

To obtain a Kronecker Product, another matrix should be determined. In order to give more overview, there are

two alternatives of that matrix. Firstly, a non-square form matrix. Let say it as matrix  $B = \begin{bmatrix} 11 & 11 \\ 0 & 0 \\ 11 & 11 \end{bmatrix}$ . The reasons

to establish this matrix are firstly to show why a non-square matrix cannot be inverted and secondly why if there is at least one zero rows cannot be inverted as well. Furthermore,

$$A^{-1} \otimes B = \begin{bmatrix} \frac{12}{11} & 3 & -\frac{14}{11} \\ -\frac{18}{11} & -4 & \frac{21}{11} \\ 1 & 2 & -1 \end{bmatrix} \otimes \begin{bmatrix} 11 & 11 \\ 0 & 0 \\ 11 & 11 \end{bmatrix} =$$

$$KP = \begin{bmatrix} 12 & 12 & 33 & 33 & -14 & -14 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 12 & 12 & 33 & 33 & -14 & -14 \\ -18 & -18 & -44 & -44 & 21 & 21 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -18 & -18 & -44 & -44 & 21 & 21 \\ 11 & 11 & 22 & 22 & -11 & -11 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 11 & 11 & 22 & 22 & -11 & -11 \end{bmatrix}$$

KP matrix is a 9 x 6 form (non-square matrix).

Remember that a matrix can be said having an inverse as if  $A \cdot A^{-1} = I$ ; where I is a matrix identity. Meanwhile, a matrix is able to be told as a matrix identity as if the diagonal elements of matrix are 1 (one). Whereas, the others element are 0 (zero). Based on this requirement, it can be ensured that a matrix identity should be a square form matrix. Since 9 by 6 is not a square form matrix, it proves that KP matrix does not have an inverse.

The next alternative is a square form matrix. Let say that the matrix  $B = \begin{bmatrix} 11 & 11 & 11 \\ 0 & 0 & 0 \\ 11 & 11 & 11 \end{bmatrix}$ .

That,

$$A^{-1} \otimes B = KP = \begin{bmatrix} \frac{12}{11} & 3 & -\frac{14}{11} \\ -\frac{18}{11} & -4 & \frac{21}{11} \\ 1 & 2 & -1 \end{bmatrix} \otimes \begin{bmatrix} 11 & 11 & 11 \\ 0 & 0 & 0 \\ 11 & 11 & 11 \end{bmatrix} = \begin{bmatrix} 12 & 12 & 12 & 33 & 33 & 33 & -14 & -14 & -14 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 12 & 12 & 12 & 33 & 33 & 33 & -14 & -14 & -14 \\ -18 & -18 & -18 & -44 & -44 & -44 & 21 & 21 & 21 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -18 & -18 & -18 & -44 & -44 & -44 & 21 & 21 & 21 \\ 11 & 11 & 11 & 22 & 22 & 22 & -11 & -11 & -11 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 11 & 11 & 11 & 22 & 22 & 22 & -11 & -11 & -11 \end{bmatrix}$$

Now, the form of matrix KP is square (9 by 9). This 9 by 9 matrix can be inverted when  $KP \cdot KP^{-1} = I$ . In this case, let we symbolize the matrix identity as matrix C and the  $KP^{-1}$  as matrix P. Where,

$$C = \begin{bmatrix} C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16} & C_{17} & C_{18} & C_{19} \\ C_{21} & C_{22} & C_{23} & C_{24} & C_{25} & C_{26} & C_{27} & C_{28} & C_{29} \\ C_{31} & C_{32} & C_{33} & C_{34} & C_{35} & C_{36} & C_{37} & C_{38} & C_{39} \\ C_{41} & C_{42} & C_{43} & C_{44} & C_{45} & C_{46} & C_{47} & C_{48} & C_{49} \\ C_{51} & C_{52} & C_{53} & C_{54} & C_{55} & C_{56} & C_{57} & C_{58} & C_{59} \\ C_{61} & C_{62} & C_{63} & C_{64} & C_{65} & C_{66} & C_{67} & C_{68} & C_{69} \\ C_{71} & C_{72} & C_{73} & C_{74} & C_{75} & C_{76} & C_{77} & C_{78} & C_{79} \\ C_{81} & C_{82} & C_{83} & C_{84} & C_{85} & C_{86} & C_{87} & C_{88} & C_{89} \\ C_{91} & C_{92} & C_{93} & C_{94} & C_{95} & C_{96} & C_{97} & C_{98} & C_{99} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

From the matrix above, it is obvious that the diagonal elements of C should be 1 and the others are 0.

The computation can be simplified by firstly checking the diagonal elements of  $KP \cdot KP^{-1}$  or  $KP \times P$  ( $C_{11}, C_{22}, C_{33}, C_{44}, C_{55}, C_{66}, C_{77}, C_{88}, C_{99}$ ). Where,

$$C_{11} = (12 \times P_{11}) + (12 \times P_{21}) + (12 \times P_{31}) + (33 \times P_{41}) + (33 \times P_{51}) + (33 \times P_{61}) + (-14 \times P_{71}) + (-14 \times P_{81}) + (-14 \times P_{91})$$

$$C_{22} = (0 \times P_{12}) + (0 \times P_{22}) + (0 \times P_{32}) + (0 \times P_{42}) + (0 \times P_{52}) + (0 \times P_{62}) + (0 \times P_{72}) + (0 \times P_{82}) + (0 \times P_{92})$$

$$= 0 \implies \text{it means that } C \neq I \text{ (matrix C is not equal to matrix identity)}$$

In conclusion, it can be said that matrix KP is a non-inverted matrix.

### 5.2 Processing Requirements

Referring to the explanation aforementioned, it is clearly that matrix operations like Elementary Row Operation (ERO) and Kronecker Product (KP) Operation can be implemented into generate a cancellable biometric especially for fingerprint proposed. This concept is based on the similarity approach between cancellable



biometric and non-inversed matrix. In the former, a cancellable method is said successful when the yielded image cannot be reverted to the original image. The same goes for the latter. In matrix domain, if the goal is to obtain a revocable matrix, then the non-inverse matrix requirement should be done to make the matrix non-invertible.

