International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 6 –OCTOBER 2016 (SPECIAL ISSUE)

Secured Transmission of Data over AWGN Channel Using Image Features, Steganography and AES

Mohammad Ziaullah[#1] and Roshan Ara C[*2]

[#]*Assistant Professor, Department of ECE, SECAB I.E.T, Vijayapur, Karnataka, India*

[*] *PG Scholar, Department of ECE, BLDEA'S CET, Vijayapur, Karnataka, India*

***Abstract*— Wireless security data is one of the challenges in wireless network. Because of the less and weak authentication and frequently changes, strong security mechanism are difficult to implement in such network. This paper presents a novel architecture for Image based authentication for wireless channel which is noise resilient and tampers proof. The server database stores set of images and a symmetric key is generated through Advanced Encryption Standard(AES) key generation for each user. Each user chooses an image as password from database, features are extracted from image and are encrypted with above key, the encrypted message is hidden behind an image and again encrypted using same key and transmitted via AWGN channel with tampering and noise addition. At receiver, encryption domain feature matching is introduced. As the decryption process partially exposes the data to the imposter hence, not decrypted. Therefore, it selects all the images from the database, extracts their features and encrypts them with each user keys. With the incoming encrypted and tampered features it finds closest match and authenticates the user with closest match. The proposed system effectively authenticates users even under high noise and attack. Results are compared with a without hiding over an image and text based method. Hence, image feature based authentication using steganography technique fares better than text based authentication scheme.**

***Index Terms*— authentication, encryption, security ,resilient, steganography, AWGN.**

I. INTRODUCTION

Wireless security data is one of the challenges in wireless network. Because of the less and weak authentication and frequently changes, strong security mechanism are difficult to implement in such network. Though many authentication, cryptography and watermarking techniques are proposed, rarely the effect is carried out under noisy channels. Digital images have great impact on multimedia information. Hence, image authentication has greater importance and has lead to many image authentication algorithms. Digital multimedia plays an important role in application as such in broadcasting, gathering of intelligence data, criminal investigation and also in medical field[17]. This data may be vulnerable to many malicious attacks during transmission over public channel or wireless channels and hence trustworthiness could not be achieved or guaranteed.Any tamper to image data could change the decision. Image authentication based on content aims to verify the integrity of image, which is desirable to robustness, compression and transmission errors, while able to detect tampered area. Image data is always affected in wireless channels due to multipath, Doppler frequency or environmental noise, or some packet losses.

Image steganography is the process of hiding digital data behind the images. The most common form of image steganography is LSB steganography where one bit of message data is hidden (or simply put in the least significant bit of a pixel colour). Thus variation in the colour is minimum for the observer and the image still looks similar. At the receiver side, information from all the LSBs are extracted and combined to obtain the actual information.

Content-based authentication is one of the efficient image authentication methods, where the image remains authentic even when content does not change[17]. Most of the previous efforts in content-based image authentication have mainly focused on developing the technique for transmission of data under ideal assumption of noise free channel. However, these technique and method will not work when transmitted through error-prone wireless channels. For example, any transmission bit error cause failure and also the synchronization may become a problem for security technique with some losses of packet. The remaining part of paper is organized as follows.

Section II describes literature survey. Section III gives problem definition of work. Section IV objective of the study Section V describes the proposed encryption analysis of image feature based authentication. Section . Section VI presents the result and discussions, finally, concluded this paper in section VII.

II. LITERATURE SURVEY

Advancement in the field of networking and digital media technology has created large multimedia applications. This application is used in distributed network which makes multimedia contents vulnerable to malicious attacks and privacy. For any insecure media, it is possible for an attacker to tamper with images while transmission. For such environments, to guarantee trustworthiness, images authentication are used to confirm the integrity and prevent forgery.

Nan-I Wu and Min-Shiang Hwang [1] have done study on requirements of steganography methods and PSNR, payload, hiding capacity of images. The performance analysis has been carried out for different images of capacity, PSNR, using simple LSB and optimal LSB hence compared metrics for various techniques used.

