Research Article

Low Quality Fingerprint Template Encryption Algorithm

Amjad Ali[1], Muhammad Amir[2]*, Bilal Ur Rehman[2], Zafar Khan[3] and Abid Munir[1]

[1]Department of Electrical Engineering, UET, Jalozai Campus, Khyber Pakhtunkhwa, Peshawar, Pakistan; [2]Department of Electrical Engineering, UET, Khyber Pakhtunkhwa, Peshawar, Pakistan; [3]Faculty of Engineering and IT, Northern University, Nowshera, Khyber Pakhtunkhwa, Pakistan.

Abstract: Nowadays, biometric data protection is one of the main security parameters to be looked after. In fingerprint processing, initially, appropriate proven methods are used for processing fingerprints in a sequential manner followed by the application of various encryption algorithms for ensuring protection of such biometric data. In fingerprinting, image processing techniques include: low-quality-fingerprint enhancement, normalization, binarization and thinning of fingerprint image followed by feature extraction. In this paper, a novel encryption method for minutiae based low-quality-fingerprint framework is proposed. The proposed encryption algorithm works through addition of spurious information to the originally extracted fingerprint data. The addition of spurious information is in correlation with the originally extracted features. The proposed approach is best suited for minutiae based information encryption and the proposed encryption algorithm has been tested using the standard fingerprint verification competition database (FVC-DB1-2002). The image processing techniques, the proposed encryption technique and the results were processed using MATLAB. The empirical results presented in this paper demonstrate an overall improvement through the proposed approach as the similarity standards are almost distinct. Moreover, results of the proposed technique exhibit the weakest of correlations between the original and encrypted data during extraction of low quality fingerprints thus enhancing verification and data protection.

Received: 12 October 2021; **Accepted:** 24 December 2021; **Published:** 28 December 2021
***Correspondence:** Muhammad Amir, Department of Electrical Engineering, UET, Khyber Pakhtunkhwa, Peshawar, Pakistan; **Email:** amir@nwfpuet.edu.pk
Citation: Ali, A., M. Amir, B.U. Rehman, Z. Khan and A. Munir. 2021. Low quality fingerprint template encryption algorithm. *Journal of Engineering and Applied Sciences,* 40(2): 91-99.
DOI: https://dx.doi.org/10.17582/journal.jeas/40.2.91.99
Keywords: Fingerprinting, FVC2002, Minutiae, Encryption security, Decryption correlation

Introduction

Human fingerprints consists of edges and valleys that consolidates a structure which is unique for every individual. These fingerprints develop during the fetal development inside the mother's womb and remain unchanged for the rest of one's life. Furthermore, it has been proved that no two individuals have similar fingerprints (Anil *et al*., 2016; Patil *et al*., 2011). Fingerprints have astonishing permanency and uniqueness for the term of time. Amongst the biometric traits, fingerprints offer more secure, true person recognition verification than passwords and key cards (Maltoni *et al*., 2009). Figure 1 depicts the architecture of an automatic fingerprint recognition system (Li-Kuo, 2010). Fingerprint image acquisition device is the user interface of the recognition system and consists of an image sensor that captures the fingerprint image when properly placed on it. Fingerprint image scanner plays a vital role in the recognition of an individual and has been comprehensively studied in the recent research publications and patents. After the image is obtained by the fingerprint scanner, it is preprocessed before the extraction of valuable ridge features mentioned above. At this stage, the fingerprint acquired from the scanner is analyzed and processed before the matching process. The main processes required for minutiae extraction include fingerprint image segmentation, enhancement, binarization and thinning as shown in Figure 2. Depending upon the algorithm used by the matching module, feature extraction module extracts different ridge features such as minutiae (ridge ending and ridge bifurcation), singular points (core and delta) and ridge orientation or image texture features like contrast, correlation, homogeneity and variance.

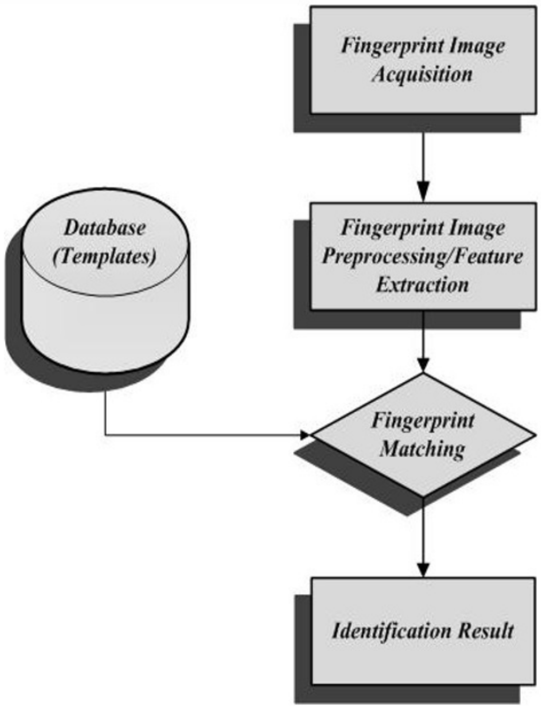

Fingerprint Image Acquisition
Database (Templates)
Fingerprint Image Preprocessing/Feature Extraction
Fingerprint Matching
Identification Result

