Volume 3, Issue 5, May 2018 ISSN (online): 2456-0006
International Journal of Science Technology Management and Research
Available online at: www.ijstmr.com

Secure Authentication Based On Video - Object & Biometric Data In Wireless Sensor Network

Ankita S. Bhadange
Department of Information Technology
MET's Bhujbal Knowledge City
Institute of Engineering Nashik, India

Krutika S. Bhamare
Department of Information Technology
MET's Bhujbal Knowledge City
Institute of Engineering Nashik, India

Pranali V.Gaikwad
Department of Information Technology
MET's Bhujbal Knowledge City
Institute of Engineering Nashik, India

Abstract-: ***In today's world security is the main concern in all type of applications or transactions like banking, online shopping. Remote authentication is the communication between server and client which is located at different location. In this type of system sensitive information is exchanged between two channels. Biometric authentication is an important component in network Security. It uses different biological traits, like fingerprints, hand pure mathematics, ear lobe, membrane and iris patterns, voice waves, keystroke dynamics, DNA and signatures. This paper proposes a robust authentication mechanism based on semantic segmentation, chaotic encryption and data hiding. QSWTs provide both invisibility and significant resistance against lossy transmission and compression, conditions that are typical in wireless networks. Finally, the Inverse Discrete Wavelet Transform (IDWT) is applied to provide the stego-object (SO).***

Keywords: Wireless Communication, Authentication ,Data hinding ,Encrypted Information.

I. INTRODUCTION

Today's e-security are in basic need of discovering precise, secure and practical contrasting options to passwords and individual recognizable proof numbers as budgetary misfortunes increment drastically year over year from PC based extortion, for example, PC hacking and data fraud . Biometric arrangements address these principal issues, in light of the fact that an individual's biometric information is special and can't be transferred. Biometrics which alludes to recognizing a person by his or her physiological or behavioral attributes has ability to recognize approved client and a faker.

Favorable position of utilizing biometric verification is that it can't be lost or overlooked, as the individual must be physically present amid at the purpose of distinguishing proof process. Distinguishing proof projects including the utilization of biometric innovation are growing quickly in creating nations. On the contrary, in negative authentication the anti-password space is created, (theoretically) containing all strings that are not in the passwords file. If crackers receive the very large anti-password file, their work will be much harder. This way, negative authentication can be introduced as a new layer of protection to enhance existing security measures within networks. This allows the current infrastructure to remain intact without accessing the stored passwords or creating additional vulnerabilities. By applying a real-valued negative selection algorithm, a different layer is added for authentication, preventing unauthorized users from gaining network access.

II. RELATED WORK

[A].Remote Authentication: Authentication is used by a server when the server desires to know precisely who is retrieving their info. Authentication is used by a client when the client requests to know that the server is scheme it claims to be. In authentication, the user or computer has to verify its uniqueness to the server or client. Normally, authentication by a server includes the use of a user name and password. Additional ways to verification can be done with cards, thumbprint, signature recognition scanning of retina, vocal sound recognition, and fingerprints. Authentication by a client generally contains the server charitable a certificate to the user in which a trusted third party. Authentication does not control what responsibilities the individual can do or what files the individual can get. Authentication simply recognizes and validates who the person or system is.

[B].Biometric Security: Biometric security is connectivity continues to range across the globe, it is clear that old security methods are simply not strong enough to protect what's most important.Biometric technology is additional open than ever before, ready to bring improved security and greater accessibility to whatever needs defensive, from a door, to your car to the password on your phone .Main aim is to achieve the goals of security.

III. LITERATURE SURVEY

In 1981, Lamport [6] proposed a remote password authentication scheme, by employing a one-way hash function. However, in his scheme a verification table should be maintained on the remote server and if intruders break into it, they can modify the table.

Liao et al. [8] proposed a scheme that utilizes the Diffie-Hellman key agreement protocol over insecure networks, which allows the user and the system to agree on a session key to encrypt/decrypt their communicated messages using a symmetric cryptosystem.

Random cryptographic keys are difficult to memorize, thus they are stored somewhere and they are released based on some alternative authentication mechanism (e.g. password). However several passwords are simple and they can be easily guessed or broken [9], [10].