Cachin [2] have proprosed information thereotic model of steganography for hiding information from passive attackers thus a secret key stegosystem has been developed .Universal data compression used in this model for steganography which is considered to be a statistical model.

Neil F. Johnson and Sushil Jajodia [3] proposed some features of information hiding techniques of steganalysis which can be used by steganaylst to detect the hidden images.

İsmail Avcibaş, et al., [4] have developed steganoanalysis algorithm using support vector machines based on binary measures. In this technique similarity of binary measure is computed using seventh and eighth bit planes of an image. LSB, SFFS techniques were implanted and performance is measured in terms of message length and capacity versus change in bit plane correlations.

Young WANG et al., [5] have developed cryptographic algorithm using low key authentication technique. The purpose of this method is to shift sensitive keywords from the text which is to be transmitted.

Steganography is a technique where a message is hidden in the form of an image or audio and thus secured data can only be transmitted to the receiver using secret keys. In this approach pixels are embedded by mathematical function which maps into 8 neighbouring pixels. The technique of specific image steganography was proposed by Bhattacharyya et al., in [6]. In which the secret key authentication can be used to communicate message end to end more securely.

A high capacity method to transform wavelet co-efficient of the secret information is emdedded into the image and transmitted retaining the integrity of wavelet co-efficient. This was proposed by Sarreshtedari and Ghaemmaghami., in [7], to transform domain image steganography.

Data can be embedded in DWT in 4x4 blocks of matrix coefficients on cover image using Genetic Algorithm based mapping. This application of Wavelet Transform and Genetic Algorithm was presented by Elham Ghasemi et al., [8]. To improve the robustness of the steganographic algorithm, frequency domain and optimal pixel adjustment process were used after embedding the message.

An adaptive Steganography technique was proposed by Safy et al. [9]. In this technique bits of payload adaptively is not exposed. They are kept hidden in wavelet co-efficient of the cover image retaining pixel adjustment optimum.

Jskolka et al., [10] designed a mechanism which provides perception for covert channel communication. This scheme is good to relate covert channels steganograhic techniques and watermarking..

Sanjeev Manchanda et al., [11] developed a model that presents random number logic based steganographic methods and layout management schemes to hide data into the image. These methods can be modified accordingly as per the need of application and features of data/images. They have used three methods with different levels of complexities i.e, simple, low and moderate level of complexity for image hiding. The encryption key is generated using random numbers.

Shiva Kumar et al. [12] proposed HDLS model for embedding and extracting payload images this is a hybrid Steganographic method by integrating transform domain and spatial domain, in this technique the cover image and payload image is separated into two cells A and B, the cover image of cell A of spatial domain is divided into its RGB component and transformed into Transform domain using DCT/DWT/FFT and embedded individually in a unique way, while the components of cell B are retained in the spatial domain only.

S.S. Maniccam and N.G. Bourbakis [14] have developed a new technique of image video encryption. It depends on SCAN methodology by which large number of scanning paths and space filling curves can be produced, it helps in first stage video compression.

Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen [15] developed a method for images of cryptosystem using vector quantization, cryptography and number theory. Vector quantization (VQ) is done by decomposing the images and then encoding them sequentially.

Aloka Sinha and Kehar Singh [16] designed a new method of Steganography, which has most significant role in keeping information secret in the open field of internet. The data is hidden in integer wavelet co-efficient and communicated to the authenticated receiver by using cryptography. To reduce the error in the embedding secrecy OPA algorithm is used. The authors have developed colour image water marking scheme through alpha channel and Steganographic model with high capacity. This method uses genetic algorithm as well as IWT for sending the secret text. Performance parameters are hiding capacity, image size and PSNR. Because of the lack of authenticity and packet loss many algorithms has been proposed. Due to the many forgery attacks on channel some of the important methodology is designed to overcome these attacks by increasing the rate of authentication.

