International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT12173125

Dual Security based on Crypto Steganography Using Two Level Learning in Assist with Dual Offbeat Shielding Design

P. M. Siva Raja, Sumithra R. P, Thanusha G

Computer Science and Engineering, Amrita College of Engineering and Technology, Nagercoil, Tamilnadu, India

ABSTRACT

Article Info
Volume 7, Issue 3
Page Number: 541-548

Publication Issue :
May-June-2021

Article History
Accepted : 18 June 2021
Published : 25 June 2021

A sensor node and other electronic devices attached to any IoT object can be involved in the communication over wireless network in IoT environments, which makes it necessary to preprocess a large amount of sensed data before storing it. Therefore, sensing data in the form of images is to be sent to the cloud storage system via wireless medium, but this suffers from image hijacking where data is manipulated, which leads to insecure transmission. To mitigate this problem, two levels of security are employed. Memory retaining is the primary level of enhancing learning which uses past experiences to extract optimal features from sensed images and then subjected to offbeat shielding activities, which include cryptographic steganography. The proposed system creates cloud storage that is protected by the optimal features learned from a neural network, thus ensuring that clouds are secure in the Internet of Things.

Keywords : Chen Chaotic System, Wrapper Based Feature Selection, Pixel Value Differencing, Glow Worm Search Optimization.

I. INTRODUCTION

The IoT alludes to systems of mixed gadgets as contrasting to customary systems of homogeneous gadgets [1]. Things, in the IoT, include an assortment of installed gadgets and smart object whose interconnection is based on to empower progressed and insightful applications and to make the correspondences and mechanization, for the maximum area in all zones, less demanding and achievable. The expansive scale execution of IoT gadgets promises to change plentiful portions of the system in which human being live [2].

For customers, new IoT items like Internet-empowered machines, home robotization facilities and vitality administration gadgets are pushing us on the road to a dream of the "shrewd home'', offering greater security and vitality, productivity [3]. The IoT design combines three layers. They are layer for perception, layer for network management and application layer. The observation layer additional name for perception layer is the least layer of the ordinary design of IoT [4]. This least layer's principle obligation is to gather valuable data/information from things or nature.

The network layer's fundamental duty is to help and secure information transmission between the third layer and recognition layer of IoT engineering [5]. This layer predominantly gathers data and conveys to the observation layer toward a few applications and servers. Essentially, this layer is a union of web and correspondence-based systems [6]. The application layer is concerned as a best layer of regular IoT design. This layer gives the customized based administrations as specified by client significant necessities.

This present layer's fundamental obligation is to interface the real hole between the clients and applications [7]. This IoT layer joins the business to achieve the ideal state smart applications with arrangements such as the calamity checking, well-being observing, transposition, fortune, medicinal and natural condition, and took care of worldwide administration pertinent to all important applications so image played a vital role in IoT applications [8]. In order to maintain the quality of an image in terms of integrity, consistency, more no of schemes has been proposed.

Difficulties for IoT security are, ensure high accessibility, notice susceptibilities and episodes, manage vulnerabilities, Predict and appropriate security issues, Secure web, portable and cloud applications, Secure correspondence, Secure obliged gadgets, Authorize and validate gadgets, Manage gadget refreshes [9]. To discourse these IoT security issues SS Layer convention or SSL had been utilized wherever information is available on the web. Sites effectively utilized SSL affirmation to scramble and secure the client's resources on the internet [10].

II. LITERATURE SURVEY

Parah et al. [14] discussed that algorithm for color image stenographic built on hybrid edge detection was utilized. Hybrid edge detection had been utilized for managing the edge and non-edge pixels of green and blue planes of cover picture. The RC4 encryption calculation was utilized to encode mystery message before inserting it in the cover picture to upgrade security of the mystery information. A delicate watermark/logo (whose size was under 1% of aggregate mystery information) had been installed, other than mystery information in the cover picture, to encourage content verification and early alter detection. Even it achieved high embedding ratio, time complexity had been high.

