Indian Journal of Science and Technology, *Vol 9(1), DOI: 10.17485/ijst/2016/v9i1/85786, January 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Remote Service Access using Biometrics

R. Punidha[1*], S. Anisha Vincy[2], Mary Judith[2] and D. Ramya[2]

[1]Department of Computer Science and Engineering, Vel Tech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai - 600062, Tamil Nadu, India; punidha@veltechmultitech.org
[2]Department of Information Technology, Vel Tech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai - 600062, Tamil Nadu, India; anishajes@gmail.com, maryjudith@veltechmultitech.org, ramya@veltechmultitech.org

Abstract

Background/Objectives: The main objective of the proposed work is to get the permission for accessing element through remote authentication by hiding encrypted biometric signal within image of the user. **Methods/Statistical Analysis:** The biometric signal is encrypted using Arnold transform algorithm and hided into the cover image with Qualified Significant Wavelet Tree (QSWT). The image of the person is denoted as cover image. The Compressed cover image gets transmitted over wireless channel for remote authentication. The Inverse Wavelet Transform is used to separate encrypted signal and the cover image. The biometric signal gets decrypted by inverse Arnold transformation algorithm. **Findings:** The Arnold transform algorithm increases the Normalized Cross Corelation (NCC) value for normalizing the image in order to improve the quality of reconstructed image. Hence, the Mean Square Error (MSE) is decreased and Peak Signal to Noise Ratio (PSNR) value is increased in the proposed work. And so the error is minimized in the proposed system compared to the existing techniques. The problems identified in the existing systems such as data loss, complexity and accuracy in biometric signal has been overcome by the proposed system. **Application/Improvements:** The proposed system can be used in military purposes for sharing confidential data. The data can be accessed over remote areas in secured maner.

Keywords: Arnold Transform Algorithm, Authentication, Biometric Signal, Remote Systems, QSWT

1. Introduction

The authentication[1] is used to confirm the identity or originality of the person by ensuring the details which are given by that person. There are two types of authentication namely positive authentication and negative authentication. In this the positive authentication is already implemented in the existing systems. In order to detect and eliminate the cyber attack the negative authentication is implemented. The examples are given below to show the difference between positive authentication and negative authentication. In the example there is a system based on password based authentication. The system contains positive authentication with a set of limited passwords for each and every user which was saved in a separate file. If the intruders crack the file the may enter into the users account. Whereas in the negative authentication, there is a anti-password space which contains the string that is not present in the password file. Here if the intruders get into the anti-password file also it is difficult to find the original password of the user. So that the negative authentication technique provides more security features than the existing positive authentication technique.

The biometrics are used in the literature[2–4]. Different layers of security are provided in the system to avoid the unauthorized access can be achieved by implementing real-valued negative selection algorithm.

The positive authentication system is used in the proposed scheme and at least two or three of the following factor should be true for security reasons:

- The user should have identity card, mobile phone, security token etc. These are ownership factor.
- The user should know password, PIN number, pattern etc. These are knowledge factor.

**Author for correspondence*

- The user should undergo fingerprint, retinal pattern, facial reorganization, DNA sequence, other biometric identifier etc. These are inherence factor.

According to the report in[5], the 12.6 million customers affected in US by fraud Identity and $4.6 billion loss for them. In overall 5.3% is the probability of people who affected in the fraud identity. In order to overcome the fraud identity the robust remote human authentication technique is introduced in many literatures[6–7]. In that many people suggest password and smart card for remote authentication. By referring advantages and disadvantages of the remote authentication technique the biometric signal is found to be best technique for authenticating purposes. The biometric signals are already used in the existing system. 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. In order to make the people to not understand the image the cryptographic technique is used to scramble the original biometric signal into scrambled image, then hide the scrambled image from the intruders steganographic technique is implemented to hide the scrambled biometric signal into the cover image that is the image of the person. In the proposed system we implemented some methods and technique to overcome the problem which has been faced in the existing remote authentication system. Here the head-and-body detector is used to extract the face and body of the person from the image that is Video Object (VO).