Hence in our proposed method encryption domain analysis of image data content is designed using the technique of steganography and AES. The image features are extracted and encrypted using 128-bit AES algorithm, and at the receiver, all database image features are extracted using haar wavelet and encrypted with same key. The received data is compared with database features, closest match gives the authentication.

III. PROBLEM DEFINITION

A technique for secured transmission over wireless channels using image features extracted using wavelet transform and hence protecting the same with AES encryption technique. As compared with text /conventional methods of securing data with text password, image password is better. Hence, our proposed technique produces good authentication results even when the channel is error and tampering are more. A comparative study is done with both text and image authentication using steganography.

IV. OBJECTIVE OF THE STUDY

The Secured authentication process is one of the major challenges in wireless data transmission. There are several factors that affect the transmission which includes different noises like white Gaussian noise, Rayleigh fading and so on. Beside this fact, the channels and transmission data are affected by tampering as wireless data is overheard by neighboring nodes. Hence, conventional cryptography based digital signature schemes are risky. On the other hand, image-based authentication schemes do guarantee better performance but are not resilient to channel errors and tampering changes.

Therefore the objective is to design a secured technique for end to end digital authentication over wireless transmission channel which should not be affected by noise or tampering.

- Developing the secured wireless transmission of image content by providing high authenticity.
- Comparing the level of authentication between conventional text password and image features used along with the method of steganography.

V. PROPOSED METHOD

The system modeling is done, that is content-based authentication approach which passes images as authentic, the work extending is digital authentication such that for image authentication method for verification must be content preserving while being sensitive to changes in modification. The efforts in previous methods of content-based image authentication are such that under the ideal assumption of reliable noise free channels, but this kind of system does not work when transmitted over error prone channels. In this system an error-prone channel is used that is AWGN channel with some signal-to-noise ratio, by taking care of synchronization which was a problem in traditional methods where packet losses are included.

The present work is formulated as image authentication scheme which produces good authentication rates over wireless channels which makes use of mainly convolution method or other error correction codes to recovers from the noisy channels, and make the computational difficult for the application, but unfortunately it consumes lot of bandwidths which reduces the effectiveness of the technique. Therefore, without any additional complexity the improvement in the security of wireless authentication system is illustrated. The proposed scheme generates only fixed size length digital signature regardless of loss of packets.

The security is achieved by structural features by adopting the filter parameterization technique. Some of the common image application involves a multiple cycles of decompression of images and then re compressing using default or user-defined parameters. It should be able to allow the acceptable manipulations passing through the authentication make alert of malicious content.

The process is explained diagrammatically in the fig.1 above. First an image is selected and its features are extracted using wavelet. An encryption is performed by using AES using the generated key, the encrypted values are hidden in image using steganography, again AES is performed on encrypted values using same key. This is transmitted over the wireless channel by first modulating using BPSK modulation.

The algorithm for the proposed method can be explained by the steps given below:

1. User registers with the system. It generates a unique 16byte key for each user. Every generated key is stored in database.
2. Once many users are registered with the system, then user's selects the transmission process by selecting a user and image from a set of images database available.

