ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

A Novel Fingerprint Template Encryption Scheme based on DNA Encoding and Genetic Algorithm

MR. Nithyakalyani[1], Dr. V. Palanisamy[2]

[1]M.Phil Research Scholar, [2]Professor&Head
[1,2]Department of Computer Science and Engineering, Alagappa University,
Karaikudi-600 003, Tamilnadu, India.
[1]itsyoursnithya@gmail.com,[2]vpazhanisamy@yahoo.com

Abstract— **With the rapid development in the field of digital technology, biometrics makes highest level of security over traditional methods like Passwords and PIN numbers. Biometric is the study of automated identification by use of physical (Fingerprint, Iris, Hand, DNA, Face) or behavioral (Voice, Signature, Keystroke) traits. Among all the Biometric traits, Fingerprint is an essential proven technology for verifying personal identity. In fact, a fingerprint template is the most universal, constant and distinctive. Meanwhile, there is a chance to attackers can access the fingerprint templates in which that are stored in a database. To secure this biometrics fingerprint templates from illegitimate users, many researchers have been proposed various techniques. In this paper, a novel fingerprint template encryption scheme based on DNA Encoding and Genetic Algorithm is proposed.Initially, the fingerprint template is decomposed into 4×4 pixel blocks and these blocks are encrypted by using genetic algorithm. Then, output sequence of the GA is mapping with DNA Nucleotide table and finally, these mapped sequences are XORed with OTP DNA sequences.Experiments are conducted on various samples toevaluate its performance using NPCR, UACI and entropy. From the results, ensures that high level of security is accomplished by this novel scheme.**

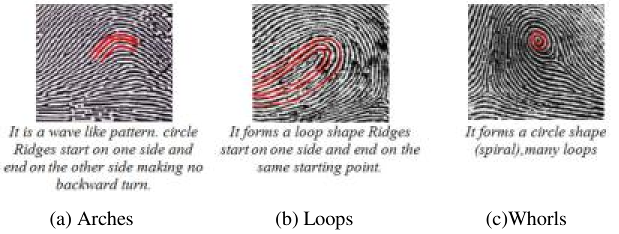
Keywords— **Biometrics, Fingerprint, Template, Security, Encryption, DNA (Deoxyribonucleic acid), Nucleotide, Genetic algorithm.**

I. INTRODUCTION

Nowadays, Security is become very important issue in biometrics system. Conventional security systems used knowledge based methods such as Passwords, pins and token based methods such as key, license, smart card. These methods are attacked by unauthorized person by using effective tools to crack the password or forged without permission of authorized holder. So a biometrics system is needed for reliable, identification and authentication. Biometrics is a security solution depend upon something one know (Password, PIN), have (Key, Smart Card), and are (Fingerprint, Face, etc.)[1].

The word Biometrics with Greek origin meets "Life Measurement" which defines Bios as life and metric as a measurement. Biometrics refers to science and technique for identifying/verifying the person by measuring and analysing human characteristics. It has the potential to distinguish between an authorized entity and faker. Person to person have unique characteristics which are used to prevent threat [2]. Thus Biometrics has no risk of forgetting it, getting in stolen, getting it copied, being used by anyone else. In general, biometric characteristics are divided in to two types. One is Static (Physiological) that refers shape of the body such as Fingerprints, Face, Iris, Hand geometry/ vein, Retinal pattern, DNA and the other is Dynamic (Behavior) that refers behavior of a person such as Signature, voice, keystroke, pulse. The hardware captures the salient human characteristic. The software interprets the resulting data and determines acceptability.

Fingerprint based biometric system is high universality, distinctiveness, permanence, performance and acceptability in comparison to others like Face, Iris, Hand geometry, Signature, and voice. It has been in use for a long time. For each person, fingerprint is unique and permanent. A person has different fingerprints in different fingers. Fingerprints for twins also considered being unique but they are having same DNA. Fingerprint uniqueness is determined by ridge patterns and valleys. A fingerprint image is read from a capture device. Features are extracted from the image and then template is created for comparison.