1.1 Remote Authentication

The one-way hash function technique was implemented in the remote password authentication scheme which was proposed by Lamport in[8]. In that system the user id and the passwords are maintained in separate verification table. It is difficult to maintain the verification table in the remote server. The attackers can modify the variables that are passwords by cracking the verification table. In order to overcome the weakness in this remote authentication technique Diffie-Hellman Key agreement protocol is reported by[9]. In this report, the session key is used to encrypt and decrypt the message which have been communicated by using the symmetric encrypt system. In that the random cryptographic keys are generated, so that it is difficult to memorize that password as well as it is difficult to store random password in the table[4]. Whereas the passwords which are used here is simple and can be easily guessed by attackers. Some users will use same password for all applications. In such case if the attacker finds the password of the user in a single application means they can easily access the other applications of the same user.

The remote authentication scheme in smartcards using dynamic user's identity is another technique which is proposed to overcome defects in the previous technique. This method is reported[10]. The use of static password in smartcards through wireless channels may leak the details about the user. In order to overcome the difficulties by using the static password that is constant password for the smart cards in the proposed scheme they are using dynamic passwords that is the password can be changed for each and every transactions. So there is no chance for intruders (or) attackers to guess the password.

1.2 Steganographic Methods

The steganographic technique is the process of hiding data into the image in order to provide the security for the data. Many compression techniques[11] are used in the literature for stegenography. The Qualified Significant Wavelet Trees (QSWTs) is used in this technique to hide the image into the cover image. The Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are used to hide data into images which is in JPEG, MPEG etc., formats. By using this methods the lossy messages are send through wireless channels without any loss during transmission and it will protect the hided data from attacks. Even though the process will protect the data loss, the loss of data will occur in some minute area. There are two components used in stegnanography of the image namely soft-authenticator watermark and chrominance watermark. The soft-authenticator watermark is used for authentication purposes to avoid image tampering. The chrominance watermark is used to enhance the compression efficiency of the image. The DWT and Integer Wavelet Transform (IWT) is combined and reported[12]. In that the encrypted key and the secret image is hided into the cover image. But it is quite complex to implement the embedding algorithm.

For the minutiae embedding of the image wavelet-based steganographic method is useful. The hided information can be easily found when the attacker knows the embedding algorithm.

2. Proposed Remote Service Access using Biometrics

2.1 Arnold Scrambling Algorithm

The process of transforming a digital image into another meaningless image by scrambling the original image is known as Arnold scrambling algorithm. By this algorithm the digital image gets preprocessed before hiding the image into the cover image. This process is also called as information disguise. The non-password technique can be followed by scrambling and hiding image into another image. So there is no need to memorize user id and password. This technique provides confidential and secure data transmission. To change the distribution of error bit in the image some watermarking techniques implies image scrambling method before hiding the image into another image. Many digital watermarking techniques uses Arnold transformation algorithm before it gets processed. This transformation algorithm undergoes images with (N^*N) pixels shows in the Equation (1).

The Figure 1 shows the coordinates for the image as (x,y), by implementing Arnold Transformation technique the coordinated (x,y) gets transformed to another point (x',y') is represented as,

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} (\text{mod } N) \quad (1)$$

The order of digital image matrix is represented by N.

The transformation specified here is two-dimensional Arnold Scrambling. Here the coordinate (x, y) which is present in the right side is the coordinates of input image. Then the coordinate (x', y') which is given in the left side is the coordinates of output scrambled image. The iterative process should be done for n successive nodes which can be expressed in Equation (2),

$$P_{XY}^{n+1} = AP_{XY}^{n} (\text{mod } N)$$
$$P_{XY}^{n} = (X,Y)^{T} \quad (2)$$

Where n denotes the number of iterations, n = 1,2,3… the iteration process will continues until all the pixel in the given image gets transformed. Where cycles undergoes transformation is denoted as *T* whereas size of the image is represented by N. Figure 2 shows transformation of image in Arnold cat's map.

The Arnold Transform algorithm shows the transformation of original image into scrambled one. So that the intruders cant get the original image even though they hack the data while transmitting over wireless channels. Because after scrambling the image gets vectorized that is the original image is not visible to others. The sender and the receiver alone knows the rounds which was undergone while generating chaotic map.

The key which was used to generate the chaotic map is very simple while comparing with other encryption technique. Then the original image will not get revealed in the wireless transmission. Therefore the Arnold transformation algorithm plays a major role in the overall encryption techniques. In this system before hiding image into another image the secrete image gets encrypted by the Arnold transformation algorithm that is given in Figure 3.

