International Journal of Security and Its Applications
Vol. 12, No. 2 (2018), pp.19-28
http://dx.doi.org/10.14257/ijsia.2018.12.2.03

Novel Approach for E-passport Authentication using Elgamal Cryptosystem

Anurag Singh Tomar[1], Sumit Kumar[2], Sandip K Chaurasiya[3] and Vanshika Shrivastava[4]

[1, 2, 3]School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India
[4]Mobivisits private limited, Indore, India
[1]anuragtomar3105@gmail.com, [2]Sumitaggarwal001@gmail.com,
[3]sandipchaurasiya@gmail.com, [4]vanshika.papa09@gmail.com

Abstract

In the modern era, research in the area of biometric data protection and data transmission, security over a network has been reached to a new level. To increase the security at the airport, new generation passport has been introduced i.e. E-passport. This passport consists of a Radio Frequency Identification chip which stores all the information of visiting passenger as well as user's biometric information. This information used by the airport authority for authentication of that user. On the other hand network security is playing a major role in the society by providing the secure communication between the parties, and by telling a person's identification. Other area which is only concern about identity of a person is biometric field; this field is working on human's unique characteristics to provide authenticity. Same authentication concept has been used in the international airport by using passports. There are many techniques have been implemented to provide more security to E-passport. However existing techniques are facing some loopholes such as replay attack, side channel attack. To remove these problems we are using ElGamal algorithm in our work. Our technique uses the value of timestamp to rectify the replay attack and digital signature to remove side channel attack issue. For increasing the authenticity level in E-passport we are taking finger print from biometric traits. We are also using hash function to enhance the biometric template security in database. Overall, it proves that it is a better security mechanism in the case of E-passport.

Keywords*: E-passport, Authentication, Elgamal, Biometric*

1. Introduction

Biometric [2] is a very secure way of identification of a person or authentication of a person. It is well known that humans naturally use some body characteristics such as face, gait or voice to recognize each other. Since, today's world has a wide range of applications that reliable identification schemes to confirm the identity of a person. Identifying humans based on their body characteristics is the main center idea of biometric security schemes in different technology applications. Conventionally, passwords and ID cards have been used to secure the systems but these methods can easily be cracked and are not very reliable. Biometric cannot be borrowed, stolen, or forgotten, and forging one is practically impossible. It is defined as a unique characteristics or traits human body. These traits are used to identifying a person. In modern world scenario the use of ID card such as UID card, pan card, passport all are based on this method.

Received (May 5, 2017), Review Result (September 28, 2017), Accepted (October 30, 2017)

ISSN: 1738-9976 IJSIA

Basically there are two types' human characteristics defined biometric features, behavioral and physical.

In behavioral biometric gaits, voice *etc.* all is traits included and where as physical covers fingerprint, iris, palm *etc.* [9] classifies these two biometric categories. In the recent years, biometrics is growing in very fast way and getting the support from the research area for the security purpose among all the applications of security.

Almost all the security system based up on this biometric authentication or identification and these of systems called as biometric systems. A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector. These feature vectors are usually stored in a database (or recorded on a smart card given to the individual) after being extracted. A biometric system based on physiological characteristics is generally more reliable than behavioral characteristics. Biometric systems have now been deployed in various commercial, civilian, and forensic applications as a means of establishing identity. The main goal of this biometric system is to provide the authenticity of a user. Cryptography field is well renowned field for the authenticity property, as well as data integrity and the privacy of the data during a communication. There are many working fields which are using cryptographic algorithm [1] associated with biometric features for providing the more security. The normal scenario of biometric system is having two phase or modes, enrollment and identification.

First phase enrollment allows the unknown user to register herself by imposing the some biometric features (depending upon the application requirement). In this phase the sensor takes the input from user as his/her trait like fingerprint, face, iris *etc.* called as templates these templates are stored in a database for further use or for user identification.

Second phase is verification, in this procedure user has to impose same trait which she/he has used in the time of registration, than the sensor takes the fresh template and compare it with the stored one if these templates are matched than user is a valid user otherwise sensor denies to allow that user. At some point of time a threshold value (a minimum value) can be set which degraded the FAR and FRR value [10].

Combine these two steps provides a secure authentication to system based on some algorithm for matching the features.

2. Literature Review

Over the past several years, there have been a number of researches has done their research in the field of authentication in many biometric applications such as smart card ,E-passport, TMIS *etc*.