Zear et al. [15] presented a multiple watermarking algorithm relied on wavelet transforms in discrete form (DWT), Cosine transform (Discrete-CT) and singular value decomposition (SVD). To improve the robustness act of the image watermark, Back Propagation Neural Network (BPNN) remained associated to the removed picture watermark to diminish the clamor consequences for the watermarked picture. Further, the side effect and mark content watermarks were additionally encoded by lossless number juggling pressure procedure and Hamming mistake revision code separately. This system achieved more embedding ratio.

Poljicak et al. [16] analyzed the Steganography method for real time data hiding. The prime goal of the examination is to create steganography strategy with expanded heartiness to accidental picture preparing assaults and demonstrated the legitimacy of the technique progressively applications. The strategy depends on a discrete cosine change (DCT) where the estimations of a DCT coefficient were altered. This system provided more security on an image but it lacked in embedding ratio in terms of high mean square error.

Srijan et al. [17] explained that Secured information transmission was one of the main problems looked in the realm of Web. As the measure of information on Web is growing every day, the significance of information security is likewise expanding. A rare approach like cryptography, watermarking, steganography was utilized to upgrade the information to be transmitted. This paper used a steganography calculation in the spatial space utilizing the idea of pixel tweak. This system achieved more embedded ratio.

Poljicak et al. [18] discussed the Steganography method for real time data hiding. The primary objective of the exploration was to create steganography technique with expanded vigor to unexpected picture handling assaults. Moreover, it demonstrated the legitimacy of the technique progressively applications. The strategy relies on a discrete cosine change (DCT) where the estimations of DCT coefficients were altered with a specific end goal to shroud information. This system achieved more embedding ratio but time complexity had been high.

III. IMMUNE CLOUD STORAGE IN IOT BY FEATURE SELECTION RELY ON LEARNING WITH CRYPTO BASED SREGANOGRAPHY

Since IoT is a context aware computing, more number of sensed data have to be preprocessed before storing. Most of the existing techniques for preprocessing have experienced high time and space complexity problems since IoT is sustainable only for light weight mechanisms and also the sensed data from one phase to another phase would be sent through wireless medium in IoT so it is highly susceptible to data hijacking which leads to degradation in data integrity and confidentiality.

The proposed system has involved in two tier processes for learning which preprocess the sensed data to get best features as well as for data encapsulation based on crypto based steganography to achieve dual offbeat shielding. Since data to be stored is gathered from sensor network; it includes both nonlinear and linear data. In order to remove those unwanted data, effective preprocessing techniques are required. In the proposed system machine learning algorithms based on memory retaining are used to preprocess that data which is gathered from the sensor nodes.

In preprocessing phase, optimized recurrent neural network is introduced and it has two sections first one is training section and another one is testing phase. In training phase short term memory is adapted to enhance the preprocessing with past history. Even though an optimized recurrent neural network achieved memory retaining for better calculation based on frequent updating of weights on each node in the hidden layer, it suffers time complexity. In order to overcome the time complexity problem, deep belief network is adapted with wrapper-based feature selection based on genetic algorithm.

Then best features would be utilized in both cryptography as well as steganography for providing the data security in IOT. Here the Cryptography technique, Chaotic AES (Advanced Encryption Standard) can be utilized on the features extracted from the Deep Learning networks with reduced number of iterations.

Even though an image is encrypted, it may be modified by attacker using decryption techniques. In this, Dual image based LSBPVD (Least significant Bit

Substitution-Pixel Value differencing) using modulus function is utilized for performing the steganography process with dual stego image. Accordingly, the embedding capacity and visual quality can be improved. Thus, we can have an extensive security analysis, which demonstrates the satisfactory security level of the new scheme with reduced complexity.

Finally, Optimized ANN can be utilized as an analytics methodology which would check whether our storage is correct. Here, the stego images produced by the proposed steganography algorithm with cover image which can be tested by Artificial Neural Network. This features of Stego image is matched with the features extracted from the deep learning process to check whether there is any attack or not. To speed up this process we are utilizing the Anarchic Fuzzy optimization algorithm which comprises of fuzzy c-mean and Improved Glow Worm search optimization.