Because after scrambling the image gets vectorized that is the original image is not visible to others. The sender and the receiver alone knows the rounds which was undergone while generating chaotic map.

2.2 Discrete Wavelet Transform

The Discrete Wavelet Transform is used to hide information like text, audio, video, images etc., into cover image. The Discrete Wavelet Transform is also known as DWT. Analysis on multiresolution of image is done by Discrete Wavelet Transform. The steganographic technique is implemented in the discrete wavelet transform. In this technique the cover image is divided into four equal parts with respect to the resolution of the image that is (128*128) bits.The four parts is represented as low, middle and high frequencies that is represented as LL, HL, LH and HH. There are two operation which undergoes in DWT namely Horizontal operation and vertical

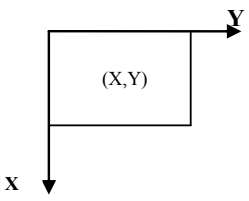

Figure 1. Image coordinates.

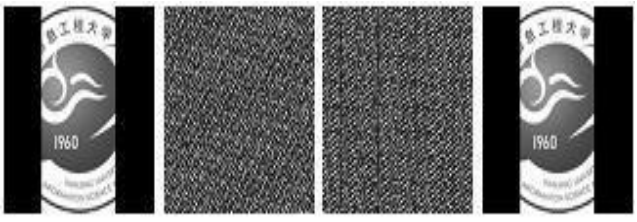

Figure 2. Image transformation.

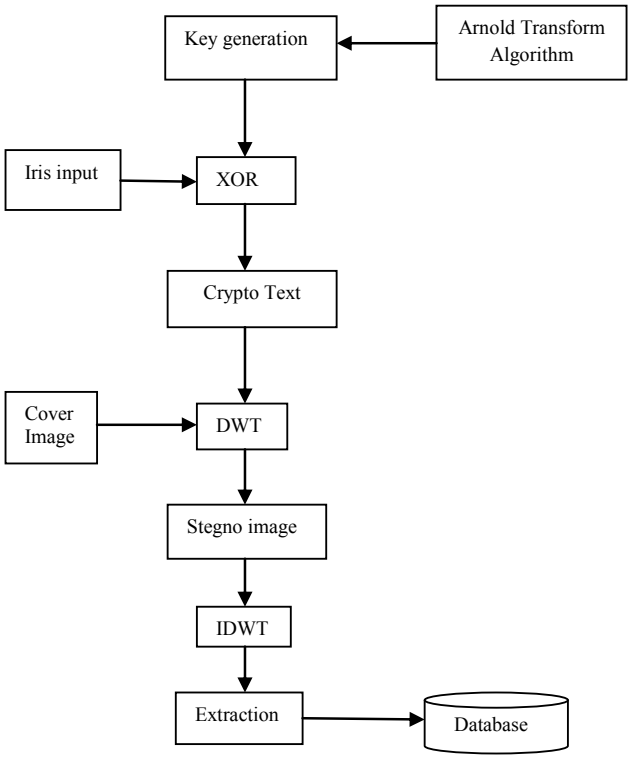

Figure 3. Block diagram for remote authentication.

operation. First step undergoes horizontal operation that is the analysis done in horizontal direction the pixels from left to right and then stores the addition of the near by pixels in the left side. The subtraction of the neighboring pixels is done and the difference value is stored into the right side. In the original image left side that is sum denotes Low frequency part (L) and the right side that is the product denotes High frequency part (H). Then the image undergoes four level of decomposition that is given in the Figure 4.

Vertical operation is done in second step. The pixels are analyzed in vertical direction that is from top to bottom. The addition of the near by pixels is performed and on the top the sum valued gets stored. Then the subtraction of the neighboring pixel is performed and on the bottom the difference value gets stored. Then LL, LH, HL, HH are the four sub-bands will generated after this process. The original image is same as the low frequency band in sub-bands. The higher level DWT is obtained after decomposing the LL sub-bands. The vertical, horizontal, diagonal sub-bands are represented as LH, HL, HH respectively. The process which undergoes horizontal operation is given in Figure 5. Then the vertical operation is given in Figure 6. The DWT is the process of hiding

