International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

Review on Steganographic Mechanism for Remote Authentication Using Biometric

Miss.Manisha N.Narote[1], Prof.S.K.Korde[2]

[1] *Student , ME CSE,PREC Loni, Maharashtra, India*

[2] *Asst.Professor, CSE, PREC Loni, Maharashtra, India*

Abstract - In day today's life security is more important. In wireless communications sensitive data is frequently interchanged, needs remote authentication. Remote authentication consist the submission of encrypted information, along with visual and audio cues (e.g. human voice, facial images/videos.). Trojan Horse and other attacks can cause serious problems, specially at the time of remote center exams or interview (for personnel hiring).This idea proposes a adhoc authentication mechanism based on semantic segmentation, using chaotic encryption and data hiding.The password or any other security measure can be edit easily so using this security approach we can make data more secure.The information is first encrypted with biometric samples of particular authenticated persons this become more secure. By Steganographic technique this image is hidden so double security is provided.Due to complexness steganalytic attacks, to different transmission losses and JPEG compression ratios as well as bandwidth efficiency measures, indicates the promising performance of the proposed biometrics-based authentication idea.

Keywords: *Steganography, Biometric, Fingerprint-recognization.*

I. INTRODUCTION

A user authentication scheme is a technique employed by a server to authenticate the legality of a user before anyone is allowed to access the service or resource which is provided by the server. Due to the Internet's openness and lagging of security concern, the user authentication scheme is one of the most important security primitives in the Internet activities [6].

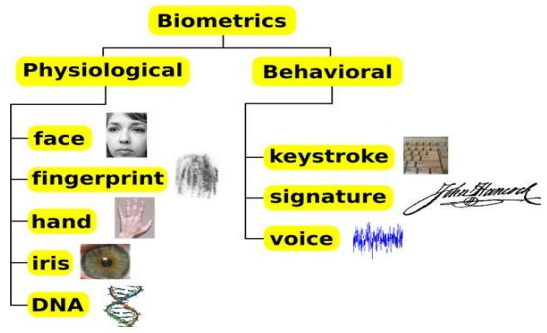

Fig1.Biometrics

There are many authentication schemes have been proposed up to now. But, most of these schemes have both the advantages and disadvantages.

II.STEGANOGRAPHY

Steganography is the art and science of hiding communication, a steganographic system thus combines hidden content in unremarkable cover media so as not to attempt an eavesdropper's attack. In the past, people used hidden tattoos or invisible ink to convey steganographic information content. Today, computer and network technologies provide easy-to-use communication channels for steganography.The information-hiding process in a steganographic system starts by identifying a covermedium's redundant bits (those that can be modified without destroying that medium's integrity).The embedding process creates a stego medium by replacing these redundant bits with information from the hidden message. Even if secret content is not revealed, the existence of it is: modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called statistical steganalysis.The data security approach when combined with encryption and steganographic techniques for hidden communication by hiding it inside the multimedia files[4][5].

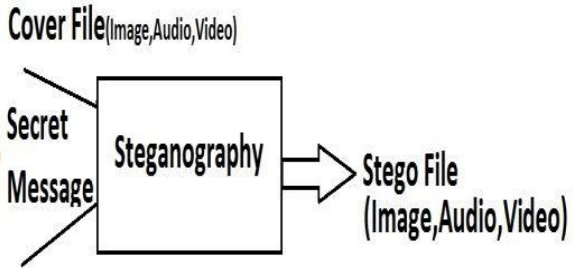

Fig.2 Steganography

The maximum results are achieved by providing the security to information before transmitting it through the internet[2]. The files like audio, video, images, contains collection of bits that can be further translated into images, audio and video.

