2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG) | 979-8-3503-2478-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/SEB-SDG57117.2023.10124538

Framework on Enhancing Biometric Template Protection Transformation Scheme Using Residue Number System

Omotosho Folorunsho Segun[1], Babatunde Ronke Seyi[2], Gbolagade Kazeem Alagbe[3]

[1,2,3]*Computer Science Department, Faculty of ICT, Kwara State University, Malete, Nigeria.*
funshosegun10@gmail.com ronke.babatunde@kwasu.edu.ng kazeem.gbolagade@kwasu.edu.ng

Abstract- ***Biometric technology was introduced into our applications and smart devices to provide a dependable approach to the problem of user authentication. However, study has proven that there are susceptible points in typical biometric systems which are prone to manipulation by hackers. The most concerned is biometric template attacks, reason for various biometric template techniques proposed by researchers in the literature to secure biometric raw template. The main challenge of most biometric template protection techniques is decrease in recognition performance when compare to unprotected system. Also, most of them required Auxiliary Data (AD) for verification. This study will leverage on features of Residue Number System (RNS) by integrating it with Biometric Template Protection (BTP) Transformation technique. The Model simulation was carried-out, the result generated shows that there was no reduction in recognition performance as compare to unprotected biometric system. Since RNS is a carry-free arithmetic and parallel operations, the overall computational time is less when compared to unprotected biometric system.***

Index Terms – Biometric, Traits, Template, Transformed, Residue Number System (RNS)

I. INTRODUCTION

Biometric technology offers a reliable identification of a person based on physiological or behavioral traits which includes fingerprint, face, iris, hand geometry, voice, palm print handwritten signatures and gait [1]. Reliability is one of the reasons for placing trust in in any recognition system [2].

We integrate biometric technology in our applications to provide a dependable approach to resolve the issues of rightful owner in identification management system [3]. Biometric technology helps to resolve the issue of rightful owner to an applications or devices through authentication [4]. It bond digital data to our identity in a consistent and unambiguity manner.

Security Threats with biometric technology.

Security threats refers to risks that can arise as a result of using biometric system due to certain points in biometric system which an intruders can use to sabotages the system. Researches have shown that all these points are viable entries of attack to the system [2]. The most devastating of these attacks, is the one targeted against the biometric template. This poses great danger because biometric template is derived from an individual trait which cannot be revoked, hence, the need for biometric template protection algorithms [5].

Characteristics of Ideal Template Protection Scheme

An excellent biometric template protection technique must satisfy certain criteria/conditions as stated in ISO/IEC 24745: (2011), [6] and 30136: (2018), [7] on biometric template protection [31]. The four points are highlighted below:

(1) Diversity: it should not allow the use of the template secured to gain access to other databases that uses the same traits, so that the user's privacy can be ensured.

(2) Revocability: Once the template is compromised the scheme should allow retract of it, and a new one reissue based on the same biometric data.

(3) Security: Computationally obtained original biometric template from the secured template should not be easy.. This characteristic prevents an adversary from developing a physical spoof of the biometric trait from a stolen template.

(4) Performance: There should be no decline in recognition performance when compare to unprotected system.

The main issue is, how to design a scheme to satisfy the above conditions [8, 9]? This study will leverage on security provided by RNS features through its forward conversion to secure a biometric template. .

The outline is as follows: Section II extensively examined related works that has been carried out on biometric template protection transformation techniques Section III provides an insight to residue number system. While section IV gives detailed explanation of the proposed framework with evaluation metrics to be

Authorized licensed use limited to: Durban University of Technology. Downloaded on May 23,2023 at 12:16:50 UTC from IEEE Xplore. Restrictions apply.

used Section V present the model simulation and discuss on the performance based on the results obtained, conclusion in section VI.

II. LITERATURE REVIEW

A. Issues with biometric template protection techniques proposed in the literature.

Despite desperate efforts to secure biometric technology through various proposed biometric template protection techniques, there still exists unresolved issue associated with most of those techniques. Especially, diminishing in recognition performance when compare to unprotected system. Also, most of them required Auxiliary Data (AD) for verification. Some of these techniques are depicted in the table 1 below.

