ISSN: 0976-9102 (ONLINE)
DOI: 10.21917/ijivp.2018.0258

ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING, AUGUST 2018, VOLUME: 09, ISSUE: 01

USAGE OF BIOINFORMATIC DATA FOR REMOTE AUTHENTICATION IN WIRELESS NETWORKS

R. Priscilla and M. Karthi

Department of Information Technology, St. Joseph's Institute of Technology, Chennai, India

Abstract

Authentication is the step to approve the correctness of an attribute of a individual or entity group. Sensitive information might help in making the authentication. Regularly this encrypted information is processed via wireless network and which need remote authentication for information access process. In the proposed work, a robust authentication technique is performed, which is based on segmentation, symmetric encryption and data hiding. If a user wants to be remotely authenticated, initially user has to select a video. The user's biometric signal is encrypted using a symmetric encryption method. After encrypted information is vectorized the information hiding process is accomplish using Qualified Significant Wavelet Trees (QSWTs). QSWT is effectively achieve the invisibility and resistance during attacks and stability in data hidden process. Also, the Inverse Discrete Wavelet Transform (IDWT) is applied to extract the hiding data from the stego-object subsequently an appropriate decryption process to recover the biometric image. Experimental results are stated that the proposed method would turnout security virtue and robustness. Triple DES technique is used in the proposed work. This is the technique that is used to encrypt the biometric data into a scrambled format which is difficult to understand by the attackers. It is a very useful and efficient method of encryption because of its tendency to use less data for performing its services.

Keyword:

Railway Accident, Decision Making, D3 Algorithm

1. INTRODUCTION

The current growth in technology has also led to an increased rate of vulnerability of the data that is being transferred using the wireless networks. To achieve this, we perform activities like encryption, authentication and several other procedures. Authentication is the act of confirming the truth of an attribute of a datum or entity. This process may involve to justify the identification of an individual or software application, track the root of an artifact [6]. It is very important to make sure that proper emphasis has been provided to the process of authentication as it plays a very vital role in protecting the integrity of a system by protecting the confidential data that is being transferred in Wireless Networks [7].

There are several techniques used to perform authentication in the modern era of technology. The majority is based on passwords or smart cards. Using biometric data for carrying out authentication is an emerging trend which has gained a lot of attention lately. Biometrics has already been incorporated in remote authentication [8].

In order to investigate their full potentiality, biometrics can be incorporated in hybrid crypto-Steganographic schemes. In particular, cryptographic algorithms can scramble biometric signals so that they cannot be understood, while Steganographic methods can hide the encrypted biometric signals so that they cannot be seen [9]. The paper uses this principle to confront the problem of remote human authentication over wireless networks under loss tolerant protocols. The key features used in the work are Triple DES and Quality Wavelet Significant Trees [10]. QSWT helps us to find the significant points within which the encrypted biometric data can be hidden properly without loss [11].

According to a report, in overall 5.3% is the probability of people who are affected by fraud identity. In order to overcome fraud identity, the robust remote human authentication technique is introduced [12]. In that many people suggest password and smartcard for remote authentication. By referring advantages and disadvantages of the remote authentication technique, the biometric signal is found to be the best technique for authentication purposes. The biometric signals are already used in the existing system [13]. For submitting as password in the smart cards alone, the biometric signal is used. In the hybrid crypto-steganographic schemes, the biometric signal can be implemented [14].

1.1 VIDEO OBJECT EXTRACTION

This is a process which is used to extract a particular type of object from an image or a video. In this case, we use a man as the object to be chosen. The image of the man is extracted by removing the background noise which helps us to increase the efficiency of the system and to prevent unwanted data loss.

1.2 QUALITY SIGNIFICANT WAVELET TREES

QSWT is an advanced technique within Discrete Wavelet Transforms (DWT). QSWT is used to detect the significant points within the Video Object in which the encrypted biometric data can be hidden with very high precision and efficiency. QSWTs approach is covers in order to choose the coefficient values where the encrypted biometric data must be casted. It is also used to divide the image into multiple sub-bands in which the vectorized data can be stored.