It is a wave like pattern. circle Ridges start on one side and end on the other side making no backward turn.
It forms a loop shape Ridges start on one side and end on the same starting point.
It forms a circle shape (spiral),many loops

(a) Arches (b) Loops (c)Whorls

Fig. 1Ridge patterns models

Template security is very essential in the development of biometric system because unauthorized person can stolen this template, can be replaced or altered in the communication channel between the database and matcher[3]. Encrypting the templates is the remedy to this susceptible attack. In practices, cryptography approach is used for encryption. Cryptography is the one of the best way to secure the information with concerning 3 goals such as confidentiality, data integrity and availability [4]. Sender use cryptographic algorithm for enciphering the secret data in unreadable format and send it via the communication channel. An intended recipient only deciphering the secret by using decryption algorithm with secret key so that the secret message is can't alter or read by intruders. In the area of cryptography, various algorithms such as DES, AES, IDEA and Blow Fish etc., were designed in past years which is not suitable for image encryption. Nowadays, DNA (Deoxyribonucleic acid) cryptography is the new emerging technique in which DNA used as an information carrier.

This modern technique has the capability of vast storage capacity than traditional approach and the aim of the DNA is to encrypting secret data in DNA strands. DNA is composed of four nucleotides such as 'A' terms Adenine, 'C' terms Cytosine, 'T' terms Thymine, and 'G' terms Guanine [5, 6]. These bases are encode into two bit binary as A= (00), C= (01), G= (10), T= (11) and for example, pixel value is 160 then it is represented in binary form 10100000 and its DNA sequence is GGAA. The time taken for DNA cryptography is hour, deals with DNA strands (108 tera-bytes) per gram when compared to conventional cryptography [7]. DNA computing is the backbone for the development of DNA cryptography. L.Adleman *et al.* [8] have been credited for introduced DNA Computing and after that, DNA cryptography was born and many researcher being research on DNA cryptography.

II. Related Literature Review

Ashish Gehani *et al.* [9] proposed first experimental model of DNA Cryptography in which use two methods are substitution and bitwise XOR OTP cryptosystem for encrypt messages. Jie Chen *et al.* [10] introduced novel paradigm for encoding/decoding two dimensional images by use of molecular theory and OTP. Sherif T. Amin *et al.* [11] enhancing the security by implement YAEA algorithm which is termed as "Yet Another Encryption Algorithm" based on symmetric approach. A novel concept is introduced by Qiang Zhang *et al.* [12] in which addition operation of DNA sequences are used and it has capable to resist exhaustive, statistical attack and differential attack. In the area of DNA based Cryptography, robust algorithm based symmetric block cipher is designed by Souhila Sadeg *et al.* [13] in which perform translation from DNA to mRNA and again from mRNA to amino acids.

Qiang Zhang *et al.* [14] have been credited with development of another novel algorithm for image encryption by using the DNA sequence addition combined with chaotic maps. Feasible approach is presented by Qiang Zhang *et al.* [15] for enciphering images based on DNA Fractal. Kuldeep Singh *et al.* [16] ensure that cross chaotic map is the best fit to encrypting images through the experimental results. Morteza SaberiKamarposhti *et al.* [17] proposed new hybrid method based on the combination of chaotic shuffling and DNA sequence. The superior algorithm is developed by Lili Liu *et al.* [18] for encoding color image in which not need to biological experiment and provide high level of security than other DNA based algorithms.

Hongjun Liu *et al.* [19] have suggested novel method based confusion and diffusion for encrypting images. A hybrid scheme for encryption using DNA in which key image is transmitting over the secure channel was proposed by Grasha Jacob *et al.* [20]. DNA is combined with JPEG ZigZag coding scheme is presented by Grasha Jacob *et al.* [21] for transfer images with secure and merits of this method is that encipher image size is equal to that of the plain image and also no need of key image.

Qiang Zhang *et al.* [22] have recommended the new method which has the strong capability to resist statistical attack. The method based DNA and chaotic map technique for securing the Iris was suggested by Anil Johny *et al.* [23]. Grasha Jacob *et al.* [24] came out with an innovative Key Dependent S-Box and DNA method for sending confidential images with high potential of security.

