Adaptive Encryption Technique to Protect Biometric Template in Biometric Database using a Modified Gaussian Function

E. N. Ajimah[1,*], O. N. Iloanusi[2], M. C. Eze[3] and S. Olisa[4]

[1,2,3,4] DEPARTMENT OF ELECTRONIC ENGINEERING, UNIVERSITY OF NIGERIA, NSUKKA, ENUGU STATE. NIGERIA

E-mail addresses: [1] ajimahnnabuezeedmund@gmail.com , [2] ogechukwu.iloanusi@unn.edu.ng ,

[3]martin.eze@unn.edu.ng, [4] samuel.olisa@unn.edu.ng

ABSTRACT

Fingerprints as a type of biometrics, appear to be the most populous and most acceptable means of individual identification and verification. We leave our fingerprints on virtually anything we lay our fingers on. The chance however, of casually leaving our fingerprints at several location without our knowledge, exposes mankind to much more insecurity. The biometric templates identifies us as those imprint features they get from our body, thus; losing them by any sort means losing who we actually are. In this paper, protection of biometric (fingerprint) template is an important issue that was dealt with. The protection of fingerprint in the database of the Automatic Fingerprint Identification System (AFIS) using a modified Gaussian equation to encrypt the image and store as template in the database and decrypt the template to compare with the reference data during verification. This technique of encryption successfully encrypt and decrypt without degrading the original image sample. The simulation of the image was carried out on a MATLAB environment whereas the verification was performed using the GrFinger environment.

Keywords*: Humanity, Protection, Identity, Template, Fingerprints, Encryption and Decryption.*

1. Introduction

Biometrics is defined as the science of recognizing or verifying the identity of a human being based on their physiological or behavioural characteristics [1]. Physiological characteristics which have to do with humans physical attributes include; fingerprints, hand geometry, hand vein, retina scan, and facial image. Behavioural characteristics are actions which are carried out by human which include someone's; signature, voice, gait etc. though these are naturally dependent on physical characteristics [2], [3]. Biometric as a word, has its origin from two Greek words which are: *bio* which means *life* and *metric* which means *measure*. Conventional security systems used either *knowledge-based methods*

(passwords or PIN) [4], [5], and *token-based methods* (passport, driver license, Identity Card, voters card) and were prone to fraud because Personal Identification Numbers (PIN) could be forgotten or could even be guessed by a criminally minded person whereas the tokens could be lost, duplicated or even be stolen [6]. To handle the need for strong security system the biometrics becomes the key player to successfully achieve it. Over a hundred years human body traits, especially fingerprints were applied in forensics, but quite shocking when this was almost becoming popular, a new discovery of biometric emerged - the use of biometric for personal authentication (identification and verification) [7]. In 1893, the home ministry office in The United Kingdom discovered that no two persons (even in the case of identical twins) have the same fingerprint [7]. This idea simply describes the distinctiveness of fingerprint. The discovery of the uniqueness of fingerprint has led to the identification of persons in law enforcement departments. The law enforcement keep records of the fingerprints of criminals, so if a match of a latent fingerprint that is found in the crime scene happens to be in their database, the person can easily be arrested and interrogated [8]. This is basically done by lifting the latent fingerprint (hidden fingerprint left accidentally without the knowledge of the person) at the crime scene and compares with what is in their database. In an exact sense fingerprint experts are trained for the recognition of the fingerprints and also nailing down the perpetrators of evil and crime in a society [7].

Biometric security is now playing an important role in securing our modern day computer since our biometric can stand as a natural passcode [9]. Biometric security provides identification of users through something the user could be uniquely identified with measurement of any of their physical characteristics such as fingerprints, retinal patterns and even DNA [10]. Security of biometric templates is important as these templates serve as security to the entire system. Authentication can be achieved in three broad views which are; what you know (passwords, PIN-codes etc.), what you have (smart-cards, token, national identity card etc.) and what you are? Is dependent on your biometric-a quality that differentiates you from others, [11], [12]. The biometrics ('*what you are*') appear to be the most futuristic of the three type of user authentication. In this thesis, the focus is on securing biometrics, and all that it would take to perform optimally in a security system. When a biometric security system is implemented two main stages are required: firstly, the user's biometric is scanned into the system and the main features of the biometric scanned are then extracted. Secondly, a compact and expressive digital representation of the user's biometric is stored as a template on the database [2]. When a person attempts to enter the system, the process is repeated. If a match is found among the templates on the database, the user is granted access to the system (this condition is called a ***hit***) and if not (in this case it is called a ***miss***) the user is denied access to the system [13]. Biometrics can be used for both steps, identification requiring a one-to-many search in the templates database and verification a one-to-one comparison of the measured biometric with the template that is associated to the claimed identity [14].