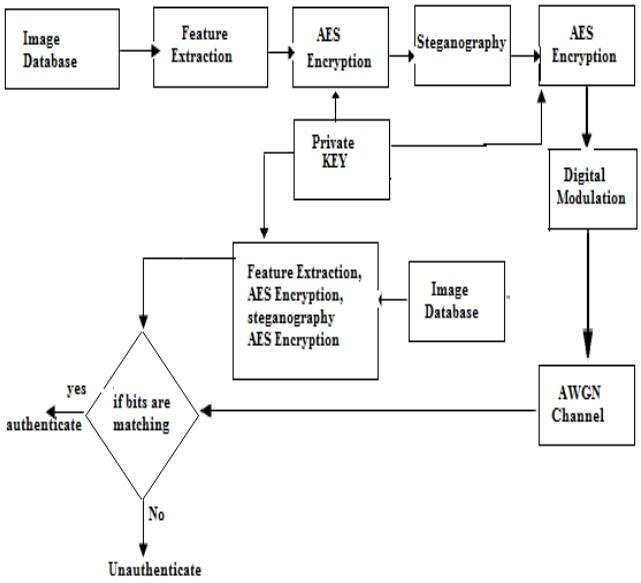

Fig1. Proposed System Block Diagram

3. Extraction of wavelet features from image is done. The features are nothing but standard deviation and mean of decomposed images, decomposition of images is done by using haar wavelet transform.
4. The extracted features of images are 16values and are encrypted using Rinjdeal, which is symmetric encryption. For encryption user data key is used which is generated initially.
5. Encrypted feature values are hidden behind an image and processed through AES encryption then transmitted over channel.
6. Baseband modulation is used and technique of bipolar coding to convert data.
7. Addition of noise is done with specified signal-to-noise ration, this make the resulting signal amplitude fluctuating.
8. As per user choice some bits are changed, this process is called tampering where the bits are changed which makes the actual data to change.
9. At the receiver side, the receiver does not know which image's feature had come, which user has sent, whether data is noise affected or not, hence it select all the images from the database and extract the wavelet features of all the images.
10. The receiver uses the same key which is stored in the data base.
11. It encrypts the image features extracted along with steganographic data values with all the keys available in database and compare with stored database features.
12. The distance is calculated between the received image feature stored in database with the all the image features extracted from database using Euclidean distance.
13. The distance which is smallest is assumed to be authenticated.

VI. GRAPHS AND DISCUSSIONS

The below Fig 2 shows the plot for data transmitted over AWGN channel with noise addition. This graph shows actual data along with the noise affected.

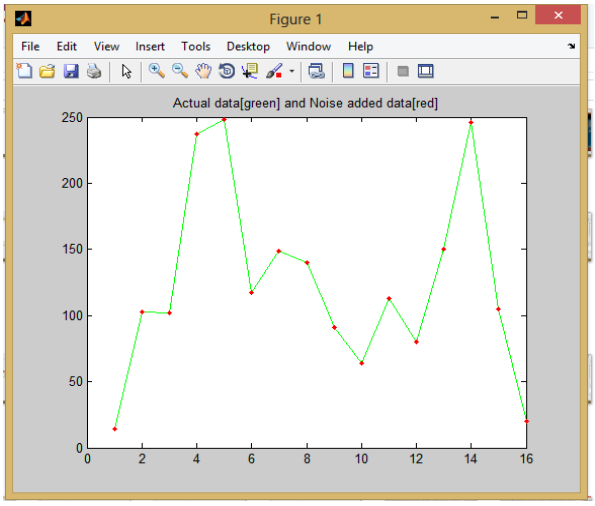

Fig 2: transmitted data with noise addition

Fig 3 below shows the plotted graph for encrypted data along with the noise. It is plotted for bytes along x axis and encrypted values along y axis. The figure shows both the transmitted encrypted data and also tampered bytes.

