ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

A Secured Data Transmission using Genetic based Encryption Techniques over Wireless Networks

Mrs. K. Rajasri, S. Sathiyadevi, Mrs. S. Tamilarasi

***Abstract*—The speedy development in wireless networks entails the defending data while transmitting in the network. To employ cryptographic algorithm is difficult view in wireless networks. Biometric features such as face, voice, fingerprint, iris, and retina can be possible options to produce a cryptographic key over a predictable cryptography and improve the security. In this paper cryptographic key production using cancelable iris to grant security, authentication code is discussed. This proposed technique has three benefits in excess of previous method. First, authentication code is produced to grant authentication and rectitude. Second, to grant security records is encrypted using two fish encryption key produced from the iris biometric of the receiver. Third, randomization is offers using genetic operator to save from a variety of attacks. The proposed model is examined next to security attributes authentication, confidentiality, integrity. It is establish that it endures against cryptanalytic attack. Analysis taken place by the means of performance and security.**

***Index Terms*—Genetic Algorithm, Two Fish Algorithm, Encryption, Wireless Network**

I. INTRODUCTION

Biometric is a method so as to utilizes the human‘s physical and behavioral attribute. Hence it is further reliable than the conventional methods. Of every one the biometric techniques iris recognition is most excellent since no two human‘s iris will be the similar, still if they are twins. Besides the left and the right of an entity’s iris differs which covers method for consistency.

Biometric is constantly a substitute for the password standard authentications method. However if biometric is negotiation, it is missing evermore and probably for each application wherever the biometric is applied. If the similar biometric is applied for the several applications, a user preserve be tracked from single application toward the through cross-matching biometric databases. In its place cancelable adaptation is used to satisfy the requirement of the application along with it can be organized in huge deployments[5].

***Mrs. K. Rajasri**, Assistant Professor, Department of Computer Science, Christ College of Engineering and Technology, Pondicherry University, Pondicherry, India,*

***S. Sathiyadevi**, Department of Computer Science, Christ College of Engineering and Technology, Pondicherry University, Pondicherry, India,*

***Mrs. S. Tamilarasi**, Department of Computer Science, Christ College of Engineering and Technology, Pondicherry University, Pondicherry, India,*

One of the search algorithm is a genetic algorithm standard on the mechanics of usual selection and usual genetics [7]. While précised by Tomassini [8], the most important idea is that in organize for a population of those to adapt to various atmosphere, it should perform like a usual method. This means that endurance and imitation of an entity is encouraged by the elimination of ineffective or destructive behavior and by satisfying useful performance. The genetic algorithm [9] belongs toward the family of progressive algorithms, beside among genetic programming, progress strategies, and progressive programming. Progressive algorithms can be considered as a wide group of stochastic optimization techniques. An progressive algorithm preserves a population of applicant solutions for the trouble at hand. The population is after that developed by the iterative function of a rest of stochastic operators. The rest of operators typically consists of alteration, recombination, and selection otherwise something extremely related. Globally acceptable, if sub-optimal, solutions toward the trouble are establish in a lot the similar method as populations during nature adapt to their neighboring atmosphere.

Using Tomassini’s terms [8], genetic algorithms (GAs) regard as an optimization problem since the environment wherever feasible solutions are the those living during to environment. The degree of adaptation of an individual toward its environment be the matching part of the fitness purpose assessed on a solution. Likewise, a position of feasible solutions obtains the position of a population of organisms. An individual be a string of an binary digits otherwise some further set of symbols drawn as of a finite set. Every encoded individual during the population may be sighted as a representation of a exacting solution to a problem.

Twofish [6] is a symmetric block cipher; a single key is employed for encryption and decryption. Twofish has a block size of 128 bits, along with allows a key of any length up to 256 bits. (NIST needed the algorithm to allow 128-, 192-, and 256-bit keys.) Twofish is speedy on equally 32-bit as well as 8-bit CPUs (smart cards, embedded chips, and the like), along with in hardware. As well as it is flexible; it can be employed into network applications wherever keys are modified normally also in applications where present is tiny otherwise no RAM and ROM presented.

Accomplishment of hard-cryptographic algorithms are concerning and challenging beside the security attacks. So the proposed approach to create a genetic based non-invertible cryptographic key as of the cancelable Iris minutia template and auxiliary propose a model designed for secure

authentication. In this paper we as well check the encryption and decryption time required by our generated key.