Figure 1: *Automatic fingerprint recognition system.*

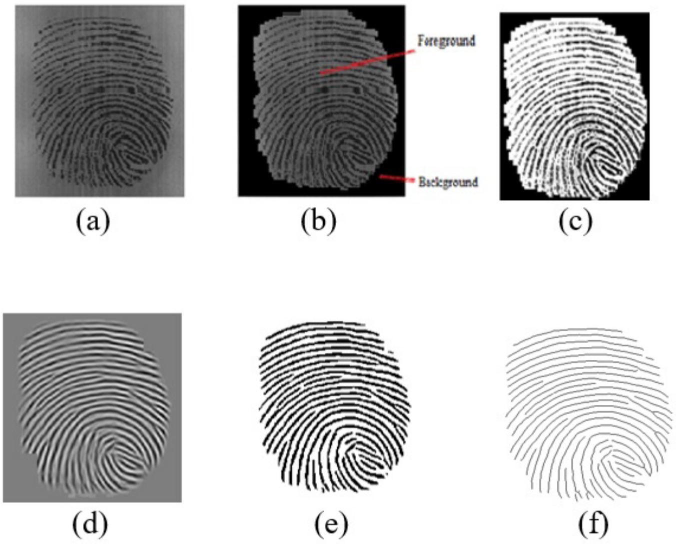


Figure 2: *(a) Fingerprint original image (b) Segmentation (c) Normalization (d) FP image enhancement (e) Binarization (f) Thinning.*

Fingerprint matching algorithms, as apparent from their name have a task to compare two fingerprints and determine the similarity/ differences or match/ non-match between them. Matching two fingerprint images is a complex problem in fingerprint recognition, mainly due to the large intra-class variations and small inter-class variations of images obtained during acquisition.

Before the advent of digital biometrics, fingerprints were recorded by inking the finger and rolling it from nail to nail in a controlled manner across a piece of paper. Nowadays, in Automatic Fingerprint Recognition Systems (AFRS), "live scan" devices, called fingerprint scanners (or readers) are used for on-line acquisition of images from fingers (Andrew, 2002). The acquisition type in which an inked impression of the finger tip on a piece of paper is acquired by the scanner is called off-line acquisition. The major part of a fingerprint scanner is the image sensor which is manufactured using optical and solid-state or ultrasound technology (Tartagni and Guerrieri, 1998; Ross and Jain, 2004).

As fingerprint images are acquired using devices from different manufacturers so their intensity varies. By using equalization, the image's background and foreground areas are contrasted. The equalization has an end goal to achieve a significant difference in intensity levels through separating background and foreground features (Jain *et al.*, 1997; Krutsch and Tenorio, 2011). Using normalization, we can change the range of values for pixel intensity so the whole picture intensity is changed to a pre-defined value and thus pixel-wise normalization can be carried out (Saddique *et al.*, 2005). The process of changing a grayscale 256 level image to a 2-level binary image is known as binarization. The process is executed on ridges and valleys with a threshold of 0 (Grdiet and Garg, 2013).

The ridges are represented as black while valleys are represented as white colored. A binary image input to the thinning process produces another binary image in which the ridges and valleys are only one pixel wide whereas the connectivity and the original contour must be maintained (Ji *et al.*, 2007). The most important task to recognize an individual is possible if we have his minutiae features (Mwema *et al.*, 2015). The most widely used features are edge and bifurcation which has to be properly extracted from image (Das, 2012).

The biometric data in itself deserves a high degree of protection. The data may provide additional information about the background of an individual. Hence, the features extracted must be stored in encrypted form through template protection techniques inside the database. This is done in order to avoid any possible hacking attack and using the information for mala-fide purposes or with an intent to deceive the system.

This work has focused on the enhancement of low-quality fingerprint images through extracting best arranged features, utilizing a new encryption approach and on using a simple but still hard to hack encryption approach. In order to ensure data protection, the goal to achieve in this work was to acquire a zero percent fingerprint similarity standard and have no correlation between the original and encrypted data after the application of the proposed algorithm. But an ideal outcome was limited by the processing capability at the time. Still, a similarity standard of almost zero and a weakest correlation between the original and encrypted data was achieved. The following sections respectively present the literature review, methods employed by FVC2002 database, experimental results, discussion and conclusions.

Literature review

Literature reveals that in some cases original minutiae are stored in database without encryption (Jain *et al*., 1997). Reportedly, there are eight different types of attacks that has been carried out on various biometric systems. In order to counter such attacks, we found that mostly systems try to secure their fingerprint templates (Mwema *et al*., 2015). A two-stage features enrolment and validation process uses fingerprint features and a secret key which is also derived from another template to scramble the features and then store them in the database (Das, 2012). The minutiae are transformed in both stages of the system i.e. in the enrolment and identification stages and then the matching process is performed (Chen, 2011). For a complete image encryption, turbo encryption is used. This method is only useful for complete images and is not effective for only minutiae based encryption (Mao *et al*., 2011). The biometric information directly recorded in a database is more susceptible to information hacks than those which are template encrypted. Figure 3 here shows the minutiae features of a fingerprint.

