SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

TRACK-S-IT: Multiobject Tracking-based Steganography for Securing IoMT Data

Sahar Magdy[1], Sherin Youssef[2,*], Karma M. Fathalla[2]

[1] Department of Computer Engineering, Pharos University, Alexandria Governate 21648, Egypt
[2] Department of Computer Engineering, Arab Academy for Science and Technology, Alexandria Governate 5422020, Egypt

ARTICLE INFO

Article history:
Received 20 December 2023
Received in revised form 9 May 2024
Accepted 6 June 2024
Available online 10 July 204

Keywords:

Steganography; security; IoMT; deep learning; tracking MOT; AES; least significant bit

ABSTRACT

Internet of Medical Things (IoMT) facilitates medical services including real-time diagnosis, remote patient monitoring, and real-time medicine prescriptions. IoMT incorporates Internet of Things in medical systems. However, IoMT devices are often built with no security in mind, which make them susceptible to various attacks, such as data theft, manipulation, and denial of service. Therefore, security and privacy are essential for the wider adoption and trust of IoMT. In this paper, a video tracking- based CryptoStegno model is proposed to secure private and medical records in an IoMT environment. Private information protection is made possible through crypto-steganography. An added layer of protection is guaranteed through video tracking technology, where data is embedded at multiple tracked objects. In addition, video steganography handles the issue of embedding capacity via utilizing multiple frames. Thus, this paper proposes a novel CryptoStegno model for embedding medical and private data based on video Steganography. Also, AES cryptography is used to encrypt the data before the embedding process to provide a high level of security. Hence, the proposed approach provides robustness and security to the data. On a variety of video sequences, the proposed scheme is examined using different metrics to ensure the robustness of the model such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Structural Similarity (SSIM) Index, and Bit Error Rate (BER). In terms of PSNR, an improvement of around 2% of was achieved compared to the state of the art, while 5% and 9% improvements were achieved in terms of SSIM and RMSE, respectively.

1. Introduction

Internet of Things (IoT), Machine Learning (ML), and Artificial Intelligence (AI) are examples of advanced technology that have been widely recognized and acknowledged as possible remedies to ease the strain on the healthcare system [1]. The emergence of these technologies encouraged the adoption of Health 4.0 in the healthcare industry. Internet of Medical Things (IoMT), enables medical events like real-time diagnosis, tracking patients remotely, and medication prescriptions in real-time because of the integration of the Internet of Things in medical systems [2,3].

* *Corresponding author.*
E-mail address: sherin@aast.edu

https://doi.org/10.37934/araset.48.1.227239

IoMT's major objective is to interconnect Cloud computing, Artificial Intelligence, visual sensors, and Wearable devices, collecting data such as prescription history, diagnostic notes, test results, treatment plans, pharmacy refill requests, invoicing information, insurance claims about patients, personal and payment information [4].

As a result, medical records have made their way online, opening them to security leaks, and can be 50 times more lucrative than financial data for thieves. Intruders can alter the discourses of a variety of medical inventions, which poses a severe threat to the lives of patients [5,6]. The management of IoT devices, more particularly (IoMT), allows hackers to use botnets to steal patient information. Therefore, it is essential that medical data are secured [7].

Leon Medical Centres published a detailed list of the stolen information, which included social security numbers, financial and insurance information, etc. Hackers will submit their data to the deep web in order to get counterfeit passports, ID cards, and social security cards. Buyers may use the data to make fraudulent IDs, buy pharmaceuticals or medical supplies, or submit bogus insurance claims. It can also be marketed to persons without insurance who would use it to buy cheap prescription medications or medical supplies. Additionally, using a fake provider number along with a patient identification number, the uninsured could submit false insurance claims. A patient's personal medical record could no longer be accurate, which is another risk. If vital details like blood type and medicine allergies are changed in the patient's record, it might be fatal [8].

In Addition, Medibank (one of the biggest Australian private health insurance providers) would pay $1 billion in compensation in November 2022 as hackers targeting the business released the largest batch of sensitive data yet in an effort to force it to pay a ransom. The damaging cyberattack that has impacted 10 million customers including 1.8 million international customers. Moreover, 700 patients' records were revealed in a week that included mental health issues, terminating pregnancies, and drug and alcohol use which has been called Australia's most intrusive cybercrime [9]. Thus, it is essential to safeguard sensitive data against invasions and unauthorised access so Steganography techniques are used to obscure confidential data across diverse data transmission channels [10-12].