Another interesting and very promising category of remote user authentication schemes involves smart cards using dynamic users' identities per transaction section [11]_[13]. These methods aimed to overcome a common drawback of older remote authentication schemes using smart cards: user's identity was static in all the transaction sessions, which may leak some information about that user and can create risk of ID-theft during the message transmission over an insecure channel. However, vulnerabilities of those methods were also found. Madhusudhan and Mittal [14] proposed a set of security requirements and goals for dynamic ID-based remote user password authentication schemes, and through their respective cryptanalysis, proved that both Wang's et al. The authors in [1] have achieved 5% of increased throughput when it was tested for Iris Detection. Russel Ang and Rei Safavi-Naini [2] used Reed– Solomon algorithm and 128 bit binary vector is achieved by thresholding bits generates bio-key for face biometrics. keystroke biometrics was proposed by Anil K. Jain Michigan in [3] and they obtained 8-bit random number (the "salt") hardened unbreakable password. U. Uludag has developed Baseline PCA Algorithm which ensures SAFE securities by providing valid biometric authentication [4]. The authors in [5] have used fuzzy logic algorithm which can tolerate more variation in the biometric characteristics and to provide stronger security. Nearest neighbor algorithm is used for finger print estimation by V. Prasath kumar.

One more system is proposed, an automatic embedded software generation framework that can create and evolve Zigbee applications. The framework consists of two major modules, pattern extraction and code generation. Pattern extraction and development are designed to provide Zigbee application with model reuse and modification. SysML serves as a medium between pattern development and code generation. A smart shopping cart application has been implemented using this pattern based software framework.

IV. PROPOSED SYSTEM

This proposed framework is, 1. Biometrics based human confirmation over remote channels under blame tolerant conventions. 2. Automatic extraction of semantically important video objects for installing the scrambled biometrics data 3. Chaotic figure, which works like an onetime cushion, to encode biometrics identifiers.

a. Capturing video object: In this stage client profile and face can be caught by Remote server. Before catching human face, each client needs to enlist their profile data into the server. When enlistment prepare has finished, server catch the face. On catching, video mode consequently catches picture protest from that video. Caught client confront naturally putting away into the server.

b. Uploading biometrics and hiding into video object: When human face catching procedure is finished, server will catch the client suitable biometrics. Here biometrics are not specifically putting away into the server. Each biometrics must be scrambled and watermarked into the client confront. For encryption here we will apply blowfish calculation. This calculation read each pixels estimations of the biometrics and change the pixel estimations of it. After encryption handle, server will install scrambled biometrics into the human face. For installing (watermarking) we will apply Least Significant Bit (LSB) strategies. These procedures will read each lines and segments of the biometrics and implanting into the suitable lines and sections of the human face. So every watermarked picture is kept up in the server.

c. Chaotic Encryption: The chaos-based image cryptosystem works in two parts[2]. The plain image is assumed at its input. The confusion stage is the pixel permutation where the position of the pixels is twisted above the entire image without upsetting the assessment of the pixels and the image becomes distorted. The pixel arrangement is accomplished by a chaotic system [1,2]. The chaotic actions is handled by the initial conditions and control parameters which are resulting from the 16-character key. To progress the safety, the second stage of the encryption method sight refining the value of each pixel in the whole image an vital tool to protect image from attackers. The basic idea of encryption[5,6] is to alter the message in the diffusion stage, the pixel values are reconstructed one by one beside the sequence generated from one of the three chaotic systems selected by external key. Mainly chaotic encryption is used for randomness which is more suitable for image encryption chaotic maps are used.

d. **Remote server authentication**: In the module, remote server confirmation will be performed. On the off chance that client needs to get to the application implies he/she needs to give his face and biometrics to the server. Server will coordinate face with each face on the database. On the off chance that server distinguished the coordinated face implies, server will remove the unique finger impression from that picture. In the wake of removing, server checks the face and biometrics into the coordinated face and biometrics. In the event that both are matches just server will confirm the client.

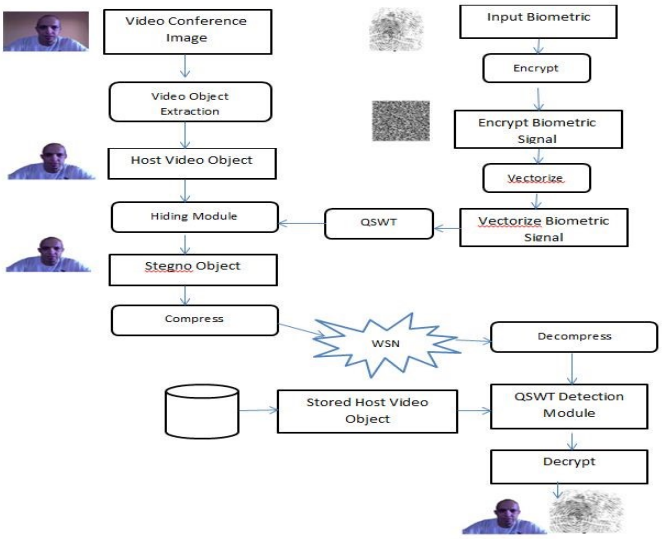

Fig 1: Block Diagram of System

V. ALGORITHUM USED

[1].Message Recovery:

Step 1: Initially the received stego-object XO and original video object X are decomposed into two levels with seven sub-bands using the DWT.