The required conditions of the transformation process are used as parameters to quantize the non-invertibility standard of the cancellable template. Suppose the input  $A$  is not imposed by one of the condition, such as INV operation. It is possible for intruder to extract the result of the KP ( $A^{KP}$ ) and ERO ( $A^{ERO}$ ) operations because of the similarity appearance of  $A$ ,  $A^{KP}$ , and  $A^{ERO}$ . The same case happens as well if ERO operation is eliminated from the generating cancellable system. The only implementation of KP and INV is not enough to shield the cancellable template from an inversion attempt of the intruder. The intruder can experiment to inverse the cancellable template and disannul the arbitrary matrix of the KP operation. Thus, the three conditions of the non-invertibility requirement have to be implemented concurrently.

Furthermore, this situation requires a qualified input  $A$  for the system. No noise is allowed in each element of the input to avoid mismatch result in the matching step of the system. The noise can alienate an authorized person from his own cancellable template. So, he will be judged as an imposter hereupon. Therefore, fingerprint pre-processing step is required to enhance the quality of the input image to reduce the false matching.

As we know, this research works in matrices domain. Hence, the requirement of a square form image is determined as well. Region of Interest (RoI) process is used to select a particular area of fingerprint as an input. Moreover, this research offers a new approach of RoI step by optimizing the using of another step in fingerprint process i.e. ridge orientation, ridge frequency, and core-point identification]. Ridge orientation and –frequency is needed to specific an area dense with ridge and valley of fingerprint pattern. Meanwhile, core-point is needed as a reference point of RoI.

Another fingerprint step that is required in this research is fingerprint classification. This step is need for enrolment and verification process. Fingerprint classification step will classify a registered and acquired into its classification to simplify the acknowledging process of the fingerprint. The classification process will join a registered fingerprint into its particular pattern class. Then by using this standard, an acquired fingerprint will be pointed into its pattern class as well to ease the searching process.

## 6. Experimental Results

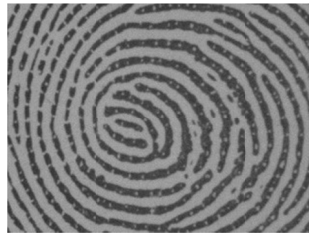
The proposed cancellable approach is implemented into several fingerprint's databases i.e. FVC 2002: DB1\_B to DB4\_B, FVC 2004: DB1\_B to DB4\_B, and BRC: DBI-Training/Test/DBII. This implementation aims to observe the performance result of the proposed approach based on the specific character of each databases. However, to short the time, we only use several variant of the fingerprint in database BRC DBI to check the diversity and reusability character of the algorithm.

The term of diversity and reusability is used to check the ability of the cancellable system to distinguish and modify the cancellable template from the same input in case of compromising trial by imposter. Variable to be determined is the dissimilarity between the transformed template and transformed template for diversity; and the original input and the cancellable template for reusability. The experiment is conducted into the same fingerprint in the database. For BRC database, every fingerprint has ten different variants divided into two parts. It means that each part has five different variants of the same fingerprint.

Two fingerprints of each part are used for this experiment. One is as registered data and the other as acquired one. Meanwhile, the three others are utilized in authentication step. One of the two fingerprints used for the experiment will be transformed into ten transformed template (cancellable template). Each transformed template is generated by a different arbitrary KP matrix and different ERO order. Later, the other one is used as an acquired transformed template. The following figure illustrates the transformation process of the original fingerprint input into a transformed form by combining the arbitrary matrix in KP and the order in ERO.

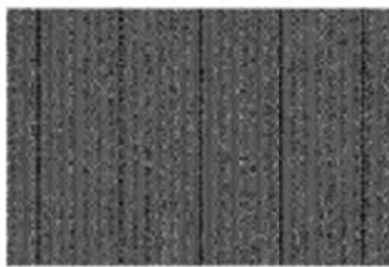
Figure 6 shows a complete transformation of the original input of the fingerprint. The transformed template camouflages the appearance of the fingerprint into a distinctive presentation. The histogram presents the different sight of each template to show the variant of the template regarding to the kind of KP and ERO formulas implemented into the input fingerprint. As aforementioned in the previous sub-chapter, the one way transformation guarantees system from revertible trial of the imposter. The variant of the transformed templates show a huge possibility to reproduce a dissimilar template in case that the registered template is compromised by an authorized person. The diversity of the transformed template enables the system confidently to generate the cancellable template automatically as a response of the invalid usage.

**Original Input  
BRC Database**

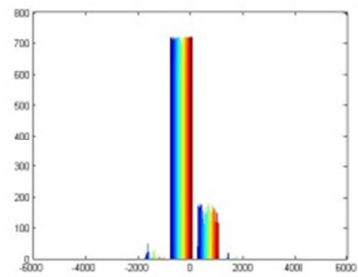
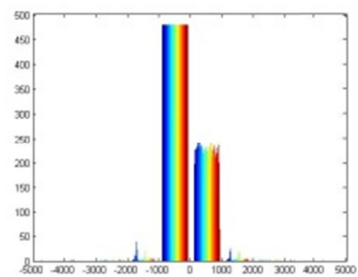
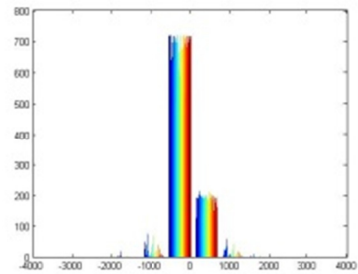