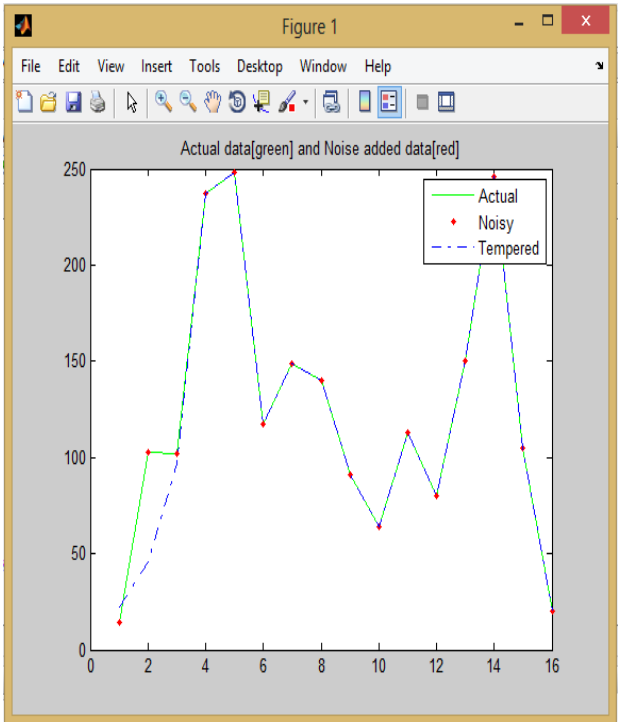

Fig 3. Transmitted data along with tampered data

The below table 1 shows the comparison between image and text which is tested with different SNR values with no tampering. The achieved accuracy of image-based is good as compared with text-based method. As the value of SNR is increased the rate of authentication is also increased. Hence, image-based content authentication provides more security and robustness.

SNR in dB	Proposed Accuracy in%	Accuracy of Text in %
-10	60	47
-5	70	54
0	80	61
5	80	75
10	80	78
20	90	83

The below Fig 4 shows the rate of authentication achieved is better than the conventional method of authentication and it is also compared with the text based authentication for various values of SNR

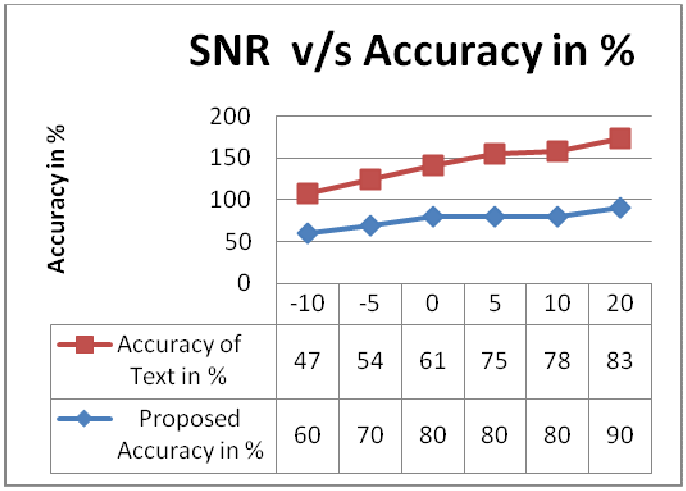

Fig.4 Achieved accuracy for both image and text with no bytes tampered for various values of SNR.

The table 2 below shows the comparison between image and text. The rate of accuracy for image is more as compared with text-based method even under tampering effect.

Bits Tampered	Accuracy of Proposed system in %	Accuracy of Text Based system in %
1	80	74
2	70	65
5	60	41
8	35	20
10	20	9
16	12	0

The below Fig.5 shows the rate of authentication achieved is better even under tampering effects. The accuracy decreases as the number of tampering bytes are increased. It can also be seen that rate of accuracy is less for text based authentication.

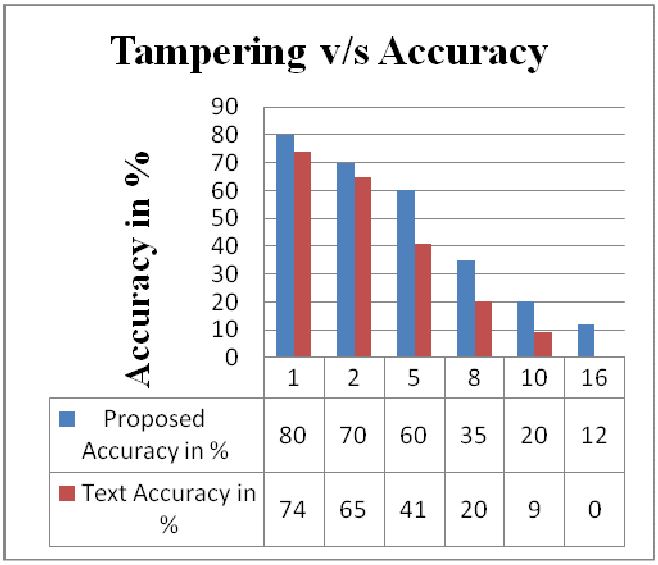

Fig.5 Achieved accuracy for both image and text with various bytes tampered for fixed SNR