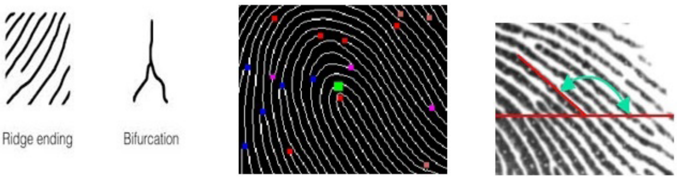


Figure 3: *Minutiae features.*

In this paper, first we present a novel technique for securing the template using symmetric encryption so the original minutiae will not be stored in the database. Secondly, we show that the proposed method is more efficient in terms of processing time because it avoids two time data encryption i.e. for enrollment and validation and finally, it is demonstrated that the keys are not generated from another template but totally user dependent. The minutiae feature and private secret keys are used as arguments to our proposed framework. After processing, the proposed system returns the encrypted scramble minutiae. This cipher minutiae are only recoverable and usable to a legitimate user who possesses the private key. Even if the data is stolen, this data is now useless to any other system and would not be processed by the host security system because of the unavailability of the private key. Our proposed approach requires eight private keys and each key can be of a different or same size entirely depending upon the user.

Materials and Methods

FVC2002 database

For our analysis, we worked on the second Fingerprint Verification Competition database, which is widely used for fingerprint verification algorithms. The database is prepared by Biometric System Laboratory, University of Bologna, Italy (FVC, 2002). The database contains 31 member images including 21 industrial personnel, 6 academics and 4 others. The dataset contains 4 databases, each database contains 80 images and these fingerprint images are widely used for fingerprint verification.

The essential shortcomings in the framework emerges from the way human biometrics features are not confidential. Although biometric attributes of an individual cannot be changed but if a biometric identifier has been bargained, an aggressor can utilize this data to build up a fake dataset that can trick the framework into tolerating his permission.

Consequently, the algorithm will most likely be unable to distinguish impure information when the coordinating procedure is totally self-ruling and without human checking. Biometric data contains information obtained from individuals, which can be used to identify them. This raises problems of data protection and privacy.

Minutiae are the input to the framework which are property of the individual. In order to hide this data from unauthorized access, first we add some dummy data to the original data. The dummy data's size depends on the size and location of the original data which enriches the encryption because spurious minutiae are not fixed so trespasser would not be able to detect the correct length and correct location and hence cannot decrypted and use the data. Secondly, the spurious minutiae are mixed with the original data so if a hacker tries to delete the spurious minutiae, he or she might delete the original minutiae and hence the system will deny them access.

Proposed method

The Minutiae based low quality fingerprint recognition with novel template encryption and protection algorithm was performed using a two steps method: Image processing and Features encryption.

Image processing

In the above mentioned algorithm, pre-processing techniques are applied in order to acquire good features from a fingerprint image. But initially, it is important to consider that fingerprint sensors are designed by various manufactures and in most cases, each manufacturer uses a different technique for the creation of a fingerprint template i.e. fingerprint image captured by the sensor and matching it with the reference template residing inside the enrollment database. Two main parameters were considered at the initial capturing by the sensor (a) rate of false negatives also referred to as rate of annoyance and (b) rate of false positives. Rate of false negatives means percentage of times the reference template fails to match a legitimate print captured by the sensor while rate of false positives means percentage of times the reference template matches an illegitimate print. The confidence interval for avoiding such dragging parameters was almost 100% in our case-study due to fewer number of right thumbs (Four to be exact). Even with dirty thumbs, the algorithm was able to keep the false positive rate equal to zero.

Enhancement

An image is called an enhanced image if one or more attributes of the image are modified to acquire more information accordingly for need of other automated image processing techniques or human viewing. To get an enhanced definition of the fingerprint image, noise of valleys and ridges has to be reduced. For reliable estimate minutiae locations, enhancement techniques are applied prior to minutiae extraction.

Normalization

To control the contrast of image's pixel and recognize edges and valleys, equalization was performed which depends on the local property of fingerprint images. The image I is characterized as $P\ x\ Q$ matrix which shows (m, n) as pixel intensity at m^{th} row and n^{th} column. If $I(m, n)>P$ then;

$$G(m,n) = Q_0 + \sqrt{\frac{(VAR_0(I(m,n) - Q)^2)}{VAR}} \quad \dots(1)$$

Else $$G(m,n) = Q_0 - \sqrt{\frac{(VAR_0(I(m,n) - Q)^2)}{VAR}} \quad \dots(2)$$

Where VAR_o, Q_o, VAR and Q were calculated from the given image (Ross and Jain, 2004).

Binarization

The captured grayscale image has normally 256 levels. Through binarization we convert that image to a two level binary image in which foreground is allocated an esteem 1 and background is allocated an esteem 0. Bernsen method is used which figures the threshold value from image pixels (Latha and Chakarvarthy, 2012).

$$MBernsen = \frac{Qlow\ + QHigh}{2} \quad \dots(3)$$

The applied window has gray level esteem of Q_{low} and Q_{high}.