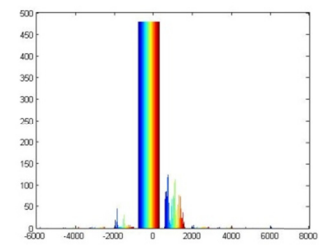
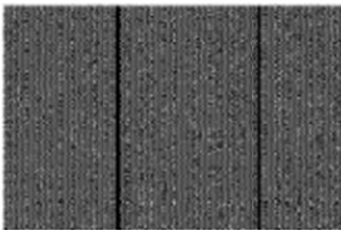
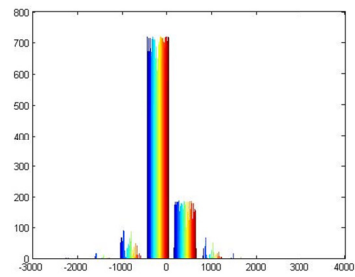
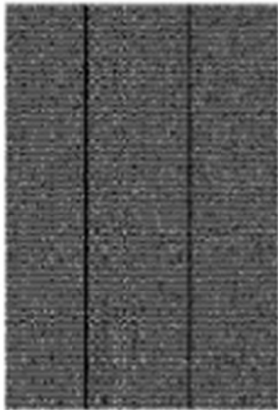
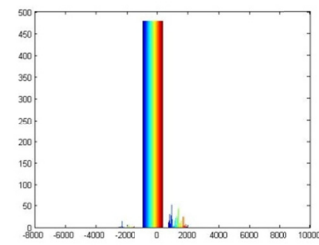
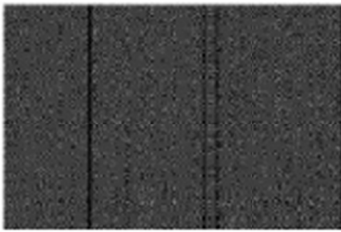
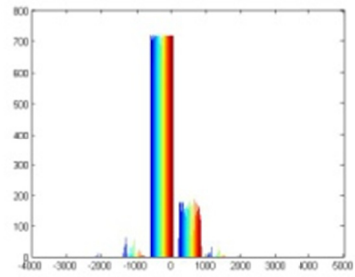
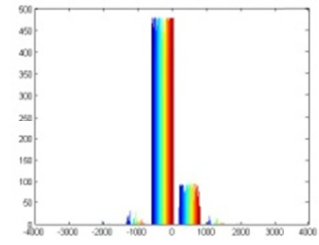
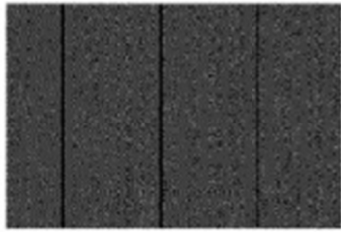
**KP and ERO Formulas:**  
Five Rows Interchanging  
Five Columns Zeroing  
Five Rows Multiplying

**Transformed Templates**



**Histogram Presentation**





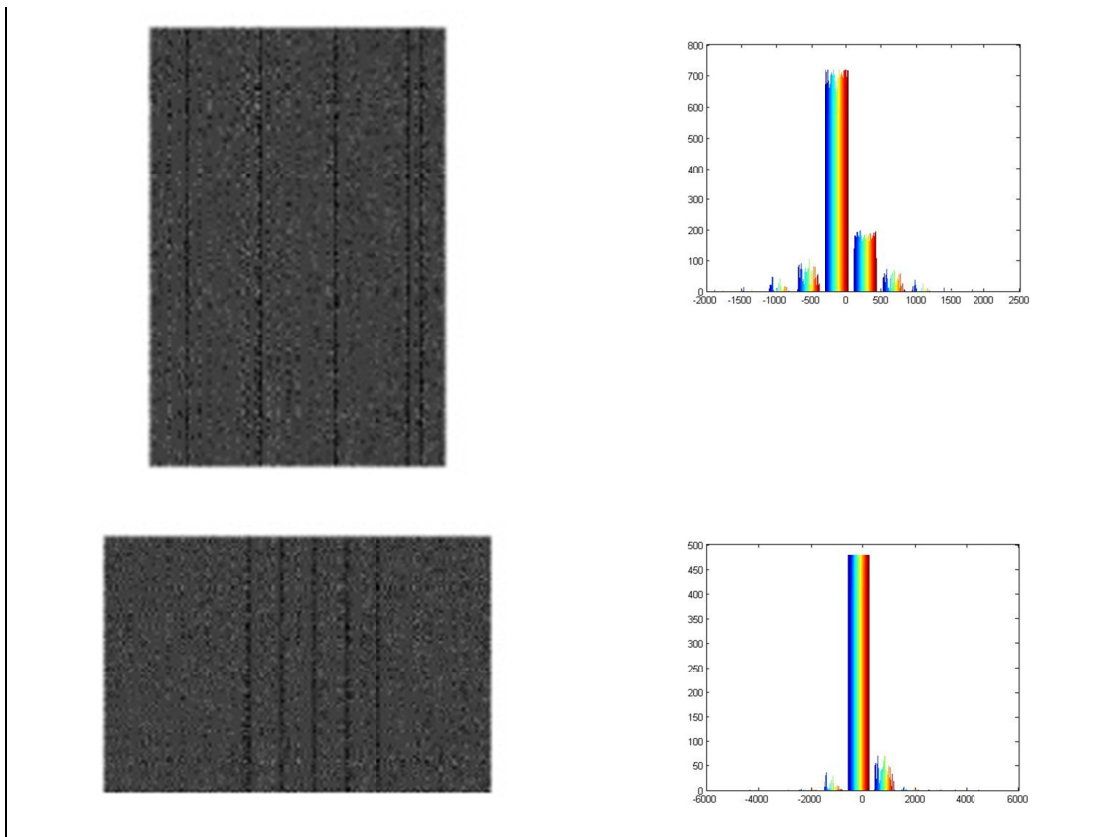


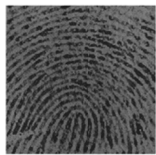
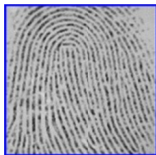
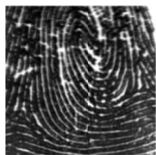