1.1 Challenges facing Biometric Template and need for its Security

Security is a very important aspect in every establishment, and one of the ways to attain a strong security environment is to secure the security system itself. There are several loopholes where imposters tend to exhibit some of their ugly skill to hack the system. There are a number of attacks by intruders on a biometric system at the sensor, feature extractor, database and matcher levels. There are proposed

solutions to these problems in this field of research on different sub-systems of biometrics system and communication links (channels) connecting each of the sub-systems [15]. Despite all the efforts in the struggle to secure the biometric system researchers have not been able to successfully provide absolute security to biometric system against these attacks. Templates stored in database are the targets of most of many of the '***identity-thieves***' (intruders), thus, securing templates stored in databases is a very crucial in biometric recognition [16]. In this work the focus is on the database biometric-template and a technique that can protect biometric templates stored in the database.

1.2 Review of existing works on biometric template protection

So many works have been done in an attempt to secure biometric templates that would be stored in the database of the (Automatic Biometric Identification Systems) AFIS [17], [18], [19], [20], [7], [11], [21], [22]. Most of the work are based on protecting fingerprint template that will be stored in the database of the AFIS with the motive to curb identity thievery.

Fuzzy technique was employed by [21] and [22] in their works; 'Biometric Mobile Template Protection: A Composite Feature Fingerprint Fuzzy Vault' and 'Securing Fingerprint Template: Fuzzy Vault Minutiae Descriptors' respectively. [11], worked on security of Side Channel Attack (SCA). [7], worked on biometric template protection by employing salting, non-invertible transform and key-binding biometric cryptosystems. [23], used bio-convolution to protect online signature database. In [20], helper data and fuzzy extractor was used to protect biometric template. In [19], non-invertible transformation approach was used to protect facial biometric template. [17], worked on the use of geometrical transformation to protect a minutiae based fingerprint template.

In this article the protection of fingerprint template was done using a modified Gaussian function. The encryption algorithm of this function is so reliable that the encrypted image can never be traced without having a clue of the encryption key. In the decryption phase of this work is just perfect that the decrypted image gives exactly the original image without any degradation.

2. Why Protection of AFIS is needed

The attacks are spotted at various points of the biometric system, these stages of attack are: at the sensor level, the channel between the sensor and the feature extractor, attack on the feature extractor, attack on the channel between the feature extractor and the matcher, the attack on the matcher, the attack on the channel between the matcher and the database, the attack on the channel between the matcher and the output decision and the attack on the template in the database. Of all these attacks, the most intriguing is the attack on the template in the database. Database security is the back-bone of the success of Automatic Biometric Identification System (ABIS) [12] [21] [6] [10].

2.1 The Fingerprint Template Database Protection

In this MATLAB oriented work, special consideration was given to the protection of the biometric template which was successfully implemented by employing the encryption and decryption techniques with the modified Gaussian function as the key to the encryption. The encryption is obtained by obtaining the logarithm of the product of the key and logarithm of the sum of the original image and the key. The

following algorithm achieves the encryption of the original image:

i. Sum the original image with the encryption key.
ii. Take the logarithm of the result in i.
iii. Take the product of the encryption key and the result in ii.
iv. The logarithm of the result in iii decrypts the image.

The following equation 4.1 summarizes the proposed encryption.

$$I_{Encrypt} = \log_e[Key.* \log_e(I_{original} + Key)] \quad (1)$$

In order to get back the original image the following algorithm decrypts the encrypted image,

i. Taking the exponent of the encrypted image.
ii. Divide the result of i. by the encryption key.
iii. Take the exponent of the result in step ii.
iv. Subtract the encryption key from the result in step iii.

Equation (2) is the mathematical summery of the decryption steps enumerated above

$$I_{Decrypt} = -Key + e^{\frac{e^{I_{Encrypt}}}{Key}} \quad (2)$$

The following sub-headings below are the step-by-step method to achieving the proposed technique to protect the stored template in the data base of a biometric system.