Thinning

Scale-wise each element in binary image has more than one pixel in size through thinning we make each element one pixel wide. The thinned image has comparatively less data than the binary image. A 2-D iterative NN, like PCNN (Johnson and Padgett, 1990), at the t_{th} $(t \geq 0)$ iteration the dynamical conduct of PCN may be detailed as:

$$\begin{cases} U_{mn}(t) = \overline{X_{mn}}(t)[1 + \sum_{i=1}^{p} \sum_{j=1}^{q} W_{ij}\phi_{ij}(t)] \\ Y_{mn}(t) = f\left(U_{mn}(t) - \theta_{mn}(t)\right) \end{cases} \quad \dots(4)$$

Where; X_{mn} means the change estimation of the load signal of N_{mn}, i.e., if $X_{mn} = 0$, at that point $X_{mn} = 1$; generally, $X_{mn} = 0$. Each connecting input $^{\phi}ij(t)$ $(1 \le i \le p$ *and* $1 \le j \le q)$ can be figured by:

$$\phi_{ij}(t) = \overline{M_{ij} \oplus Y_{ij}(t)} = \begin{cases} 1, if\ M_{ij} = Y_{ij} \\ 0, else \end{cases} \quad \dots(5)$$

The exclusive ORed function connect weight W_{ij} by its comparing component M_{ij} in the template matrix M which is computed by:

$$W_{ij} = \begin{cases} 1, if\ M_{ij} = 0\ or\ 1 \\ 0, else \end{cases} \quad \dots(6)$$

Minutiae extraction

The two most widely used features for recognition are ending and bifurcation. We found an edge if the intensity of a pixel varies suddenly to its neighbor's pixel. Nowadays, Sobel edge recognition along with interlocking to our both kernels is a slight alteration form of main distinction.

$$E'x\ to\ Ex = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix} \quad \dots(7)$$

To get a signal kernel, *Ex* and *Ey* can be connected. The greatness of gradient is to restore the Euclidean norm of intensities of G_x and G_y tested at pixel *(x, y)*.

$$(G_X(x,y))G_Y(x,y))^T\|_2 = \sqrt{G_X(x,y)^2 + G_Y(x,y)^2} \quad \dots(8)$$

The edge's orientation Θ can be calculate from edge Point using.

$$\theta = arctan\ (Gy/\ Gx) \quad \dots(9)$$

Encryption and decryption

The information obtained from the particulars of fingerprint image is ciphered through novel encryption algorithm. We used symmetric key encryption for this purpose. The decryption process reverses the encryption; through which we get the original data back if the legitimate user provides the correct secret key.

Proposed algorithm of encryption

The extracted minutiae features are step-wise encrypted using the proposed encryption algorithm shown through the block diagram shown in Figure 4. To hide the minutiae from an unauthorized person and keep it accessible only to a legitimate user, we coded the algorithm using different MATLAB library supported encryption techniques. The minutiae information (plain data), read from the thumb finger of the person, is the input to the algorithm. The plain data represents the information hidden in the minutiae; this data is the property of the authorized person which is required to be further analyzed for making it secure. To keep the data secret and make the encryption more suitable chaff points are added. This chaff points addition depends on the extracted feature, are added to the original minutiae locations which enrich the encryption in two ways, (a) By Adding spurious minutiae trespasser would not be able to detect the correct length of the exact data so he would get extra data as well which would lead him to wrong results hence the data is more secure. (b) Spurious minutiae are mixed with the original data so the intruder would not be able to extract the original ones and will get wrong result. Since data is taken from different variables the dimensions might not be adjusted to further work on it, we change its dimensions by reshaping different variables into one matrix and hence data is also mixed by changing its shape which enable us to work on it further. This method makes the encryption process more secure and difficult to understand for trespasser. Secret keys are the unique thing which identify the authorized person and allow access to him. In this algorithm, four input keys are required whose length can vary from 0 to 64 values length for better encryption. These keys are adjusted to make it work with data. Secret keys are used to work on data as its variable. Nucleotide sequence is performed to reverse the data as this changes the last element with first element, similarly second last with second element and so on.

Results and Discussion

Figure 5 shows the original extracted features diagrammatically. After encryption the same image's cipher data looks quite different from the original as shown in Figure 6. Since the encryption process depends on secret keys, if the same fingerprint image is encrypted with different secret keys the resultant ciphered features will be significantly different from each other. Meanwhile, Figure 7 shows the extracted features i.e. ridge ending and bifurcation are stored in an MS Excel file. We also encrypted the x, y location and orientation of minutiae along with the ridge ending and bifurcation. This scenario is depicted through Figure 8 which shows image 101_8B encrypted with key K1 and Figure 9 showing the same image encrypted with key K2.