The following segments describe the paper orderly: Section II to create a cryptographic key as of the cancelable Iris minutia template. In section III Analysis the Performance and Security and as a final point we conclude in section V.

II. PROPOSED WORK

In this proposed work secured authentication model, the data integrity and authentication of the data is provided from end to end authentication code and security be granted through the created non-invertible key as of the cancelable template of the minutiae rest of the Iris. Genetic two point crossover operator is concerned on created vectors by which revocability is accomplished. The calculation requirement and encryption-decryption time is too evaluated further. The most important purpose of the proposed approach is to increase the data security in wireless networks.

In this model [1] we implicit that Iris images of cluster members are stored in the database. As an alternative of storing the symmetric key, symmetric key is created together. In the initial step minutiae points are generated from the receivers Iris and transformed into cancelable template.
Behind transforming cancelable template is to be applied the two points cross over genetic point and generated the cryptographic key K.

The randomization pair of selection indices through the cancelable transformation be stored during the vector and two points of crossover operator are attached to the vector. Behind the key generation the authentication code is attached to the vector. The sender side is encrypted the vector with private key generated and the receiver side reverse process takes place. The data is to be encrypted among generated key K. Behind the generated Authentication AU. Finally, sent the data to the receiver as authentication code, encrypted vector and encrypted data.

At the receiver side reverse procedure takes place. At the receiver side authentication code AU, encrypted vector and encrypted data are extracted.

By utilizing private key, encrypted vector to be decrypted. As to create authentication code AU'. It will check the authentication code is match or not. If it does not equivalent among the AU after that process be expired since data integrity and authentication are violated.

If authentication code match is found in that case employing indexes of arbitrary pair as well as crossover point the key K is generated and next the receiver side using cancelable transform. Hence here both the side symmetric key is to be generated. The data is decrypted using this generated key K.

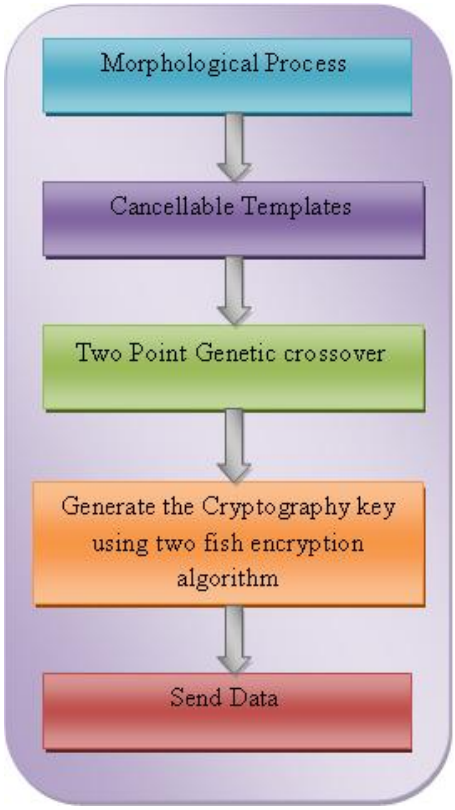


Figure 1: Sender Side Process

A. *Minutiae Extraction From Iris*

The Iris Recognition using some modules is to be applied to develop the accuracy a decrease the time complexity. Generally, after detecting the Iris element, the eyelid as well as eyelashes hamper and decrease the efficiency of the scheme, in this manner affecting the FAR and FRR stages.

In sectoring, the iris region of the most excellent bits on the left and right part are merely considered so with the purpose of the interference of eyelid and eyelashes are entirely ignored. since the consequences achieved by employing merely the most excellent iris bits, the effectiveness of the scheme is developed to a superior degree yielding better FAR and FRR stages while evaluated to the existing systems.

Sample of edges and grooves along with finer points can be employed to decide the uniqueness of Iris. finer points are limited edge qualities that arise at whichever a edge split or a edge ending. Iris is preprocessed to eliminate the noise and unrelated information. This can be implemented employing Mat lab.

1) *Morphological Operators*

The morphological operators [2] are employed to take out the pupil area at a distance as of the further areas of the eye. They are using five morphological operators are:

Morphological Edge

Edges are perceived by convolving the icon through a effortless convolution kernel invented by Sobel and Feldman.

$$\text{Edge Image} = ((E < T) * 255) \qquad (1)$$

Where E = sqrt (H.*H + V.*V), T represents Threshold, H stand for the horizontal edges of the innovative image, V stand for the vertical edges of the innovative image and E stand for the pixel gradients of the innovative image.