VII. CONCLUSION

In this work, a modified scheme of authentication for image content is proposed using AES and steganography. The image features and the wavelet parameterization are incorporated in to conventional method of crypto system to enhance the level of robustness and security. And also the use of Steganography make the system more secured hence no computational complexity is required for this proposed scheme therefore used for suitable wireless communication and other real time application. A case study on text based password is also simulated and hence authentication of data confirming that the image based content authentication using image features, Steganography and AES are more robust and secure than text based password.

REFERENCES

[1] Nan-I Wu and Min-Shiang Hwang, "Data Hiding: Current Status and Key Issues," *International Journal of Network Security*,Vol.4, No.1, pp.1-9, January 2007.

[2] C Cachin, "An Information-Theoretic Model for Steganography," *Journal Information and Computation*, Vol.192, No.1, pp.41-56, 2004.

[3] Neil F Johnson and SushilJajodia, "Steganalysis: The Investigation of Hidden Information," *Proceedings of IEEE International Conference on Information Technology*, pp. 113-116, September 1998.

[4] İsmail Avcibaş, Mehdi Kharrazi, Nasir Memon and Bülent Sankur, "Image Steganalysis with Binary Similarity Measures," *EURASIP Journal on Applied Signal Processing*, (2794-2757), 2005.

[5] Yong WANG, Qichang HE, Huadeng WANG, Bo YIN and Shaoling DING, "Steganographic Method Based on Keyword Shift," *Information Management and Engineering (ICIME)*, pp.454-456, 2010.

[6] Bhattacharyya S, Kshitij and A P Sanyal G, "A Novel Approach to Develop a Secure Image Based Steganographic Model using Integer Wavelet Transform," *International Conference on Recent Trends in Information, Telecommunication and Computing*, pp.173-178, 2010.

[7] Sarreshtedari S and Ghaemmaghami S, "High Capacity Image Steganography in Wavelet Domain," *International Conference on Consumer Communications and Networking*, pp.1-6, 2010.

[8] Elham Ghasemi, Jamshid Shanbehzadeh and Nima Fassihi, "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm," *Proceedings of International MultiConference of Engineers and Computer Scientists*, 2011 Vol. I.

[9] R O El Safy, H H Zayed and A El Dessouki, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform," *International Conference on Networking and Media Convergence*, pp.111-117, March 2009.

[10] Jaskolka, Jason Khedri and Ridha, "Exploring Covert Channels," *Hawaii International Conference on System Sciences*, pp.1-7, 2011.

[11] Sanjeev Manchanda, Mayank Dave and S. B. Singh, "Customized and Secure Image Steganography through Random Numbers Logic" Signal Processing: *An International Journal, Volume 1: Issue (1)*, 2008.

[12] K B Shiva Kumar, K B Raja, R K Chhotaray, Sabyasachi Pattnaik, "Steganography Based on Payload Transformation", *IJCSI International Journal of Computer Science Issues*, Vol. 8, Issue 2, March 2011.

[13] K B Shiva Kumar, K B Raja, Sabyasachi Pattnaik, "Hybrid Domain in LSB Steganography", *International Journal of Computer Applications (0975 – 8887) Volume 19– No.7*, April 2011.

[14] S.S.Maniccam, N.G. Bourbakis, ―Lossless image compression and encryption using SCAN‖, Pattern Recognition 34, 1229-1245 (2001).

[15] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, ―A new encription algorithm for image cryptosystems‖, *The Journal of Systems and Software* ,58 (2001),pp 83-91.

[16] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, ARTICLE IN PRESS, 2003, 1-6, www.elsevier.com/locate/optcom.

[17]M. Ziaullah, P. Shetty and S. Kamal, "Image feature based authentication and digital signature for wireless data transmission," *2016 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, 2016, pp. 1-4.