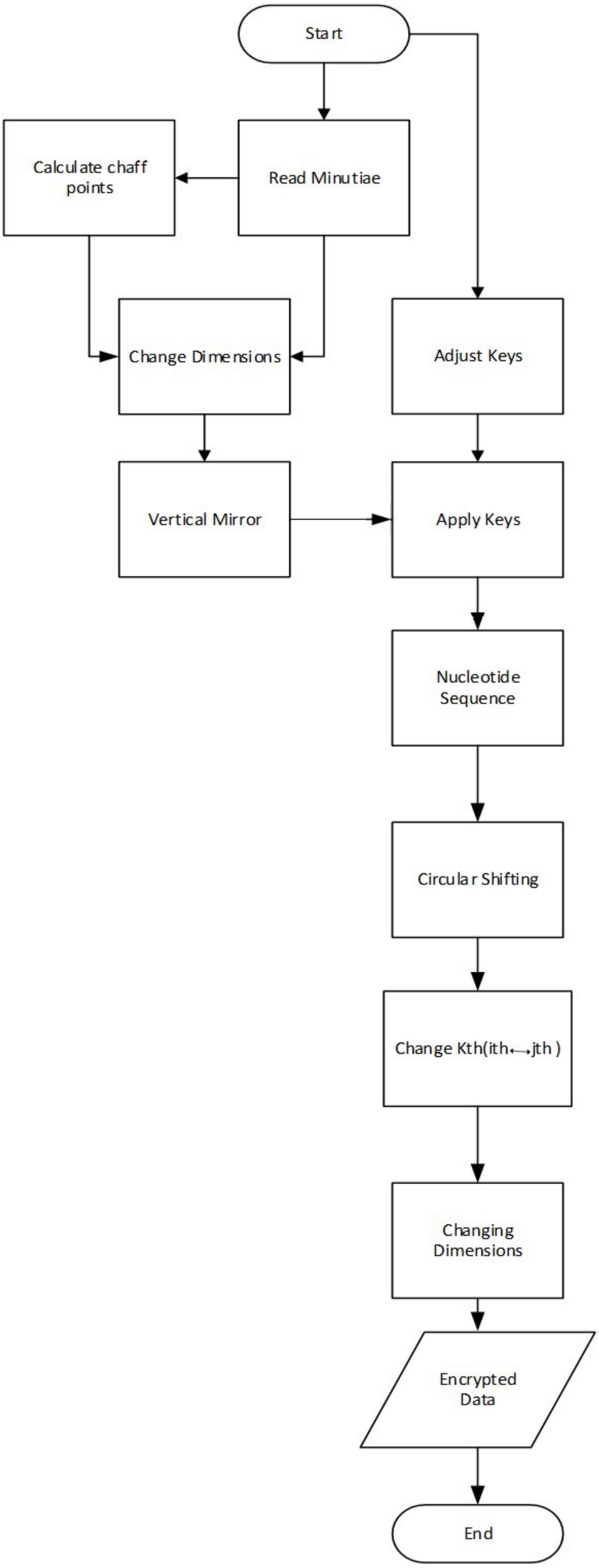


Figure 4: *Proposed Algorithm.*

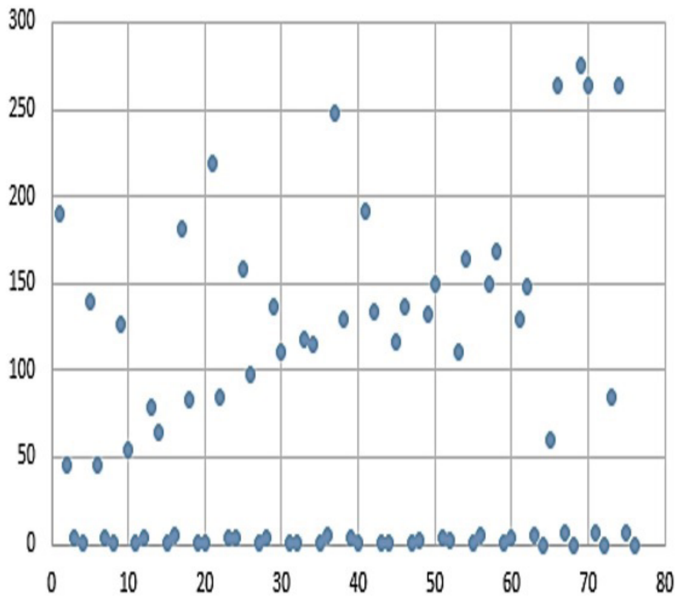
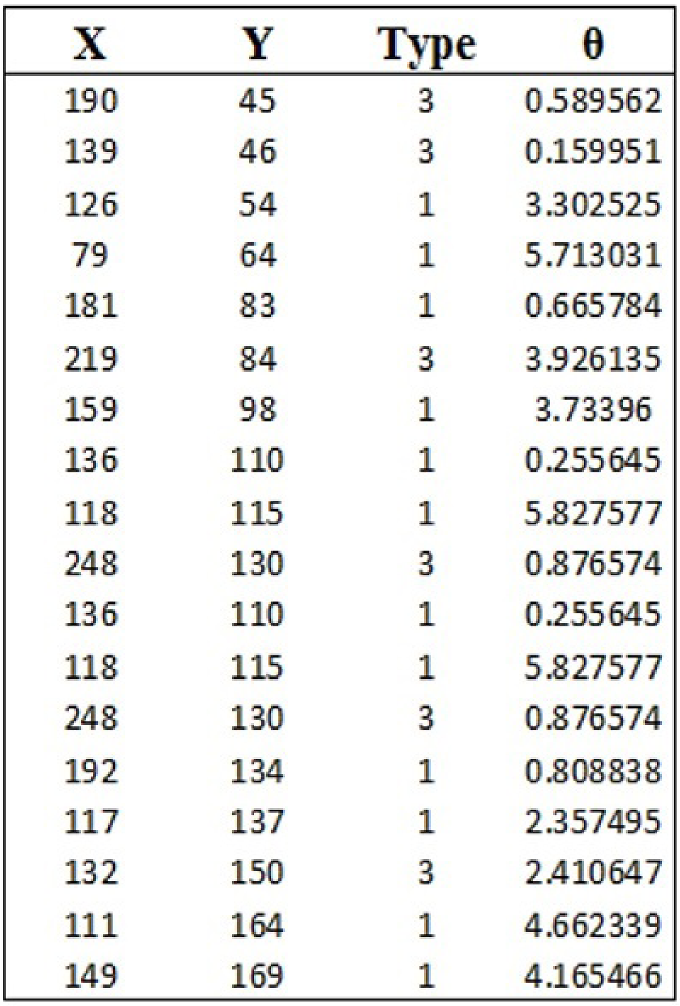