Ritu Gupta *et al.* [25] have designed novel algorithm using DNA complementary rule for encrypting images. The novel hybrid method based DNA, Genetic algorithm and logistic map is suggested by Rasul Enayatifar *et al.* [26] and reduce correlation, increase entropy are the merits of this novel scheme. R Sridevi *et al.* [27] have introduced the concept of DNA cryptography with DES algorithm for secure image transfer with confidentiality and integrity.

R. Guesmi *et al.* [28] have proficiently put forward the novel hybrid scheme in which chaotic mapping, DNA sequence and SHA-2 for encrypting images with good effect and also key space is large. Chunyan Song *et al.* [29] use the Spatiotemporal Chaos to confusing the DNA encrypted image rows and columns in order to improving the security.

III. Proposed Fingerprint Template Encryption Scheme

While fingerprint systems have several advantages than traditional security systems, there are some issues of fingerprint data are arises which is vulnerable to attack. Thus, essentially need to keep the storage of template with securely. In order to protect the fingerprint templates, Genetic algorithm with DNA based cryptography is proposed in this paper.

In this proposed approach, as depicted in the following Figure 2, fingerprint grayscale image is retrieved from corresponding database.

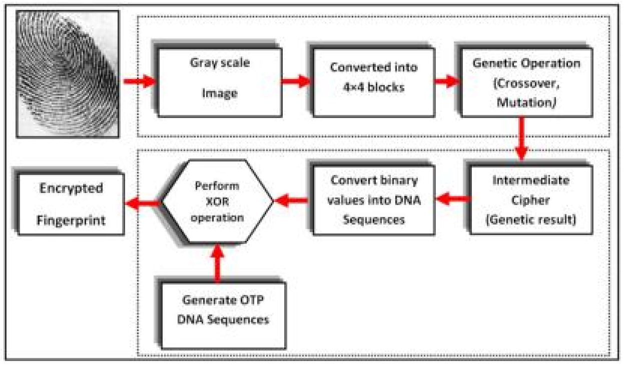

Gray scale Image
Converted into 4×4 blocks
Genetic Operation (Crossover, Mutation)
Intermediate Cipher (Genetic result)
Convert binary values into DNA Sequences
Perform XOR operation
Encrypted Fingerprint
Generate OTP DNA Sequences

Fig. 2 Block diagram of the proposed method

The image is divided into 4×4 pixel blocks andthen converted into binary values.On this binary sequence, thegenetic algorithm, in turn, is employed to use two point crossover and inverse mutation operations. Then genetic sequences are mapped into DNA Nucleotide according to the following Figure 3. To enhancing the security level, OTP based DNA sequence is generated randomly. Then it is XORed with mapped DNA sequence. Finally, the fingerprint image is encrypted efficiently by the proposed scheme. To decipher the original fingerprint template, the reverse process of the encryption is utilized.

Algorithm: Proposed Fingerprint Template Encryption

Step 1: Fingerprint image (F_i)is divided into4×4 pixel blocks.
Step2: Each pixel is encoded in binary numbers and transform into one dimensional array sequence(F_{binary}).
Step3: Initiate a genetic algorithm

$$\left.\begin{array}{l}\text{- Crossover}\\ \text{- Mutation}\end{array}\right\}F_{genetic}$$

Step 4:$Enc_{DNA} = F_{genetic} \rightarrow$DNA Nucleotide Tale ($F_{DNA\_NUC}$)
Step 5: OTP DNA sequence is generated randomly(DNA_{OTP}).
Step 6: Then,$F_{Enc} = Enc_{DNA} \oplus DNA_{OTP}$.