TABLE 1: Review of Template Protection Schemes Proposed in the Literature

Authors	**Techniques**	**Open issue**
Jain. et al, 2008, [9]	Salting transform	The problems for users to keep & not forget secrete key
Nagar et al, 2010, [10]	Biophaser	It is easy to invert when the key is known to adversary
Kareem Kamal et al, 2012, [12]	Non-invertible transform	It is easy for an impostor to invert when the key is known .
Ghany et al, 2012, [13]	Hybrid (transformation with cryptosystem)	The difficulty of generating key.
Bringer J. et al, 2013, [14]	Homomorphic encryption	Slightly high in computational time and communication overhead
Zhe et al, 2016, [16]	Key binding (fuzzy vault)	It is possible to statistically analyze points in vault and use it to stage attack.
Marta Gomez-Barrero et al, 2017, [17]	Multi-biometric template protection based on Homomorphic Encryption	Higher computational time of operation
Loubna Ghammam, Morgan Barbier, Christophe Rosenberger, 2018, [18]	Enhancing the Security of Transformation Based Biometric Template Protection Schemes.	The need of seed, inform of secret key.
Luca Debiasi et al, 2019, [3]	Biometric Template Protection in the Image Domain Using Non-invertible Grey-scale Transforms	The proposed schemes offer a trade-off between recognition performance loss and unlinkability in most cases.
C. Kant and S. Chaudhary, (2020), [19]	A Watermarking Based Approach for Protection of Templates in Multimodal Biometric System"	Increase complexity and storage space
B. Samira, R. H. Lamia and E. B. A. Najoua (2021), [22]	Biometric Template Security Using Watermarking Reinforcement Based Cancellable Transformation.	The need for helping data in form of secret key floor the second cancellable transformation
Lahmidi, A., Moujahdi, C., Minaoui, K. et al.(2022), [22]	On the methodology of fingerprint template protection schemes conception:	The system may be compromised when the key is stolen.

Authorized licensed use limited to: Durban University of Technology. Downloaded on May 23,2023 at 12:16:50 UTC from IEEE Xplore. Restrictions apply.

	meditations on the reliability	

III. INSIGHT TO RESIDUE NUMBER SYSTEM (RNS)

A residue number system (RNS) is numeral systems that represent integers by their values modulo, using several pairwise coprime integers called the moduli. RNS speed up arithmetic operations by splitting numbers into smaller parts in such a way that each unit is independent of the other [24,25]. It is based on the congruence relation which explains that two (2) integers a and b are said to be in congruent modulo m if m divides exactly the difference of a and b; mathematically represented as a≡b(mod m). E.g 10≡4(mod 3) If q and r are the quotient and remainder respectively of integer division of a by m that is a=q.m+ r then by definition a≡r(mod m)where r=⟦|a|⟧_m, that is, r is the residue of a with respect to m. The number m is a modulus or base and we shall assume that its value excludes unity which produces only trivial congruencies [27].

RNS is capable of uniquely representing all integers X that lie in its dynamic range, that is, (0≤X<M) where the dynamic range (M) is determined by the multiplication of the moduli sets.

A. RNS Architectures

The architectures of RNS is made up of three (3) components;

a) Forward converter,
b) Residue arithmetic units
c) Reverse converter.

In any RNS design, input operands are given in either binary or decimal format and must be converted to RNS notation before computation can be performed. The final results must be re-presented in the same way as the input operands. Hence, the need for a forward and reverse processor in RNS designs [25, 29].

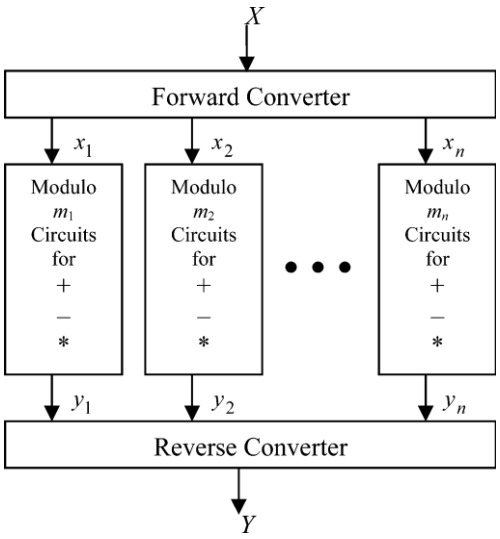


Figure.1. Diagrammatic representation of a typical RNS system [24]

The result of arithmetic operations of RNS forward conversion must be converted back into its corresponding weighted binary number before using it outside of RNS.

B. Residue Representation

In RNS, the base consists of an N-tuple of integers, ⟦{m_i}⟧_(i=1)^N where individual member is called a modulus.

Given any base, the RNS representation,⟦{r_i}⟧_(i=1)^N where r_i are integers defined by a set of N equations

$$x = q_i m_i + r_i \quad \ldots\ldots (1)$$

i = 1, 2, … N and q_i is an integer so chosen that 0≤r_i<m_i . It is clear that q_iis an integer value of the quotient x⁄m_i which is denoted by ⌊x⁄m_i ⌋.

The quantity r_i is the least +ve integer remainder of the division of x by m_i and is denoted as x mod m_i, i.e., ⟦|x|⟧_(m_i). (1) this can simply be re-written as;

$$x = m_i [x/m_i] + ⟦|x|⟧_{(m_i)} \quad \ldots (2)$$

C. Arithmetic Operations

The standard arithmetic operation of addition/subtraction and multiplication are easily implemented with residue notation depending on the choice of moduli, but division operation is much more difficult, since it is not a closed operation. [26].