1.3 TRIPLE-DATA ENCRYPTION STANDARD (3-DES)

This is the technique that is used to encrypt the biometric data into a scrambled format which is difficult to understand by the attackers. It is a very useful and efficient method of encryption.

The proposed scheme is a positive authentication system where multiple techniques for data protection like remote authentication, cryptography and steganography are combined together. Biometric data is encrypted and then hidden within a Video Object by performing mechanisms like 3-DES and QSWT. This increases the safety of the data and reduces the vulnerability.

2. RELATED WORK

This section explains the various researches related to the Rail Accident data report

2.1 VIDEO OBJECT BASED AUTHENTICATION

Ntalianis et al. [1] concentrates on providing Remote Authentication to the data that is being transferred in Wireless Networks by making use of Biometric data. The project works by creating a Video Object from a frame extracted from a video data. A biometric data is then encrypted by using a Chaotic encryption technique to create a scrambled image of the original biometric data. This scrambled image is then vectorised to create small easily transferable components. The QSWT technique is used to detect the significant points present in the Video Object to hide the vectorised scrambled biometric image. This technique helps us to create sub-bands which are very efficient in hiding the data and transmitting them successfully.

The main advantage of this method is its resistance to lossy transmissions. The usage of chaotic encryption makes the process of decrypting the messages very complex. This is both advantageous and disadvantageous because, it is very effective against attackers and also consumes a very large amount of data.

2.2 KEY AGREEMENT AUTHENTICATION

Chuang et al. [2] uses key agreement schemes in order to protect the biometric data that is being used for remote authentication in multi-server environments. However, in this scheme a verification table should be maintained on the remote server and if intruders break into it, they can modify the table. Therefore, many different solutions have been proposed. The most popular of which is based on long and random cryptographic keys. A scheme that utilizes the Diffie-Hellman Key agreement protocol over insecure networks, allows the user and the system to agree on a session key to encrypt/ decrypt their communicated messages using a symmetric crypto system. Random cryptographic keys are difficult to memorize; thus, they are stored somewhere and they are released based on some alternative authentication mechanism (Example: Passwords) [4].

In cryptography, a key-agreement protocol is a protocol whereby two or more parties can agree on a key in such a way that both influence the outcome. If the key agreement procedure contains security flaws, unintended parties can get hold of the key and use it to decrypt all the transmitted messages that are encrypted with this key [5].

2.3 BIOMETRIC AUTHENTICATION

He et al. [3] is the one that proved the effectiveness of biometric data in Remote Authentication in Multi-Server Environments. This work added protection to the biometric data that is transferred using wireless networks. This conventional scheme needs to make their independent registration with each respective server in a multi-server in order to permit an end user accessing the service. This has led to the adoption of multi-server authentication in which, a user accesses services of multiple servers after registering themselves at only one central authority. Since the user-memorized passwords are of low entropy, it is possible for an attacker to guess them.

This work uses biometric information of the user to enhance the security of the scheme. This scheme provides two-factor security using a password and a smartcard. Since the user passwords are of low entropy, an attacker may guess them and break their security. Thus, in this work, the security of the previous scheme is enhanced by including biometric information such as fingerprint, retina, iris, or palm prints, as it is difficult for an attacker to copy, guess, or forge a biometric key. Biometric authentication systems compare a biometric data capture to stored, confirmed authentic data in a database. If both samples of the biometric data match, authentication is confirmed. Biometric authentication works by comparing two sets of data: the first one is preset by the owner of the device, while the second one belongs to a device visitor. If the two data are nearly identical, the device knows that “visitor” and “owner” are one and the same, and gives access to the person. The system won’t store the actual image of the fingerprint, but a mathematical representation of it.

3. PROBLEM STATEMENT

The architecture diagram for the process of remote authentication using biometric data is illustrated in the Fig.1 below.