In this research, a secure crypto-steganography technique is introduced. Nowadays, every public place contains CCTV (Closed Circuit Television) cameras used to monitor large areas to ensure the safety of the public, collect image data, and provide an in-depth description of the activities that were captured. The large number of frames captured by the sensing network makes it ideal for data hiding without affecting the original frames. Not only the videos captured by the CCTV will ensure the safety of the public, but also, they will be used to ensure the safety of the private data of the patients.

This research is divided into: Section 2 illustrates the proposed model, while Section 3 shows the evaluation results and the experiments made to ensure the efficiency of the proposed model. Finally, Section 4 concludes and discusses the results.

2. Methodology

The proposed model is divided into three main parts as shown in Figure 1 Tracking Moving Pedestrian, encrypting the important medical records into the moving Pedestrians being tracked using a robust efficient technique so the records won't get cracked or damaged, and finally decrypting and extracting the records when needed.

2.1 Tracking Moving Pedestrian

Visual detecting and tracking techniques are now widely used in a variety of application situations. Complicated algorithm models have been created and used in visual tracking techniques thanks to the quick growth of high-performance computing technology. The precision of visual tracking has improved as more valuable data from real-world situations has been gathered, and its use has become more widespread.

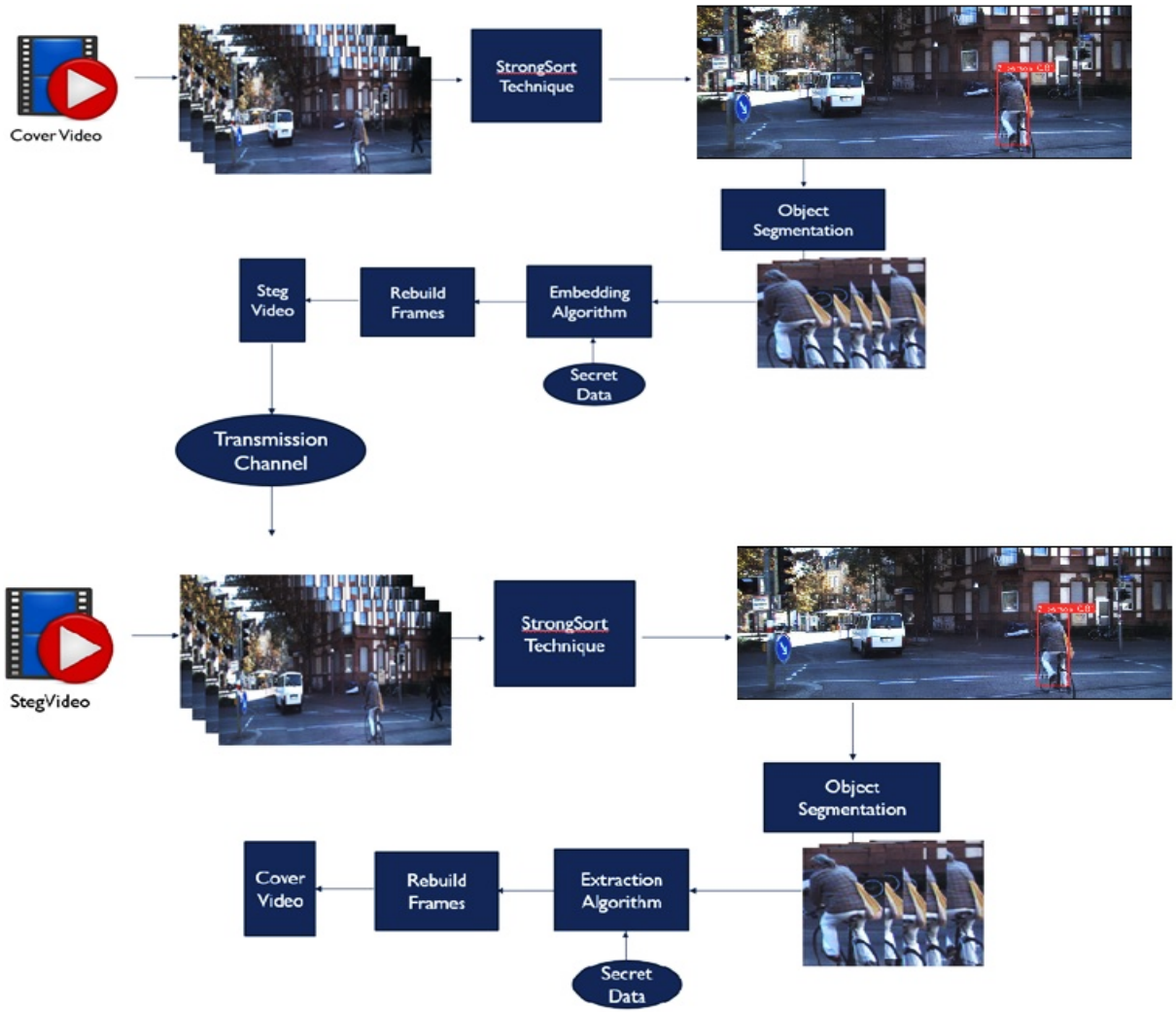

Fig. 1. Proposed model

Due to its enormous promise in a commercial application, multiple object tracking (MOT) has attracted a lot of interest. Given a video sequence, it attempts to forecast numerous pedestrian paths while maintaining their identities. Tracking-by-Detection (TBD) based algorithms have seen great success over the past ten years thanks to improvements in foot recognition algorithms.

In the proposed model, StrongSort technique [13] is utilized. StrongSort was implemented using DeepSort [14] which is the earliest techniques for using the deep learning model for the MOT challenge. It is asserted that DeepSORT's performance shortcomings are caused more by its antiquated methods than by its tracking methodology, so after merely adding advanced components to DeepSort in different areas, resulting in the suggested StrongSort.

