International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 4, April 2016

Webcam Based Remote Authentication via Biometrics over Insecure Channels Using Steganography

[1] Devika Mohan, [2]Devika J H, [3]Athira S Nair, [4]Devika R, [5]Lailathun Nasooha, [6]Dileep V K
[1-5]Department of Computer Science, B.Tech, [6] Assistant Professor, Department of Computer Science,
L B S Institute of Technology for Women (LBSITW)

Abstract: — ***Remote authentication has much application in today's world. Such authentication usually involves transfer of sensitive information via insecure channels. There is a need for a simple, reliable and moreover secure mechanism for authentication. This paper proposes a webcam based authentication scheme using fingerprint biometrics and steganography. A reasonable quality fingerprint image of the user to be authenticated is used for this purpose. This image is enhanced using HDR local adaptation mechanism. The enhanced biometric signal is then embedded with metadata containing the information of the image source and then encrypted using an encryption scheme based on Rubik's cube principle. Initially the video object of the user to be authenticated is segmented from the video feed. The encrypted biometric signal is then hid inside this image using a steganographic method utilizing side match. Minutiae points are extracted from the recovered, decrypted fingerprint..image..on..the..authenticating..side..for..fingerprint..matching.***

I. INTRODUCTION

Authentication is a crucial factor in exchanging sensitive, confidential information over remote channels. The users of these information may need to prove their authenticity before accessing any remote resource. It involves ensuring identity of a person. For ensuring authentication atleast two or preferably all three factors should be verified.

1) Something the user has such as security tokens, ID cards etc.
2) Something the user knows such as a password
3) Something the user is or does such as biometrics.

Many remote authentication schemes are proposed in the literature including password based authentication, authentication using smart cards, software tokens etc. Authentication based on biometrics has it advantage over these existing schemes based on the fact that it cannot be stolen, like tokens and cards. The biometric traits are something the user posses. Fingerprint biometrics is the most advanced and time tested technique among all the biometric authentication techniques. However majority of the users may not posses fingerprint scanners. So there is a need for the alternative way to extract the biometric feature. [1] proposes an efficient and simple webcam based method for obtaining fingerprint information. [2] Discusses a mechanism to enhance the fingerprint recognition using this image by HDR toning in local adaptation mode. [3] discusses minutiae detection from webcam generated fingerprint images which is a crucial step in fingerprint matching. The enhanced finger- print image is encrypted using a new image encryption method utilizing the principle of Rubik's cube. This encrypted biometric signal is hid inside the host image using steganographic method based on side match.

The paper is organized into four sections .Section II discusses the related works in literature. Section III describes the proposed system and section IV discusses scope for future work.

II. RELATED WORKS

A. Authentication Methods

First in its kind password authentication scheme was proposed by Lamport [5] in 1981 which uses one way hash function for password authentication. In this scheme a verification table is maintained, which consist of user identifier and password for all registered users. The verification table is stored on a remote server. The main disadvantage of the system is that if the attackers breaks in to the server and gets hold of verification table, they can modify it.

Another scheme used for remote authentication is using smart cards. There is no need of maintaining a verification table on the remote server here and stolen verify attacks can be solved .Here timestamps are used to resist reply attacks. In [6] the proposed method comprise of three phases that includes registration phase, login phase and authentication phase. This increases security and efficiency of authentication. Today many attacks exist which can break authentication using smart card. In [7] Ravi Singh,Pippal,Jadhar examines different types of such attacks like impersonation attacks, offline password guessing attack, parallel session attack, reflection attack, insider attack, attack on perfect forward secrecy and so on. The main disadvantage of smart cards is easy loss of information and slow adaptation. There is also a chance of loss of smart card. On such cases the user need to wait for the re-issue of card. Smart cards are also unable to perform complex computation due to low power. Moreover the user must have the smart card with him/her at the time of authentication.

Two factor authentication is another popular remote authentication method. [8] describes a method of implementation of two factor authentication. This paper discusses two factor authentication based on synchronous authentication, PIN and init-secret. The password is created as a one-time pad valid for 60 sec after which it expires. The main disadvantage of software tokens is that they require some amount of user training and need controlled environment for deployment.

The advantage of using biometric over the traditional authentication scheme is that it utilizes the intrinsic human physical and behavioral traits which are unique to each individual. [9] and [10] discuss the advantages of using the biometric as a reliable authentication scheme. The physical characteristics used for biometric authentication are fingerprint, DNA, face, retina or behavioral features. The behavioral characteristic includes rhythm, gestures, voice etc. The main advantage of using biometrics is that the object cannot be stolen like tokens, keys and cards. The scheme is moreover cost effective and fast.