Morphological widen

The morphological widen pertains the widen operation rule to enlarge the boundary of the image. According to regulation, the significance of the output pixel is the higher limit significance every one of the pixels during the input pixel's region. If the pixel be location to 1, in that case the output pixel is position toward 1 in a binary image.

$$G(j, k) = F(j, k) \oplus H(j, k) \qquad (2)$$

Where F (j, k) for $1 \leq j, k \leq N$ be a binary-valued image and H (j, k) for $1 \leq j, k \leq L$, Where L be an odd integer, called a construction element as well as it is a binary-valued array

Morphological Attrition

The morphological attrition indentures the boundary. It make use of the attrition operation rule. The imperative states the pixels exterior the image edging are assigned the uppermost value presented by the data type. The pixel significances are presumed to be rest to 1 intended for binary images. The highest assessment for unit8 images be 255 for grayscale images.

$$G(j, k) = F(j, k) \ominus H(j, k) \qquad (3)$$

Where again H (j, k) is an odd size L x L composition element.

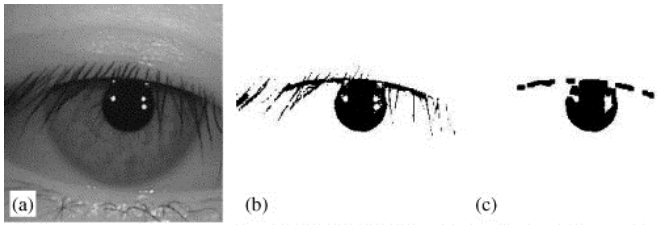
Morphological Load

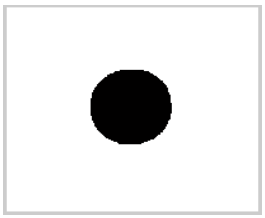
While non-absence connectivity is indicated, the morphological load, fills gap pixels scheduled the outside edge of an image so as to are not linked to the environment.

Morphological obvious Border

The pixels that are brightness than the neighboring as well as attached toward the image border are contained by using morphological obvious border. It utilize the morphological reconstruction. In rebuilding the input is visor image. The indicator image equivalents the visor image beside the borders and be non-zero. In all supplementary cases it equivalents zero.

Under figure illustrates the final output image behind applying the entire morphological operators.





(d)

Figure 2. Morphological Operation (a) Iris image (b) Binary image (c) Edge image after deleting noise region (d) Binary image after morphological operation

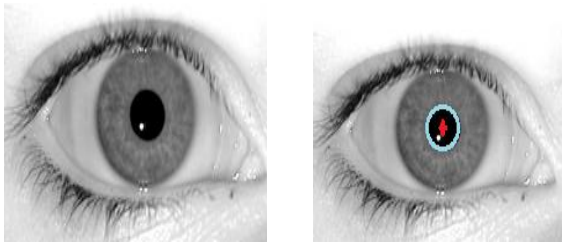
2) Middle And Inner Boundary Localization

The gray position histogram is evaluates and intended. T represents Threshold value is decided based on the strength correlates through the 1st important reach your peak as the histogram. By employing the under equation, the intensity assessment that equivalents T or intensity assessment that is smaller quantity than the assessment or T are modified to zero (black). The intensity assessment superior than the value of T are modified to 255(white). Where, I(x, y) is importance value of position (x, y), g(x, y) is the modified pixel value.

$$g(x, y) = 0, \text{ if } I(x, y) < T \qquad (4)$$
$$g(x, y) = 255, \text{ otherwise}$$

$$\max_{(r, x_p, y_o)} \left| G_\sigma(r) * \frac{\delta}{\delta r} \iint_{r, x_0, y_0} \frac{I(x, y)}{2\pi r} ds \right|$$

Consequently by the beyond process the pupil region is segmented as well as from the first and the last represent points of Threshold the middle of the pupil region is obtained. Subsequently those are connected to appearance the diameter of the pupil and as of which the middle point is decided. Therefore the iris inner circle is acquired using the middle and the radius as in figure 3 (a) and (b) respectively.