The key advantage of the StrongSort algorithm is its ability to handle complex scenarios with multiple moving objects. It can track objects that move at different speeds, change directions abruptly, or interact with each other. Moreover, it can adapt to changing conditions such as lighting changes, camera jitter, or partial occlusions without losing track of the objects. Overall, the StrongSort tracking algorithm has proven to be an efficient and reliable method for object tracking in real-world applications.

2.2 Encryption of Medical Records

After tracking multiple objects, objects were extracted from the frames as shown in Figure 2.

Fig. 2. Cropping the moving objects from each frame

The medical records will be embedded in the moving objects' frames, and since there are multiple frames, then a remarkable amount of data could be hidden without damaging the original frame. Moreover, the part that contains the hidden data will change its place along the frames which makes it even harder to get captured.

As shown in Figure 3, The embedding algorithm is divided into two steps to ensure the security of the records which are encrypting the data to ensure its security then embedding the data into the frames of the tracked objects.

2.2.1 The AES encryption algorithm (advanced encryption standard algorithm)

The Advanced Encryption Standard (AES) is a widely adopted encryption technique used to secure sensitive data in various systems [15]. It was developed as a replacement for the outdated Data Encryption Standard (DES) and has become the standard encryption method for securing data both at rest and in transit. AES uses symmetric-key for cryptography, meaning that both the recipient and sender use the same key to encrypt and decrypt messages.

Cryptography techniques can't be used alone though or it will grab the attention of the attackers, whom will be tempted to alter the data to get any info about the secret encrypted data, eventually destroying the protected data. Cryptography techniques protect the contents of the secret data but not the existence of the data transmitted.

2.2.2 Least significant bit (LSB) steganography

Least significant bit (LSB) steganography is a technique of hiding information within the least significant bits of digital media like images, audio, or video files [16]. In this method, the original data remains intact while additional hidden data is added to it. The LSB steganographic algorithm replaces

the least significant bit of each pixel in an image with a binary code from a secret message. As the changes are made only to the least significant bit, they are almost imperceptible to human eyes and do not affect the quality of the image.

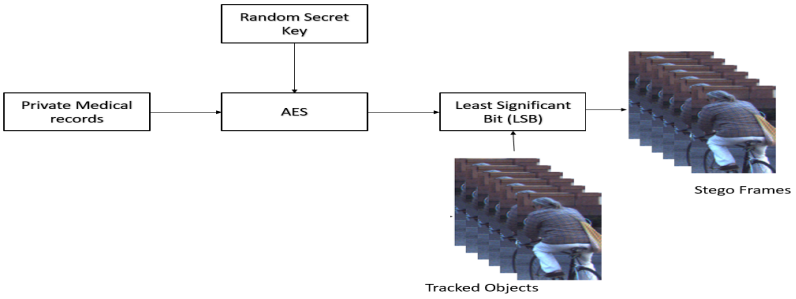

Fig. 3. Embedding Proposed Model

After the data is encrypted inside the cropped frames of the tracked object, the stego frames are rebuilt to output the stego video file only to be transmitted and saved on the IoMT cloud.