Fingerprint biometrics is the most reliable of all the biometrics schemes. Ravi Singh and Duttatrega [11] discusses the advantages of using fingerprint for authentication. The ridges and valleys of fingerprint are unalterable and unique. The commonly used fingerprint matching are pattern matching and minutiae based matching. It is experimentally shown that the fingerprint based system have very low False Rejection Ratio (FAR).

B. Encryption

Modern encryption methods use keys to encrypt and decrypt messages. The encryption results in generation of "digital gibberish" which is unidentifiable without decrypting with the key.

DES is the Data Encryption Standard which was originally published by the NBS and it is a block cipher which enables the encryption of 64-bit block plaintext in to 64-bit block cipher texts by using a secret key. It is possible to brute-force the key generated by DES in finite time using modern processors and is hence unreliable for high end application.

RSA cryptosystem is the most popular and widely used public key cryptosystem. The security of the algorithm relies on the difficulty of factorizing large numbers or solving the discrete logarithmic problems. The main disadvantage of RSA algorithm is its computational complexity and hence slow performance moreover, Genkin et al [12] describes an acoustic cryptanalysis key extraction attack which can extract full 4096-bit RSA decryption keys from laptop computers with in an hour. [13] discusses the evaluation of various asymmetric and symmetric encryption algorithm such as AES, DES etc. The main disadvantage of AES algorithm is that it is slow and the key is shared resulting in low security.

Several chaotic based digital image encryption algorithms are proposed in literature[14]. Here pseudo-random bits are generated for implementing the chaos theory which shows extremely complex and unpredictable behavior and high sensitivity to initial conditions. The advantage of using chaos based encryption over traditional encryption schemes is the high computational power, speed and ease of implementation. [15] Analyzes different chaos based image encryption schemes. However these algorithms utilize relatively small key spaces and hence offer limited security.

A novel digital image encryption algorithm is given in [16], which utilizes the Rubik's cube principle to scramble the original image which offers more security than chaotic systems. This system is adopted in this paper which can resist exhaustive attack, statistical and differential attacks.

III. PROPOSED SYSTEM

A. Web Camera Fingerprint Image Extraction and HDR Toning

The fingerprint image of the user to be authenticated is initially taken using a reasonable quality web camera. An image pre-processing technique called HDR toning is used to achieve much higher definition on the image. The local adaptation mode in HDR toning in used here which "modifies the amount of brightness or darkness based on pixels surrounding it i.e. locality based enhancement. This creates an illusion that the image has more contrast, which is of maximum requirement in contrast-impoverished HDR images "[16]. The pre-processed fingerprint image is embedded with metadata indicating its origin details. Normally jpeg contains metadata specifying the date and time information of the image taken, the specifications of camera etc. In addition we embed the information on the PC from which the picture was taken namely its MAC address onto the image. These metadata can be reviewed on the receiver side to validate the image's origin.

B. Encryption of the Biometric Signal

The encryption of the biometric signal is done using the image encryption algorithm based on Rubik's cube principle specified in[17].

C. Hiding of Fingerprint Image onto Host Image Using Steganography Based On Side Match

Initially the head and shoulder image of the user to be authenticated is automatically segmented from the video feed taken by the front facing web camera. The fingerprint image is then hid inside this host video object by the steganographic method proposed in [18]. The method exploits the correlation between neighboring pixels in order to estimate smoothness or contrast of the picture. The fingerprint image is initially vectorized in order to be embedded into the host image. The embedding in done in such a way that the number of bits to be embedded for each pixel is decided by the correlation between adjacent pixels. This ensures large data hiding capacity and less distortion as compared to other LSB based steganographic methods. This method is blind and hence does not require the original image to retrieve the hidden image.

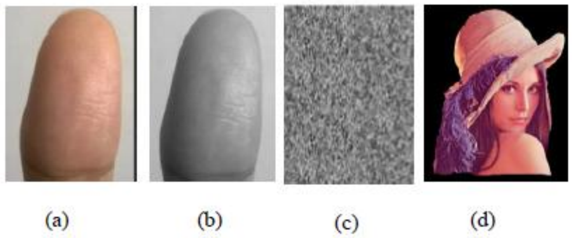

Fig 1.(a) Fingerprint image taken from web cam (b) Grayscale image of the fingerprint (c) Encrypted Fingerprint image (d) Stego-object (Lena) containing the encrypted fingerprint image D. Recovery and Decryption of the Image from Stego Image

On the receiver side the hidden image is recovered from the stego-image by the reverse procedure used for hiding. The biometric signal is then decrypted using the decryption algorithm specified in [17].

