Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 7, pp. 1981–1990
DOI : 10.47974/JDMSC-1838

WSN recruitments for encrypted medical image transmission securely

Israa Hussain Abdalla *
Ministry of Education
Directorate of Education Baghdad
Karkh
Iraq

Rusul Fadhil Yaser †
Ministry of Education
Directorate of Education Baghdad
Baghdad
Iraq

Abstract

In both the open community and the military, wireless sensor networks (WSNs) demonstrate incredible promises for a variety of complex applications. Due to system assaults on the detection of energy and remote correspondence innovations, individual data without specific insurance is not reasonable for approval. Wireless Ad-Hoc Networks (WANET) additionally presents a number of security and risk concerns related to remote communication. This article explores issues and difficulties related to security in WANET-based remote sensor organizations. Survey-arranged security instruments for remote sensor networks are differentiated between security and risk in the article. Even though encryption and decoding calculations are moderately complex, information moves high (Mobility of Node) within the system. Second, a "review" idea is presented here to improve productivity in handling the security issue in WANET through consideration of remote sensor arrangements and confirmation of the server. Biometric data can be used to create a digest. To increase the reliability and availability of biometric frameworks, we demonstrate how this concept can be employed.

Subject Classification: *68P25, 68P30.*

Keywords: *Wireless ad-hoc networks (WANET); image encryption/decryption.*

* *E-mail:* **isrhussain40@gmail.com (Corrsponding Author)**
† *E-mail:* **rusulfadhil77@gmail.com**

1. Introduction

WANET has a dynamic topology and is independent, framework less, and self-sorting out. Messages are transmitted via a shared, error-prone radio guide. There are a lot of ways to crack WANET since hubs are portable. WANET hubs serve as both hosts and switches, they should also be equipped with transceivers. Additionally, ad-hoc systems must have a battery life and a preparing power. The exercises of nodes are not facilitated with the help of focal controllers in portable systems[1][2].

1.1 *Information Networks for the Military*

It has become necessary to have solid and predictable correspondence in various fields of the modern computerized military. It is common practice to send gadgets to move military vehicles, tanks, and trucks, which jot down data haphazardly [3].

1.2 *An Integrated Sensor System with a Network*

A sensor system is one of the uses of WANET. Sensors in its system detect a particular approaching sign and are sent to a fitting goal hub through a network of hubs [4].

1.1.1 Applications in the Automotive Industry

At present, many studies are being conducted on automotive systems. Traffic lights should frame specially appointed systems that allow vehicles to communicate with one another and with each other[5]. As a result of this system, drivers will have access to data regarding pavement conditions, clogs, and mishaps in front of the transfer stream which will help them upgrade the process [6].

1.1.2 Services Provided by Emergency Services

There are often ad hoc systems established for salvaging after floods, earthquakes, and other calamities. Lately, security has assumed a significant role in unfriendly remote special appointed conditions to ensure secure correspondence. Security exhibitions in remote, specially appointed settings are difficult to stage due to their characteristic vulnerabilities[7]. A noxious hub in WANET can attack all directions and target any hub at any time, unlike a restless system. Attacks can either be latent or detached, such as data disclosure, commandeering assemblies, revocations, hub pantomimes, and many more. WANET actually requires

every hub to trust its neighbor hub for communication, as trust support is built into the directing conventions [8]. It implies that WANET has a clear resistance process. It follows that hubs with insufficient physical security are vulnerable to catching, trading off, and commandeering because they are all self-governing units and go anywhere. Whenever WANET hubs are large, tracking traded-off or harmful hubs becomes difficult. It is essential that special arrangements for remote systems meet the following requirements: Confidentiality ensures the goal hub can comprehend the information. Even if the gatecrasher finds valuable data within the information being sent, he should not have an option of inferring it from it[9]. A person's honesty ensures that their information is undisturbed and undamaged. Confirmation provides assurance of the personality hub. In order for a system to remain accessible, it must always be operational. As long as neither the sender nor the collector denies support, there is no denial of support[10].