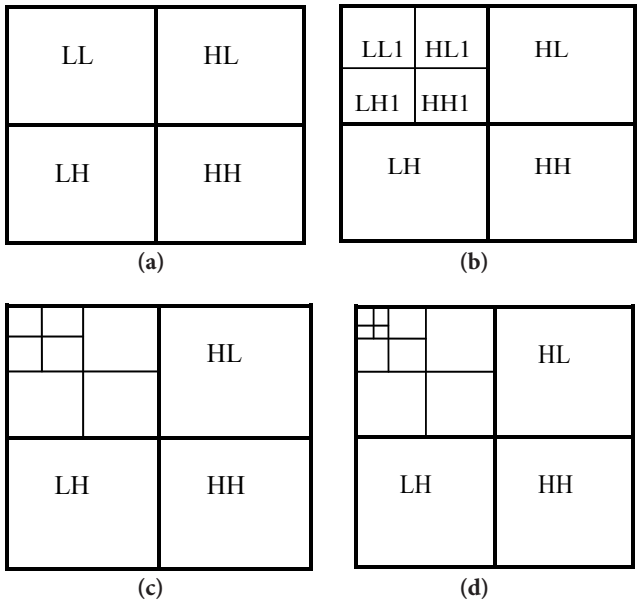

Figure 4. Image decomposition. **(a)** One level. **(b)** Two level. **(c)** Three level. **(d)** Four level.

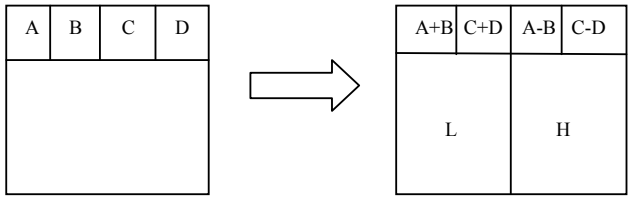

Figure 5. The horizontal operation.

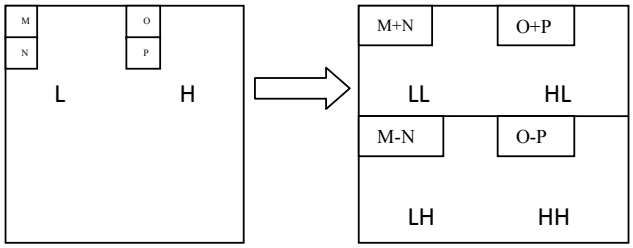

Figure 6. The vertical operation.

image into another image. Then the image is divided into four different parts with respect to the pixels (240*240 pixels). Then the image is inserted to the parts with low frequency level. The horizontal operation and the vertical operation is given in the below diagram.

3. Experimental Evaluation

The experimental values are examined to compare the efficiency, robustness, effectiveness and accuracy of the

proposed system with the existing system. The experiment for our proposed system is done with 500 biometric signals and 500 images. The analysis starts with the Encryption of the image. Here the encryption of the image is done with the Arnold Transform algorithm which consist of the cover image as well as the secret image. The table with experimental result for encryption of the image is given below in Table 1.

From the above tabular column the observed value of alpha gets increases from 0.01. The chart for the above tabular column is given Figure 7.

Table 1. Analysis of Arnold Transform algorithm with various quality of cover image and the secret image

Cover Image	Secret Image	ALPHA	PSNR (in dB)	NCC	MSE
Ship.png 512*512	Sea.png 512*512	0.02	46.2564	0.99 62	4.6355e +005
Sea.png 512*512	Sky.tiff 256*256	0.02	45.1204	0.99 65	5.2535e +005
Peppers. tiff 256*256	Star.jpg 600*420	0.012	46.1205	0.99 56	2.2562e +005
Ship.png 512*512	Sea.png 512*512	0.012	45.2358	0.99 42	3.2634e +005
Sea.png 512*512	Sky.tiff 256*256	0.012	44.3256	0.99 65	5.2315e +005
Peppers. tiff 256*256	Star.jpg 600*420	0.01	42.0318	0.99 36	4.2356e +005
Ship.png 512*512	Sea.png 512*512	0.01	43.1524	0.99 63	5.2365e +005
Sea.png 512*512	Sky.tiff 256*256	0.01	46.2531	0.99 43	6.2315e +005
Peppers. tiff 256*256	Star.jpg 600*420	0.09	47.2356	0.99 52	8.23105e +005
Ship.png 512*512	Sea.png 512*512	0.09	45.2356	0.99 49	2.3248e +005
Sea.png 512*512	Sky.tiff 256*256	0.09	44.2531	0.99 85	1.2307e +005
Peppers. tiff 256*256	Star.jpg 600*420	0.06	45.2355	0.99 62	5.3246e +005
Ship.png 512*512	Sea.png 512*512	0.06	47.3264	0.99 45	2.3267e +005
Sea.png 512*512	Sky.tiff 256*256	0.06	46.1524	0.99 51	1.2305e +005