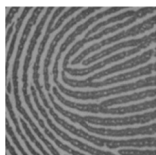
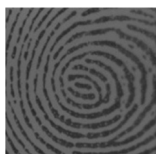


Figure 6. The Variant of Fingerprint Transformed Procedures

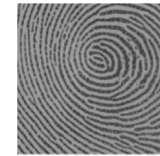
In this research, we utilized one fingerprint as a registered data of each database we used. And another six of fingerprint for BRC and eight for FVC2002&2004 are as an enquired fingerprint. It means that there are 80 kinds of fingerprints existing in this database where one of those is selected as the owner representative in database. From the 79 fingerprints left, only seven fingerprints that are categorized into accepted, rejected, false accepted, and false rejected, while the remaining 72 are totally rejected and are not included in those categories as the results of classification step implementation. This step is not only saving time during the process, but also helps the system to shrink number of fingerprints to analyze. During this stage, an enquired input will be grouped into its particular class so that an inappropriate fingerprint would be rejected automatically before it continues to a matching step since each fingerprint in the same database is already categorized into its own class. In this experiment, we used minutiae extraction feature [7, 8, 9] as an input of the cancellable system. The main reason is because minutiae already have a different appearance contrasted with the original fingerprint. Hence, it is become an idea to optimize the minutiae extraction as an input of the system.

In term of the performance evaluation of the system, we used the authentication step to evaluate the ability of the proposed method to authenticate whether the inputs of fingerprint are a genuine owner or an impostor. This categorizing process justifies the genuineness of the fingerprint by implementing some criterion as a scoring for both an established fingerprint and the input fingerprint as an enquiry fingerprint. The first criterion is by directing the input into its fingerprint classification group to shortage the identification process. Next is by calculating the distance between core and tent arch (TA) of the fingerprint. The third criterion is by scoring a minimum and maximum distances of matrices values of minutiae between an original fingerprint registered in database and several fingerprints from the same owner as information to calculate the distance value of each pixel of the fingerprint, so that variant possibility of a genuine fingerprint can be decided later even when the acquisition process of each fingerprint is taken differently. The next criterion is by evaluating the scoring of minimum and maximum distances of matrices values of minutiae between the genuine data and a false data to score the value to reject an input. The last criterion is by setting a threshold value of accepted and rejected decision as the result of the third and the fourth criteria. The evaluation is started by determining an equal error rate (EER) of each database.

Table 1. EER Comparasion amon All Databases

Databases	EER	GAR/FAR	Threshold		
FVC2002	DB1	0.063	1/0.125	0.475	
	DB2	0.063	1/0.125	0.475	
	DB3	0.063	1/0.125	0.375	
	DB4	0.063	1/0.125	0.425	
FVC2004	DB1	0.063	1/0.125	0.525	
	DB2	0.063	1/0.125	0.175	
	DB3	0.063	1/0.125	0.175	
	DB4	0.063	1/0.125	0.325	
BRCDBI	Test	0.083	1/0.167	0.675	
	Training	0.083	1/0.167	0.625	

BRCDBII - 0.083 1/0.167 0.675



It has become commonplace in the authentication step that not all the accepted or rejected fingerprints are true genuine and true impostor. These conditions are known as false genuine and false impostor. False genuine and impostor would create a problem if its rates (EER) are huge. Hence, fingerprint with the lowest EER has a chance to become a better fingerprint in the database. However, EER is not the only requirement to acknowledge which fingerprint has a better error rate. In this research, threshold value is also determined as a parameter to know which fingerprint in the same database has the lowest error rate. The reason is because threshold value would show an excuse level for the authentication system to decide the authenticity of the fingerprint. Finding an error rate for each fingerprint in the database is required to discover the characteristic of the database after imposed by the proposed algorithm. Based on the experiment, the lowest level of the error rate for databases FVC2002 and FVC2004 is in 0.063. Meanwhile, the highest EER and the threshold of each EER could be dissimilar. In term of the threshold score, the highest score would represent a better condition of the fingerprint. If a fingerprint has a high threshold score, it means that the enquired fingerprint would be recognized by system as an authorized fingerprint even with a high qualification matching score. However, the threshold rate does not become a prior regulation to decide which fingerprint has a better error rate but EER with the lowest score does.

The next thing to be evaluated is duration needed to execute the proposed algorithm. Time consuming is a concerning issue to be determined since there are two different input of the fingerprints adapted in generating a cancellable feature and its authentication process. This first combination of input is cancellable step; core-point step; classification step; authentication step (using an original fingerprint image). The second is cancellable step; core-point step; classification step; RoI step; authentication step (using a cropping input). Furthermore, the total times of each combination are compared to see which combination is better. The approach has been tested by using Intel Core i5-2430M CPU@2.40GHz; 4.00 GB installed RAM; and MATLAB version 7.10.0 (R2010a). The following tables illustrate time taken by system to execute all steps of the research. From each table, the comparison among different sub-databases in the same database is shown to provide the different percentage between original input and RoI input in order to show which input has a better time to run all steps.