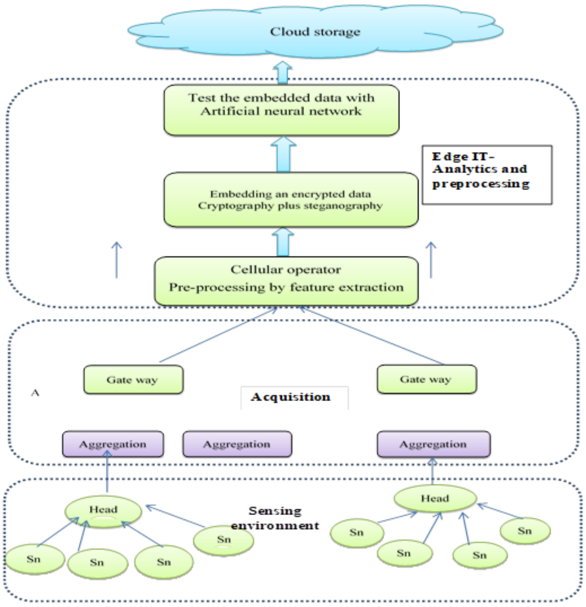
Cloud storage
Test the embedded data with Artificial neural network
Edge IT-Analytics and preprocessing
Embedding an encrypted data Cryptography plus steganography
Cellular operator
Pre-processing by feature extraction
Gate way
Gate way
A
Acquisition
Aggregation
Aggregation
Aggregation
Head
Head
Sensing environment
Sn
Sn
Sn
Sn
Sn
Sn
Sn
Sn

Figure 1. Dual learning-based security using crypto steganography in IoT environment

A. Sensing and acquisition

Since IoT based applications are rely on the context aware computing, a greater number of sensor nodes is deployed. Each sensor node in the IoT based network would involve in detecting physical conditions, perform computation on those sensed data and communicated with the sensor head. Each sensor node has limited energy so it would send the sensed data to the head of the sensor network instead of sending directly to the base station.

B. Gateway

The Gateway is a critical piece of IoT communication network structure whose part is to interconnect the end gadgets to the primary user of the network. This is required to give convention interpretation and practical mapping between the unconstrained networks and their constrained counterparts, such as ieee802.11-ieee802.15.4, IPv4/v6-6LoWPAN, XML-EXI, HTTP-CoAP and others. It permits the sensed data from the head of the sensor network would be sent to the cellular operator through gate way.

C. Efficient memory retaining RNN

Since data are gathered using sensor nodes S= (s0, s1…………..sn) and collected resources which is defined as G= {img1, img2, img3… imgn} are transmitted through the gate way, it includes both linear and nonlinear data. In order to remove the unwanted data, it requires data preprocessing techniques. Since sensor nodes deliver real time information, machine learning which is combined with feature selection algorithm are adapted to preprocess the sensed data.

The specialty of an optimized recurrent neural network is that it has used memory cell which is controlled by forget layer for storing enough amount of data in hidden layers of the neural network so it has taken more time to set weightage for each neuron in the hidden layer. In order to set weightage for each neuron in the hidden layer optimally, deep belief network with wrapper-based feature selection is adapted.

The formula for the current state is derived by:

$$ht = f(s,xt) \tag{1}$$

Where ht is the new state, is the present state and xt is the current input. Previous output is represented as xt-1 = imgn.

D. Dual security based on crypto steganography

Since preprocessed data would be transmitted through the wireless medium to the cloud storage, transmitted data is in risk of stealing by malicious user in the IoT environment so crypto based steganography is employed for maintaining data integrity, confidentiality and privacy of the data which is sensed in the IoT environment.