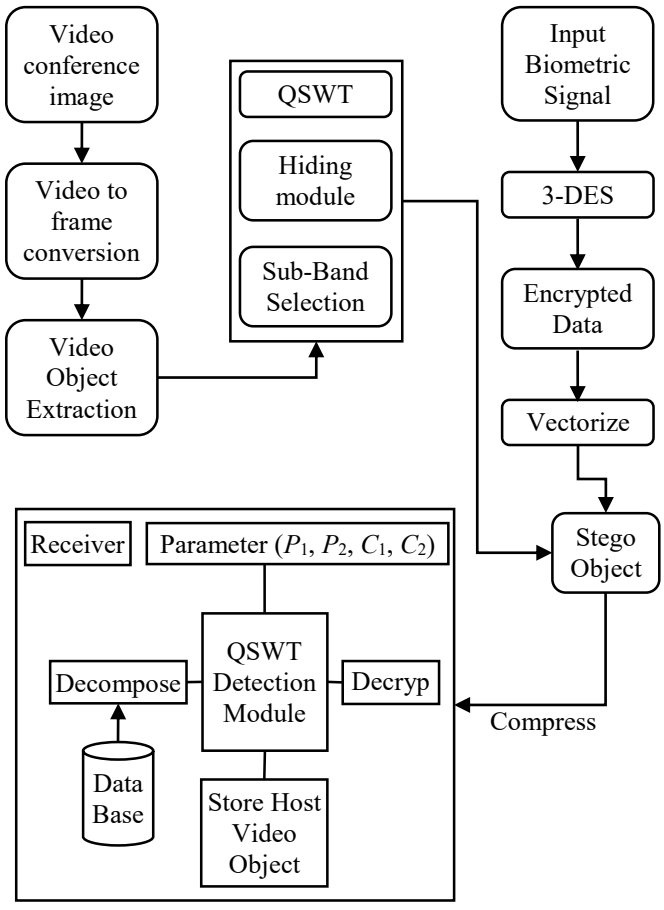

Fig.1. Process of Remote Authentication using Biometric Data

3.1 VIDEO TO FRAMES CONVERSION

This is the first module of the proposed system. Here, the video is converted into frames using certain Matlab codes. Once a frame has been selected, a video object is extracted from the

frame by using video object detection mechanisms. Video object detection is more difficult compared to image-based object detection. Previous researches stated that implement the object detector frame by frame is unreliable also makes process as slow. But multi-frame feature extractions proved best in increasing the accuracy, but it fails in speed. Feature propagation-based methods proved that effective in increasing speed, but fails to satisfy the desired accuracy. This process is presented in Fig.2.

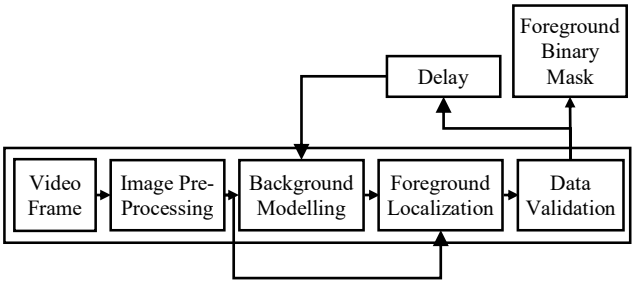

Fig.2. Modules Description

In the proposed work, we use Head-and-Shoulder Video object detection technique. A statistical model-based video segmentation algorithm is presented for head-and-shoulder type video. This algorithm uses domain knowledge by abstracting the head-and-shoulder object with a blob-based statistical region model and a shape model. The object segmentation problem is then converted into a model detection and tracking problem. At the system level, a hierarchical structure is designed and spatial and temporal filters are used to improve segmentation quality. Simulation results are offered to compare MPEG-4 performance with H.263 on segmented video objects with respects to compression efficiency, bit rate adaptation and functionality. There are several parameters based on which, the head-and-shoulder detection is performed.