2. Literature Related Works

Data security upgrades over the past few years have shown numerous difficulties and limitations. Researchers can also use the literature survey to gain a deeper understanding of key management issues in a network and improve their research in this field as a result [11]. In their work, Wange et al., Cheing et al., Chadded et al., Hsaio et al., and Xaing et al. suggest several useful strategies for using real-time steganography. In an effort to prevent interceptors from accessing important data, a method was discussed for embedding it into the host image. Further, it improved the stego-image quality while increasing embedding capacity. Moreover, steganography and watermarking, as well as cryptography, were compared [12,13,14,15,16,17].

By Po-Hsain and Lakshmei et al., analyzed a reversible image-sharing scheme with real-time signal processing applications. The scheme was found to have a higher embedding capacity and computational efficiency in comparison to other methods. A number of researchers have discussed steganography techniques for text and image security, including Ratan et al., Zhung et al., Qien et al., and Abdullah et al. Capacity issues were resolved and image quality improved. By choosing the best secret key, we were able to embed the stego-image faster, improving the quality of the result. There are several types of algorithms, schemes of lightweight encryption, attacks, Encryption of images, encryption of chaotic, policies of key management, issues of key escrow, multiple and dynamic keys, key

distribution, encryption, schedule, and schemes of exchange, as well as node failures and dynamic path allocations that are examined in these studies [18-21]

3. Analyzing Informative Biometrics System

Data can be used to validate a person's character through biometrics, an increasingly popular technique for recognizing extraordinary human qualities. The application of biometrics entails analyzing physical attributes, such as fingerprints and retinal images, as well as home attributes. Biometric systems offer some potential solutions for WANET validation since they require minimal involvement from the client and are closest to the client's personality[20]. If a hub catch is possible in antagonistic conditions, it is imperative for strategic WANET to monitor the nearness of credible clients on a regular basis. There are advantages and disadvantages to every biometric method. A biometrically compromised system is also permanently lost for any app that utilizes it, so it may need to be re-encrypted for each new application[18].

4. Proposed Concealing Information Technique

Prospects for Senders: A Proposal

1. The first image of a recording position has 24 bits per pixel in the raw image file and text file. Due to its low computational complexity, it is typically associated with small images with 24×24 pixels and gigantic images with 512×512 pixels.
2. R-G-B levels can be encoded in this procedure as well as dim-level images. Once the image document has been selected, the content record containing mystery data is selected.
3. An anonymous variable key, stego-key, is used to share the sender and beneficiary information. If the key is substantial, only the beneficiary is capable of unlocking the image and recovering mystery information.
4. Alterations and patching of exchange components are proposed for the encoding of data and stego-key images.

Distribution of Stego-keys and pre-processing of biometrics:

To encrypt data in this model, the receiver's retina-based cryptographic key is used. Users must distribute the key before a transaction can be carried out. A retina sensor is used to acquire and preprocess retinal images.

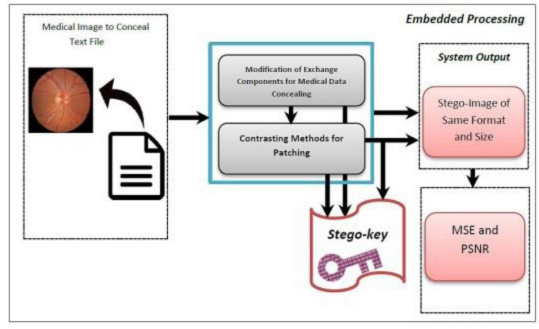

Figure 1

Illustrates How Steganography Performs from the Sender Perspective

A mystery communication and a mystery content document must be concealed inside the image record in Figure 1 by installing an image file. Stego-images contain mystery information. Next, select the stego-key encoding. Embedding involves replacing pixels with keys and mystery communication in the Exchange segment modification system to hide information. The principal part of the first pixel was filled with a double structure when the key became paired. Within the first half of the next pixel, the message is transformed into a double structure, and within the second half, it takes on a twofold structure. Differentiating the stego-image fixing process increases security. A PSNR and MSE check will be conducted for stego-images from the same organization and size for over-live procedures as shown in Figure 2.

1. Sentries send stego-images to clients and beneficiaries so they can get a sense of their authenticity. A stego-image is interpreted using mystery information by real clients using stego-keys.
2. Stego-images can only be decoded by a real client holding the equivalent transmit key that the beneficiary has accepted as stego-key.
3. By patching projected exchange modules, an algorithm for extracting stego-images can be developed.