Figure 5: *Original extracted features of image 101_1B.*



X	Y	Type	θ
190	45	3	0.589562
139	46	3	0.159951
126	54	1	3.302525
79	64	1	5.713031
181	83	1	0.665784
219	84	3	3.926135
159	98	1	3.73396
136	110	1	0.255645
118	115	1	5.827577
248	130	3	0.876574
136	110	1	0.255645
118	115	1	5.827577
248	130	3	0.876574
192	134	1	0.808838
117	137	1	2.357495
132	150	3	2.410647
111	164	1	4.662339
149	169	1	4.165466

Figure 6: *Extracted sample data.*

Statistical analysis

The data before the encryption and after the encryption are different from each other. We have applied a statistical tool called Normalized Cross Correlation (NCC) available in MATLAB to find the similarity index between the plain data and the ciphered data. For matching, this method utilizes brute-force analysis. Figure 10 meanwhile shows a sample of the similarity index between the original data and the encrypted data regarding image 101_1B.

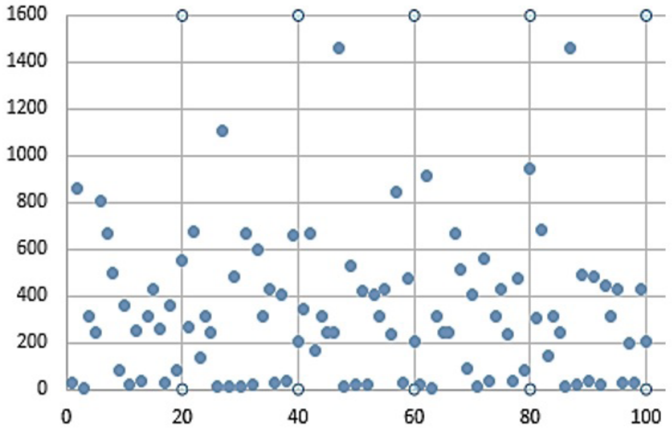


Figure 7: *Encrypted features of image 101_1B.*

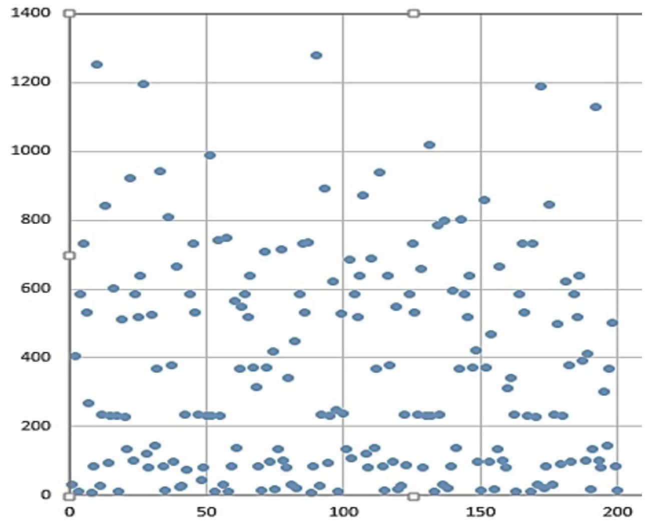


Figure 8: *Image 101_8B encrypted with key K1.*

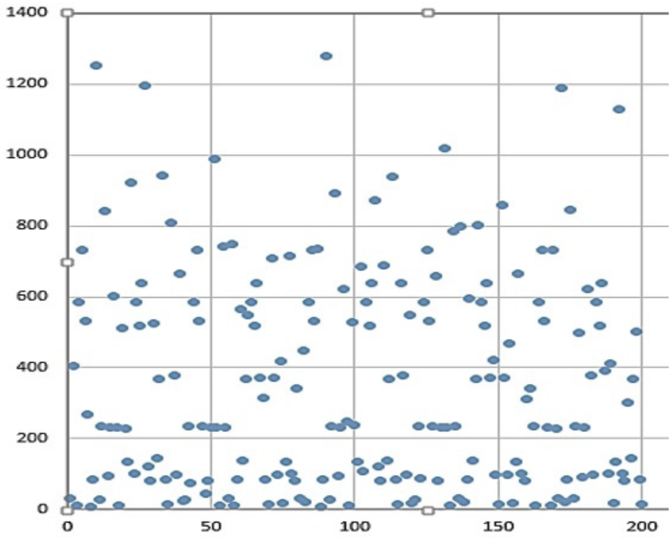
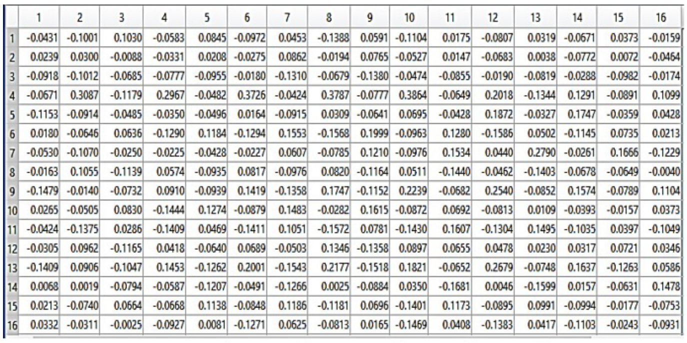