II.PROPOSED SYSTEM

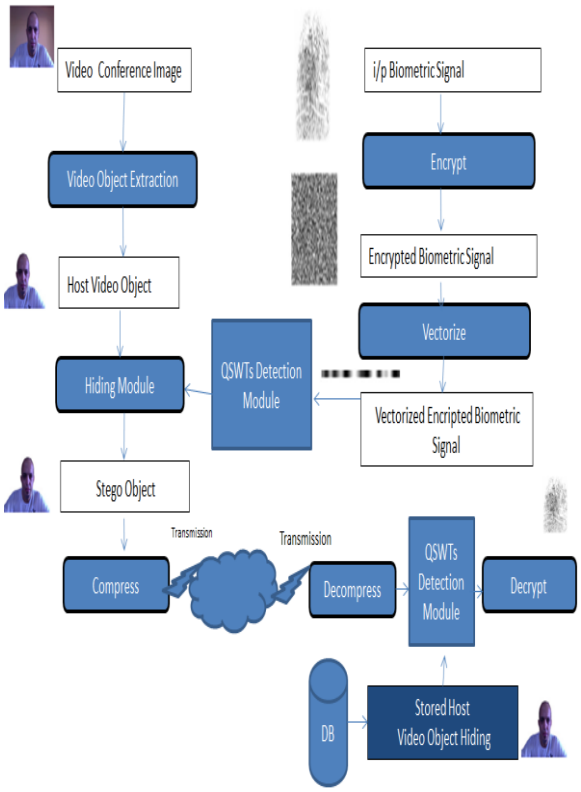

Fig3.Working of proposed system

In Proposed system firstly video conferencing the object is extracted with the host object then it is going through the hiding module this consist of QSWT I. e. Qualified Significant Wavelet Tree this is beneficial where lossy transmission and compression in wireless network. In this module the input signal is also encrypted with biometric samples so individuals identity is encrypted then vectorise this biometric signal [4]. Then stego object which is compressed is transmitted to decompress through QSWT's module and decrypted. Database of stored host object which is hidden is also maintained.

III.ADVANTAGES

1. Non intrusive.
2. Cheap technology also available
3. Very high accuracy.
4. High Accuracy

IV.APPLICATIONS OF BIOMETRIC SYSTEMS

a) Fingerprint verification system manufactured by Digital Person, Inc., is used for computer and network login.
(b) Fingerprint-based point of sale (POS) terminal manufactured by Indivos, Inc., that verifies the customers before charging their credit cards and speeds up payment in retail shops, restaurants and cafeterias.
(c)Fingerprint-based door lock manufactured by BioThentica Corporation used to restrict access to premises is shown.
(d)Immigration and naturalization service accelerated service system (INSPASS), which is installed at major airports in the U.S., is based on hand geometry verification technology developed by Recognition Systems, Inc., and significantly reduces the immigration processing time.
(e) Border passage system using iris recognition at London's Heathrow airport.
(f) Ben Gurion airport in Tel Aviv (Israel) uses Express Card entry kiosks fitted with hand geometry systems for security and immigration.
(g)The Face Pass system from Village is used in POS verification applications like ATMs, therefore obviating the need for PINs.
(h) The Identix Touch Clock fingerprint system is used in time and attendance applications.

Fig.4. Applications of Biometric

CONCLUSION

Using biometric signals we can encrypt information with biometric sample and transmission is done through video or any other media. This information is hidden in the form of steganography image. 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. 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/bifurcations in case of fingerprints).

FUTURE SCOPE

Biometric signal which contains encrypted image or video can be divided into number of frames so that it is more secure this feature can be extended. Image can be divided into no. of pixels clustering is done and that mapping leads to more security.

References

[1]K. Zebbiche, L. Ghouti, F. Khelifi, and A. Bouridane, "Protecting fingerprint data using watermarking," in Proceedings of the 1st NASA/ESA Conference on Adaptive Hardware and Systems. IEEE Computer Society, 2006, pp. 451–456.

[2] K. Zebbiche and F. Khelifi, "Region-based watermarking of biometric images: Case study in fingerprint images," International Journal on Cryptography and Information Security, vol. Article ID 492942, 2008.

[3] T. Hoang, D. Tran, and D. Sharma, "Remote multimodal biometric authentication using bit priority-based fragile watermarking," in Proceedings of the 19th International Conference on Pattern Recognition. IEEE Computer Society, 2008, pp. 1–4.

[4] T.-Y. Chen, C.-H.Ling, and M.-S. Hwang, "Weaknesses of the yoonkim- yoo remote user authentication scheme using smart cards," in Proceedings of the 2014 IEEE Workshop on Electronics, Computer and Applications. IEEE, 2014, pp. 771–774.

[5] S. Areepongsa, Y. F. Syed, N. Kaewkamnerd, and K. R. Rao, "Steganography for a low bit-rate wavelet based image coder," in Proceedings of the IEEE International Conference on Image Processing, vol. 1. IEEE, 2000, pp. 597–600.

[6] D. Kundur, Y. Zhao, and P. Campisi, "A steganographic framework for dual authentication and compression of high resolution imagery," in Proceedings of the IEEE International Symposium on Circuits and Systems, vol. 2. IEEE, 2004, pp. 1–4.

[7]D.He and D.Wang, "Robust biometrics-based authentication scheme for multi-server environment," IEEE Systems Journal, pp. 1–8, 2014.

[8] M. Ramkumar and A. N. Akansu, "Capacity estimates for data hiding in compressed images," IEEE Transactions on Image Processing, vol. 10(8), pp. 1252–1263, 2001.