3.2 THE ENCRYPTION MECHANISM

In most contemporary schemes security of the encrypted content mainly depends on the size of the key. In this paper, the generated key has size equal to the size of each biometric signal. Each key is generated by a C-PRBG. C-PRBGs that are based on a single chaotic system can be insecure, since the produced pseudorandom sequence may expose some information about the employed chaotic system. The basic idea of the C-PRBG is to generate pseudo-random bits by mixing three different and asymptotically independent chaotic orbits. According to this scheme the generation of each bit is controlled by the orbit of the third chaotic system, having as initial conditions the outputs of the other two chaotic systems [15].

After generating the initial pseudo-random key, the cipher module is activated. Before encryption, the samples of each biometric signal are properly ordered. In case of 1D signals (e.g. voice) the order is defined by the sequence of samples, while in 2D signals (e.g. fingerprint image) pixels are line per line zigzag scanned from top-left to bottom-right, providing plain text pixels P_i. Next, we take into consideration the fact that multiple iterations of chaotic functions lead to slow ciphers, while a small number of iterations may raise security problems. In order to avoid iterations while maintaining high security standards, the proposed scheme combines three chaotic block ciphers (including the time variant S-boxes) to implement a complex product cipher. In most contemporary schemes security of the encrypted content mainly depends on the size of the key. In this paper, for each biometric signal a key that has size equal to the size of the signal to be encrypted is produced. In particular, the first component of the proposed encryption module is the C-PRBG, which controls the rest of the encryption process [16].

Triple DES algorithm has a key of 56 bits (K_1, K_2 and K_3) which is used to perform the ciphertext = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$, where initially DES encrypt with key (K_1), decrypt with key (K_2), then encrypt with key (K_3). Decryption is the reverse: plaintext = $D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$, where DES decrypt with key (K_3), encrypt with key (K_2), then decrypt with key(K_1).

3.3 HIDING THE ENCRYPTED BIOMETRIC SIGNAL

To hidden the encrypted biometric signal in the video object, we use the stego-object method. It effectively hidden message also protect the message even if data losses in case of transmission and compression QSWTs can also do it better way, because it provides fast and accurate data recovery, after various signal processing manipulations. let consider that the video object has been extracted using the method. After perform the experimentation on diffident numbers of levels, it stated that use of two levels provide the best resolution [17].

The approach is implemented as a DCT-DWT dual domain, but the authenticator watermark is not encrypted. A similar approach combining DWT and Integer Wavelet Transform (IWT). Considering that the stego-object (or a distorted version of it) has reached its destination, the encrypted biometric signal is initially extracted by following a reverse (to the embedding method) process. Towards this direction let us assume that the recipient of the stego-object has also received the size of the encrypted 2D biometric signal, the scaling constants and possesses the original host video object.

3.4 MESSAGE RECOVERY

The main focus of this work is very challenging: to investigate the possibility of remote authentication over wireless channels under lossy protocols. As a result, our interest during steganography is much more on robustness to manipulations (compression, losses during transmission etc.) and less on robustness to steganalysis. In cryptography, the system is broken when an attacker can read the secret message (it does not matter how he does this). On the other hand, breaking a steganographic system has three stages: the attacker can detect that steganography has been used, the attacker extracts the embedded message from the host and the attacker is able to read the embedded message.

4. EXPERIMENTS AND RESULTS

4.1 VIDEO TO FRAME CONVERSION AND OBJECT EXTRACTION

The video that has been provided is converted into frames. The suitable video object is extracted from the video frame.

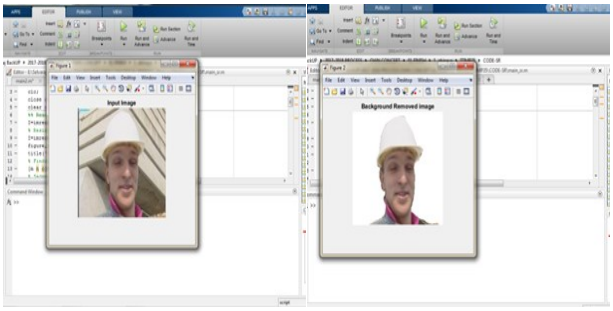

Fig.3. Video to Frame Conversion and Object Extraction

4.1.1 Processing Input Biometric Data and Encryption:

The selected form of biometric signal is processed. The Biometric signal is then encrypted into a scrambled format.