Illustration

1) Original gray level image is read and converts into 4×4 blocks of pixel value matrix say F_i.

$$F_i = \begin{bmatrix} 150 & 110180 & 120 \\ 140 & 160170 & 100 \\ 150 & 180160 & 190 \\ 160 & 170120 & 100 \end{bmatrix}$$

2) Each pixel is encoded in binary numbers

$$F_{binary} = \begin{bmatrix} 10010110 & 0110111010110100 & 01111000 \\ 10001100 & 1010000010101010 & 01100100 \\ 10010110 & 1011010010100000 & 10111110 \\ 10100000 & 1010101001111000 & 01100100 \end{bmatrix}$$

3) Transforms into 1D binary sequence

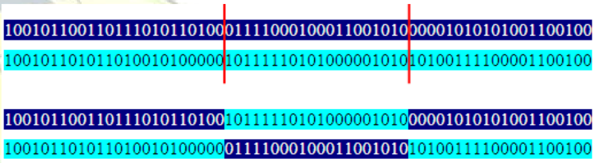
{10010110, 01101110, 10110100, 01111000, 10001100, 10100000, 10101010, 01100100, 10010110, 10110100, 10100000, 10111110, 10100000, 10101010, 01111000, 01100100}

4) Above binary sequences are divided into two equal halves.

1001011001101110101101000111100010001100101000001010101001100100

1001011010110100101000001011111010100000101010100111100001100100

5) Apply two-point crossover on above equation. means Here random points are 24 and 44.



100101100110111010110100 01111000100011001010 00001010101001100100
100101101011010010100000 10111110101000001010 10100111100001100100

100101100110111010110100 10111110101000001010 00001010101001100100
100101101011010010100000 01111000100011001010 10100111100001100100

6) Apply inverse Mutation operation

0110100110010001010010110100000101011111010111110101010110011011

0110100101001011010111111000011101110011010101011000011110011011

7) Again it is converted back into binary pixel array

$$F_{genetic} = \begin{bmatrix} 01101001 & 1001000101001011 & 01000001 \\ 01011111 & 0101111101010101 & 10011011 \\ 01101001 & 0100101101011111 & 10000111 \\ 01110011 & 0101010110000111 & 10011011 \end{bmatrix}$$

8) A result of the genetic algorithm is given as an input of the DNA encryption.

Nucleotide	Binary Number
A	00
C	01
G	10
T	11

Fig. 3Nucleotide and Binary Number Conversion

9) Mapping binary value into nucleotide base according to Figure 3. It is an intermediate cipher for further encryption.

$$Enc_{DNA} = \begin{bmatrix} CGGC & GCACCAGT & CAAC \\ CCTT & CCTTCCCC & GCGT \\ CGGC & CAGTCCTT & GACT \\ CTAT & CCCCGACT & GCGT \end{bmatrix}$$

10) Now generate 64 bit OTP key which is generated random manner, it is change for next time. DNA always encode in to two bit base.

CGTACTAAGGGCGTACCTTTAAAGCATCGGAACC
CGTACGGGCGTAATTGGGATTCGGTACGCC

11) Then, it is represent in matrix format

$$\mathrm{DNA_{OTP}} = \begin{bmatrix} \mathrm{CGTA} & \mathrm{CTAAGGGC} & \mathrm{GTAC} \\ \mathrm{CTTT} & \mathrm{AAAGCATC} & \mathrm{GGAA} \\ \mathrm{CCCG} & \mathrm{TACGGGCG} & \mathrm{TAAT} \\ \mathrm{TGGG} & \mathrm{ATTCGGTA} & \mathrm{CGCC} \end{bmatrix}$$

12) Perform XOR operation between $\mathrm{Enc_{DNA}}$ and OTP DNA sequences. Binary values of $\mathrm{Enc_{DNA}}$ areXORed with $\mathrm{DNA_{OTP}}$.

$$\mathrm{F_{Enc}}= \begin{bmatrix} \mathrm{AACC} & \mathrm{TGACAGAG} & \mathrm{ACGA} \\ \mathrm{AGAA} & \mathrm{CCTGACGA} & \mathrm{ATGT} \\ \mathrm{ATTT} & \mathrm{GATCTTCC} & \mathrm{CACA} \\ \mathrm{GCGC} & \mathrm{CGGAAGGT} & \mathrm{TTTG} \end{bmatrix}$$

13) Now DNA code is transform back into decimal pixel to acquire encrypted fingerprint.

$$\mathrm{F_{Enc}}= \begin{bmatrix} 5 & 22534 & 245 \\ 32 & 94\ 24 & 160 \\ 86 & 141245 & 68 \\ 153 & 104\ 43 & 254 \end{bmatrix}$$

14) To decrypt the fingerprint, DNA based cryptography image is taken as an input and AGCT characters are encode according (00, 01, 10, and 11).