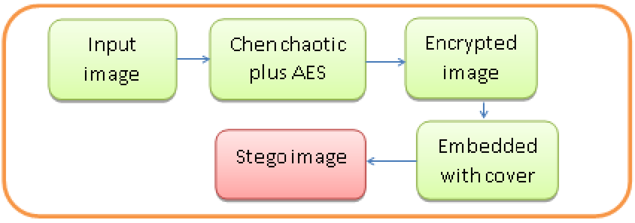

Figure 2. Dual security Workflow of the encryption process

E. Encryption using Chen chaotic system

In this phase, an advanced encryption standard is incorporated with Chen chaotic system for reducing no of repetitions and the input image which is to be encrypted would be selected based on equation (11) which holds the value of the best features of an image. The key streams for both permutations and substitution stages would be generated by Chen chaotic system mathematically; the general parametric Chen system is described by

$$\begin{aligned} \frac{dx}{dt} &= a(y-x), \\ \frac{dy}{dt} &= (c-a)x+cy-xz, \\ \frac{dz}{dt} &= -bz+xy \end{aligned} \tag{2}$$

Where a b c represents the parameters as real. The initial condition () would determine its orbit from which the permutation and substitution key streams are quantified. It is the immediate candidate for the secret key.

F. Embedding the encrypted data

Since encryption techniques are based on key, it is vulnerable to decode the encrypted one by malicious users so in this work an encrypted data would be embedded with a cover image in order to improve the security of the encrypted data. Here Pixel value differencing with least significant bit approach is amalgamated for embedding encrypted data on a cover image.

Initially the difference Di = pi − pi+1 for each block of two consecutive pixels pi and pi+1 of image from Cn would be calculated then started searching for the quantization range table for Di to determine how many bits will be embedded. Then the range Ri would be calculated by Ri=[li,ui], where li and ui are the low level bound and the upper bound of Ri, and $\lfloor \log 2\ (ui-li) \rfloor$ is the number of embedding bits. Read m secret bits from the secret bit stream and transform it into decimal value b. Calculate the new difference $\bar{d}ı$=li+b. Ensure both di and $\bar{d}$i are in the similar range to obtain novel pixel values $\bar{p}ı$ and $\overline{pı+1}$. Finally, the pixels pi and pi+1 of nth block would be replaced by the pixels $\bar{p}ı$ and $\overline{pı+1}$ of the stego image. After that in order to improve the embedding capacity, modulus function is applied. The embedding of secret key is carried out by u=2m.

$$\bar{x} = xi+ei-(LSBm(xi-1)+ LSBm(xi))Mod(u) \tag{3}$$

Where i is the position of the pixel in the cover image. e is the secret bit value and x' is the new value of pixel after encoding of the secret encrypted data .x is the host value of pixel in an image and m indicates the number of host bits that used to embed the data.

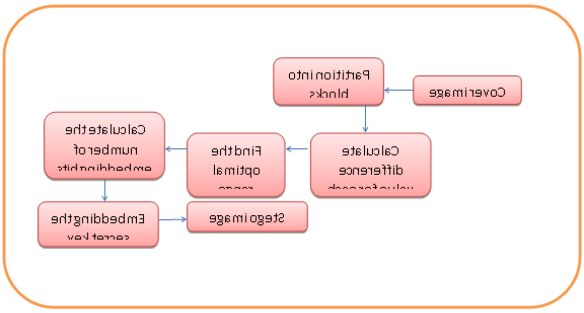

Figure 3. Embedding the encrypted image into a cover image

IV. RESULT ANALYSIS

A. Comparison of proposed system with existing techniques

In this section, the proposed system is compared with existing approaches like dual steganography combined with AES, Steganography with DES and Steganography with AES to evaluate the performance of the proposed system. In order to evaluate the proposed system following parameters are concerned Encryption time, Encryption memory, Mean Square Error Value, Peak Signal to noise ratio and embedded ratio.