D. Forward Conversion

This is performed by a forward converter through decomposing of a weighted binary number into a residue represented number using the specify moduli set, that is, it is the conversion from a conventional

Authorized licensed use limited to: Durban University of Technology. Downloaded on May 23,2023 at 12:16:50 UTC from IEEE Xplore. Restrictions apply.

representation to a residue one by dividing the number X by each of the given moduli and then collect their remainder [27]. As an example, given moduli set {3, 4, 5}, the number 8 can be represented in RNS as:

$$x_i = |X|_{m_i} \ldots\ldots (3)$$

$$x_1 = |X|_{m_1} = |8|_3 = 2;\ x_2 = |X|_{m_2} = |8|_4 = 0\ ;x_3 = |X|_{m_3} = |8|_5 = 3$$

Thus, the RNS representation of 8 is$(2, 0, 3)_{RNS(3,4,5)}$.
The basic technique in converting binary to RNS was presented by [26, 27].

E. Reverse Converter

The conversion from residue notation to a conventional one (binary or decimal representation) is known as reverse conversion. Two (2) most widely used techniques of reverse conversion are the Chinese Remainder Theorem (CRT) and Mixed Radix Conversion (MRC). Many other methods have been devised but are still based on the CRT and MRC [29].

F. FEATURES OF RESIDUE NUMBER SYSTEM

RNS possesses coherent and unique properties which are:

FI. Parallelism of operation

Operations of addition, subtraction, and multiplication are performed on RNS numbers in parallel without carry propagation between residue digits. Each modulus of the moduli set has its own arithmetic processor that consists of a Modulus Adder, a Modulus Subtractor, and a Modulus Multiplier. This resulted in high-speed addition, subtraction, and multiplication.

FII. Unstructured number system

The digits are not arranged on particular order.

FIII. Unweighted number

In RNS representation carries no weight information unlike the binary and decimal number system, therefore, error in one digit position cannot affects another digit position.

FIV. Choice Of Moduli Selection

Choice of moduli set has effect on the speed, dynamic range and hardware complexity of RNS architecture.
Moduli selection in RNS can be divided into two restricted and unrestricted.
The moduli set should not be large so that the operations modulo will require minimum computational time to complete [28, 30, 26].
The moduli selection should be given a major consideration when designing a RNS system.

IV. THE PROPOSED SYSTEM

A simple approach to secure a biometric system would be to integrate RNS with the biometric template protection transformation algorithm as shown in figure 2. Carry-free arithmetic is one of the features of RNS thus, arithmetic operations such as integer addition, subtraction and multiplication computation are done independently and in parallel in each of the channels [30].
RNS will also, eliminate the need to remember auxiliary data during verification.
Thus, BTP algorithm based on RNS will be faster due to its parallel computing nature.

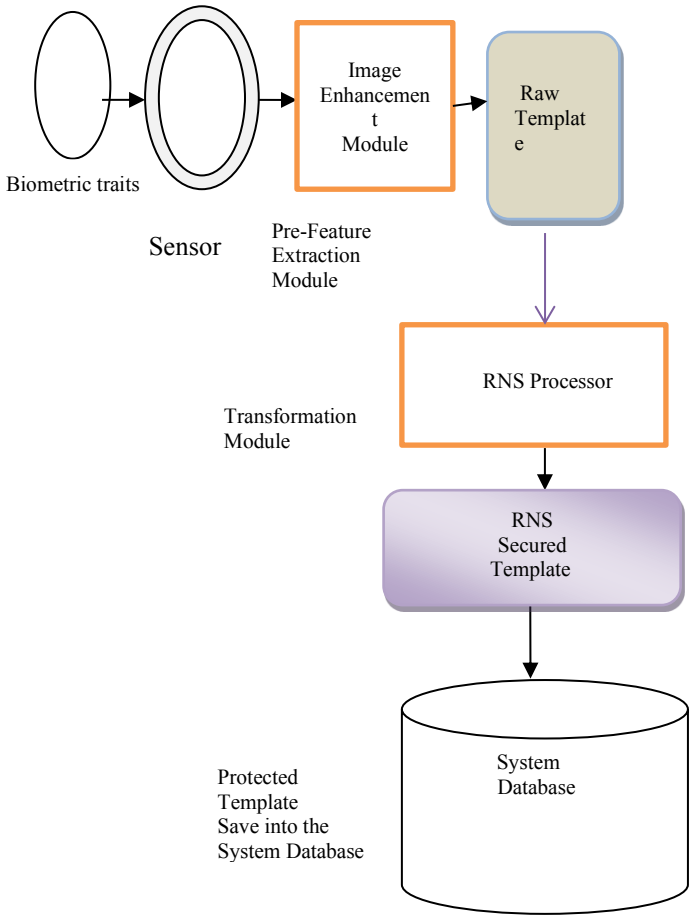


Figure 2: Architectural Framework of RNS Template Protection Scheme

Authorized licensed use limited to: Durban University of Technology. Downloaded on May 23,2023 at 12:16:50 UTC from IEEE Xplore. Restrictions apply.

A. Design Approach

There are two phases to the designed. Phase one deal with the Enrollment that is acquired of dataset. Then, second phase, verifications, implemented through testing.