(a) (b)

Figure 3: (a) Centre of the pupil detection (b) inner boundary localization

3) Outer Boundary Localization

Daugman's integro differential operator [4] is to be used for perceiving the iris outer boundary afterward the pupil's inner boundary is forecasted. The integro differential operator is to be provide as follows:

$$\max_{(r, x_p, y_o)} \left| G_\sigma(r) * \frac{\delta}{\delta r} \iint_{r, x_0, y_0} \frac{I(x, y)}{2\pi r} ds \right| \qquad (5)$$

Where I(x, y) is an eye image, G σ(r) is an Gaussian smoothing function, R is an radius and S is the circle of contour is given by y0, x0,r.

.

Thus, the beyond Equation the Daugman_s integro differential operator is utilized to decide the iris outer boundary. The outer boundary perceiving of iris is exposed in figure 6 beside among the inner boundary and the middle of Iris.

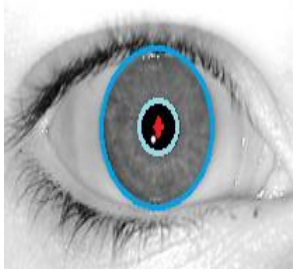


Figure 4: Outer boundary localization

4) Sectoring

In before normalization using the sectored the iris regions. Since for each the proposal of this paper, we sector the iris sections going on the left and right sides by angles 20, 40 and 60, and after that the normalization phase is conceded out designed for the sectored iris regions. The white areas during the left and the right area of the figure 5 illustrate the most excellent bits sections of iris.

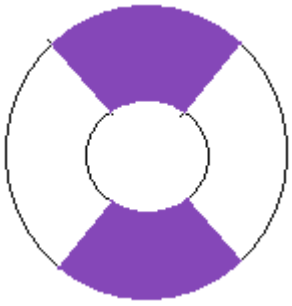


Figure 5. Sectoring the iris

5) Normalization

The below represent the Normalization equation:

$$I(x(r,\varphi),y(r,\varphi),y(r,\varphi))=I(r,\varphi) \quad (6)$$

$$x(r,\varphi)=(1-r)x_p(\varphi)+rx_i(\varphi) \quad (7)$$

$$y(r,\varphi)=(1-r)x_p(\varphi)+ry_i(\varphi) \quad (8)$$

Where I(x, y) is an eye image, Gσ(r) is an Gaussian smoothing function, r is an radius and S is the circle of contour is given by y0, x0, r.

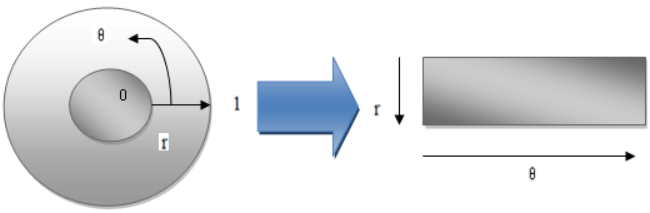
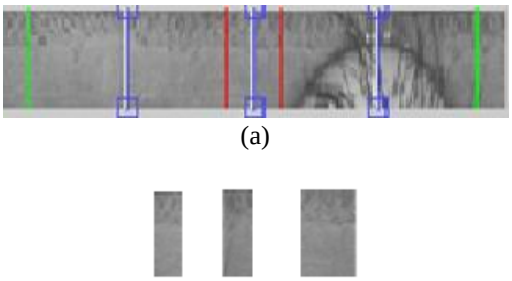


Figure 6: Daugman‘s rubber sheet model

Where $\varphi = (\theta/m)$, m = 3n, here n series from 3, 4, 5… matching toward the value of (φ) subsequently that eyelid and eyelashes are not taken into part. Here _r‘ and _θ‘ are the distance between the inner and the outer boundary of iris and the angle of variations severally as exposed.

Using the equations (6), (7), (8) the sectored regions as of the normalized image is exposed in figure 7 (a) and (b). After that though making the iris code, the code is created merely intended for the sectored division of the iris.