Vijayakrishnan *et al* [11] In this paper author has described about security and privacy issue of proposed technique for first and second generation e-passport *i.e.* Extended Access Control (EAC) proposed by the European Union (EU), for protecting the biometric information. This scheme has some security loop hole at the time of implementation. To remove this drawback author has suggested here a proposed here an on-line authentication mechanism for electronic passports that addresses the weakness in existing implementations, of both The International Civil Aviation Organization (ICAO) and EU using ICAO PKI implementation, which requires very slight changes in current infrastructure. Author has presented an on-line secure e-passport protocol that addresses many weaknesses in both the first and second generation e-passport protocols. This protocol also used existed PKI infrastructure in the first generation e-passport standard and eliminates the need for sending different certificate to the server in the second generation. This mechanism made e-passport in OSEP protocol less vulnerable to DOS based attacks

Mohemad *et al* [12], same as the Vijayakrishnan's study this paper provided a secure mechanism between the e-passport and inspection system (IS), to enhance the communication. Author has discussed here an online authentication mechanism based on Elliptic curve Diffie- Hellman key exchange protocol. The curve has created by the

biometric data and it used comparatively small size key. Parameters of ECC have been taken from biometric templates *i.e.* fingerprint template. It used to enhance the combination between the chip and the IS.

Usha *et al* [3]. In this paper, the author mentioned about enhanced security mechanism based Elliptic Curve Cryptography (ECC) which uses a variation of Diffie-Hellman key agreement protocol between E-Passport and the Examination System (ES). This method uses elliptic curve parameters A, B and G that are derived from the minutiae points of the fingerprint which are stored in a chip embedded in E-passport itself and database. She has used here a base DOV which is defined here as home country of a visitor. The parameter of ECC A, B, and G are derived from each minutia points of fingerprint. From these values shared secret session key between E-Passport and ES is generated. Complete authentication phase has covered in three phases registration phase, ES authentication phase and the E-passport holder authentication. Author has used FVC 2004 public database and R303A scanner for the fingerprint values.

K Hemanth *et al* [4]. Blind authentication protocol has been proposed in this paper which is probably more secure according to author, which concerns about the user's privacy, his biometric information protection and some security draw backs. This blind protocol defines as it reveals only identity of user to server, no other information will reveal to server. This protocol has designed in such a manner that the communication between user and server is of very less computational cost. As this protocol is based on the asymmetric encryption it takes all the advantages of biometric authentication as well as the public key cryptography's. This scheme is providing security from various attacks.

Poorni *et al* [5], this scheme is also provides authentication based on Blind authentication protocol, which is defines previous paper it says that it will disclose only the user's identity no other information. To reduce the computational cost and enhance security she has used ElGamal algorithm which is an asymmetric algorithm, it increase the biometric authentication and the public key cryptography's security. Authentication works on the public network and concerns about the template protection and there retraction. This method assured that accuracy does not affected by authentication in encrypted zone. Author has used hildtich thinning algorithm for feature extraction and the artificial neural network as the working classifier between user and server, which reduced the computation cost at the user's side.

Tan *et al* [6] deals with the smart card authentication in telecare medicine environments. Author discussed about password authentication by applying biometric technique and hash functions. He did security analysis on various attacks within this session between user and server. There are three phases between user's smart card and the server first registration phase, second login phase and third is authentication and key agreement phase. After completion of this process user can update his/her password within the smart card due to security reason. This analysis covered attacks like replay attack impersonation attacks, off-line password guessing attacks and the stolen verifier attacks.

Yan *et al* [7]. After Tan's scheme of authentication in TMIS environment, Xiaopeng find out that tan's schemes is secured from various attacks but it is vulnerable to Denial-of-Service attack. So the author gave a proper solution to this draw back which not only prevent from this attack even enhance the performance also. Tan's weakness which is improved in this paper is fundamental property of hash function which says that the outputs are very sensitive to small perturbation of its input, *i.e.* the output will change even one bit of the input is changed. In password update phase user gives biometric information which is slightly different from the registered one, and this is the drawback of Tan's scheme. In this paper, discussed scheme is providing prevention from Denial-of-service attack by setting some thresh hold value for template matching as well as server spoofing attack and modification attacks also.

Omid *et al* [8] explained about the draw backs of Yan's scheme, which was the improved version of Tan's scheme. Author discussed here security flaw of Yan's scheme

that, it is not secure from some attacks *e.g.* off line guessing password attack, impersonation attack and provide no forward security property and it is also not very efficient in the password update phase. To remove these drawbacks Omid had used here random oracle concept and for providing more security and correctness to it he used BAN logic for further use. All the security analysis is done on AVISPA tool. This mechanism provided not only more security but also the efficient computational time with in the communication in the TMIS environment.