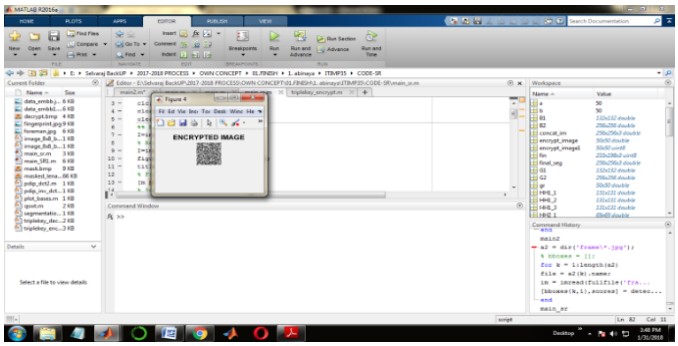

Fig.4. Processing Input Biometric Data and Encryption

4.1.2 Creation of Stego-Object:

The stego-object is created by hiding the encrypted biometric data within the image.

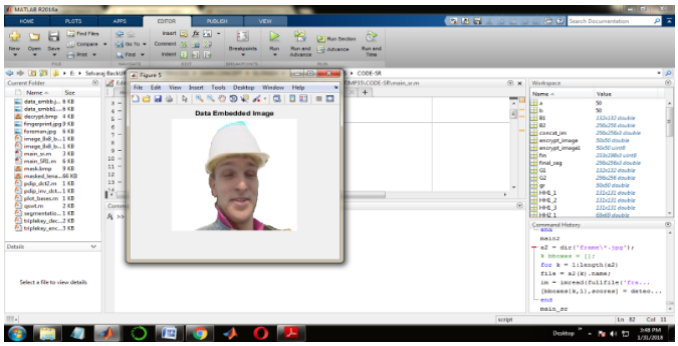

Fig.5. Stego-Object

4.1.3 Recovery of Encrypted Biometric Data:

On the receiver end, the encrypted biometric signal is extracted from the stego-object.

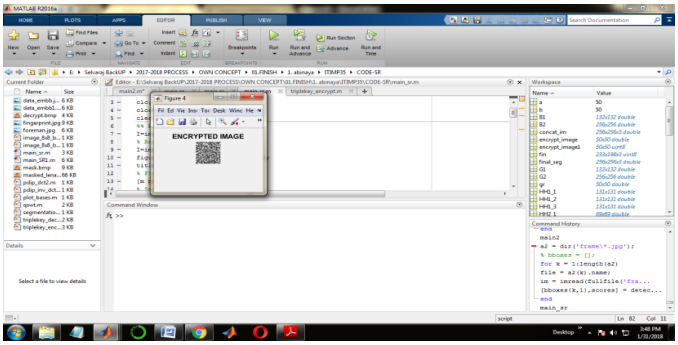

Fig.6. Recovery of Encrypted Biometric Data

4.2 DECRYPTION

The biometric data is converted back into its original form.

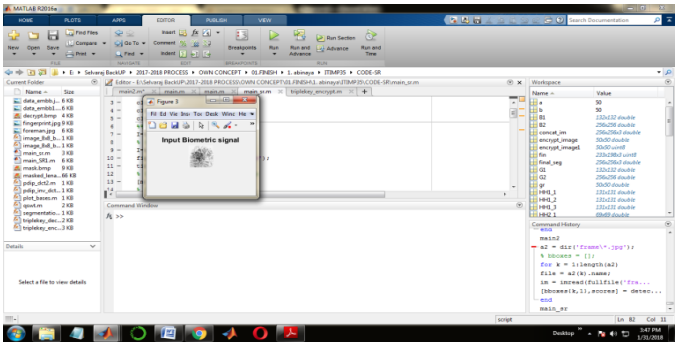

Fig.7. Decryption

4.3 RECOVERY OF VIDEO OBJECT

Finally, the video object is recovered and stored in the database.