1) MSE:

TABLE I

COMPARISON TABLE FOR MSE

Data Size (in KB)	Dual Steganography Combined with AES	Steganography Combined with DES	Steganography Combined with AES	Proposed
10	0.3227109	0.4995313	0.449846	0.31
20	0.4156016	0.5329297	0.396492	0.32
40	0.6013047	0.5052734	0.454565	0.30
60	0.4822031	0.5118359	0.417235	0.29
80	0.5302891	0.6456641	0.46752	0.28
100	0.551367	0.497305	0.65925	0.27

In proposed system, least significant bit encoding is combined with PVD which increases the hiding capacity with less distortion to embed the encrypted data into the cover image by altering the difference value between two contiguous pixels so this approach perfectly embedded the data in fewer time when compared to existing techniques such that when sixe is 100, the proposed system experienced the less mean square error value of 0.27 whereas existing approaches like duel steganography combined with AES, Steganography with DES and Steganography with AES experienced 0.551367, 0.497305 and 0.65925 respectively.

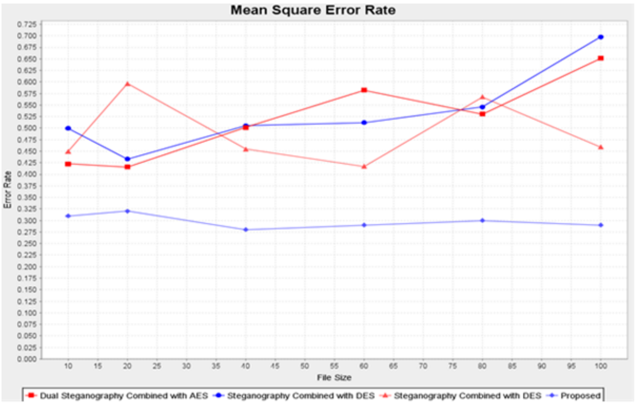

Figure 4. Comparison graph for mean square error

2) PSNR

TABLE II

COMPARISON TABLE FOR PSNR

Data Size (in KB)	Dual Steganography Combined with AES	Steganography Combined with DES	Steganography Combined with AES	Proposed
10	53.042667	51.145177	51.60016	99.23

20	57.501167	56.894584	52.14845	99.12
40	55.092265	51.095539	54.07282	98.23
60	52.307861	51.039496	51.927	98.16
80	56.981724	54.227387	52.478	98.03
100	52.673192	54.164578	53.94774	98.45

In proposed system, Chen chaotic system is combined with AES for reducing the number of repetition for basic operations such as substitution and permutation which is involved in the traditional AES based encryption and pixel vertex differentiating technique is combined with least significant bit encoding for embedding process increased the quality of the embedded image so it achieves high PSNR value when compared to other existing techniques such that when size is 100, the proposed system experienced the high PSNR value of 98.45 whereas existing approaches like duel steganography combined with AES, Steganography with DES and Steganography with AES experienced 52.673192, 54.164578 and 53.94774 respectively.

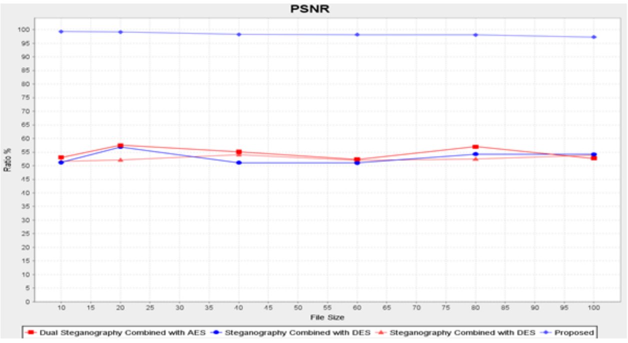

Figure 5. Comparison graph for PSNR value

V. CONCLUSION

The proposed two level learning model in assistance with the dual offbeat shielding design for effective preprocessing and securing data has taken less encryption time (124 sec) and Due to adaptation of chen chaotic system which reduces iterations involved in conventional AES system, the proposed system has taken less memory of (18.358KB) in which encryption algorithm is executed. It accomplished high peak signal to noise ratio of 98.45 and less mean square error value of 0.27 as the scheme implants data by altering the variance value between two contiguous pixels which increases hiding capacity with less distortion. Besides it achieved the average accuracy of 97% with embedding rate of 50%. By this way the proposed system has exposed better performance in enhancing protected cloud storage on IoT environment when compared to existing systems.