Figure 9: *Image 101_8B encrypted with key K2.*

Analysis of results

As shown in Figure 10, the similarity index can have three different esteems, the esteem 0 represents that there is no relationship between the ridge ending and bifurcation data at all. A perfect positive relationship is identified if esteem is +1. Meaning both of the variable data move in the same fashion while esteem -1 represents a perfect negative relationship which shows both variables are different in nature.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	-0.0431	-0.1001	0.1030	-0.0583	0.0845	-0.0972	0.0453	-0.1388	0.0591	-0.1104	0.0175	-0.0807	0.0319	-0.0671	0.0373	-0.0159
2	0.0239	0.0300	-0.0088	-0.0331	0.0208	-0.0275	0.0862	-0.0194	0.0765	-0.0527	0.0147	-0.0683	0.0038	-0.0772	0.0072	-0.0464
3	-0.0918	-0.1012	-0.0685	-0.0777	-0.0955	-0.0180	-0.1310	-0.0679	-0.1380	-0.0474	-0.0855	-0.0190	-0.0819	-0.0288	-0.0982	-0.0174
4	-0.0671	0.3087	-0.1179	0.2967	-0.0482	0.3726	-0.0424	0.3787	-0.0777	0.3864	-0.0649	0.2018	-0.1344	0.1291	-0.0891	0.1099
5	-0.1153	-0.0914	-0.0485	-0.0350	-0.0496	0.0164	-0.0915	0.0309	-0.0641	0.0695	-0.0428	0.1872	-0.0327	0.1747	-0.0359	0.0428
6	0.0180	-0.0646	0.0636	-0.1290	0.1184	-0.1294	0.1553	-0.1568	0.1999	-0.0963	0.1280	-0.1586	0.0502	-0.1145	0.0735	0.0213
7	-0.0530	-0.1070	-0.0250	-0.0225	-0.0428	-0.0227	0.0607	-0.0785	0.1210	-0.0976	0.1534	0.0440	0.2790	-0.0261	0.1666	-0.1229
8	-0.0163	0.1055	-0.1139	0.0574	-0.0935	0.0817	-0.0976	0.0820	-0.1164	0.0511	-0.1440	-0.0462	-0.1403	-0.0678	-0.0649	-0.0040
9	-0.1479	-0.0140	-0.0732	0.0910	-0.0939	0.1419	-0.1358	0.1747	-0.1152	0.2239	-0.0682	0.2540	-0.0852	0.1574	-0.0789	0.1104
10	0.0265	-0.0505	0.0830	-0.1444	0.1274	-0.0879	0.1483	-0.0282	0.1615	-0.0872	0.0692	-0.0813	0.0109	-0.0393	-0.0157	0.0373
11	-0.0424	-0.1375	0.0286	-0.1409	0.0469	-0.1411	0.1051	-0.1572	0.0781	-0.1430	0.1607	-0.1304	0.1495	-0.1035	0.0397	-0.1049
12	-0.0305	0.0962	-0.1165	0.0418	-0.0640	0.0689	-0.0503	0.1346	-0.1358	0.0897	0.0655	0.0478	0.0230	0.0317	0.0721	0.0346
13	-0.1409	0.0906	-0.1047	0.1453	-0.1262	0.2001	-0.1543	0.2177	-0.1518	0.1821	-0.0652	0.2679	-0.0748	0.1637	-0.1263	0.0586
14	0.0068	0.0019	-0.0794	-0.0587	-0.1207	-0.0491	-0.1266	0.0025	-0.0884	0.0350	-0.1681	0.0046	-0.1599	0.0157	-0.0631	0.1478
15	0.0213	-0.0740	0.0664	-0.0668	0.1138	-0.0848	0.1186	-0.1181	0.0696	-0.1401	0.1173	-0.0895	0.0991	-0.0994	-0.0177	-0.0753
16	0.0332	-0.0311	-0.0025	-0.0927	0.0081	-0.1271	0.0625	-0.0813	0.0165	-0.1469	0.0408	-0.1383	0.0417	-0.1103	-0.0243	-0.0931

Figure 10: *Sample coefficient of correlation between plain and cipher data of Image 101_8B.*

Conclusions and Recommendations

To avoid storage of the original biometric image or template, the area of biometric cryptography came into existence which is a collection of emerging technologies. Through biometric cryptography, biometric templates are securely bound with digital keys. For such encryptions, various techniques such as RSA encryption, Advanced Encryption Standard (AES), Turbo and Circular encryption techniques are employed. On the other hand, our proposed minutiae based low-quality-fingerprint recognition with novel template encryption and protection algorithm uses best suited pre-processing techniques. It also focuses primarily on feature encryption of ending and bifurcation. It performs different operations on the features so that output and input are different. The similarity index shown in this paper suggests that the plain and cipher data has a weaker relationship. There are many encryption methodologies but most of them could not be applied at such a low computational overhead cost. The proposed algorithm is easy to implement and provides good results. This algorithm is suitable for implementation on devices with low memory constraints. Here, we do not prefer to generate automatic secure keys, although we have some ideas of secure keys generator in future work, here the selection of keys depends on the user selection although the level of security changes with the selection of keys, which shows that the cipher data still depends on the user input but in future the cipher data will be made independent of the user input. Furthermore, the complexity of the proposed algorithm is very much low because the primary focus of the proposed approach was to develop a security system for low memory systems, if the low memory constrains are overcome the proposed approach may be further improved.