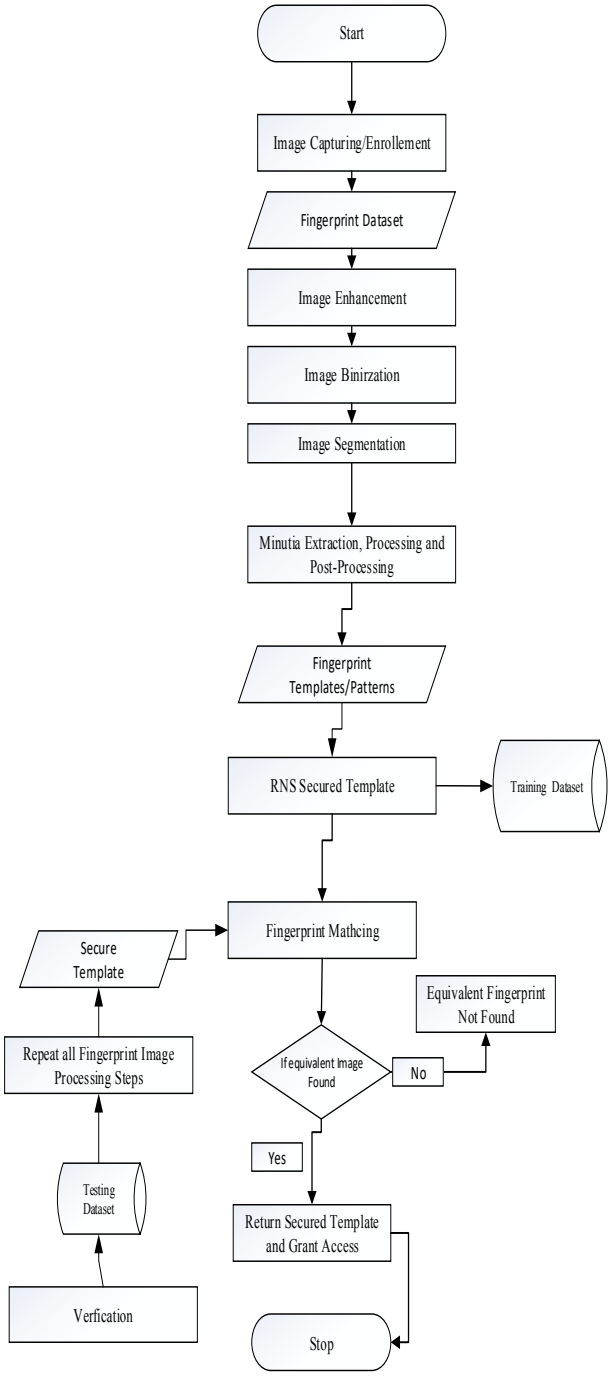


Figure 3: System flowchart of the scheme

B. Design Process

The scheme will be designed to secure biometric template using the Residual Number System. The developed model will be subjected to integrity and efficiency test to validate it. Experimentation of the secured model will be carried out using a step-wise image processing on acquired fingerprint images. The dataset to be used for the experiments will be taken from fingerprint datasets, FVC 2002 DB1. The FVC 2002 was the Second International Competition for Fingerprint Verification Algorithm. Histogram equalization and Gabor filter will be used for image enhancement. Then, image binarization which will be followed by image segmentation using block direction estimate, the next approach will focus on minutia extraction which comprises of thinning, after the minutia extraction stage the minutia post processing which will comprises of false minutia removal, termination and bifurcation. The template generated will then be protected by the residual number system using the forward conversion process before the template matching is carried out as shown figure 3.

BI. Secure Template Generation

After the fingerprint image has undergone standardized images processing stages and raw template extracted. The forward conversion process of the RNS is will be used to secure the raw template.

BII. Forward Conversions

A weighted binary number is decomposes into a residue represented number by forward converter based on moduli set used for the operation.

BIII. Choice of moduli set

The moduli set value of m1 = 3, m2 = 4, m3 = 5, having used $\{2n\text{-}1, 2n, 2n+1\}$ with value of n at 2, will be used for the implementation. The RNS forward conversion will help to generate a secured three share image that will act as input layer to the matching stage.

BIV. Matching

When all detail from two fingerprint images is extracted in the chosen area of interest for verification, a minutia matching is done.

BV. Technical Performance Evaluation Metrics

ISO/IEC 24745 international standard on biometric template protection stated that any protection techniques

Authorized licensed use limited to: Durban University of Technology. Downloaded on May 23,2023 at 12:16:50 UTC from IEEE Xplore. Restrictions apply.

should not depreciate in recognition performance when compare to unprotected system.

a) Recognition accuracy of the scheme

The proposed technique will be subjected to standard known accuracy metrics such as:

- True Acceptance Rate (TAR)
- True Rejection Rate (TRR)

False Rejection Rate (FRR)

- False Acceptance Rate (FAR)
- Equal Error Rate

b) Storage Space Requirement

c) Throughput

BVI. Resistance of the proposed scheme to attacks

The scheme will be subjected to the following attacks so as to test the strength the of the system to attacks.

i) Zero effort attack
ii) Brute force attack
iii) Stolen biometric data attack
iv) Listening attack

V. MODEL SIMULATION

The developed systems made use of various component environments in MatLab.
The DB1 used for the experimental analysis of this framework is as shown in table 2.
A total of 80 fingers were used

Table 2: Database setup of Fingerprint images

Parameters	**Value**
Total Number of images	80
Total number of Training sets	20
Number of Testing Sets Used	60
Total number of impression per finger	8
Total number of person per class	10
False Fingerprint impression Class	10

A. Interactive Developmental Stage

The user interface below in figure 4 shows the collaboration of the two major phases and the database clearing stage.