VI. REFERENCES

[1] El-Latif, Ahmed Abd, A., BassemAbd-El-Atty, ShamimHossain, M., Samir Elmougy, and Ahmed Ghoneim.2018 "Secure quantum steganography protocol for fog cloud Internet of Things." IEEE Access (6): 10332-10340.

[2] Luong, N.C., Hoang, D.T., Wang, P., Niyato, D., Kim, D.I., and Han, Z.2016 "Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models" A Survey.IEEE Communications Surveys and Tutorials18(4): 2546- 2590.

[3] Gao, J., Li, J., and Li, Y " Approximate Event Detection over Multimodal Sensing Data.Journal of Combinatorial Optimization".

[4] Gao, J., Li, J.,Cai, Z., et al. 2015 "Composite event coverage in wireless sensor networks with heterogeneous sensors." In Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM): 217-225.

[5] Zhang, Q., Zhu, C., Yang, L.T., Chen, Z., Zhao, L., and Li, P. 2017 "An Incremental CFS Algorithm for Clustering Large Data in Industrial Internet of Things." IEEE Transactions on Industrial Informatics13(3): 1193-1201.

[6] Singh, P., Agarwal, N., Raman, B. 2016 “Don’t see me, just filter me: towards secure cloud-based filtering using shamir’s secret sharing and pob number system” Proceedings of the Tenth Indian Conference on Computer Vision.Graphics and Image Processing, ACM12.

[7] Singh, P., Raman, B.,Misra, M.2017 “Just process me, without knowing me: a secure encrypted domain processing based on shamir secret sharing and pob number system.” Multimedia Tools Appl,1–25.

[8] Atee, HayfaaAbdulzahra, Robiah Ahmad, NorlizaMohd Noor, Abdul MonemRahma, S., and YazanAljeroudi. 2017 “Extreme learning machine based optimal embedding location finder for image steganography.” PloS one12(2): e0170329.

[9] Komal Patel and SumitUtareja.2013 “Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm.” International Journal of Computer Applications (IJCA)63(13).

[10] Sumathi, C.P., Santanam, T., and Umamaheswari, G.2014 “A study of various steganographic techniques used for information hiding.” arXiv preprint arXiv: 1401.5561.

[11] Srivastava, Arpit Kumar, ApoorvAgarwal, and AbhinavMathur.2015 “Internet of Things and its enhanced data security.” International Journal of Engineering and Applied Sciences (IJEAS)2(2).

[12] Jung, Ki-Hyun.2018 “Authenticable reversible data hiding scheme with less distortion in dual stego-images.” Multimedia Tools and Applications77(5): 6225-6241.

[13] Jung, Ki-Hyun.2018 “Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane” Journal of Real-Time Image Processing14(1): 127-136.

[14] LeCun, Y., Bengio, Y., and Hiton, G., 2015 “Deep learning” Nature521(7553): 436-444.

[15] Liu, M., Shi, J., Li, Z., Li, C., Zhu, J., and Liu, S.2017 “Towards Better Analysis of Deep Convolutional Neural Networks.” IEEE Transactions on Visualization and Computer Graphics(1): 91-100.

[16] Wu, X., Zhu, X., Wu, G.Q., and Ding, W.2014 “Data mining with bigdata.” IEEE Transactions on Knowledge and Data Engineering26(1): 97-107.

[17] Schmidhuber, J.2015” Deep Learning in Neural Networks: An Overview.” Neural Networks61:85-117.

[18] Ngiam, J.,Khosla, A., Kim, M., Nam, J., Lee, H., and Ng, A.Y. 2011 “Multimodal Deep Learning.” in Proceedings of the 28th International Conference on Machine Learning: 689-696.

Cite this article as :

Siva Raja P M, Sumithra R P, Thanusha G, "Dual Security based on Crypto Steganography Using Two Level Learning In Assist with Dual Offbeat Shielding Design", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7, Issue 3, pp.541-548, May-June-2021. Available at doi : https://doi.org/10.32628/CSEIT12173125
Journal URL : https://ijsrcseit.com/CSEIT12173125