3. Proposed Work

Our work includes three phases Registration of country, key generation and digital signature phase, second is registration of user and third is authentication of user in the home country as well as in visiting country. The notations used in this paper are defined as follows.

X_h, Y_h : Home country private and public key
X_v, Y_v : Visiting country private and public key
Elgamal E : Encryption using Elgamal
DS h_c : Digital signature of home country
DS v_c : Digital signature of visiting country

3.1. Registration of Country, Key Generation and Digital Signature

In this phase we are registering the country along with all its details like private key, public key and all the parameters of the digital signature for every country. In our work countries are registered in the form of C1, C2 *etc.* After the country registration, the local inspection system registration is accomplished, according to this step; every country has more than one local inspection system. These local inspection system stores after the country's registration phase, with its area name like Amritsar (in our case we are considering IS1, IS2...) and with its random number say 321; in a table for further procedure. Here key generation and digital signature is based on the ElGamal algorithm steps which are showing in below Table 3.1 overall working step of ElGamal algorithm.

Table 1. Key Generation Steps of Elgamal Algorithm

Home Country	Visiting Country
Common parameter agreement Prime number q Primitive root α of q	Common parameter agreement Prime number q Primitive root α of q
Key generation	**Key generation**
Select private key a X_h, $X_h < q-1$, Compute Y_h $Y_h = \alpha^{Xh} \bmod q$, Public key PU = {q,α, Y_h},	Select private key X_v, $X_v < q-1$, Calculate Y_v $Y_h = \alpha^{Xv} \bmod q$, Public key PU = {q,α, Y_v},

ElGamal is used with digital signature, for signing the information M. The ElGamal algorithm provides the encryption and decryption process, as well as the electronically signed of messages M. A signature scheme has two main characteristics:

3.1.1. Generation

User A, a sender needs to send the signature for message M by using his/her Xa, the private key. Then User A will send the message M along with his signature in the pair (M; S) to User B.

3.1.2. Verification

User B the receiver has to be able to identify the mentioned signature by using the public key Ya (public key of User A). This signature verification process gives surety to User B that received message has sent by User A.

After the country registration there is an intermediate state *i.e.* the local inspection system registration. This registration encapsulated with the first step. These local inspection systems are the scanner systems at the international airport of any countries.

3.2. Registration of a user

After the country registration and local inspection registration step, next step is to register a user for passport. Here user has to register himself by giving some personal detail like name, address, age and his biometric information in our case we have taken fingerprint trait as the biometric information, at the Passport Seva Kendra for getting a new passport.

3.3. Authentication of User

After the user registration phase, user authentication phase is there, there are two scenarios for this process, first when user is in the home country and second when he is visiting another country. In home country generally passport number are used as an identification proof especially in India. There are some basic encryptions and decryption steps have followed in our approach. The basic data encryption and decryption has done by symmetric algorithm DES and asymmetric algorithm ElGamal.

Table 2. Encryption and Decryption Steps of Elgamal Algorithm

Encryption of Message	Decryption of Cipher Text
Select M message belongs to [0 q-1], Select k integer belongs to [1 q-1], Calculate One Time key $K= (Y_B)^k \bmod q$, Encrypt the message M1 in cipher pairs (C2 C1), $C1 = \alpha^k \bmod q$, $C2 = KM \bmod q$.	
C1,C2 →	
Compute	
	$K = (C1)XB \bmod q$, $M1 = (C2K^{-1}) \bmod q$.