2.3 Modified Gaussian Key

The encryption key used in the protection of the biometric template is derived from the Gaussian function. The modified Gaussian key is very reliable and provides total security as an intruder will find it very difficult if not impossible to know what template was actually stored there. This technique leaves no clue to an intruder as the stored template will make no sense to the person. Here is the modification of the Gaussian function (the proposed key for the protection of the biometric template).

The discrete Gaussian function is stated as shown in equation (3),

$$\boldsymbol{G(m,n) = e^{\frac{-(m^2+n^2)}{2\sigma^2}}} \quad (3)$$

Where ***m*** is the row of the filter and ***n*** is the column of the filter

Inverse of the Gaussian function ***G(x)*** as in (1), $\boldsymbol{M_G(x)}$ is obtained as shown in equation (4)

$$M_G(m,n) = [G(m,n)]^{-1} \quad (4)$$

$\boldsymbol{M_G(x)}$ is the *Modified Gaussian Key* which was used in encryption and decryption of fingerprint images in this research work. Substituting ***G(x)*** in equation (4) we obtain equation (5)

$$M_G(m,n) = e^{[\frac{-(m^2+n^2)}{2\sigma^2}]^{-1}} \quad (5)$$

Simplifying equation (5) we obtain equation (6);

$$\boldsymbol{M_G(x) = e^{\left|\frac{(m^2+n^2)}{2\sigma^2}\right|}} \quad (6)$$

The modified Gaussian key has the same size as the fingerprint image.

Encrypting the fingerprint is mathematically shown in equation (7)

$$\boldsymbol{I_{Encrypted} = \log_e[M_G.* \log_e(I_{original} + M_G)]} \quad (7)$$

$I_{Encrypt}$ = *Encrypted image*

$I_{Original}$ = *Original image*

Decrypting the fingerprint is mathematically shown in equation (8)

$$\boldsymbol{I_{Decrypt} = -M_G + e^{[e^{(I_{encrypt})}./M_G]}} \quad (8)$$

$I_{Decrypt}$= *Decrypted image*

Section below discourse the result obtained in this work guided by this section.

3. Experiments, Results and Discussions

This section discussed the experiments performed, the results, conclusion and recommendation. See sections below for details.

3.1 Experiments

In order to measure the strength of the proposed protection technique for a biometric template, an extensive set of experimental tests were performed. This experiments were performed in two environments namely; MATLAB (for the implementation of the algorithm of the proposed technique) and then verification using a commercial matching software called GrFinger. Hence, the experiments were carried out in two stages –First in MATLAB and secondly using GrFinger,

3.1.1 Experiment performed in MATLAB Environment

This is actually the first stage of the experiment, which was to encrypt the image that will be stored in a database as template and decrypt the template during matching. The experiment was on a public-domain database FVC2000-DB2-A, which contains 800 fingerprints (100 fingers each give 8 different impressions). The dimension of each fingerprint image is 256×364 (the width is 256-pixels and the height is 364-pixels). The images are in .TIF image format (Tagged Image File Format .TIFF).

3.1.2 Experiment Performed in Grfinger Environment

The decrypted and original images were converted from TIFF to BMP in MATLAB environment prior to the experiments. At this phase of the experiment one hundred fingers with eight impressions each, already converted from to BMP were verified with one out of the eight impressions of each of the fingers. The second to eighth (seven of the impressions of each finger) impressions were enrolled and the first impression were used to verify these impressions. This experiment is repeated for all the hundred fingers.

3.2 Results and Discussions

Since the proposed algorithm is image oriented, it becomes easier to be worked on in MATLAB than in some other programming environment like C#, C++ etc. So the encryption and decryption were done in MATLAB whereas its evaluation was done on a GrFinger matching environment.

3.2.1 Result from the MATLAB Environment

The encryption algorithm as discussed in section was followed to achieve a successful in encrypting and decrypting a fingerprint image on the MATLAB environment. Figure 1 shows the original image, encrypted image and decrypted image when run on this environment.