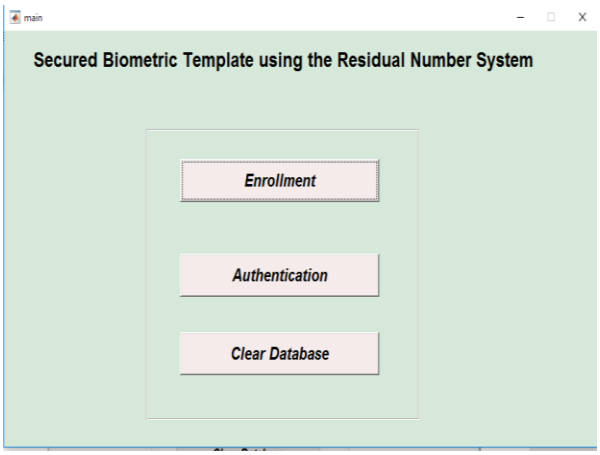


Figure 4: Collaborative Interface for the developed system

B. RNS Secured Template

The minutiae generated was secured by the using the forward conversion process of the residual number system with moduli sets value of m1 = 3, m2 = 4, m3 = 5, having used {2*n*-1, 2*n*, 2*n* +1} with value of n at 2. The result helps to enhance fingerprint template by converting the minutiae into residues, the obtained results are shown in the figure 5a and 5b respectively below:



Figure 5a: RNS Secured template

Authorized licensed use limited to: Durban University of Technology. Downloaded on May 23,2023 at 12:16:50 UTC from IEEE Xplore. Restrictions apply.

	1	2
1	333	
2	555	
3	666	
4	666	
5	666	
6	666	
7	666	
8	666	
9	666	
10	666	
11	666	
12	666	
13	666	
14	666	
15	666	
16	666	
17	666	
18	666	

Figure 5b Aggregation of the residues

The figure 5a shows the secured template generated for two fingerprints input by a subject, while the figure 5b highlights the aggregation of the residues.

C. Authentication stage

The authentication stage provides the platform to test the model with probe finger print images that are not enrolled, this process also followed the same pattern as that of enrolment, the probe finger print image input image is filtering by Gabor, binirazation, thinning, minutiae extraction, lastly, converting the minutiae to residues which is then allotted to the matching algorithm. The generated residue is matched with saved residue in the system database for yes or no action.
Threshold for the matching phase was set at values between 0.48 - 1. The correctly classified images return values that are between the threshold ranges.

D. Recognition Performance Evaluation

This section presents the results of the evaluation of the model using widely known performance evaluation indices in biometric recognition system. This includes; false acceptance rate, false rejection rate and recognition accuracy.

DI. False Acceptance Rate (FAR) – This is used to measure the instances of the biometric system, when it wrongly accepts a user that has not enrolled in the system.

FAR is the ratio of the number of false acceptance divided by the number of identification attempts as shown in Equation 4.

$$FAR = \frac{number\ of\ false\ acceptance}{number\ of\ identification\ attempts} = \frac{FP}{FP+TN} \quad (4)$$

Where FP denote false positive (number of impostor images not classified in the database) and
TN denotes the true negative (number of impostor images wrongly classified in the database).

DII. False Rejection Rate (FRR) – This is measure of rate at which the biometric system wrongly reject a legitimate user.

A system of FRR can be defined as the ratio of the number of false rejection divided by the number of identification attempts as shown in equation 5

$$FRR = \frac{False\ rejection}{number\ of\ identification\ attempts} = \frac{FN}{TP+FN} \quad (5)$$

Where;

- FN denotes false negative (number of images wrongly mismatched during classification).
- TP denotes true positive (number of images correctly matched during classification).

DIII. Recognition Accuracy (RA)

The recognition accuracy is measured by the percentage of the recognition of fingerprint per total number of tested fingerprint images of the same person. This is shown in equation 6

$$\text{Recognition Accuracy (\%)} = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (6)$$

Where:
TP represents true positive
TN represents true negative
FP represents false positive
FN represents false negative

Authorized licensed use limited to: Durban University of Technology. Downloaded on May 23,2023 at 12:16:50 UTC from IEEE Xplore. Restrictions apply.