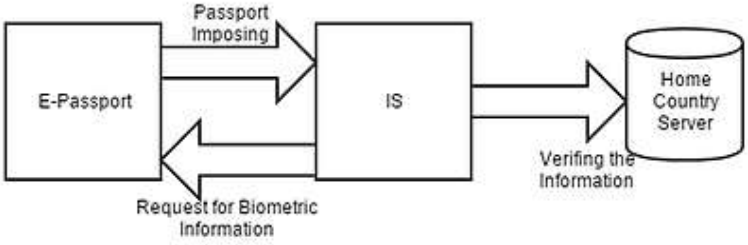

Figure 1. Authentication Process, when user in Home Country

Second scenario of authentication phase is when user is in another country, in this case user goes to visiting country's local inspection system example Newyork, and there he / she impose his E-passport up on the IS. After the imposing passport on IS, IS will send an encrypted message (IS id|| DES E (secret key, passport number)), to the visiting country server. Here this encryption is DES encryption, and the used secret key and IS id in this session, are stored in the database of visiting country. After receiving the encrypted message from IS, visiting country server checks its validity by matching the local inspection system id number, if it is valid IS then process will continue otherwise it simply discard the request. In positive scene IS valid, than server will decrypt the message DES D (secret key, passport number) and read the passport number. Server gets the home country code from the passport number than visiting country will send (DS vs || ElGamal E (Y_h, passport number)) to the home country. Here DS vs is the visiting country digital signature. When this message is received by home country server, it will check the authenticity of visiting country by matching the digital signature that concatenated with the message to digital signature from the global table. If the signature matched then home country server will decrypt the message by ElGamal D (ElGamal E (Y_h, passport number)) and check the validity of user, by searching his passport number in the home county's database. If passport number is matched in the home country's database then it will send the biometric information of user (DS hs || ElGamal E (Y_h, information)) in order to match the current biometric information with the stored one at the sensor. After getting the message visiting country will check the validity of home country and then it extract the information and match from the present biometric trait. If both templates are match then user is welcome in the country otherwise he is a suspicious user. Table 3.2 is showing the encryption and decryption steps in ElGamal algorithm.

Following diagram is showing the complete process of our work including E-passport which is imposing by user on the IS. GET CHALLEENGE command has used by IS to E-passport for getting the passport number. Than further process takes place through visiting country server to home country server. Figure 3.2 shows a topological representation of the presented scenario.

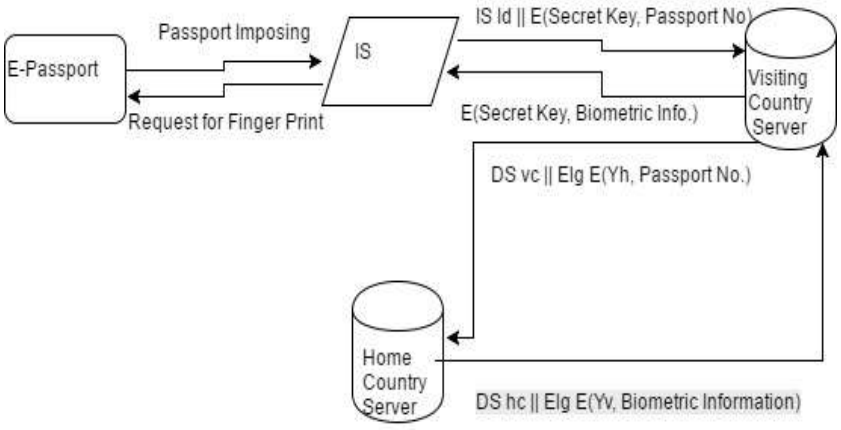

Figure 2. Authentication Process, when user in Visiting Country

In this diagram the encryption and decryption process between the E-passport and visiting country IS, is done by symmetric algorithm DES and the next pair of cryptographic process which is held between both the countries (home and the visiting country) servers are completed by an asymmetric algorithm ElGamal.

4. Results and Discussions

Our work includes three phases as Registration of country, Key Generation and digital signature generation, Registration of user and Authentication (within the home country and within the foreign country). This is the mimic scenario of the airport where a passenger is travelling to another country. Three phases and their implementation results have been included in subsequent section.

4.1. Authentication Phase

When a user operates his passport to inspection system there can be two possible authentications takes place:

- User operates with-in the country
- Out of the country *i.e.* foreign visit.

4.1.1. When user Operates Passport with-in the Country

Basically here in India passport uses of a identification purpose, in any field where verification is needed of a person there passport number can be used as the verification number. After filling the passport number the system enquires about the passport number from the central database of the country. If the biometric information is valid than the user will be the authorized otherwise system simply discards his request. On the other hand if we look in foreign country as the home country then there passport uses as the identification like the passport number but in some cases like massive accidents or some doubt full situation in crime, user can be identified by the fingerprint, by imposing his finger on the scanner.