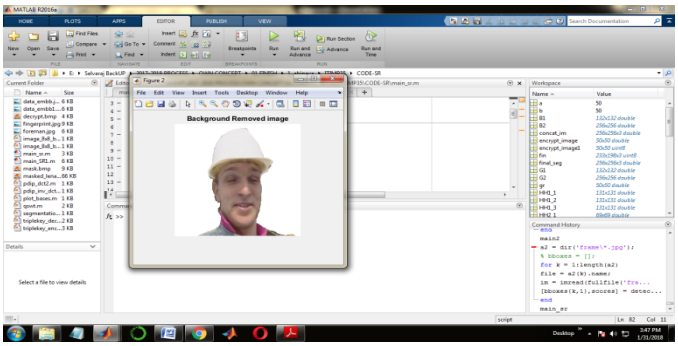

Fig.8. Recovery of Video Object

Eventually, the robustness of the proposed system is examined with help of various analytic tools available in the market like StirMark, StegSpy, PhotoTitle and etc.

Using the tools, we have analysed the set of images available in phototitle and petit colas based on various constrains like Stego attack. In this case the bandwidth range variation of various images is pictorially represented in Fig.9. This graph clearly shows that accuracy between Type A and Type B images where, Type A denoted objects covers only the face area where as Type B indicated the objects covers upper body area also.

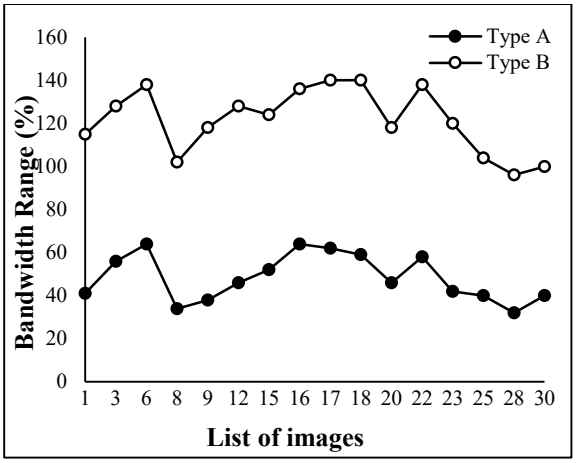

Fig.9. Bandwidth range savings for various video objects

5. CONCLUSION

Biometric signals enter more and more into our everyday lives, since governments, as well as other organizations, resort to their use in accomplishing crucial procedures (e.g. citizen authentication). Thus, there is an urgent need to further develop and integrate biometric authentication techniques into practical applications. Towards this direction in this paper the domain of biometrics authentication over error-prone networks has been examined. Since steganography by itself does not ensure secrecy, it was combined with a chaotic encryption system. The proposed procedure, except of providing results that is imperceptible to the human visual system, it also outputs a stego-object that can resist different signal distortions, and steganalytic attacks. Experimental evaluation and detailed theoretical security analysis illustrate the performance of the proposed system in terms of security.

6. FUTURE ENHANCEMENT

In future research, the effects of compression and mobile transmission of other hidden biometric signals (e.g. voice or iris) should also be examined. The problem of lost biometric data is also of high interest. Techniques from the areas of image error concealment, region restoration or region matching can be used for this purpose. For instance, the lost biometric data can be concealed from the authentication module, so that it attempts to perform authentication even though parts are missing (parts that do not contain any crucial information, e.g. terminations or bifurcations in case of fingerprints). Finally, the hash value of a biometric identifier could be utilized (which could save us from seeking large video objects or lead to much more robustness to losses), so that there is a centralized authentication service (trusted third party) and the biometric identifier could not be retrieved by other legal entities.