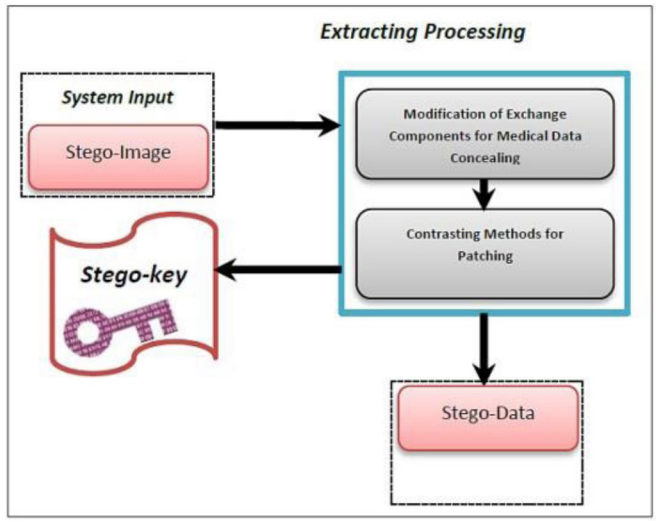

Figure 2

Projections using the Steganography technique used by the Image Security Receiver

A stego-image is sent by the dispatcher to the beneficiary or genuine client by using the Steganography Technique for collecting. Stego-keys are required to access mystery information contained in stego-images owned by genuine clients. In order to be authentic, a similar key must be inserted into the authentic client, which is represented by the image. Patching procedures and exchange alteration systems are utilized in the stego-image-extracting process. Finally, we have access to the secret data implanted in our system.

Stages for implementing steganography algorithms

Stage 1: Messages are indicated in an image using the key associated with the message, which forms the basis of security.

Stage 2: There are r pixels in every image.

Stage 3: A frame is created by taking the first pixel, then the second, then the third, etc.

Stage 4: From these assembled pixels, mutual images are framed and scrambled with neighborhood keys and passed on to the next hub.

Stage 5: The middle of the road hubs unscramble the image and decode it with the shared neighborhood key with the following hub and pass it on.

Stage 6: Unscrambling the image with a neighborhood key and a message explicit key returns the common image to the goal hub.

Stage 7: Each common image is repeated, and afterwards the first messages are revised back using the list numbers.

5. Findings Based on Experiment

In this sense, it would be appropriate to calculate the restriction to anchor hubs, in light of the fact that they know their locations, but not their areas. In contrast to anchor hubs, which know their locations, they do not know their areas, so it is necessary to calculate restrictions based on this information. Performing large complex gatherings in the system is quite a bit difficult, resulting in increasingly entangled tasks as shown in Table 1. Due to its unique generator, this framework is powerful enough to resist numerous attacks, making it faster. Our proposed biometric cryptosystem is explained below.

Table 1

Biometric Computational Time Accuracy (ms) in the WANET

Protocols	Registering	Logging + Authenticating	Calculating	Time of Accuracy (ms)
An 8K High-Resolution	4TH	13TH	16TH	50.176ms
An Optical Zoom (Zoom:15x)	5TH	10TH+4tsym	12TH + 6tsys = 16TH	57.58ms
An 4K High-Resolution	3TH	8TH + 4TMAC + 6RC5	10TH + 4TMAC + 6RC5	38.42ms
Precision	8TH	19TH	26TH	80.89ms
An Optical Zoom (Zoom:30x	8TH	17TH	23TH	80.48ms
HD Low-Resolution	3TH	9TH+4Trc5	11TH+4Trc5	37.31ms

6. Conclusion

Several methods utilizing biometrics and cryptography, or interruption recognition frameworks, are presented that offer a more secure alternative than correspondence over the system. These models are fairly powerful and able to connect with the real environment, they are not as efficient and vigorous as they should be. In order for face prints to be coordinated and gathered, fingerprints must be produced. In some regions, acknowledgment is given for verifying and maintaining biometric records and enrolling in secure steering by means of identification. Despite state-of-the-art review information, studying interruption locations is still necessary to plan efficient cryptographic calculations.

References

[1] D. Hu, L. Wang, W. Jiang, S. Zheng, B. Li, A novel image steganography method via

[2] deep convolutional generative adversarial networks, IEEE Access 6, 38303–38314 (2018).