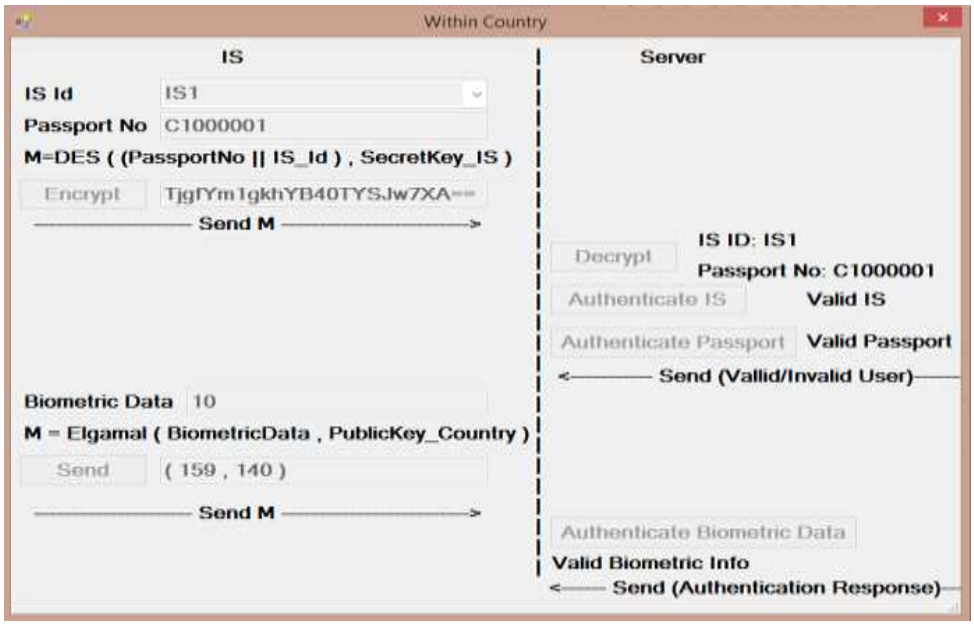

Figure 3. Authentication Process, when user in Home Country

4.2.2. When User Operates Passport in Foreign Country

This authentication process takes place in the two portions. First authentication of the local inspection system by its country database second is authentication of user from the home country database. When a user imposes his passport to visiting country's example C2 local inspection system say IS1 then this system sends its data along with the passport number to its country, then visiting country's database checks the validity of their local inspection system if the local inspection system is authenticated then further process takes place otherwise it simply discard the request. In this process the visiting country server sends the data in encryption form to the home country server, after receiving the message from visiting country, home country first checks the validity of visiting country by matching its digital signature stored in global table. If the visiting country is valid than home country decrypt the message and passes the further information. Encryption and Decryption of the data is done here by using DES and ElGamal. Figure 4.5 shows the authentication of user, local inspection system and country (both home and visiting).

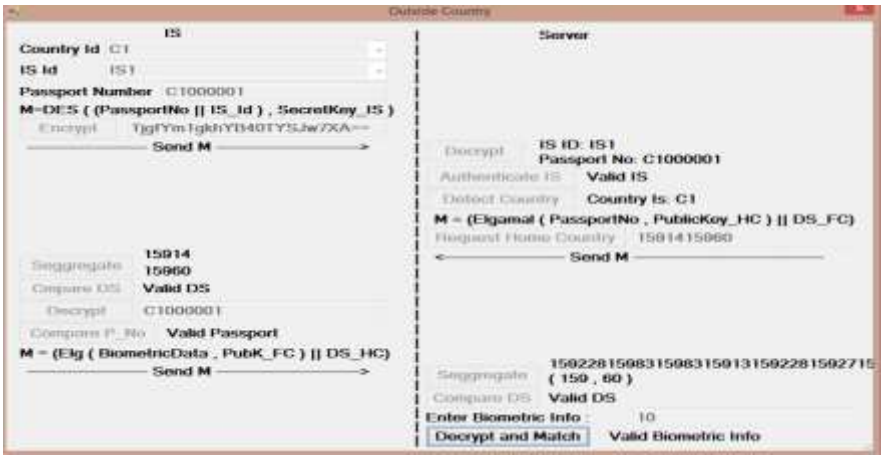

Figure 4. Authentication in Visiting Country

There is a complete interface through which all these registration can be done.

Comparison with Existing Techniques:

Existing techniques use any symmetric cryptographic techniques or some asymmetric cryptographic techniques. Most of the works include RSA as underlying cryptosystem. However the border security devices are resource constraints in nature which does not perform well with RSA and in some aspects with ECC also because of power analysis attack and its complex nature. On the basis of [4] we can limit the key size, which is based on some criteria like

1. Life span: this is the expected time for protect the information.
2. Security boundary: Basically a threshold value of a successful attack.
3. Computational environment: this is the expected change to attackers in available computational resources.
4. Cryptanalysis: the expected developments in cryptanalysis.