(a)

(b)

Figure 7: (a) sectored regions for n=5 (b)Sectored images

6) Iris Code Generation And Indexing

As follows the phases for Iris indexing. Behind segmentation and normalization as exposed in Figure 7(a) and (b), the normalized iris images be consistently yielded into obstructs, and calculate the number of corners in every obstruct. Subsequently, also yield the disguise off code into obstructs, along with if there survive disguised regions during the obstruct, a standard will record this obstruct as 0, as well as other blocks are marked as 1. Behind that, label each block Iij by an indexing code C (i. j) obeying the rule as follows:

$$C_D(i,j) = \begin{cases} -1, & \text{if } F_{ij}=0 \\ 0, & \text{if } \left(\frac{N_{ij}}{\sum N_{ij}} < Th\right) \text{ and } (F_{ij}=1) \\ 1, & \text{if } \left(\frac{N_{ij}}{\sum N_{ij}} \geq Th\right) \text{ and } (F_{ij}=1) \end{cases} \quad (9)$$

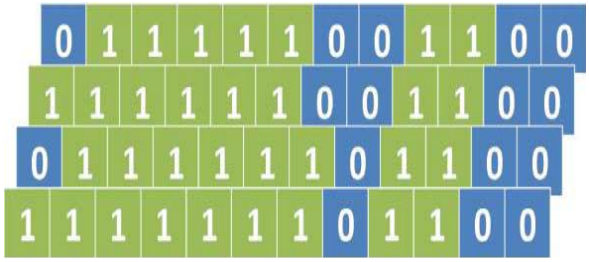
The remaining division of the iris section is too to be applied for verification while it is also a division of the sample hence in order to take away the unwanted regions in it (i.e.) eyelid and eyelashes occluded areas a latest method is applied at this point during which the affected pixels be numbered as -1 during the image as well as the remaining pixels be allocated among the values of 0 and 1 standard on the thresholds. The figure 8 illustrate how it determination look like

Figure 8: (a) Iris Code Generation

(b) Iris Code Generation in the affected region

-1 shows in the listed indexing code, as well as we cannot

distinguish whether this block includes thick or thin textures, which means it preserve be any 1 or 0. To build certain the identity determination be establish the iris code be supposed to be associated to four iris indexing codes as tracks:



At this point the -1 is detached by evaluating the below and the above row of the block also by switching its value to 1 or 0 standard on the adjacent pixel contrast which evaluates the adjacent pixels of the -1 pixel region through the further values during the blocks also the utmost emerged value in the adjacent pixels be allocated toward the -1 pixel.

Now during verification the pixels value patterns are compared with transformed templates and then verified. Once extreme minutiae are suppressed, finally marked position of minutiae are stored in the file which is further used to transform into cancelable Iris template.

B. Cancelable Iris Generation from Transformed Minutiae Points

This part clarifies the technique of transformation of extracted minutiae points into the transformed points as well as generation of cancelable iris.

The Generation of cancellable iris template is explained by the following steps,

1. Consider the extracted minutia points and their equivalent co-ordinates are represented. These co-ordinates be transformed with stored as vector.

2. Find the another corresponding prime number of every value in vector C as well as store it keen on vector P.

3. After that the discrete exponential function [10] is applied toward generate the vector PDE.

4. It can be applied on individual element of C among their corresponding values in P.

5. If the discrete exponential value is obtained prime, after that value is appended to the vector PDE or the next corresponding prime number be obtained as well as appended to PDE.

6. The next step is configuration of RP is to be done with random pair selection form PDE. The indexes used for random selection of the pairs from PDE.

7. The random pairs selected be detached from PDE and also process is to be repeated until PDE is empty.

8. The selected pair is represented and the pair taken out from the PDE.

9. The pair of values during each pair are selected be prime numbers.

10. The pair of values is to be prime numbers hence resultant number is also prime number and which is approximately infeasible to factorize, like explained in RSA factoring challenge [11].

11. The employment of prime number factoring with discrete exponential guarantees that, achieving minutiae point co-ordinates as of transformed points is really difficult. Then the distance between every point through respect to every further point require to be computed.

12. The space calculation between two points calculated.

13. Subsequently values are sorted keen on a separate array. Since this sorted array unique values be taken out and the values achieved are denoted as vector form.

14. These values be sorted more, as well as the unique values are represented.

15. Therefore this way, the generated unique values referred as the cancelable iris template. Using these unique values, we create a non-invertible cryptographic key.