Table 2. Time Needed for Database FVC 2002 (in Second)

No.	Time Needed	Steps					Total	Time Deficits (%)
		Cancellable	Core-Time	Classification	Region of Interest	Authentication		
1.	DB1	Original	0.8589	0.5542	0.7269		0.000187	23.85
	RoI	0.4834	0.4099	0.5048	0.2316	0.000130	1.62983	
2.	DB2	Original	1.1610	0.9232	0.7592		0.000204	39.33
	RoI	0.5269	0.4190	0.5255	0.2538	0.000142	1.725342	
3.	DB3	Original	0.8333	0.6627	0.6941		0.000187	27.89
	RoI	0.4825	0.3837	0.4811	0.2320	0.000130	1.57943	
4.	DB4	Original	0.9826	0.7814	0.6855		0.000184	36.33
	RoI	0.4765	0.3789	0.4751	0.2291	0.000128	1.559728	

Table 3. Time Needed for Database FVC 2004 (in Second)

No.	Time Needed	Steps					Total	Time Deficits (%)
		Cancellable	Core-Time	Classification	Region of Interest	Authentication		
1.	DB1	Original	1.0951	0.8709	0.6966		0.000187	40.47
	RoI	0.4842	0.3850	0.4829	0.2328	0.000130	1.58503	

2.	DB2	Original	0.7731	0.6148	0.6820		0.000183	2.070083	25.06
		RoI	0.4738	0.3768	0.4725	0.2280	0.000127	1.551227	
3.	DB3	Original	1.0568	0.8218	0.6878		0.000190	2.566590	38.29
		RoI	0.4903	0.3805	0.4772	0.2357	0.000132	1.583832	
4.	DB4	Original	0.8942	0.7111	0.7009		0.000188	2.306388	30.84
		RoI	0.4873	0.3875	0.4860	0.2343	0.000131	1.595231	

Table 4. Time Needed for Database BRC (in Second)

No.	Time Needed		Steps					Total	Time Deficits (%)
			Cancellable	Core-Time	Classification	Region of Interest	Aunthentication		
1.	DB1	Original	0.5049	0.4015	0.7120		0.000191	1.618591	0.0057
	Test	RoI	0.4943	0.3931	0.4929	0.2380	0.000133	1.618433	
2.	DB1	Original	0.4762	0.3787	0.6842		0.000184	1.539284	-1.04
	Training	RoI	0.4750	0.3777	0.4737	0.2287	0.000128	1.555228	
3.	DB2	Original	0.6159	0.4898	0.7584		0.000203	1.864303	7.59
		RoI	0.5262	0.4184	0.5247	0.2535	0.000142	1.722942	

Overall, it is obvious that the system using a RoI input consumes less time than an original input except for database BRCDB1Training even though the former system has one more step included in process (RoI step). The size of the input fingerprint significantly contributes to reduce time taken for the process. The following table shows the contribution of the size differences to time taken by the process.

Table 5. Correlation between the size differences of the input fingerprint and the time taken by the process (%)

No.	Time Needed		Databases			
			FVC 2002	FVC 2004	BRC	
1.	DB1	Size	43.13	54.86	DB1 Test	1.81
		Time	23.85	40.47		0.0057
2.	DB2	Size	53.95	38.08	DB1 Training	0.25
		Time	39.33	25.06		-1.04
3.	DB3	Size	41.11	53.38	DB2	14.04
		Time	27.89	38.29		7.59
4.	DB4	Size	51.21	45.30		
		Time	36.32	30.84		

Table 5 clearly shows the affiliation between the size of the input of fingerprint and the duration taken to complete all the processes. A big input would require more time in the process. However in this research case, it cannot be denied that the size difference should not be narrow such as database BRCDB1Training. Because the system that is used a fingerprint with RoI size needs RoI selection step in its process. It means that it would demand more time to execute the process. Nevertheless, table 6.15 proves that this case is not a big obstacle in this research.

Another parameter considered in the performance of the system is the size of the arbitrary matrix that is used to produce a cancellable feature of the fingerprint. The reason is because the size of that matrix could affect the time consumed in running the process. Therefore, the variant of matrix size was simulated to check its influence into the time taken along the running of the process for databases FVC2002, FVC2004, and BRC.

Figure 7 shows the simulation trend by increasing the size of matrix started from 1 x 1 until 25 x 25 while recording the time consuming along the simulation. During the simulation, it is found that the time taken would be tended to increase as well as the increasing of the size of the matrix. However, at matrix 3 x 3, the trend is tended to lower before going up again at matrix 4 x 4. Therefore, the size of the arbitrary matrix used in this research is matrix 3 x 3.

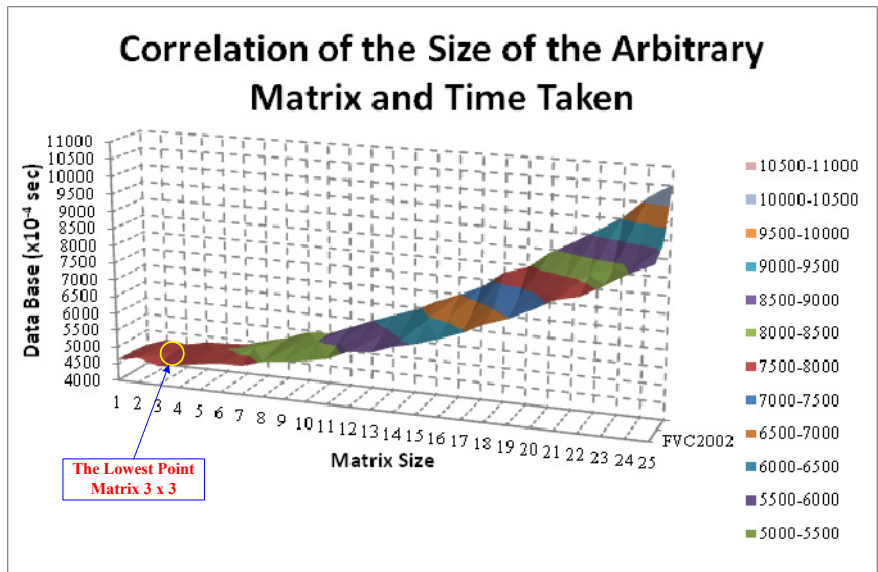


Figure 7. The Correlation between the size of the arbitrary matrix and the time taken of the process

In ERO operation, the most important issue to be discussed is the best number of zero rows and columns needed to make sure that the cancellable template is safe from the impostor. The analysis is done by doing several simulations i.e. increasing number of the zero rows, increasing number of the zero columns, and using the zero rows and columns simultaneously while increasing the number zero rows and columns as well. These increasing simulations is done by starting from one until  $n/3$  rows/columns, where  $n$  is size of the input of the fingerprint. The reason to choose  $n/3$  as the limit to increase the number of rows and columns is because it would erase the detail information of the fingerprint feature. The following figure is illustrated all simulation done in the research.