Table 3. Comparison between Various Asymmetric Algorithms

PARAMETRS	**ECC**	**RSA**	**Proposed technique (ElGamal)**
Side channel attacks	Possible	Possible	Not possible
Replay attack	Possible	Possible	Not possible
Cipher text	Complex	Less complex	Complex
Simulation speed	Fast	Slow	Fast
Calculation time	More	Less	Less
Power consumption	More	More	Less
Type of algorithm	Asymmetric	Asymmetric	Asymmetric
Key size length	126	>1024	1024
Hardware and software implementation	Efficient but time consuming	Not very efficient	Faster and efficient
Scalability	Good scalability	No scalability	Good scalability
Mathematically	Complex	Less complex	Less complex
Understand ability	Tough	Easy	Easy

It is evident and crystal clear from this comparison that ElGamal is resolving the previous attacks on existing technique. It provides additional security to data by using digital signature concept. Based on this comparison we can say that ElGamal is functional and beneficial technique for the data transmission.

Our work includes three phases as Registration of country, Key Generation and digital signature generation, Registration of user and Authentication (within the home country and within the foreign country). This is the mimic scenario of the airport where a passenger is travelling to another country. Three phases and their implementation results have been included in subsequent section.

5. Conclusion

We have surveyed here various techniques of authentication based on biometric features. The paper has mentioned types of authentication in different fields *i.e.* E-passport, smart card and tmis environment. These techniques has implemented on different software and platforms some of them having some security loop hole like in E-passport, ECC has been used and ECC algorithm facing power analysis attack problem, side channel attack problem. To remove this demerit of ECC here I am proposing a technique which will work on ElGmal algorithm. This algorithm will also use biometric information for authentication and its private key will be the biometric trait of human being that will be in the form of numeric value. In this technique I will also use the concept of cancelable templates for preventing the attacks on database of user information.

References

[1] W. Stallings, "Cryptography and Network Security", Pearson Education, Inc., publishing as Prentice Hall, **(2006)**.
[2] S. G. Kanade, D. Petrovska-Delacrtaz and B. Dorizzi, "Enhancing Information Security and Privacy by Combining Biometrics with Cryptography", in Synthesis Lectures on Information Security Privacy and Trust, Morgan Claypool Publishers, **(2012)**.
[3] U. Subramaniam and K. Subbaraya, "A Biometric Based Secure Session Key Agreement using Modified Elliptic Curve Cryptography", International Arab Journal of Information Technology (IAJIT), vol.12, issue 2, **(2015)**.
[4] K. Hemanth, S. Asadi, D. Murali, N. Karimulla and M. Aswin, "High Secure Crypto Biometric Authentication Protocol", International Journal of Computer Science and Information Technologies, vol. 2, no. 6, **(2011)**, pp. 2496-2502.
[5] A. Poorani, B. Vaishnavi and G. Gokila Deepa, "Enhancing Security in Biometric System Using Blind Authentication Protocol", International Journal of Emerging Technology and Advanced Engineering, vol. 3, Issue 3, **(2013)**, pp. 233-237.
[6] Z. Tan, "An efficient biometrics-based authentication scheme for telecare medicine information systems", Przeglad Elektrotechniczny, vol. 89, **(2013)**, pp. 200-204.
[7] X. Yan, W. Li, P. Li, J. Wang, X. Hao and P. Gong, "A Secure Biometrics-based Authentication Scheme for Telecare Medicine Information Systems", J. Medical Systems, **(2013)**, pp. 37-42.
[8] O. Mir and M. Nikooghadam, "A Secure Biometrics Based Authentication with Key Agreement Scheme in Telemedicine Networks for E-Health Services", Wireless Personal Communications, **(2015)**, pp. 2439-2461.
[9] S. Shrivastava and S. Shantaiya, "Multibiometric Cryptosystem- Review", International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 3, Issue XII, **(2015)**.
[10] S. Sonkamble, R. Thool and B. Sonkamble, "Survey of Biometric Recognition Systems and their applications", Journal of Theoretical and Applied Information Technology, **(2005)**, pp. 45-51.
[11] V. Pasupathinathan, J. Pieprzyk and H. Wang, "An on-line secure e-passport protocol", Proceedings of the 4th international conference on Information security practice and experience, Sydney, Australia, **(2008)**, , pp.14-28
[12] M. Abid and H. Afifi, "Secure E-Passport Protocol Using Elliptic Curve Diffie-Hellman Key Agreement Protocol", Proceedings of the 2008 The Fourth International Conference on Information Assurance and Security, **(2008)**, pp.99-102.