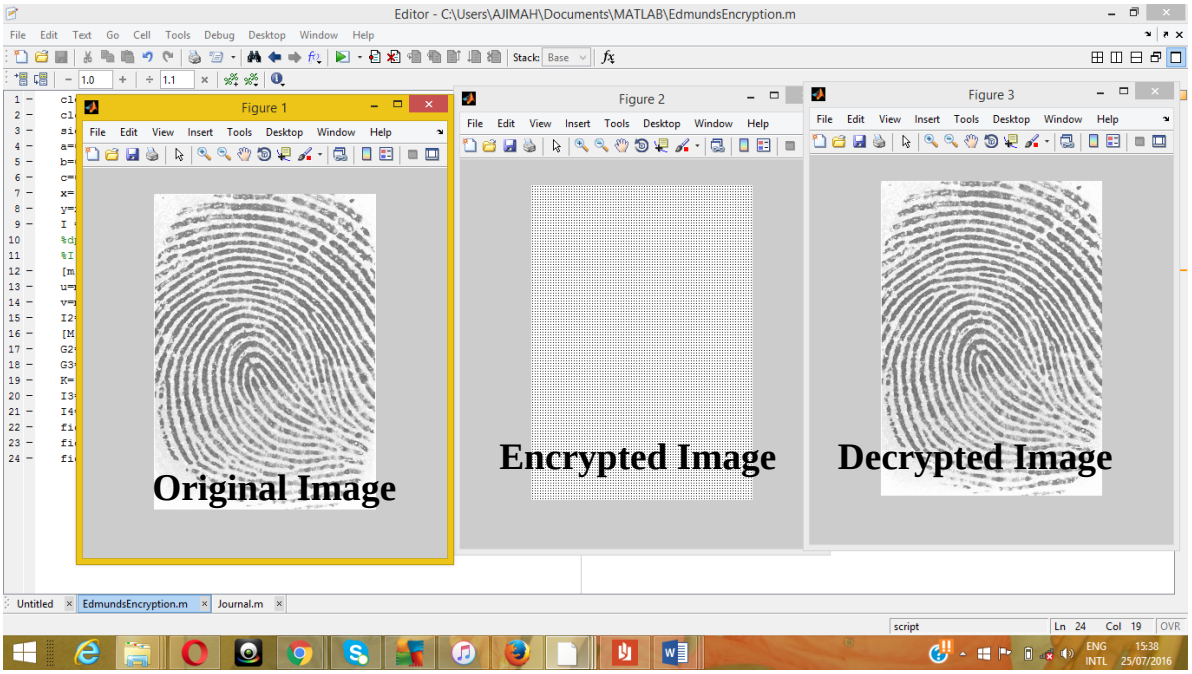

Figure 1. The Figure Shows the Original, Encrypted and Decrypted Image from the MATLAB experiment.

In order to validate that resulting decrypted images are not degraded in quality, the original images and decrypted images are all verified using a commercial matcher in the second phase of the experiment. The GrFinger was used in the validation in this work.

3.3.2 Result from the GrFinger Environment

The essence of using the commercial matcher, GRFinger, is to obtain match scores for the original as well as the decrypted images.

Since the database has 800 images of 100 individuals in the original and decrypted images, where each individual has 8 impressions, 100 images were enrolled while 700 images constituted the query or input fingerprints for matching for both original and decrypted images. Each of the 700 query prints were verified with their matching mates and their match scores were obtained. A scenario is shown in Figure 2.