Acknowledgements

Authors would like to thank the entire academic and support staff of the Department of Electrical Engineering, UET Peshawar, KPK, Pakistan for their academic input and facilitating role.

Novelty Statement

This paper proposes a new fingerprint encryption methodology for achieving a weaker correlation between the original and encrypted data for enhancing data protection.

Author's Contribution

The idea proposed in this paper was conceived by Amjad Ali. Feasibility of the research methodology was conducted by Muhammad Amir. Hardware set-up and software structure was worked on by Zafar Khan and Abid Munir respectively while results of the methodology were comparatively verified by Bilal Ur Rehman.

Conflict of interest

The authors have declared no conflict of interest.

References

Andrew, W., 2002. System and method for transforming fingerprints to improve recognition. US Patent Application No. US20020126883.

Anil, K., K. Nandakumar and A. Ross. 2016. 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recog. Lett., 79(1): 80-110. https://doi.org/10.1016/j.patrec.2015.12.013

Chen, H., 2011. A novel algorithm of fingerprint encryption using minutiae-based transformation. Pattern Recognit. Lett., 32(2): 305-309. https://doi.org/10.1016/j.patrec.2010.09.007

Das, R., 2012. Multimodal biometric systems: How they can help to protect against physical and logical threats. Keesing J. Doc. Ident., 1(37): 15-18.

FVC, 2002. Fingerprint verification competition database. http://bias.csr.unibo.it/fvc2002/

Grdiet, P. and N. Garg. 2013. Binarization techniques used for grey scale images. Int. J. Comp. Appl., 71(1): 8-11. https://doi.org/10.5120/12320-8533

Jain, A., L. Hong and R. Bolle. 1997. On-line fingerprint verification. IEEE Trans. Patter. Anal. Mach. Intell., 19(4): 302-314. https://doi.org/10.1109/34.587996

Ji, L., Z. Yi. L. Shang. and X. Pu. 2007. Binary fingerprint image thinning using template based PCNNs. IEEE Trans. Syst. Man Cyber. Part B: Cybernetics, 37(5): 1407-1413. https://doi.org/10.1109/TSMCB.2007.903369

Johnson, J. and M. Padgett. 1990. PCNN models and applications. IEEE Trans. Neural Netw., 10(3): 480-498. https://doi.org/10.1109/72.761706

Krutsch, R. and D. Tenorio. 2011. Histogram equalization, application note. Document No. AN4318, 1-9.

Latha, M. and Chakravarthy. 2012. An improved Bernsen algorithm approaches for license plate recognition. IOSR J. Electron. Commun. Eng., 3(4): 2280-2285. https://doi.org/10.9790/2834-0340105

Li-Kuo, C., 2010. High performance fingerprint image-processing method. US Patent No. US20100303310.

Maltoni, D., D. Maio. A.K. Jain and S. Prabhakar. 2009. Handbook of Fingerprint Recognition, 2nd edition, Springer-Verlag. https://doi.org/10.1007/978-1-84882-254-2

Mao, Q., C. Qin. B. Xu. and X. Guo. 2011. Turbo based encryption with error correction capability. J. Comp. Inf. Syst., pp. 2876-2885.

Mwema, J., S. Kimani and M. Kimwele. 2015. A conceptual technique for deriving encryption keys from fingerprints to secure fingerprint templates in unimodal biometric systems. Int. J. Comp. Appl., 118(9): 18-30. https://doi.org/10.5120/20773-3252

Patil, S., S. Chandal and R. Gupta. 2011. Fingerprint image enhancement techniques and performance evaluation of the SDG and FFT fingerprint enhancement techniques.

Semant. Scholar, 2(2): 184-190.

Ross, A. and A. Jain. 2004. Biometric sensor interoperability: A case study in fingerprints. Proceedings of International ECCV Workshop on Biometric Authentication. Czech Republic. https://doi.org/10.1007/978-3-540-25976-3_13

Ross, A. and A. Jain. 2004. Biometric sensor interoperability: A case study in fingerprints. Int. Works. Biomet. Authent., pp. 134-145. https://doi.org/10.1007/978-3-540-25976-3_13

Saddique, S., M. Sikandar. H. Khiyal. A. Khan and M. Khanum. 2005. Sequential algorithm using Euclidean distance function for seed filling. J. Theor. Appl. Inf. Technol., 19(1): 9-14.

Tartagni, M. and R. Guerrieri. 1998. A fingerprint sensor based on the feedback capacitive sensing scheme. IEEE J. Solid-State Circ., 33(1): 133-142. https://doi.org/10.1109/4.654945