2.3 Decryption of Medical Records

As show in Figure 4, to Extract the Medical Records from the saved videos, StrongSort is used to extract the moving objects and crop them out of the frame before the extraction phase.

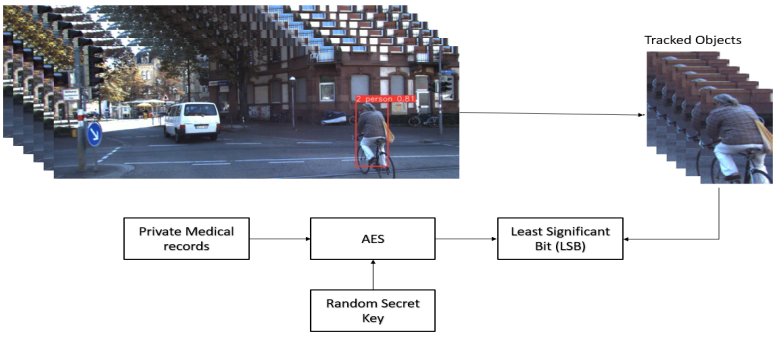

Fig. 4. Extraction proposed model

3. Evaluation and Tests

3.1 Datasets

Kitti Dataset is used in this experiment which contains 21 training sequences and 29 test sequences. It's mainly used to test tracking but is used to embed hidden secret data in it due to its small size so it won't add complexity to the model [17].

Change Detection Dataset is also used in this experiment to ensure the validity of the model. It consists of two datasets, 2012Dataset and 2014Dataset that contains several video categories with 4 to 6 each [18].

3.2 Tracking Performance

The strength of the tracking algorithm is vital in the proposed model, so the chosen tracking algorithm was evaluated on multiple datasets to ensure its robustness in different settings. According

to the results, StrongSort was proved to be the most dependable tracking technique, not only to track multiple pedestrians but also tracking multiple objects such as cars, bicycle…etc.

i. Multiple Object Tracking Accuracy(MOTA): This metric is used to compute the accuracy for the tracker part and the detection part of the tracking algorithm as shown in Eq. (1).

$$MOTA = 1 - \sum_t \frac{FN+FP+IDS}{GT} \quad (1)$$

where, FN (False Negatives) The frames that were marked as absent even though their presence. FP (False Positives) the objects that were tracked and detected despite their absence in the frame. IDS is the number of ID switches and GT is right number of ground truth objects in the image.

ii. Multiple Object Tracking Precision (MOTP): Since MOTA doesn't measure the localization of the moving objects, MOTP is used to calculate the precision of the detection as shown in Eq. (2). it's similar to mAP metrics. TP (True Positive) which refers to the objects tracked and detected correctly and S is the number of frames.

$$MOTP = \frac{1}{|TP|}\sum_{TP} S \quad (2)$$

iii. Identification Metrics (IDF1): This metrics focus more on the capability of the algorithm to accurately associate same objects together. It combines the IDP (ID Precision) and the IDR (ID recall) as shown in Eq. (3).

$$IDF1 = \frac{|IDTP|}{|IDTP|+0.5|IDFN|+0.5|IDFP|} \quad (3)$$

iv. Higher Order Tracking Accuracy (HOTA): This metric is the interconnection of detection and association IOU scores as shown in Eq. (4).

$$\text{HOT } A = \sqrt{\text{Det } A * AssA} \quad (4)$$

where DetA is the detection accuracy while the AssA is the association IOU.

StrongSort achieved the highest scores when evaluated on MOT16 [19], which contained 14 complex video sequences which are illustrated in Table 1.

Table 1
Evaluation of StrongSort on MOT16 compared to previous research

Tracking Techniques	MOTA	HOTA	MOTP	IDF1
Yongjie Xue *et al.,* [20]	61.30%	-	79.04%	-
Deepsort [14]	61.40%	-	79.01%	-
FairMot [21]	74.90%	-	-	72.08%
StrongSort [13]	78.50%	63.50%	88.02%	79.50%

Moreover, StrongSort achieved high scores as well on both MOT17 [22] and MOT20 [23] benchmark datasets as shown in Table 2 and Table 3 respectively. MOT17 contained the same 14 complex video sequences in MOT16 but with a new, more accurate ground truth. However, MOT20 benchmark contains eight challenging and complex video sequences.