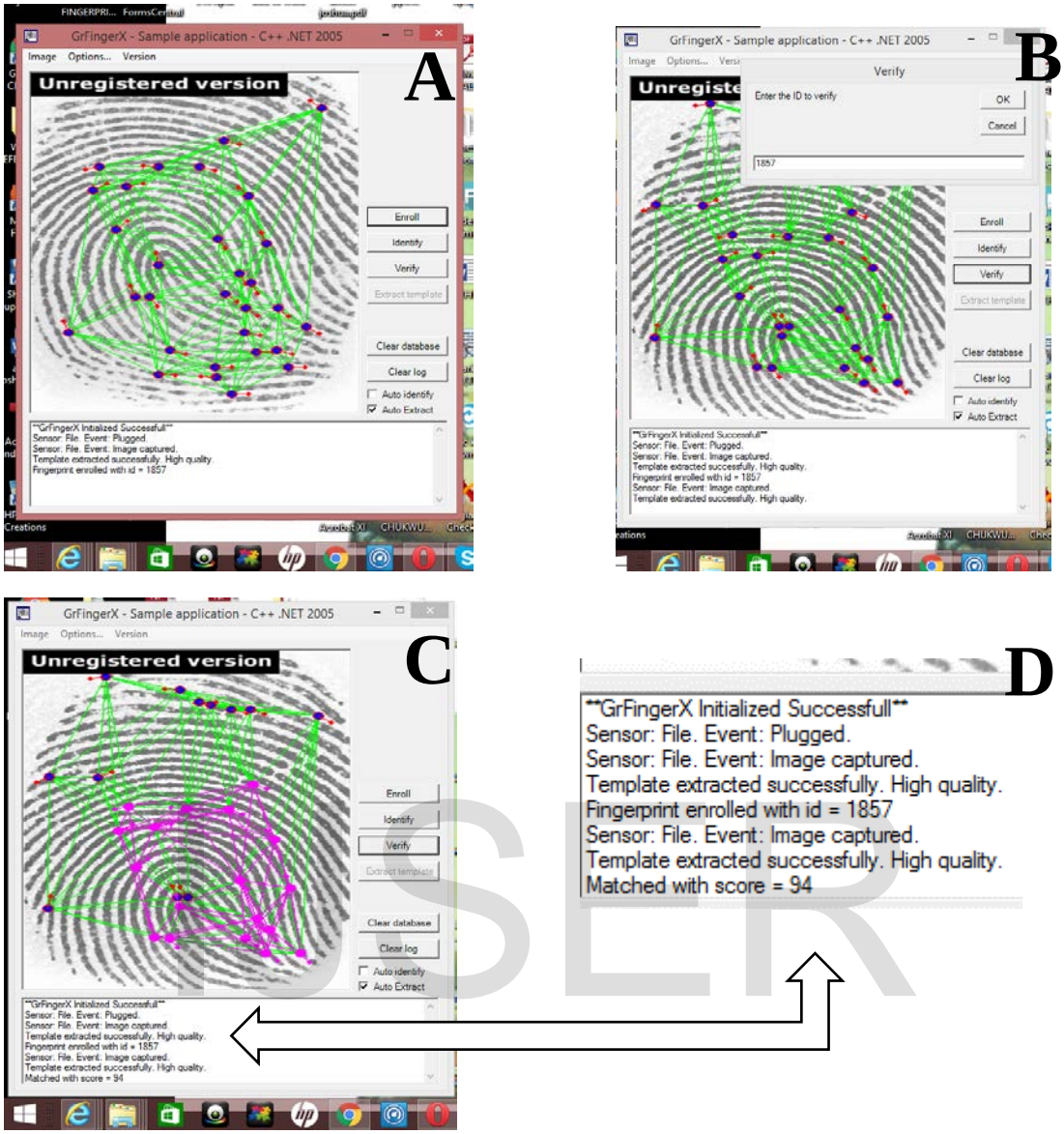

Figure 2. From the GrFinger environment the labels: A → Fingerprint sample showing Extracted Salient Point in Blue Dots and Relative Distances shown in Green thence Enrolled. B → Dialogue Box for Verification, where the Enrolled ID will be entered for Verification. C → The Verified Map is in Pink Lines and Points. D → Showing the Match Score of the Verification.

700 Match scores obtained for the original as well as the decrypted images. The distribution of the scores is shown in Table 1.

Table 2 shows the true matches and false matches at a threshold of 25. This is the default set threshold of the commercial matcher. In other words, all scores below 25 are regarded as non-matches while scores on or above 25 are regarded as valid matches.

Table 1. A Detailed Result from the Verification of the Fingerprint before Encryption and after Decryption with Fingerprint Match Score at Bins of 25.

Fingerprint Match Score with bins of 25	**Number of Fingerprint Impressions with bins of 25**	
	Original Image	**Decrypted Image**
0-24	129	129
25-49	109	109
50-74	119	119
75-99	101	101
100-124	81	81
125-149	54	54
150-174	49	49
175-199	31	31
200-224	13	13
225-249	03	03
250-274	06	06
275-299	02	02
300-324	01	01
325-349	01	01
400-424	01	01
Total Number of Impressions for Verification	**700**	**700**