-13.2515	-48.5150	-62.6468	-50.0396	-16.3391	24.1932	54.9296	63.7668
14.1556	-28.0481	-57.4675	-62.1471	-40.5157	-1.9108	37.4970	62.6071
39.7504	-1.8382	-41.5896	-63.1917	-59.4876	-29.4826	12.6003	49.4918
58.7400	25.1083	-18.0617	-54.2500	-66.9095	-51.6159	-15.1277	27.3705
67.7559	47.9171	9.0100	-34.3391	-62.9618	-65.2899	-40.8292	-0.0031
65.3777	64.5113	35.1631	-8.5376	-48.4109	-68.1412	-60.0694	-27.9643
54.2384	69.3609	55.6404	18.7757	-25.8578	-59.8850	-69.6673	-51.7492
32.5657	63.1902	67.3054	43.1696	0.9109	-41.9890	-68.1936	-67.5786

Figure 8. Illustrating of the original feature of the fingerprint

-13.2515	-48.5150	-62.6468	-50.0396	-16.3391	24.1932	54.9296	63.7668
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
39.7504	-1.8382	-41.5896	-63.1917	-59.4876	-29.4826	12.6003	49.4918
58.7400	25.1083	-18.0617	-54.2500	-66.9095	-51.6159	-15.1277	27.3705
67.7559	47.9171	9.0100	-34.3391	-62.9618	-65.2899	-40.8292	-0.0031
65.3777	64.5113	35.1631	-8.5376	-48.4109	-68.1412	-60.0694	-27.9643
54.2384	69.3609	55.6404	18.7757	-25.8578	-59.8850	-69.6673	-51.7492
32.5657	63.1902	67.3054	43.1696	0.9109	-41.9890	-68.1936	-67.5786

Figure 9. One row of the original feature of the fingerprint replaced by zero row



-13.2515	-48.5150	-62.6468	-50.0396	-16.3391	24.1932	54.9296	63.7668
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
39.7504	-1.8382	-41.5896	-63.1917	-59.4876	-29.4826	12.6003	49.4918
58.7400	25.1083	-18.0617	-54.2500	-66.9095	-51.6159	-15.1277	27.3705
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
65.3777	64.5113	35.1631	-8.5376	-48.4109	-68.1412	-60.0694	-27.9643
54.2384	69.3609	55.6404	18.7757	-25.8578	-59.8850	-69.6673	-51.7492
32.5657	63.1902	67.3054	43.1696	0.9109	-41.9890	-68.1936	-67.5786

Figure 10. Two rows of the original feature of the fingerprint replaced by zero rows

-13.2515	-48.5150	-62.6468	-50.0396	-16.3391	24.1932	54.9296	63.7668
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
39.7504	-1.8382	-41.5896	-63.1917	-59.4876	-29.4826	12.6003	49.4918
58.7400	25.1083	-18.0617	-54.2500	-66.9095	-51.6159	-15.1277	27.3705
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
65.3777	64.5113	35.1631	-8.5376	-48.4109	-68.1412	-60.0694	-27.9643
54.2384	69.3609	55.6404	18.7757	-25.8578	-59.8850	-69.6673	-51.7492
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

Figure 11. Three rows of the original feature of the fingerprint replaced by zero rows

-13.2515	0.0000	-62.6468	-50.0396	-16.3391	24.1932	54.9296	63.7668
14.1556	0.0000	-57.4675	-62.1471	-40.5157	-1.9108	37.4970	62.6071
39.7504	0.0000	-41.5896	-63.1917	-59.4876	-29.4826	12.6003	49.4918
58.7400	0.0000	-18.0617	-54.2500	-66.9095	-51.6159	-15.1277	27.3705
67.7559	0.0000	9.0100	-34.3391	-62.9618	-65.2899	-40.8292	-0.0031
65.3777	0.0000	35.1631	-8.5376	-48.4109	-68.1412	-60.0694	-27.9643
54.2384	0.0000	55.6404	18.7757	-25.8578	-59.8850	-69.6673	-51.7492
32.5657	0.0000	67.3054	43.1696	0.9109	-41.9890	-68.1936	-67.5786

Figure 12. One column of the original feature of the fingerprint replaced by zero rows

-13.2515	0.0000	-62.6468	-50.0396	0.0000	24.1932	54.9296	63.7668
14.1556	0.0000	-57.4675	-62.1471	0.0000	-1.9108	37.4970	62.6071
39.7504	0.0000	-41.5896	-63.1917	0.0000	-29.4826	12.6003	49.4918
58.7400	0.0000	-18.0617	-54.2500	0.0000	-51.6159	-15.1277	27.3705
67.7559	0.0000	9.0100	-34.3391	0.0000	-65.2899	-40.8292	-0.0031
65.3777	0.0000	35.1631	-8.5376	0.0000	-68.1412	-60.0694	-27.9643
54.2384	0.0000	55.6404	18.7757	0.0000	-59.8850	-69.6673	-51.7492
32.5657	0.0000	67.3054	43.1696	0.0000	-41.9890	-68.1936	-67.5786

Figure 13. Two columns of the original feature of the fingerprint replaced by zero rows

-13.2515	0.0000	-62.6468	-50.0396	0.0000	24.1932	54.9296	0.0000
14.1556	0.0000	-57.4675	-62.1471	0.0000	-1.9108	37.4970	0.0000
39.7504	0.0000	-41.5896	-63.1917	0.0000	-29.4826	12.6003	0.0000
58.7400	0.0000	-18.0617	-54.2500	0.0000	-51.6159	-15.1277	0.0000
67.7559	0.0000	9.0100	-34.3391	0.0000	-65.2899	-40.8292	0.0000
65.3777	0.0000	35.1631	-8.5376	0.0000	-68.1412	-60.0694	0.0000
54.2384	0.0000	55.6404	18.7757	0.0000	-59.8850	-69.6673	0.0000
32.5657	0.0000	67.3054	43.1696	0.0000	-41.9890	-68.1936	0.0000