Step 2: Using the size a * b, the embedded positions are detected by following the hiding process described in subsection V-A.

Step 3: The resulting hidden message coefficients $w_i^{(2)}$ And $w_i^{(1)}$ are averaged and rearranged to provide the encrypted biometric signal.

Step 4: The original biometric signal is recovered by decrypting the enciphered signal (see subsection IV-F).

[2].QSWT Algorithm:

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) QSWTs approach is incorporated in order to select the coefficients where the encrypted biometric signal should be casted.

Algorithm 1 QSWTs Estimation

```
procedure QSWTest(I, S, L)
/* I = input frame */
/* S = subband selection (e.g. LH) */
/* L = subband level (e.g. 3) */
/* Thresholds T1 and T2 are globally defined */
[LL, LH, HL, HH] ← DWT(S, L − 1)
S_{L−1} ← LH
[LL1, LH1, HL1, HH1] ← DWT(LL, 1)
S_L ← LH1
t ← 0
QSWT[t] ← ∅
N ← rows(S_L)
M ← columns(S_L)
for i = 1 to N do
    for j = 1 to M do
        if S_L(i, j) is In_Node AND |S_L(i, j)| > T1 then
            C1 ← S_{L−1}(2i − 1, 2j − 1) is In_Node AND |S_{L−1}(2i − 1, 2j − 1)| > T2
            C2 ← S_{L−1}(2i − 1, 2j) is In_Node AND |S_{L−1}(2i − 1, 2j)| > T2
            C3 ← S_{L−1}(2i, 2j − 1) is In_Node AND |S_{L−1}(2i, 2j − 1)| > T2
            C4 ← S_{L−1}(2i, 2j) is In_Node AND |S_{L−1}(2i, 2j)| > T2
            if (C1 AND C2 AND C3 AND C4) then
                QSWT[t] ← S_L(i, j) + S_{L−1}(2i − 1, 2j − 1) + S_{L−1}(2i − 1, 2j) + S_{L−1}(2i, 2j − 1) + S_{L−1}(2i, 2j)
                t ← t + 1
return QSWT
```

CONCLUSION

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 are imperceptible to the human visual system, it also outputs a stego-object that can resist different signal distortions, and steganalytic attacks.

REFERENCE

1. Madero, "Password secured systems and negative authentication", Ph.D. dissertation, Dept. Eng. Manage., MassachusettsInst.Technol.,Cambridge, MA,USA,2013.[Online].Available:http://hdl.handle.net/1721. 1/90691.
2. Pascual and S. Miller, "Identity fraud report: Data breaches becoming at reasure trove for fraudsters", Javelin Strategy Res., Pleasanton, CA, USA, Tech. Rep. 1/2013, 2013.
3. E.J. Yoon and K.Y. Yoo, "Robust biometrics-based multiserver authentication with key agreement scheme for smart cards on elliptic curve cryptosyste" J. Supercomput., vol. 63, no. 1, pp. 235255, Jan. 2013. Ankit Anil Agarwal, Saurabh Kumar Sultania, Gourav Jaiswal and Prateek Jain on RFID Based Automatic Shopping Cart in Control Theory and Informatics; ISSN 2224-5774 (print) ISSN 2225-0492 (online),Vol 1, No.1, 2011
4. H. Kim,W. Jeon, K. Lee,Y. Lee, and D.Won, "Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreementscheme", in Computational Science and Its Applications (Lecture Notes in Computer Science), vol. 7335. Berlin, Germany: Springer-Verlag, 2012, pp. 391-406.
5. Ann Cavoukian and Alex Stoianov Biometric Encryption "Chapter from the Encyclopedia of Biometrics".
6. W. Stallings, Cryptography and Network Security: Principles and Practices. Prentice-Hall, 5th edition, Upper Saddle River, NJ, USA, 2010.
7. 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, pp. 727–740, 2006. J.Awati and S.Awati, "Smart Trolley in Mega Mall," vol.2, Mar 2012.
8. M. Jakobsson and M. Dhiman, "The benefits of understanding passwords," in Mobile Authentication, ser. SpringerBriefs in Computer Science. Springer New York, 2013, pp. 5–24.
9. M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in Proceedings of the 17th ACM Conference on Computer and Communications Security. ACM, 2010, pp. 162–175.