Table 2: Shows the True Matches and False Matches at a Threshold Of 25

Fingerprint Image	Original Image	Decrypted Image
Total number of Non-Matches at Threshold of 25 (i.e. scores at the range of: 0≤SCORE≤24)	**129**	**129**
Total number of Matches at Threshold of 25 (i.e. scores greater than or equal to 25: SCORE≥25)	**571**	**571**
Total Number of Impressions for Verification	**700**	**700**

False Non-Match Rate (FNMR)

False Non-Match Rate (FNMR) is the ratio of the total number of true biometric that were rejected at a given threshold to the total number of impressions presented for verification in percentage. Mathematically we have;

$$FNMR(\%) = \frac{Total\ FNMR\ @\ threshold\ 25}{Total\ Number\ of\ impression}$$

The FNMR result below was for original image;

$$FNMR(\%) = \frac{129}{700} \times \frac{100}{1}$$

$$FNMR(\%) = \mathbf{18.43}\%$$

The FNMR result below was for decrypted image;

$$FNMR(\%) = \frac{129}{700} \times \frac{100}{1}$$

$$FNMR(\%) = \mathbf{18.43}\%$$

True Match Rate (TMR) or True Acceptance Rate (TAR)

This is the ratio of the total number of true biometric that were accepted at a given threshold to the total number of impressions presented for verification in percentage. Mathematically TMR is expressed as;

$$TMR(\%) = \frac{Total\ TMR\ @\ threshold\ 25}{Total\ Number\ of\ impression}$$

The TMR/TAR result below was for the original image;

$$TMR(\%) = \frac{571}{700} \times \frac{100}{1}$$

$$TMR(\%) = \mathbf{81.57}\%$$

The TMR/TAR result below was for the decrypted image

$$TMR(\%) = \frac{571}{700} \times \frac{100}{1}$$

$$TMR(\%) = \mathbf{81.57}\%$$

During the verification exercise, at a threshold set at 25, a number of the genuine fingerprints, 129 out of 700, failed to match with the enrolled fingerprint template from the same finger. This exercise was made for both the original images and for decrypted image. In both cases the same result was found as: 129 false non-matches (False Non Match Rate (FNMR) is 18.43%) and 571 true matches (True Match Rate (TMR) is 81.57%). Thus; the Table 3 shows this distribution in a tabular form.

Table 3. Table Showing the True Match Rate (TMR) and True Non Match Rate (TNMR) Scores of Original Images and Decrypted Images

Fingerprint	Total number of impression for verification	True Matches	True Non-Matches	True Match Rate **(TMR)**	False Non-Match Rate **(FNMR)**
Original	**700** *impressions*	**571**	**129**	**81.57%**	**18.43%**
Decrypted	**700** *impressions*	**571**	**129**	**81.57%**	**18.43%**

The bar-charts in Figure 3, Figure 4 and Figure 5 are from results in Table 1.

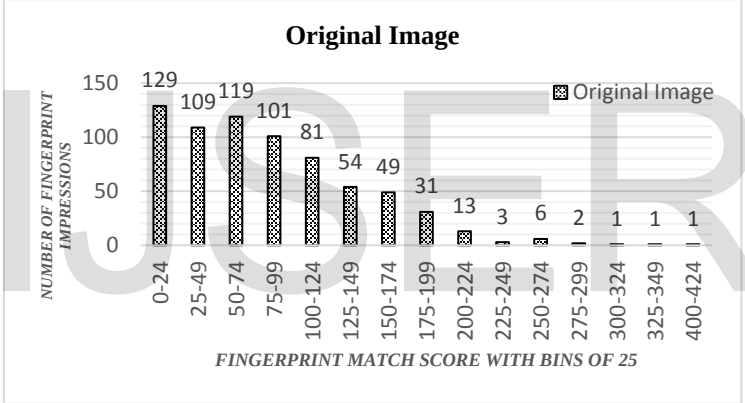

Figure 3. Chart Showing the Distribution of the Match Scores of the Original Image with Bins of 25