REFERENCES

[1] Klimis Ntalianis and Nicolas Tsapatsoulis, "Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks", *IEEE Transactions on Emerging Topics in Computing*, Vol. 4, No. 1, pp. 156-174, 2016.

[2] M.C. Chuang and M.C. Chen, "An Anonymous Multi-Server Authenticated Key Agreement Scheme based on Trust Computing using Smart Cards and Biometrics", *Expert Systems with Applications*, Vol. 41, No. 4, pp. 1411-1418, 2014.

[3] D. He and D. Wang, "Robust Biometrics-Based Authentication scheme for Multi-Server Environments", *IEEE Systems Journal*, Vol. 9, No. 3, pp. 1-8, 2014.

[4] E.J. Yoon and K.Y. Yoo, "Robust Biometrics-based Multi-Server Authentication with Key Agreement Scheme for Smart Cards on Elliptic Curve Cryptosystem", *Journal of Supercomputing*, Vol. 63, No. 1, pp. 235-255, 2013.

[5] A. Madero, "Password Secured Systems and Negative Authentication", Master Thesis, Engineering Systems Division, Massachusetts Institute of Technology, pp. 1-52, 2013.

[6] Al Pascual, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters", Technical Report, Javelin Strategy and Research, pp. 1-82, 2013.

[7] M. Jakobsson and M. Dhiman, "The Benefits of Understanding Passwords", Available at: https://pdfs.semanticscholar.org/51a0/22d608f9ccab3a10dcf7a48f249f7e189e6e.pdf.

[8] H. Kim, W. Jeon, K. Lee, Y. Lee and D. Won, "Cryptanalysis and Improvement of a Biometrics-based Multi-Server Authentication with Key Agreement Scheme", *PLoS ONE*, Vol. 13, No. 3, pp. 391-406, 2012.

[9] R. Madhusudhan and R.C. Mittal, "Dynamic Id-based Remote User Password Authentication Schemes using Smart Cards: A Review", *Intelligent Algorithms for Data-Centric Sensor Networks*, Vol. 35, No. 4, pp. 1235-1248, 2012.

[10] M.K. Khan, S.K. Kim and K. Alghathbar, "Cryptanalysis and Security Enhancement of a 'More Efficient and Secure Dynamic Id-based remote User Authentication Scheme", *Computer Communications*, Vol. 34, No. 3, pp. 305-309, 2011.

[11] L. Mary Glandence, M. Karthi and V. Maria Anu, "A Statistical Comparison of Logistic Regression and different Bayes Classification Methods for Machine Learning", *ARPN Journal of Engineering and Applied Sciences*, Vol. 10, No. 14, pp. 1-14, 2015.

[12] W. Stallings, "Cryptography and Network Security: Principles and Practices", 5th Edition, Prentice-Hall, 2010.

[13] M. Weir, S. Aggarwal, M. Collins and H. Stern, "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords", *Proceedings of 17th ACM Conference on Computer and Communications Security*, pp. 162-175, 2010.

[14] Y. Wang, J. Liu, F. Xiao and J. Dan, "A More Efficient and Secure Dynamic Id-based Remote USER Authentication Scheme", *Computer Communications*, Vol. 32, No. 4, pp. 583-585, 2009.

[15] I.E. Liao, C.C. Lee and M.S. Hwang, "A Password Authentication Scheme over Insecure Networks", *Journal of Computer and System Sciences*, Vol. 72, No. 4, pp. 727-740, 2006.

[16] L. Lamport, "Password Authentication with Insecure Communication", *Communications of the ACM*, Vol. 24, No. 11, pp. 770-772, 1981.

[17] L. Mary Gladence, M. Karthi and T. Ravi, "A Novel Technique for Multi-Class Ordinal Regression-APDC", *Indian Journal of Science and Technology*, Vol. 9, No. 10, pp. 1-8, 2016.