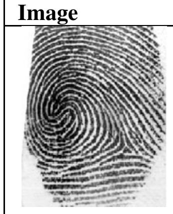
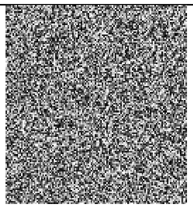
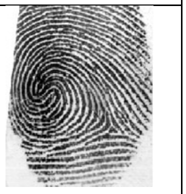
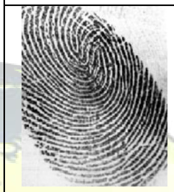
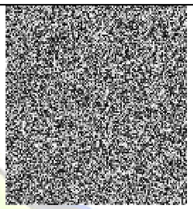
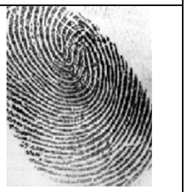
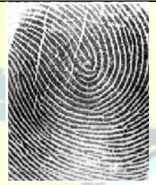
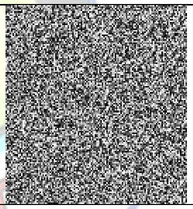
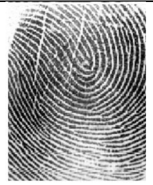
15) Then, reciprocal of two-point crossover and inverse mutation is used to produce original fingerprint.

IV. Experimental Results and Analysis

A. *Experimental Results*

The strength of the proposed biometric template encryption scheme is evaluated by tested various fingerprint image samples. The experiments conducting on CASIA database which is composed of 20,000 unique users' fingerprint images[30]. Table 1 shows that the experimental results of the original fingerprint images, enciphered images and deciphered images.The results of the mentioned samples, encoding templates of fingerprint have been done and acquire same outcome.

TABLE I
EXPERIMENTAL RESULTS ON FINGERPRINT IMAGE SAMPLES

Original Fingerprint Image	**Encrypted Image**	**Decrypted Image**
		
		
		

B. *Performance Analysis*

In general, enciphered image is completely differing from plain image. Such difference could be calculated by NPCR and UACI. Here, performance is analysed by NPCR, UACI and Entropy analysis.

1) NPCR and UACI: Number of Pixels Changing Rate (NPCR) which means change rate of the no of pixels in image. If NPCR get close to 100% then plain image is highly encrypted.

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i, j)}{M \times N} \times 100\%$$

UACI is term of Unified Average Changing Intensity which is used to measuring the average intensity of pixels difference between the plain image and enciphered image. If UACI around 33% then it is more sensitive resist differential attack.

$$\mathrm{UACI} = \frac{1}{M \times N}\left[\sum_{i,j} \frac{\left|F_i(i, j) - F_{ENC}(i, j)\ \right|}{255}\right] \times 100\%$$

Fingerprint image samples are calculated by using above formulas. Table 2 shows that NPCR and UACI values of original fingerprint and encrypted fingerprint.

TABLE II
NPCR AND UACI VALUES OF FINGERPRINT IMAGE SAMPLES

Image Name	NPCR (%)	UACI (%)
Fingerprint1	99.76	33.38
Fingerprint2	99.64	33.42
Fingerprint3	99.65	33.62

NPCR of original and encrypted Fingerprint images gets nearly to 99.68 and UACI values are around 33.38respectively.

2) *Entropy Analysis:* It is used to depict the randomness of source data. The ideal entropy of encrypted image gets near to 8. The Table 3 describes the entropy values of fingerprint encrypted and decrypted image.

$$E=\sum_{i=0}^{255}\left[P(S_i)\log_2\left(\frac{1}{P(S_i)}\right)\right]$$

TABLE III
ENTROPY VALUES OF FINGERPRINT IMAGE SAMPLES

Image Name	Entropy	
	Original Image	Encrypted Image
Fingerprint1	7.1478	7.9982
Fingerprint2	6.7256	7.9968
Fingerprint3	6.9845	7.9974

The entropy values of original Fingerprint1, Fingerprint2, and Finngerprint3 are 7.1478, 6.7256 and 6.9845 respectively. Nevertheless, the entropy values of encrypted Fingerprint1, Fingerprint2, and Fingerprint3 are 7.9982,7.9968 and 7.9974 respectively. These values are close to 8 ensures that proposed scheme highly resist against statistical attacks.