Table 3 Probe Fingerprint images Result

Technique	True Positive	False Positive	True Negative	False Negative
Fingerprint Developed Model	**58**	**1**	**9**	**2**

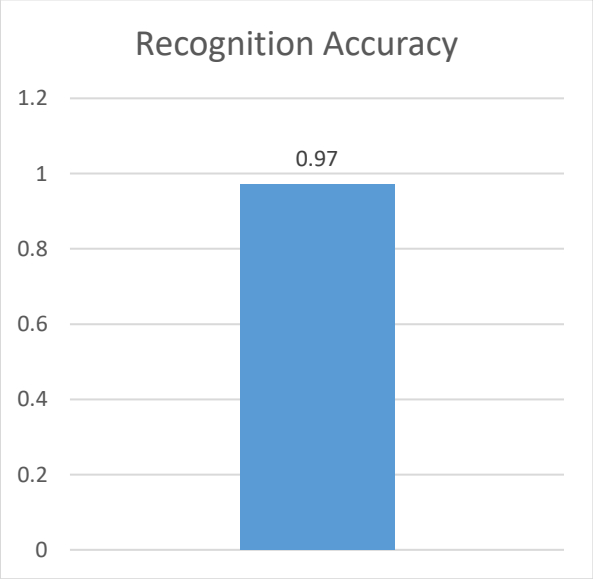
E. Comparative Performance Evaluation

EI. Recognition Accuracy

The Table 4 shows that the developed model was able to attain a recognition accuracy of 97%.

Table 4 Evaluation Result

Metric	True Positive
False Rejection Rate (FRR)	**0.02**
False Acceptance Rate (FAR)	**0.1**
Accuracy	**0.97**



The figure 6: Recognition Accuracy

EII. Enrolment Time

The enrolment time as depicted in table 5a and 5b shows the execution time for each algorithm to complete the cycle of their operation or processing for enrollment of fingerprint template. The results were listed based on the inclusion of RNS and without RNS.

Table 5 (a): Enrolment result without RNS

Fingerprint Samples	Enrollment Time
Sample 1	20.1507
Sample 2	19.3595
Sample 3	19.3342
Sample 4	19.3237
Sample 5	19.3497
Sample 6	19.198
Sample 7	19.2138
Sample 8	19.3134
Sample 9	18.7695
Sample 10	20.459

Table 5 (b): Enrolment result with the inclusion of RNS

Fingerprint Samples	Enrollment Time
Sample 1	33.0144
Sample 2	32.8271
Sample 3	33.5421
Sample 4	31.0175
Sample 5	40.3276
Sample 6	33.7723
Sample 7	33.8543
Sample 8	33.4126
Sample 9	32.7577
Sample 10	32.4063

EIII. Comparative results based on average of the total samples

The average enrolment time as depicted in table 6 shows the execution time for each algorithm to complete the cycle of their operation or processing of enrolling users in the system database, the graph as shown in figure 7 indicate that the enrollment of the fingerprint template without RNS outperformed the RNS based in terms of computational time, as its enrollment took a lesser time since it's a direct saving of the raw template into the system database.

Authorized licensed use limited to: Durban University of Technology. Downloaded on May 23,2023 at 12:16:50 UTC from IEEE Xplore. Restrictions apply.

Table 6: Average Enrolment Time

	Avg. Enrollment Time
Enrollment without RNS	19.44715
Enrollment with RNS	33.69319

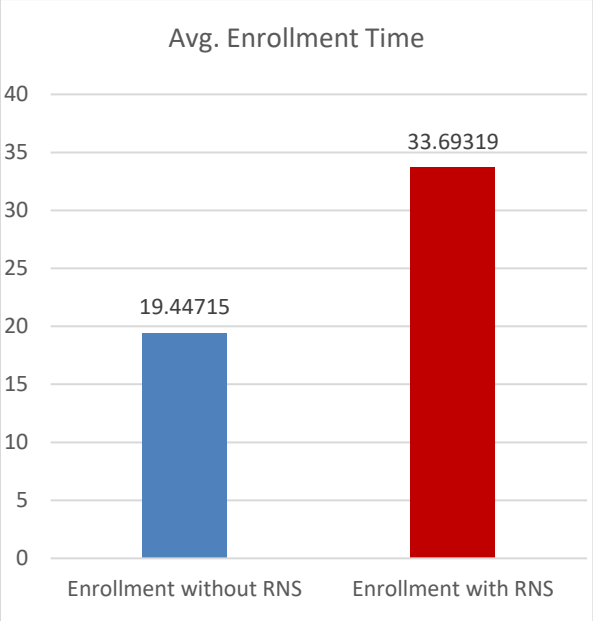


Figure 7: Average Enrolment Time

EIV. Authentication Time

The authentication time as depicted in table 6a and 6b shows the execution time for each algorithm to complete the cycle of their operation or processing of authenticating a fingerprint template. The results were listed based on the inclusion of RNS and without RNS.

Table 6 (a): Authentication result without the inclusion of RNS

Fingerprint Samples	Authentication Time
Sample 1	6.9319
Sample 2	25.9822
Sample 3	15.4315
Sample 4	7.8123
Sample 5	22.2099
Sample 6	15.2379
Sample 7	8.2909
Sample 8	10.1744
Sample 9	9.4433
Sample 10	6.1342

Table 6 (b): Authentication result with inclusion of RNS

Fingerprint Samples	Authentication Time
Sample 1	0.40394
Sample 2	0.37983
Sample 3	0.35737
Sample 4	0.38043
Sample 5	0.39689
Sample 6	0.54845
Sample 7	0.41364
Sample 8	0.39976
Sample 9	0.45671
Sample 10	0.42356

EV. Comparative results based on average of the total samples

The average authentication time as depicted in table 6 shows the execution time for each algorithm to complete the cycle of their operation or processing of retrieving and matching a secured template, the graph as depicted in figure 8 gives a clear indication that the authentication of the fingerprint template with RNS based secured outperformed the ordinary one without the RNS in terms of computational time, as its retrieval took a lesser time.