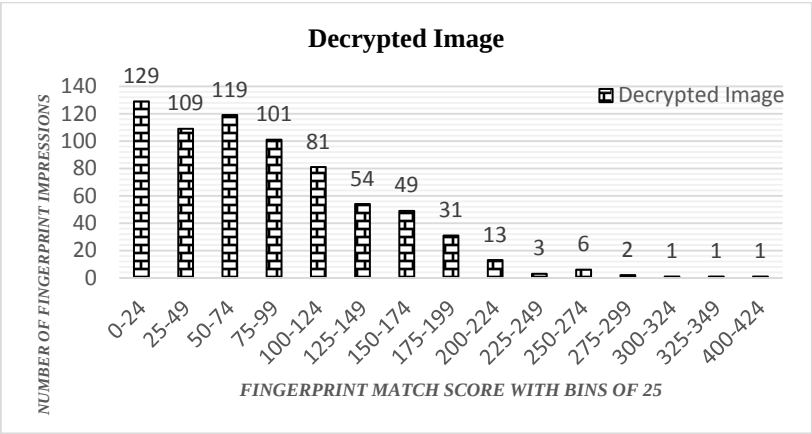

Figure 4. Chart Showing the Distribution of the Match Scores of the Decrypted Image with Bins Of 25

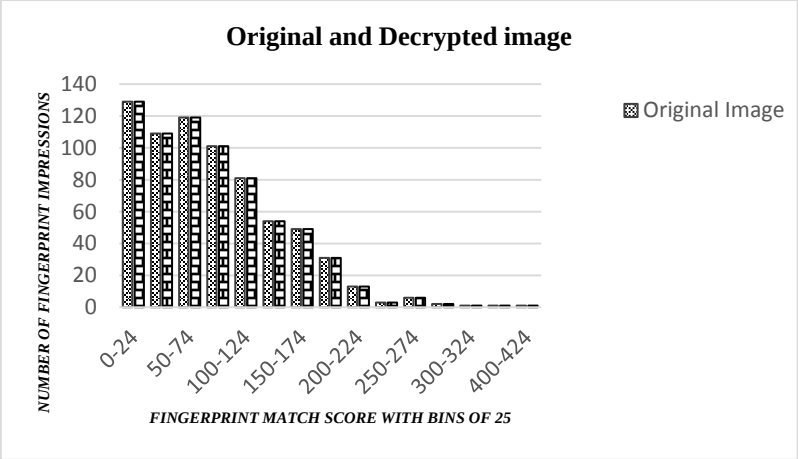

Figure 5. Chart Showing the Distribution of the Match Scores of the Original and Decrypted Image with Bins of 25

The bar-charts in Figures 3, 4 and 5 are plotted from the result of the verification exercise as tabulated in Table 1. Figure 3 shows a bar-chart of the distribution of the match scores of the original image in bins of 25. Figure 4 shows a bar-chart of the distribution of the match scores of the decrypted image in bins of 25. Lastly, Figure 5 is a bar-chart showing comparatively the distribution of the match scores of the original and decrypted fingerprint image in bins of 25. The chart in Figure 5 shows that the proposed encryption algorithm did not in any form cause degradation to the images since the bars of both the original and decrypted fingerprint images are found to be both equal in height and width at each bin of scores on the chart.

4. Conclusion and Recommendation

4.1 Conclusion

The proposed encryption technique was designed to be adaptive such that it could adapt to handle images of any dimension. The encryption key, derived from the Gaussian function was designed to secure the biometric template that would be stored in a biometric database. The biometric template was successfully shielded, leaving no clue of the original print in the stored template for an intruder to attack. From the experimental evaluation on the GrFinger it was observed that the match scores of all images before encryption is exactly the same as the match scores after decryption. The match rates - True Non-Match Rate (TNMR) and True Match Rate (TMR) of the fingerprints before encryption and after decryption are the same. The error rates – False Match Rate (FMR) and False Non-Match Rates (FNMR) are also the same. These results show that the proposed encryption and decryption algorithm did not in any way degrade the encrypted images.

4.2 Recommendations

For further research on this work I recommend;

- The use of ***Verifinger*** (a more efficient fingerprint authentication software) instead of the ***GrFinger*** used in the verification phase of

this work. The ***Verifinger*** can evaluate multiple fingerprints at a go, this would make the work faster and less stressful or burdensome.

- Work has to be done to incorporating image enhancement algorithm to our encryption algorithm, since this could improve the proficiency of the entire work. This would reduce the error rates in matching.

In the future other authors' algorithms may be compared with the proposed algorithm for fingerprint template protection, to see how it improves the state-of-the-art.

References

[1] K. R. Nalini, S. Andrew and M. B. Ruud, "Automated biometrics," *IBM Thomas J. Watson Research Center*, vol. I, no. 1, p. 11, 2000.