C. *Comparative Analysis*

The proposed fingerprint template encryption scheme is compared with many other existing schemes[2, 14–20] are listed in Table 4.

TABLE IV
COMPARISON OF ENTROPY, NPCR, UACI MEASURES WITH EXISTING SCHEMES

Schemes	Entropy (sh)	NPCR (%)	UACI (%)
Propsoed Scheme	7.9982	99.76	33.38
Zhang *et al.*	7.9936	99.62	33.36
Song *et al.*	7.9967	99.58	33.49

Figure 4 shows that the Entropy, NPCR and UACI values of the proposed method is better than the existing method. So the image security is improved by the proposed Scheme.

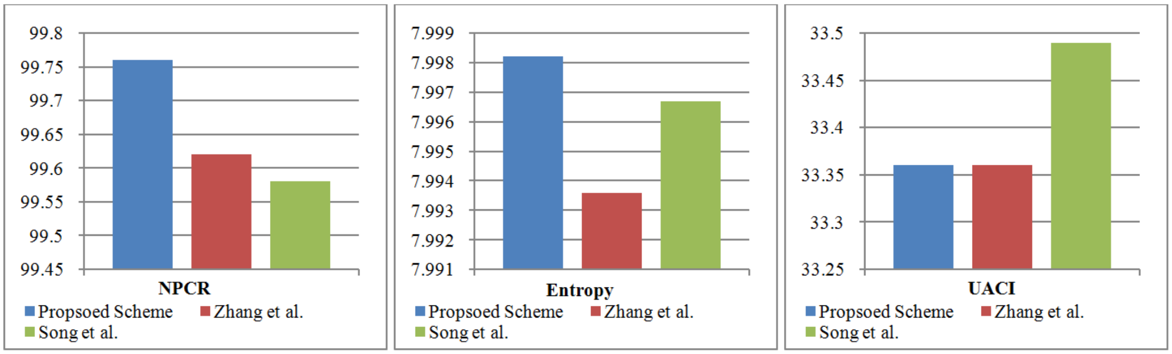


Fig. 4Graphical representation of existing and proposed scheme

V. CONCLUSIONS

Since the authentication of biometrics techniques over open network occurs more and more, security of such techniques is more important. DNA cryptography has been emerging technology at present. In this proposed scheme, human fingerprint is encrypted by using the properties of DNA and Genetic algorithm which ensures preserving the privacy of the template. Moreover, OTP DNA sequences are generated randomly which is never reused and it improves the security of basic OTP approach by use of DNA codons. To analysis the performance of the proposed scheme, NPCR, UACI, and Entropy are used. Thus,the combination of Genetic algorithm and DNA Cryptography could be used for authentication of fingerprint template efficiently and securely.

REFERENCES

[1] Ashbourn, Julian. Biometrics: Advanced identity verification: the complete guide. Springer, 2014.

[2] Sharma, Monika. “Fingerprint Biometric System: A Survey.” International Journal of Computer Science & Engineering Technology (IJCSET) 5.07 (2014): 743-747.

[3] Jain, Anil K., Arun Ross, and Umut Uludag. “Biometric template security: Challenges and solutions.” Signal Processing Conference, 2005 13th European. IEEE, 2005.

[4] Behrouz A Forouzan, Debdeep Mukhopadhyay, “Cryptography and Network Security, McGraw-Hill , Second edition, 2010.

[5] Zhang, Mingjun, *et al*. "Interactive DNA sequence and structure design for DNA nanoapplications." NanoBioscience, IEEE Transactions on 3.4 (2004): 286-292.

[6] Watson, J. D., and F. H. C. Crick. "A structure for deoxyribose nucleic acid." A century of Nature: twenty-one discoveries that changed science and the world (2003): 82.