C. Minutiae Detection from the Recovered Decrypted Fingerprint Image

The minutia extraction from the finger print image involves 4 steps. First the RGB image is converted into gray scale image. The initial preprocessing step involves image enhancement, binarization, flow estimate and filtering.[19].Image enhancement is done to enhance the quality of the image so that the ridges and valleys are clearly visible. This increases the matching of the fingerprint images.

The fingerprint enhancement is done in two steps. Initially histogram equalization is performed which improves the global contrast of the image by adjusting the intensity distribution of the image. The next step involves binarization of image which converts the gray scale image to a binary image. This step converts the 256 level gray scale image to 2 level binary image. The 0 level indicates a ridge and 1 indicates a furrow.[19]

The next step in minutia detection involves selection of region of interest (ROI) from the enhanced image. This involves fingerprint image segmentation (flow estimate). After the ROI has been estimated the minutia points are estimated using a series of steps involving ridge thinning, minutia marking and false minutia removal.

IV. FUTURE WORK

The method proposed in this paper can be used for human authentication in applications like remote examination, personal interview etc. On that note, the proposed method which involves image steganography can be extended to video steganography where the biometric signal can be hidden inside the video stream prior to starting an interview or examination.

REFERENCES

[1] Mohammed Omar Derawj , Bian Yang and Christoph Busch, "Fingerprint Recognition with embedded cameras on mobile phones", Article January 2012.

[2] "Using webcam to enhance fingerprint recognition", conference paper, April 2014, http://www.csse.uwa.edu.au/pk

[3] Amrata A Khindre, V.A More, "An approach to touchless fingerprint recognition using matlab", www.ijettcs.org ,volume 3, issue 4, july-aug-2014.

[4] Klimis Ntalianis ,Nicolas Tsapatsoulis ,member, IEEE, "Remote Authentication via biometrics: A robust video-object steganographic mechanism over wireless networks.".

[5] L. Lamport, "Password authentication with insecure communication,"Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981.

[6] Chin-chen and Jung-san LEE," an efficient and secure remote authentication scheme using smart cards".

[7] Ravi singh pippal, Jaidhar C.D and Shashikala Tapaswi,"Security issues in Smart card authentication scheme".

[8] Manav singhal and Shashikala tapaswi,"Software tokens based two factor authentication scheme".

[9] Anil k Jain, Fellow, IEEE, Arun Ross, member, IEEE and Sahil prabhakar, mamber ,IEEE,"An Introduction to Biometric recognition".

[10] Vaclav matyas and Zdenek Riha, Facaulty of informatics, masaryk university, "Biometric authenticaiton security and usability".

[11] Ravi subhan and Dattatreya P Mankame,"A Study of Biometric approach using Fingerprint Recognition".

[12] D.Genkin, A.Shamir and E.Tromer,"RSA key extraction via low bandwidth acoustic cryptanalysis".

[13] Karilyn Lao, Richman Lo and Robert.M ,"Performance evaluation of Encryption".

[14] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on the 3d chaotic baker map, " International Journal of Bifurcation and Chaos, vol. 14, no. 10, pp. 3613–3624, Oct. 2004.

[15] Abhishek Misra, Ashutosh Gupta, Damodar Rai, " Analysing the parameters of chaos based image encryption schemes". World Applies Pogramming, vol(1),no(5),December 2011,294-299.

[16] Behera, Bibek, Akhil Lalwani, and Avinash Awate. "Using Webcam to Enhance Fingerprint Recognition." Articulated Motion and Deformable Objects. Springer International Publishing, 2014. 51-60.

[17] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle," Journal of Electrical and Computer Engineering, vol. 2012, Article ID 173931, 13 pages, 2012. doi:10.1155/2012/173931

[18] Chang, Chin-Chen, and Hsien-Wen Tseng. "A steganographic method for digital images using side match." Pattern Recognition Letters 25.12 (2004): 1431-1437.

[19] Khindre, Amruta A., and V. A. More. "Minutia Based Touchless Fingerprint Recognition."