Hiding fingerprint in a live image using Discrete Wavelet Transform for Remote Authentication

Mrs.S.Hemavathi[1, 4], R.Pavithra[2, 4], and J.Kirtika[3, 4]

[1] Assistant Professor, hemavathi.cse@sairam.edu.in
[2] Student B.E.CSE, pavithraraja81196@gmail.com
[3]Student B.E.CSE, kirtika1510@gmail.com
[4] Department of Computer Science and Engineering, Sri Sairam Engineering College, Chennai, India

***Abstract*—This paper presents an efficient Remote authentication scheme. This scheme is based on steganography and cryptography. Remote authentication scheme verifies the legitimacy of remote users' login request over an insecure communication channel. Initially, users' image is captured using a webcam. Then, one of the users' biometric images, a fingerprint is encrypted using Arnold Transform encryption algorithm and the key is generated using Chaotic Pseudo- Random Bit Generator(C-PRBG). The Discrete Wavelet transform is applied to the cover image. The image is then decomposed into four regions based on their frequencies using Shape Adaptive Discrete Wavelet transform and the highest energy band is detected using its Qualified Significant Wavelet Trees. Then, the encrypted image is hidden into the highest energy band of the cover image. Next, Inverse Discrete Wavelet Transform is applied over the cover image which is then compressed and transmitted to the receiver end. At the receiver end, the cover image is decompressed and then, the fingerprint is extracted by reverse embedding process. Then, the extracted fingerprint is decrypted. Finally, the decrypted fingerprint and the cover image are compared with the database.**

Keywords— Arnold Encryption; Discrete Wavelet Transform; Shape Adaptive Discrete Wavelet Transform; QSWT Estimation and Hiding; Fingerprint Extraction

I. INTRODUCTION

Authentication is the process or action of proving something to be true or valid. This might involve verifying the personal identities of a person or it might involve verifying the software program. There are two types of authentication. They are,

- Positive Authentication and
- Negative Authentication

Positive authentication is applied over the existing authentication systems. Negative authentication has been introduced to minimize cyber attacks. Let us assume password-based authentication. In positive authentication, there is a term known as password space which includes passwords of all the authorized users and it is very limited. If, the attacker receives the password file, then he/she will be able to crack the passwords using the available password cracking tool. But, in negative authentication anti-password space is created which contains all the strings that are not present in the password file. If, the attacker receives the anti-password file it is very difficult to crack the password. Since, anti-password file contains very large amount of data compared to password file.

Biometrics systems can identify users based on either anatomical or observable characteristics. Biometrics based personal identification techniques are increasing popularly because of its ability to differentiate between a legal user and a fraudulent

user who is illegally acquiring the access privilege of an authorized person.

II. EXISTING SYSTEM

Both the fingerprint image and the key are encrypted. Initially, users' host image is captured using a webcam and then, the users' fingerprint is encrypted using chaotic encryption algorithm. Key is generated using a Chaotic Pseudo-Random Bit Generator (C_PRBG). However, the embedding algorithm is quite complex and it is sensitive to lossy transmission. DWT-DCT based watermarking is presented. This scheme integrates cryptography and steganography together through image processing.

In particular, the system is able to perform steganography and cryptography at the same time using an image as cover objects. Steganography is done through DWT and cryptography is done through chaotic-map method. After applying both cryptography and steganography the cover image is compressed and transmitted to the receiver end. At the receiver end, the image is decompressed and the fingerprint is extracted. Then, the extracted fingerprint is decrypted and compared with the database.

III. PROBLEM DEFINITION

- Embedding algorithm is quite complex and sensitive to lossy transmission.
- Chaotic encryption algorithm does not process non-square images.
- The problem of compression remains.
- Speed of the encryption algorithm is low. Since, it encrypts both the secret image as well as the key.
- Only, the fingerprint is compared with the database.
- Nevertheless, if the contender knows the embedding algorithm, they can easily extract the hidden information.

IV. PROPOSED SYSTEM

To protect the resources from the fraudulent users, the remote user authentications have became an essential part in the communication network. This scheme comprised of four phases: Arnold encryption, QSWT estimation & hiding, Extraction, and Authentication process.

A. ARNOLD ENCRYPTION

In this phase, one of the users' biometric inputs, the fingerprint is encrypted using Arnold transform encryption algorithm. Key is generated using Chaotic Pseudo-Random Bit Generator (C_PRBG) which increases the security. The key size is equal to the size of the biometric image. Next, the encrypted biometric image is hidden into the host image of the user and transmitted to the receiver end.

B. QSWT ESTIMATION & HIDING

In this phase, the encrypted fingerprint is embedded into the host image of the user. Before hiding the fingerprint, the background of the host image is discarded using the Haarcascade function. Discrete Wavelet Transform is applied over the extracted host image. The host image is then decomposed into two levels using Shape Adaptive Discrete Wavelet Transform. Based on their three frequencies (low, mid and high), the image is divided as LL, LH, HL, and HH frequency regions providing three pairs of sub-bands (HL_2,HL_1), (LH_2,LH_1), (HH_2,HH_1). Fingerprint image cannot be hidden in the LL region. Since it has the lower energy content compared to the other three regions. So, the sub-band which has the highest energy content is detected using its Qualified Significant Wavelet Trees and the encrypted fingerprint is hidden here. After hiding the fingerprint, the host image is compressed which is then transmitted to the receiver end.