[7] Cui, Guangzhao, *et al.* "DNA computing and its application to information security field." Natural Computation, 2009. ICNC'09. Fifth International Conference on. Vol. 6. IEEE, 2009.

[8] Adleman, Leonard M. "Molecular computation of solutions to combinatorial problems." Science 266.5187 (1994): 1021-1024.

[9] Gehani, Ashish, Thomas LaBean, and John Reif. "DNA-based cryptography." Aspects of Molecular Computing. Springer Berlin Heidelberg, 2003. 167-188.

[10] Chen, Jie. "A DNA-based, biomolecular cryptography design." Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on. Vol. 3. IEEE, 2003.

[11] Amin, Sherif T., Magdy Saeb, and Salah El-Gindi. "A DNA-based implementation of YAEA encryption algorithm." Computational Intelligence. 2006.

[12] Zhang, Qiang, *et al*. "An image encryption algorithm based on DNA sequence addition operation." Bio-Inspired Computing, 2009. BIC-TA'09. Fourth International Conference on. Ieee, 2009.

[13] Sadeg, Souhila, *et al.* "An encryption algorithm inspired from DNA." Machine and Web Intelligence (ICMWI), 2010 International Conference on. IEEE, 2010.

[14] Zhang, Qiang, Ling Guo, and Xiaopeng Wei. "Image encryption using DNA addition combining with chaotic maps." Mathematical and Computer Modelling 52.11 (2010): 2028-2035.

[15] Zhang, Qiang, Shihua Zhou, and Xiaopeng Wei. "An efficient approach for DNA fractal-based image encryption." Appl. Math. Inf. Sci 5 (2011): 445-459.

[16] Singh, Kuldeep, and Komalpreet Kaur. "Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it." International Journal of Computer Applications 23.6 (2011).

[17] SaberiKamarposhti, Morteza, Ibrahim AlBedawi, and Dzulkifli Mohamad. "A new hybrid method for image encryption using DNA sequence and chaotic logistic map." Aust. J. Basic Appl. Sci 6.3 (2012): 371-380.

[18] Liu, Lili, Qiang Zhang, and Xiaopeng Wei. "A RGB image encryption algorithm based on DNA encoding and chaos map." Computers & Electrical Engineering 38.5 (2012): 1240-1248.

[19] Liu, Hongjun, and Xingyuan Wang. "Image encryption using DNA complementary rule and chaotic maps." Applied Soft Computing 12.5 (2012): 1457-1466.

[20] Grasha Jacob, Murugan A, "A Hybrid Encryption Scheme using DNA Technology", IJCSCS Vol 3, Feb 2013

[21] Jacob, Grasha, and A. Murugan. "An Encryption Scheme with DNA Technology and JPEG Zigzag Coding for Secure Transmission of Images." arXiv preprint arXiv:1305.1270 (2013).

[22] Zhang, Qiang, Ling Guo, and Xiaopeng Wei. "A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system." Optik-International Journal for Light and Electron Optics 124.18 (2013): 3596-3600.

[23] Johny, Anil, and Siyamol Chirakkarottu. "Secure Encryption Method for Biometric Iris Pattern."

[24] Jacob, Grasha, and A. Murugan. "SECURE STORAGE AND TRANSMISSION OF IMAGES BASED ON A DUAL ENCRYPTION SCHEME." (2006).

[25] Gupta, Ritu, and Anchal Jain. "A New Image Encryption Algorithm based on DNA Approach." International Journal of Computer Applications 85.18 (2014).

[26] Enayatifar, Rasul, Abdul Hanan Abdullah, and Ismail Fauzi Isnin. "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence." Optics and Lasers in Engineering 56 (2014): 83-93.

[27] Sridevi, R., and S. Karthika. "SECURED IMAGE TRANSFER THROUGH DNA CRYPTOGRAPHY USING SYMMETRIC CRYPTOGRAPHIC ALGORITHM." (2015).

[28] Guesmi, R., *et al.* "A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2." Nonlinear Dynamics 83.3 (2016): 1123-1136.

[29] Song, Chunyan, and Yulong Qiao. "A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos." Entropy 17.10 (2015): 6954-6968.

[30]http://biometrics.idealtest.org.