Authorized licensed use limited to: Durban University of Technology. Downloaded on May 23,2023 at 12:16:50 UTC from IEEE Xplore. Restrictions apply.

Table 7: Average Authentication Stage

	Authentication Time
Authentication with RNS	0.416058
Authentication without RNS	12.76485

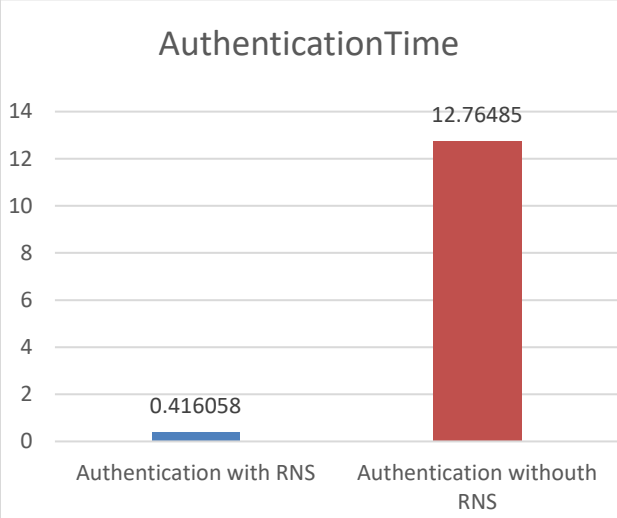


Figure 8: Average Authentication time

EVI. Comparison with previous work on transformation techniques

Based on previous work on biometric template protection transformation schemes, recognition accuracy has been a major issue due to the fact that, most of these techniques diminish in recognition performance when compare to unprotected biometric system. The proposed technique has a good fingerprint differentiating rate of 97%, which show a significant improvement in recognition accuracy of biometric template protection transformation techniques. Furthermore, there was reduction in execution time for each algorithm to complete the cycle of operation of retrieving and matching a secured template for match action.

VI. CONCLUSION

The paper started by stating privacy protection as the main reason for integrating biometric technology in our application and smart devices. However, we should not put our privacy and security concern in this technology, as certain loop holes has been identified in a biometric system, which hackers can manipulate to break into the system. The most devastating attack is the one stage against the biometric template. Hence, various techniques were propounded to secure the raw template. But most of these techniques raised one or more issues of challenges when compare to unprotected system. Therefore, the paper proposed a RNS based biometric template protection technique. . The technique will leverage on some of features of RNS such as carry-free arithmetic, parallel operations and choice of moduli set selection.

Model simulation was carried-out, the result generated shows that there was no reduction in recognition performance as compare to unprotected biometric system, which is a major issue in most biometric protection template transformation techniques. Also, there was a clear indication that the authentication of the fingerprint template with RNS based secured, outperformed the ordinary one without the RNS in terms of computational time, as its retrieval took a lesser time. Conclusively, template protection algorithm based on RNS system will achieves good recognition accuracy, faster operation and eliminate the need to remember any secrete key during verification

ACKNOWLEDGEMENTS

We sincerely commend the effort of researchers that has done a great work in this research field.

References

[1] A. K. Jain, A. Ross and U. Uludag, (2005), " Biometric Template Security: Challenges and Solutions", Proc. 13th European Signal Processing Conference (EUSIPCO), Antalya, Turkey,

[2] A. K. Jain, D. Deb, and J. J. Engelsma (2021), Biometrics: Trust, but verify, arXiv preprint arXiv:2105.06625,

[3] Luca Debiasi, Simon Kirchgasser, Bernhard Prommegger, Andreas Uhl, Artur Grudzie´n and Marcin Kowalski,.(2019), "Biometric Template Protection in the Image Domain Using Non-invertible Grey-scale Transforms" 978-1-7281-3217-4/19/$31.00 © IEEE

[4] Jain A. K, (2015), Biometric System Security, Dept. of Computer Science and Engineering Michigan State University, http://biometrics.cse.msu.edu

[5] Campisi, P. (2013). Security and privacy in biometrics: towards a holistic approach. In Security and Privacy in Biometrics (pp. 1-23). Springer London.

[6] Information Technology Security Techniques Biometric Information Protection, (2011), Standard ISO/IEC 24745

Authorized licensed use limited to: Durban University of Technology. Downloaded on May 23,2023 at 12:16:50 UTC from IEEE Xplore. Restrictions apply.