[3] Y. Ke, M.-q. Zhang, J. Liu, T.-t. Su, X.-y. Yang, Generative steganography with Kerckhoffs' principle, *Multimed. Tool. Appl*. 78 (10), 13805–13818 (2019).

[4] W. Tang, B. Li, S. Tan, M. Barni, J. Huang, CNN-based adversarial embedding for image steganography, IEEE Trans. Inf. Forensics Secur. 14 (8), 2074–2087 (2019).

[5] Z. Wang, N. Gao, X. Wang, X. Qu, L. Li, SSteGAN: self-learning steganography based on generative adversarial networks, in: International Conference on Neural Information Processing, Springer, pp. 253–264 (2018).

[6] J. Yang, K. Liu, X. Kang, E.K. Wong, Y.-Q. Shi, Spatial Image Steganography Based on Generative Adversarial Network (2018), arXiv preprint arXiv:1804.07939.

[7] C. Yu, Attention based data hiding with generative adversarial networks, Proc. AAAI Conf. Artif. Intell. 34, 1120–1128 (2020).

[8] D. Volkhonskiy, B. Borisenko, E. Burnaev, Steganographic generative adversarial networks, vol. abs/1703.05502, CoRR (2017) [Online]. Available, http://arxiv.org/abs/1703.05502 .

[9] W. Tang, S. Tan, B. Li, J. Huang, 'Automatic steganographic distortion learning using a generative adversarial network, IEEE Signal Process. Lett. 24 (10), 1547–1551, Oct (2017).

[10] I.J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio, Generative adversarial networks, Adv. *Neural Inf. Process. Syst*. 3, 2672–2680 (2014).

[11] E. Agustsson, R. Timofte, NTIRE 2017 challenge on single image super-resolution: dataset and study, in: 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 1122–1131. Honolulu, USA (2017).

[12] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Image hiding by optimal LSB substitution and genetic algorithm, *Pattern Recognit.* 34, 671–683 (2001), doi:10.1016/S0031-3203(00)00015-7.

[13] Chin-Chen Chang, Chi-Shiang Chan, Yi-Hsuan Fan, Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels, *Pattern Recognit.* 39, 1155–1167 (2006), doi:10.1016/j.patcog.2005.12.011.

[14] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, A secure and improved self-embedding algorithm to combat digital document forgery, *Signal Process.* 89, 2324–2332 (2009), doi:10.1016/j.sigpro.2009.02.001.

[15] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, Digital image steganography: survey and analysis of current methods *Signal Processing.* 90, 727–752 (2010). 10.1016/j.sigpro.2009.08.010.

[16] Ju-Yuan Hsiao, Chieh-Tse Chang, An adaptive steganographic method based on the measurement of just noticeable distortion profile, *Image Vis. Comput.* 29, 155–166 (2011), doi:10.1016/j.imavis.2010.08.010.

[17] Lingyun Xiang, Wenshuai Wu, Xu Li, Chunfang Yang, A linguistic steganography based on word indexing compression and candidate

selection, *Multimed. Tools Appl.* 77, 28969–28989 (2018), doi:10.1007/s11042-018-6072-8.

[18] S.A. Parah, J.A. Sheikh, A.M. Hafiz, G.M. Bhat, A secure and robust information hiding technique for covert communication, *Int. J. Electron*. 102, 1253– 1266 (2015), doi:10.1080/00207217.2014.954635.

[19] Sara Sajasi, Amir-Masoud Eftekhari Moghadam, An adaptive image steganographic scheme based on Noise Visibility Function and an optimal chaotic based encryption method, *Appl. Soft Comput.* 30, 375–389 (2015), doi:10.1016/j.asoc.2015.01.032.

[20] Jen-Chun Chang, Yi-Zhi Lu, Hsin-Lung Wu, A separable reversible data hiding scheme for encrypted JPEG bitstreams, *Signal Process*. 133, 135–143 (2017), doi:10.1016/j.sigpro.2016.11.003.

[21] Azmi Shawkat Abdulbaqi, Ahmed J. Obaid & Maysaa Hameed Abdulameer. Smartphone-based ECG signals encryption for transmission and analyzing via IoMTs, *Journal of Discrete Mathematical Sciences and Cryptography* (2021), DOI: 10.1080/09720529.2021.1958996.

Received September 2023