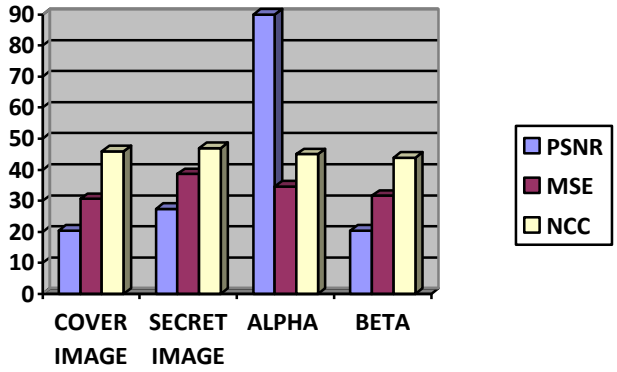

Figure 7. Chart for image encryption.

4. Conclusion

The proposed method provides confidentiality and security for the remote data authentication. The Arnold algorithm is used in the proposed system in order to reduce the complexity and minimize time consumption for scrambling the image. Then the compression technique used in this system is much simple when comparing to the existing methods. The JPEG compression technique is used to for transmitting the image over wireless channel, and the image quality is also maintained after decompression. Iris is used here as a biometric input for improving accuracy and to eliminate fraud access, where as in the existing system they used finger print as the biometric signal which can be changed during cuts and swelling of the finger. The experimental results shows that the proposed system is more accurate than the existing system.

5. Acknowledgement

The authors gratefully acknowledge the contribution of Govt. of India for Financial Assistance, DST-FIST F.NO:SR/FST/College-189/2013.

6. References

1. Shah HNM, Ab Rashid MZ, Abdollah MF, Kamarudin MN, Chow KL, Kamis Z. Biometric voice recognition in security system. Indian Journal of Science and Technology. 2014; 7(2):104–12.
2. Yoon E-J, Yoo K-Y. Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. The Journal of Supercomputing. 2013 Jan; 63(5):235–55.
3. Kim H, Jeon W, Lee K, Lee Y, Won D. Cryptanalysis and improvement of a biometrics-based multi-server

authentication with key agreement scheme. in computational science and its applications. ser Lecture Notes in Computer Science,Spinger-Verlag. 2012 Jul; 7335:391–406.
4. Chuang M-C, Chen MC. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Expert Systems with Applications. 2014 Mar; 41(4):1411–8.
5. Identity fraud report: Data breaches becoming a treasure trove fraudsters. Javelin Strategy and Research, Tech Rep; 2013.
6. He D, Wang D. Robust biometrics-based authentication scheme for multi-server environment. IEEE Systems Journal. 2014; 9(3):816–23.
7. Chen T-Y, Lee C-C, Hwang M-S, Jan J-K. Towards secure and efficient user authentication scheme using smart card for multiserver environments. The Journal of Supercomputing. 2013 Nov; 66(2):1008–32.
8. Lamport L. Password authentication with insecure Communications. ACM. 1981; 24(11):770–2.
9. Liao I-E, Lee C-C, Hwang M-S. A password authentication scheme over insecure networks. Journal of Computer and System Sciences. 1981; 72(11):770–2.
10. Wang Y-Y, Liu J-Y, Xiao F-X, Dan J. A more efficient and secure dynamic id-based remote user authentication scheme. Computer Communications. 2009 Mar; 32(4):583–5.
11. Krishnamoorthy R, Punidha R. Low bit-rate multi stage vector quantization based on energy clustered training set. Multimedia Tools and Applications. 2014; 70(3):2293–308.
12. Hemalatha S, Acharya UD, Renuka A, Kamath PR. A secure color image steganography in transform domain. International Journal on Cryptography and Information Security. 2013 Jun; 3(3).