[7] Information Technology Performance Testing of Biometric Template Protection Schemes, (2018), Standard ISO/IEC 30136
[8] K. Nandakumar and A. K. Jain, (2015), "Biometric Template Protection Schemes: Bridging the Performance Gap Between Theory and Practice", IEEE Signal Processing Magazine, Vol. 32, No. 5, pp. 88-100, September.
[9] A. K. Jain, K. Nandakumar and A. Nagar, (2008), "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, Special Issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics, January.
[10] A. Nagar, K. Nandakumar, A. K. Jain, (2010), "Biometric Template Transformation: A Security Analysis",Proc. of SPIE, Electronic Imaging, Media Forensics and Security XII, San Jose, Jan
[11] Rathgeb, C., & Uhl, A. (2011). "A survey on biometric cryptosystems and cancelable biometrics", EURASIP Journal on Information Security
[12] Kareem Kamal, Ghany A., Hesham A. , Hefny Aboul, Hassanien E., Neveen I., Ghali I. (2012) A Hybrid approach for biometric template security. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2012
[13] Ghany, K. K. A., Hefny, H. A., Hassanien, A. E., & Ghali, N. I. (2012). A hybrid approach for biometric template security. In Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012) (pp. 941-942). IEEE Computer Society.
[14] J. Bringer, H. Chabanne, and A. Patey, (2013), "Privacy-Preserving Biometric Identification Using Secure Multiparty Computation: An Overview and Recent Trends," IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 42–52
[15] Poongodi, P., & Betty, P. (2014),. A Study on Biometric Template Protection Techniques. International Journal of Engineering Trends and Technology (IJETT), 7(4).
[16] Zhe Jin , Andrew Beng Jin Teoh, Bok-Min Goi, Yong-Haur Tay. (2016), Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation. Journal homepage: www.elsevier.com/locate/pr, 0031-3203/ 2016 Elsevier Ltd.
[17] Marta Gomez-Barrero, Emanuele Maiorana, Javier Galbally, Patrizio Campisi , Julian Fierrez, ((2017), "Multi-biometric template protection based on Homomorphic Encryption " www.elsevier.com/locate/patcog, Pattern Recognition 67 149–163
[18] Loubna Ghammam, Morgan Barbier, Christophe Rosenberger, (2018),. Enhancing the Security of Transforma-tion Based Biometric Template Protection Schemes. CyberWorlds, Oct Singapour, Singapore. hal-01862157
[19] C. Kant and S. Chaudhary, (2020), "A Watermarking Based Approach for Protection of Templates in Multimodal Biometric System", Proc. Computer Science, pp. 932-941,
[20] Ilaiah Kavati, A. Mallikarjuna Reddy, E. Suresh Babu, K. Sudheer Reddy, Ramalinga Swamy Cheruku, (2021), Design of a fingerprint template protection scheme using elliptical structures, ICT Express, Volume 7, Issue 4, , Pages 497-500, ISSN 2405-9595
[21] B. Samira, R. H. Lamia and E. B. A. Najoua, (2021), "Biometric Template Security Using Watermarking Reinforcement Based Cancellable Transformation," International Conference on Cyberworlds (CW), 2021, pp. 270-277, doi: 10.1109/CW52790..00052.
[22] Lahmidi, A., Moujahdi, C., Minaoui, K. (2022).. On the methodology of fingerprint template protection schemes conception: meditations on the reliability. EURASIP J. on Info. Security. .
[23] KIM, J.; Jung, Y.G.; Teoh, A.B.J. (2022), Multimodal Biometric Template Protection Based on a Cancelable SoftmaxOut Fusion Network. Appl. Sci., 12, https://doi.org/10.3390/
[24] Neha Singh, (2008), "An overview of Residue Number System" National Seminar on Devices, Circuits & Communication November 06th – 07th, Organized by Department of ECE, B.I.T, Mesra, Ranchi- 835 215
[25] Gbolagade, K. A., & Cotofana, S. D. (2009). Residue-to-decimal converters for moduli sets with common factors. In 2009 52nd IEEE International Midwest Symposium on Circuits and Systems (pp. 624-627).
[26] Baagyere E. Y., Boateng K.O., & Gbolagade K. A. (2011). Bioinformatics: An important Application Area of RNS: Journal of Engineering and Applied Sciences 6(2): 174 -179.
[27] Omondi, A., Premkumar, B. (2007). Advances in Computer Science and Engineering: Texts. London, Imperial College Press
[28] Abdelfattah, O. (2011). Data Conversion in Residue Number System (Doctoral dissertation, McGill University), Canada.
[29] Gbolagade, K. A., Chaves, R., Sousa, L., & Cotofana, S. D. (2010). An improved RNS reverse converter for the ⟦{2⟧^(2n+1)-1,2^n,2^n-1} moduli set. In Proceedings of 2010 IEEE International Symposium on Circuits and Systems (pp. 2103-2106).
[30] Mohan P. A. (2012), Residue Number Systems: Algorithms and Architectures. Kluwer Academic Publishers. New York, NY, USA.
[31] P.Sangeetha, Mrs.B.Revathy, 2013, Secure Multibiometric Cryptosystems Using Biohashing, International Journal of Engineering Research & Technology (IJERT) ICSEM – 2013 (Volume 1 – Issue 06).

Authorized licensed use limited to: Durban University of Technology. Downloaded on May 23,2023 at 12:16:50 UTC from IEEE Xplore. Restrictions apply.