PUD2 as well as merged into CPU_D. [1]

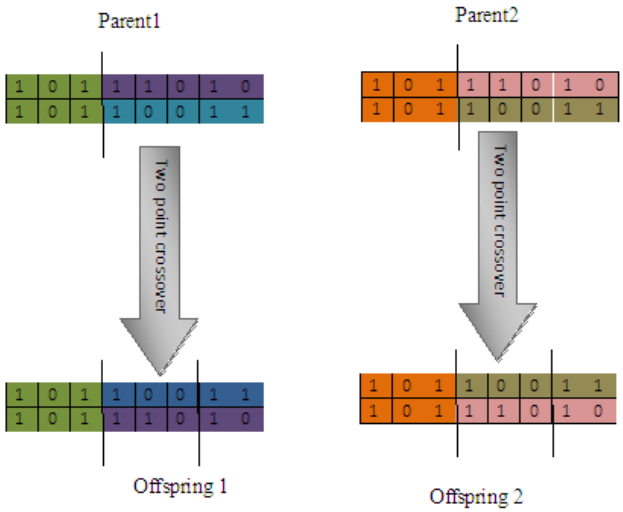


Figure 9 Genetic Two Point Cross Over

After that binary vector NIK is created employing following formula. So as to our necessary key.

NIK [1] = CPU_D (1) mod 2 where 0 < 1 < 256

This key is applied to encrypt the data utilizing Two Fish Encryption algorithm. In this produced key, the pair randomization is used it is complicated for the challenger to trace out. Furthermore the prime numbers are reproduced along with according to RSA factoring challenge impracticable to factorize. The information is extra twisted to

discover exposed the distance. After that unique values are chosen and arranged. Transposition is employed hence it is tricky for challenger to create the similar vector. The genetic crossover operator includes the randomization. Hence it is tricky to improve the template and key.

This proposed pattern can be employed in excess of any networks which detect directions as and while necessary. The records will be sent to the destination just the once forward and reverse paths are locate. Previous to sending the records during to path, the records will encrypted applying the Two Fish Encryption algorithm using created key and decrypted on the receiver part employing said process.

III. ANALYSIS

The proposed system analysed in the means of factors performance and security of algorithms.

A. Performance

The genetic optimizations do certainly roots an improvement in IRIS recognition systems more than other methods. In the part of artificial intelligence, genetic algorithms will play a vital role in system intelligence. Genetic algorithms let a system to get used to changing environments and to offer a improved computing experience for equally users and administrators of these systems.

Twofish algorithm is quite a few performance trades-offs among key-setup time and encryption speed that build it distinctive among the AES candidates. About all encryption algorithms contain various kind of key-setup routine: a method to get the key and build the round subkeys that the algorithm uses. Twofish desires to get the key and make key-dependent S-boxes and round subkeys. Twofish is greatly faster; its key setup can be as rapid as 1.5 encryptions.

Twofish has a range of options. You can get longer for key setup and the encryption accesses faster; this makes logic for encrypting large amounts of plaintext with the similar key. You can setup the key speedily and encryption is slower; this makes sense for encrypting a sequence of short blocks with fast changing keys. All of this option interoperates; they are just dissimilar ways of applying the similar Twofish algorithm. Data can be encrypted by means of one selection and decrypted with another.

B. Analysis Of Security

1) Related Key Attack

It's a half-done chosen-key attack on 10 rounds of Twofish not including the prewhitening and postwhitening. By accumulate the attack, here to use a pair of related keys. And need to get to choose 20 of the 32 bytes of each key. Then have entire control over those 20 bytes of both keys. Then anyone doesn't recognize the left over 12 bytes of key, other than they know that they are the similar for both keys. To end up with trying about 2^{64} chosen plaintexts in each key, and responsibility about 2^{34} work, to get better the left over unknown 12 bytes of key.

2) Successful Chosen-Key Attack

The successful chosen-key attack against Twofish requires choosing 160 bits of a pair of keys, and needs 2^{34} work, 2^{32} chosen-plaintext queries, and 2^{12} adaptive chosen-plaintext queries so that 10 rounds Twofish can be broken.

3) Meet-In-The-Middle Attack

The meet-in-the-middle attack on standard Twofish requires 4 rounds, 256 known plaintexts, 2^{225} memory and 2^{232} work. The successful differential attack on standard Twofish can break 5 rounds with 2^{232} work and 2^{41} chosen-plaintext queries.

There is also a successful meet-in-the-middle attack on 11 rounds Twofish with fixed S-boxes, no 1-bit rotations and no whitening which requires 2^{225} memory, 256 known plaintexts and 2^{232} work.