C. EXTRACTION PROCESS

At the receiver end, the compressed image is decompressed and the region which contains the

hidden fingerprint is detected by reverse embedding process. Then, the encrypted fingerprint is decrypted using reverse encryption algorithm.

D. AUTHENTICATION PROCESS

The decrypted fingerprint and the host image are compared with the database.

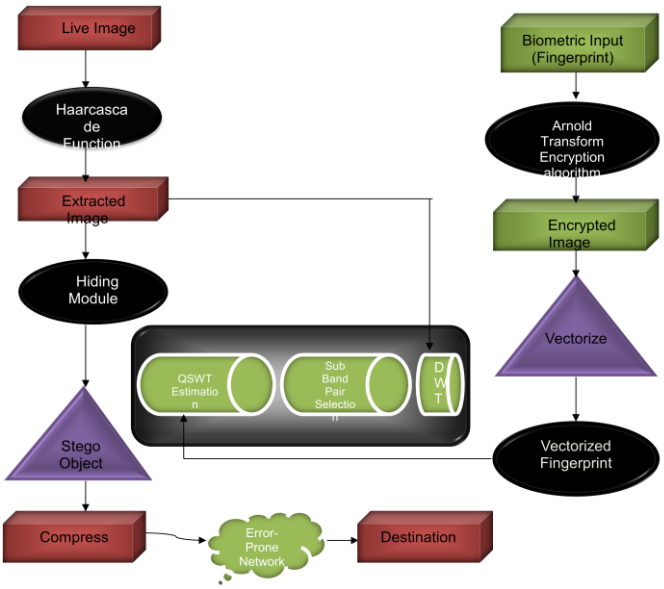

Fig. 4.1: Hiding encrypted fingerprint in a cover image

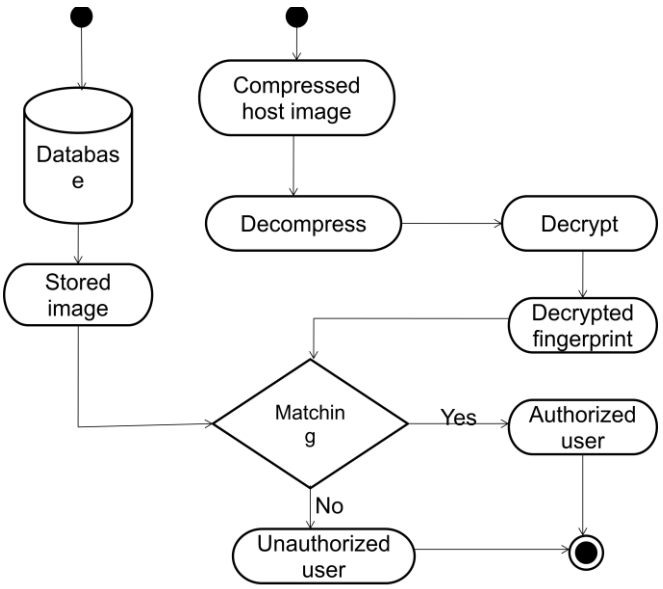

Fig. 4.2: Fingerprint extraction & authentication

V. CONCLUSION

In this paper, the domain of biometrics authentication over insecure communication network has been examined. To verify the robustness of the proposed Arnold transform encryption algorithm NIST tests were applied to the encrypted fingerprint. Results indicate that the use of Qualified Significant Wavelet Tress provides the high level of robustness and high compatibility over image and video compressions.

REFERENCES

[1] Klimis Ntalianis and Nicolas Tsapatsoulis, "Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks", IEEE Transaction on Emerging Topics in ComputingVolume: 4, Issue: 1 Jan-March 2016

[2] A. Madero, ``Password secured systems and negative authentication,''[Ph.D. dissertation, Dept. Eng. Manage., Massachusetts Inst. Technol.,Cambridge, MA, USA, 2013.

[3] A. Pascual and S. Miller, ``Identity fraud report: Data breaches becoming atreasure trove for fraudsters," Javelin Strategy Res., Pleasanton, CA, USA, Tech. Rep. 1/2013, 2013.

[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," J. Supercomput., vol. 63, no. 1, pp. 235255, Jan. 2013.

[5] 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," in Computational Science and Its Applications (Lecture Notes in Computer Science), vol. 7335. Berlin, Germany: Springer- Verlag, 2012, pp. 391406.

[6] L. Lamport, ``Password authentication with insecure communication," Commun. *ACM*, vol. 24, no. 11, pp. 770_772, Nov. 1981.
[7] W. Stallings, Cryptography and Network Security: Principles and Practice, 5th ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2010.

[8] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, ``A password authentication scheme over insecure networks,'' J. Comput. Syst. Sci., vol. 72, no. 4, pp. 727_740, Jun. 2006.

[9] M. Jakobsson and M. Dhiman, ``The benefits of understanding passwords," in *Mobile Authentication* (SpringerBriefs in Computer Science). New York, NY, USA: Springer-Verlag, 2013, pp. 5_24.

[10] M. Weir, S. Aggarwal, M. Collins, and H. Stern, ``Testing metrics for password creation policies by attacking large sets of revealed passwords," in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 162_175.