Figure 14. Three columns of the original feature of the fingerprint replaced by zero rows

-13.2515	0.0000	-62.6468	-50.0396	0.0000	24.1932	54.9296	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
39.7504	0.0000	-41.5896	-63.1917	0.0000	-29.4826	12.6003	0.0000
58.7400	0.0000	-18.0617	-54.2500	0.0000	-51.6159	-15.1277	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
65.3777	0.0000	35.1631	-8.5376	0.0000	-68.1412	-60.0694	0.0000
54.2384	0.0000	55.6404	18.7757	0.0000	-59.8850	-69.6673	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

Figure 15. Illustrating the combination of the zero row and column of the image

The ERO operations initially produce no different about the look of the cancellable template, the speed of the general process, and the matching performance of the process. All results are identical with all results that have been discussed in the previous sub-chapter. For example is an unchanged look of the cancellable template, it happens since minutiae are the feature used to generate the cancellable template. The following figure illustrates how augmenting process of zero row/column does not affect the look of the cancellable template.

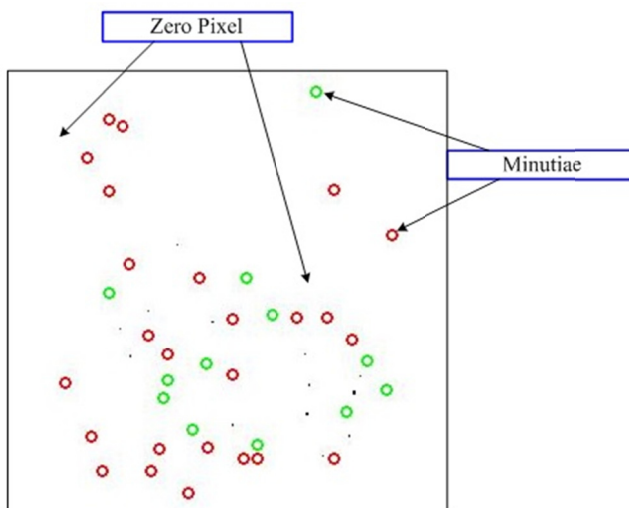


Figure 16. The unchanged look of the fingerprint features after the augmenting process of the zero row and column into the image

**7. Conclusions**

Establishing a cancellable template for a biometric technology such as fingerprint technology is a big challenge to be achieved especially related to a reissuing ability, a multi-application implementation, and a dependable issue. Implementation of several matrices operations and several fingerprint algorithm requirements becomes a

continuous approach to fulfil these three issues. Matrix application such as KP operation, ERO operation, and Inverse operation can be used as a solution to solve the issues number 1 and 2. Meanwhile, fingerprint regular steps such as fingerprint enhancement, core-point identification, region of interest, fingerprint classification, and minutiae extraction processes can be utilized to complete the last case.

Three kinds of evaluation i.e. error rates evaluation, time take evaluation, and matrices operations requirement evaluation; are performed in here to check the level/score of eleven different databases of the fingerprint. One of the evaluation shows that each database has its own characteristic depend on the type of the fingerprint acquired from the scanner of databases. If the scanner of the fingerprint produces a fingerprint with a good qualification, the error rate and the threshold of the database can be reliable as well as vice versa.

Furthermore, the time consuming along the execution process depends on the size of the input of the fingerprint. The time taken would be lessened if the size is small, vice versa. So then, for the small input of the fingerprint, even though one step would be augmented into the algorithm, the total time used of the process would not be changed significantly with the proviso that the size deficit of the input is not too thin.

Meanwhile, regarding to the implementation of the matrices operations, this procedure does not change the result or the character of the cancellable template as long as the used of the requirement of the matrices operation is not excessive.

## References

- Amengual, J. C., Juan, A., Prez, J. C., Prat, F., Sez, S., & Vilar, J. M. (1997). Real-Time Minutiae Extraction in Fingerprint Images. In *Proceeding of the 6<sup>th</sup> International Conference on Image Processing and Its Application* (pp. 871-875). <https://doi.org/10.1049/cp:19971021>
- Anton, H., & Torres, C. (2005). *Elementary Linear Algebra, Application Version: Ninth Edition*. Wiley eGrade.
- Bhattacharyya, D., Bandopadhyaya, S. K., Das, P., Ganguly, D., & Mukherjee, S. (2008). Statistical Approach for Offline Handwritten Signature Verification. *Journal of Computer Science, Science Publication*, 4(3), 181-185. <https://doi.org/10.3844/jcssp.2008.181.185>
- Bolle, R. M., Connell, J. H., & Ratha, N. K. (2002). Biometric perils and Patches. *Pattern Recognition*, 35(12), 2727-2738. [https://doi.org/10.1016/S0031-3203\(01\)00247-3](https://doi.org/10.1016/S0031-3203(01)00247-3)
- Boult, T. (2006). Robust Distance Measures for Face-Recognition Supporting Revocable Biometric Token. In *Proc. 7<sup>th</sup> Int. Conf. Autom. Face & Gesture Recog.* (pp. 560-566). [https://doi.org/10.1016/S0031-3203\(01\)00247-3](https://doi.org/10.1016/S0031-3203(01)00247-3)
- Bringer, J., Chabanne, H., & Kindarji, B. (2008). The Best of Both Worlds: Applying Secure Sketches to Cancellable Biometrics. In *Science of Computer Programming*, 74(1-2), 43-51. [https://doi.org/10.1016/S0031-3203\(01\)00247-3](https://doi.org/10.1016/S0031-3203(01)00247-3)
- Campisi, P., Maiorana, E., & Neri, A. (2008). On-line Signature Based Authentication: Template Security Issues and Countermeasures. In N. V. Boulgouris, K. N. Plataniotis, & E. Micheli-Tzanakou (Eds.), *Biometrics: Theory, Methods, and Applications*. Wiley/IEEE.
- Cappelli, R., Lumini, A., Maio, D., & Maltoni, D. (1999). Fingerprint Classification by Directional Image Partitioning. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 21(5), 402-421. <https://doi.org/10.1109/34.765653>
- Cardinaux, F., Sanderson, C., & Bengio, S. (2006). User Authentication via Adapted Statistical Models of Face Images. *IEEE Transaction on Signal Processing*, 54(1), 361-373. <https://doi.org/10.1109/TSP.2005.861075>
- Chikkerur, S., Ratha, N. K., Connell, H., & Bolle, R. M. (2008). Generating Registration-Free Cancellable Fingerprint Templates. In *BTAS08* (pp. 1-6).
- Daugman, J. G. (2003). The Importance of Being Random: Statistical Principles of Iris Recognition. *Journal of Pattern Recognition, Elsevier*, 36(2), 279-291. [https://doi.org/10.1016/S0031-3203\(02\)00030-4](https://doi.org/10.1016/S0031-3203(02)00030-4)
- Farooq, F., Bolle, R. M., Jea, T. Y., & Ratha, N. (2007). Anonymous and Revocable Fingerprint Recognition. In *Proc. Computer Vision and Pattern Recognition*. <https://doi.org/10.1109/CVPR.2007.383382>
- Furui, S. (1997). Recent Advances in Speaker Recognition. In *Proc. of International Conference on Audio and Video Based Biometric Person Authentication* (pp. 859-872). <https://doi.org/10.1109/CVPR.2007.383382>
- Ganorkar, S. R., & Ghatol, A. A. (2007). Iris Recognition: An Emerging Biometric Technology. In *Proc. Of the 6<sup>th</sup> WSEAS International Conference on Signal Processing, Robotics and Automation* (pp. 91-96).

- Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (2000). Filterbank-Based Fingerprint Matching. *IEEE Transaction on Image Processing*, 9(5), 846-859. <https://doi.org/10.1109/83.841531>
- Kanade, S., Petrovska-Delacretaz, D., & Dorizzi, B. (2009). Cancellable Iris Biometrics and Using Error Correcting Codes to Reduce Variability in Biometric Data. In *Proc. of IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 120-127).
- Kasaei, S., Deriche, M., & Boashash, B. (1997). Fingerprint Feature Extraction using Bloc-Direction on Reconstructed Images. In *IEEE region TEN Conf. Digital Signal Processing Applications* (pp. 303-306).
- Laub, A. J. (2005). Matrix Analysis for Scientists and Engineers. *The Society for Industrial and Applied Mathematics*, 139-142. <https://doi.org/10.1137/1.9780898717907>
- Lee, C., & Kim, J. (2010). Cancellable Fingerprint Templates using Minutiae-Based Bit-Strings. *Journal of Network Comp. Appl.*
- Lee, C., Choi, J., Toh, K., Lee, S., & Kim, J. (2007). Alignment-Free Cancellable Fingerprint Templates Based on Local Minutiae Information. *IEEE Trans. on Systems Man. And Cybernetics-B*, 37, 980-992. <https://doi.org/10.1109/TSMCB.2007.896999>
- Li, S. K., & Jain, A. K. (2004). *Handbook of Face Recognition*. New York: Springer Verlag.
- Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2003). *Handbook of Fingerprint Recognition*. New York: Springer-Verlag.
- Mukhaiyar, R. (2014). Alternative Approach in Generating Cancellable Fingerprint by using Matrices Operations. In *Proceeding of 56<sup>th</sup> International Symposium ELMAR-2014* (pp. 163-166). <https://doi.org/10.1109/ELMAR.2014.6923342>
- Mukhaiyar, R. (2017). Analysis of Galton-Henry Classification Method for Fingerprint Database FVC 2002 and 2004. *International Journal of GEOMATE*, 13(40), 118-123. <https://doi.org/10.21660/2017.40.92748>
- Mukhaiyar, R. (2017). Core-Point, Ridge-Frequency, and Ridge-Orientation Density Roles in Selecting Region of Interest of Fingerprint. *International Journal of GEOMATE*, 12(30), 146-150. <https://doi.org/10.21660/2017.30.tvet015>
- Nilsson, K., & Bigun, J. (2003). Localization of Corresponding Points in Fingerprints by Complex Filtering. *Pattern Recognition Letters*, 24, 2135-2144. [https://doi.org/10.1016/S0167-8655\(03\)00083-7](https://doi.org/10.1016/S0167-8655(03)00083-7)
- Ratha, N. K., Chikkerur, S., Connell, J. H., & Bolle, R. M. (2007). Generating Cancellable Fingerprint Templates. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29(4), 561-572. <https://doi.org/10.1109/TPAMI.2007.1004>
- Ross, A., & Govindarajan, R. (2005). Feature Level Fusion Using Hand and Face Biometrics. In *Proc. Of SPIE Conf. Biometric Technology for Human Identification II* (pp. 196-204). <https://doi.org/10.1117/12.606093>
- Schneir, B. (1999). Biometrics: Uses and Abuses. *Communications of the ACM*, 42(8), 1.
- Wayman, J. L., Jain, A. K., Maltoni, D., & Maio, D. (2005). *Biometric Systems: Technology, Design and Performance Evaluation*. New York: Springer Verlag. <https://doi.org/10.1007/b138151>
- Xu, W., & Cheng, M. (2008). Cancellable Voiceprint Template Based on Chaff-Points-Mixture Method. In *Proc. of International Conference on Computational Intelligence and Security* (pp. 263-266).
- Yang, B., Busch, C., Derawi, M., Bours, P., & Gafurov, D. (2009). Geometric-Aligned Cancellable Fingerprint Templates. In *Proc. of the 15<sup>th</sup> Int. Conf. on Image Analysis and Processing, LNCS*, 5716, 490-499.

### Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).