4) Differential Attack

The differential attack on these nine rounds Twofish needs 2^{41} memory, 2^{41} chosen plaintexts and 2^{254} work. Based on those results we can say that a good number efficient attack against Twofish is the brute force attack as for 128-bit key it needs 2^{128} complexity, for 192-bit key it requires 2^{192} complexity and for 256-bit key the complexity is 2^{256}.

Two fish Encryption prevents from above attacks efficiently and effectively. Depends on the key length and whether Twofish is employed for hardware based or software based encryption Twofish may do better than AES in terms of speed. A lot of people consider Rijndael has just turned into more admired than Twofish as it received additional attention because it was selected for Advanced Encryption Standard (AES) by NIST in 2001. The benefits of Twofish take in that the algorithm is unpatented and royalty-free, with no any licensing requirements.

IV. CONCLUSION AND FUTURE WORK

In the proposed system, cryptographic key is produced using cancelable biometric code and applying genetic and two fish algorithm which is powerful against any attack in networks and provides high security for data transmission. Authentication and data integrity is also provided using authentication code. Additionally data are secured using two fish encryption algorithm. The computation power low compare to other small key size algorithm, but highest security is provided. This module can be deployed to achieve high security in resource rich applications. It takes quite less time to encrypt and decrypt the message and key size changing.

In the future work, the rounds in two fish algorithm can increase, but the encryption speed will get decreased. So in future work, by modifying some aspects in algorithm the above mentioned shortcoming may get overcome.

.

REFERENCES

[1] Mehta Manisha Pravinchandra Hiteishi Milind Diwanji & Jagdish Shantilal Shah and Hemali Kotak, "Performance Analysis of Encryption and Decryption using Genetic Based Cancelable Non-Invertible Fingerprint based Key in MANET", IEEE Conference on Communication Systems and Network Technologies, 2012.

[2] Mrs. K. Rajasri, S. Sathiyadevi, S. Tamilarasi, "New Algorithm and Indexing to Improve the Accuracy and Speed in Iris Recognition", International Journal of Engineering Research and Development Volume 4, Issue 3 (October 2012), PP. 46-52.

[3] Rushdi A. Hamamreh, Mousa Farajallah "Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher"IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.5, May 2009 pg.11 to 16.

[4] J. Daugman, ―How iris recognition works, IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 21–30, Jan. 2004.
[5] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable _ngerprint templates. IEEE Transactions on Pattern analysis and Machine Intelligence, 29(4):561–572, 2007
[6] http://www.drdobbs.com/security/the-twofish-encryption-algorithm/184410744
[7] Goldberg, D. E. (1989). *Genetic Algorithms in Search, Optimization, and Machine Learning*. Boston: Addison-Wesley.
[8] Tomassini, M. (1999). Parallel and Distributed Evolutionary Algorithms: A Review. In K. Miettinen, M. Makela, P. Neittaanm aki and J. Periaux (Eds.), Evolutionary Algorithms in Engineering and Computer Science (pp. 113 – 133). Chichester: J. Wiley and Sons.
[9] Bethany Delman, "Genetic Algorithms in Cryptography"July 20004.
[10] http://en.wikipedia.org/wiki/One-way_function
[11] "RSA Factoring Challenge" from http://en.wikipedia.org/wiki/RSA_Factoring_Challenge

Mrs. K. Rajasri received the B.Tech (Information Technology) and M.Tech (Information Security) degrees in computer science and Engineering from Pondicherry Engineering College affiliated to Pondicherry University, Pondicherry. She is Assistant Professor at the Christ College of Engineering And Technology Affiliated To Pondicherry University, Pondicherry She published her manuscript in reputed journals and her research towards on Network security.

Ms. S. Sathiyadevi Received Post Graduation MCA in Computer Science And Applications From Rajiv Gandhi College Of Engineering And Technology Affiliated To Pondicherry University, Pondicherry and She is Currently Pursuing M.Tech In Computer Science And Engineering From Christ College Of Engineering And Technology Affiliated To Pondicherry University,Pondicherry. She published her manuscript in reputed journals and interested in Web Security and Network Security.

Mrs. S. Tamilarasi received B.E in computer science and Engineering From Priyadharshini Engineering College affiliated to Anna University,Vellore and She is currently pursuing Masters in Computer science and Engineering from Christ College Of Engineering And Technology Affiliated To Pondicherry University,Pondicherry. She published her manuscript in reputed journals and interested in Web Security and Network Security and pervasive computing.