[2] V. Anthony, D. Stark, R. Shantanu and Y. Jonathan, "Securing Biometric Data," *MITSUBISHI ELECTRIC RESEARCH LABORATORIES*, vol. I, no. 1, p. 18, 2009.

[3] O. Lawrence and N. Chatham, " FINGERPRINT VERIFICATION," *springer*, vol. I, no. 1, p. 2003, 2006.

[4] S. T. Corporation, "About FAR, FRR and EER," SYRIS Technology Corp. , 2004.

[5] O. Lawrence, "Comparing Passwords, Tokens, and Biometrics for User Authentication," *IEEE*, vol. XCI, no. 12, p. 38, 2003.

[6] Y. Jianwei, L. Lifeng and J. Tianzi, "An Improved Method for Extraction of Fingerprint Features," *IEEE*, vol. II, no. 1, p. 7, 2010.

[7] Anil K. Jain, Aron Ross, Umut Uludag, "BIOMETRIC TEMPLATE SECURITY: CHALLENGES AND SOLUTIONS," *BIOMETRIC TEMPLATE SECURITY: CHALLENGES AND SOLUTIONS*, vol. i, no. 3, p. 4, 2005.

[8] K. J. Anil, R. Arun and P. Sharath, "Biometrics: A Tool for Information Security," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, vol. I, no. 2, p. 19, 2006.

[9] Mrs.U.Latha, Dr.K.Rameshkumar, "A Study on Attacks and Security Against Fingerprint Template Database," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 2, no. 5, p. 5, 2013.

[10] N. Abhishek, N. Karthik and K. J. Anil, "Biometric Template Transformation: A Security Analysis," *Institute for Infocomm Research*, vol. I, no. 1, p. 16, 2007.

[11] Y. Shenglin and V. Ingrid m., "A Secure Fingerprint Matching Technique," *WBMA* , vol. I, no. 1, p. 6, 2003.

[12] Anil, K. Jain; Abhishek, Nagar; Karthik, Nandakumar, "Fingerprint Template Protection: From Theory to Practice," *Springer*, vol. I, no. 1, p. 29, 2012.

[13] S. Yagiz, L. Qiming and M. Nasir, "How to Protect Biometric Templates," *IEEE*, p. 11, 2006.

[14] R. Uday, E. Ali and B. George, "A comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion," *Springer-Verlag*, vol. I, no. 1, p. 10, 2009.

[15] G. Dr M. and K. D., "A Secured Public Key Cryptosystem for Biometric Encryption," *Research Scholar*, vol. IX, pp. 8-16, 2010.

[16] R. Arun, S. Jidnya and A. K. Jain, "Towards Reconstructing Fingerprints From Minutiae Points," *SPIE*, vol. II, no. 5779, p. 13, 2005.

[17] S. Yagiz, T. S. Husrev and M. Nasir, "A Geometric Transformation to Protect Minutiae-Based Fingerprint Templates," vol. I, no. 1, p. 8, 2010.

[18] N. K. Ratha, C. J. H. and B. R. M., "Enhancing security and privacy in biometrics-based authentication systems," *IBM system journal*, vol. XL, no. 3, p. 21, 2001.

[19] C. Moujahd, S. Ghouzali, M. Mikram, M. Rziza and G. Bebis, "Spiral Cube for Biometric Template Protection," *Springer-Verlag Berlin Heidelberg*, p. 10, 2012.

[20] T. Pim, H. A. Anton, A. K. Tom, S. Geert-Jan, M. B. Asker and N. V. Raymond, "Practical Biometric Authentication with Template Protection," *Springer-Verlag Berlin Heidelberg*, p. 11, 2005.

[21] X. Kai and H. Jiankun, "Biometric Mobile Template Protection: A Composite Feature based Fingerprint Fuzzy Vault," *School of Computer Science and IT*, vol. I, no. 1, p. 5, 2009.

[22] N. Abhishek, N. Karthik and K. J. Anil, "Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptors," *IEEE*, p. 4, 2008.

[23] M. I. P. C. S. M. J. F. Emanuele Maiorana, O.-G. Javier and N. Alessandro, "Cancelable Templates for Sequence-Based Biometrics with Application to On-line Signature Recognition," *IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS*, vol. XL, no. 3, p. 14, 2010.