Table 2
Evaluation of StrongSort on MOT17 compared to previous research

Tracking Techniques	MOTA	HOTA	IDF1
CenterTrack [24]	66.90%	57.60%	68.40%
TransTrack [25]	69.60%	59.40%	69.90%
FairMot [21]	73.70%	-	72.30%
StrongSort [13]	78.70%	70.70%	83.30%

Table 3
Evaluation of StrongSort on MOT20 compared to previous research

Tracking Techniques	MOTA	HOTA	IDF1
FairMot [21]	61.80%	57.10%	67.30%
StrongSort [13]	71.80%	61.50%	75.90%

StrongSort was also evaluated on KITTI Dataset as shown in Table 4. KITTI Dataset consists of 21 videos with 8 different classes, but the evaluation is only applied on the Pedestrian and Car classes only.

Table 4
Evaluation of StrongSort on KITTI Dataset compared to previous research

Tracking Techniques	MOTA	HOTA	IDF1
OC Sort [26]	65.10%	54.30%	85.71%
StrongSort [13]	67.37%	56.20%	89.20%

3.2 Video Quality Evaluation Metrics

Any steganography method must fulfil essential conditions for effective communication: imperceptibility and capacity. Imperceptibility refers to the visual quality of the hidden object and its minimal distortion. Capacity is determined by the amount of secret data that can be embedded without any visible changes. Robustness measures the strength of the hidden object against external attacks such as noise or compression.

While researchers have attempted to focus on these requirements separately, no technique has been developed that can balance all three parameters effectively. The primary goal of steganography is to ensure secure and obscure transmission of confidential information through a common channel without arousing suspicion. To achieve successful covert communication, high-quality stego-objects with minimal alterations should be produced, ensuring low detection rates for attackers and steganalysis.

3.2.1 Imperceptibility

Imperceptibility is calculated using MSE (Mean Square Error) Eq. (5), Peak Signal to Noise Ratio(PSNR) Eq. (6), and Structural Similarity (SSIM) Eq. (7).

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(x_{ij} - y_{ij}\right)^2 \quad (5)$$

$$\mathrm{PSNR}(x,y) = \frac{10\log_{10}\left[\max\left(\max\left(x\right),\max\left(y\right)\right)\right]^2}{|x-y|^2} \quad (6)$$

$$\mathrm{SSIM}_{(}\ x,y\big) = \frac{\left(2\mu_x\mu_y+C_1\right)+\left(2\sigma_{xy}+C_2\right)}{\left(\mu_x^2+\mu_y^2+C_1\right)\left(\sigma_x^2+\sigma_y^2+C_2\right)} \quad (7)$$

Where, m and n are the number of rows in cover image and number of columns in cover image respectively, x_{ij} , y_{ij} are pixel value from cover image and pixel value from stego image. μ is the mean intensity and σ presents the variance of the cover and stego frame respectively, moreover, C1 and C2 are constants.

Table 5 and Table 6, shows the Imperceptibility evaluation metrics (MSE, RMSE, PSNR, SSIM) on each video sequence of the Kitti and Change Detection Dataset respectively on embedding 2KB of data.

Table 5
Evaluation of Imperceptibility on KITTI Dataset

Videos	PSNR	MSE	SSIM	RMSE
V1	73.17	0.0033	0.9999	0.057446
V2	72.02	0.0041	0.9996	0.064031
V3	70.48	0.0065	0.9997	0.080623
V4	73.26	0.0032	0.9999	0.056569
V5	71.55	0.0051	0.9994	0.071414
V6	71.01	0.00435	1	0.065955
V7	73.88	0.0026	0.9995	0.05099
V8	71.18	0.005	0.9999	0.070711
V9	71.47	0.0053	0.9997	0.072801
V10	70.58	0.0067	0.9993	0.081854
V11	71.78	0.0058	0.99994	0.076158
V12	71.34	0.0064	0.9999	0.08
V13	72.79	0.0048	1	0.069282
V14	71.42	0.0059	1	0.076811
V15	70.87	0.0071	0.9996	0.084261
V16	73.08	0.0039	0.9995	0.06245
V17	71.79	0.0043	0.9999	0.065574
V18	71.48	0.0049	0.9991	0.07
V19	71.72	0.0054	0.99998	0.073485
V20	70.29	0.0068	0.99993	0.082462

Table 6
Evaluation of imperceptibility on change detection dataset

Videos	PSNR	MSE	SSIM	RMSE
V1	73.25	0.0026	1	0.05099
V2	71.78	0.0048	0.9995	0.069282
V3	70.57	0.0051	0.9999	0.071414
V4	71.95	0.0059	0.9997	0.076811
V5	72.48	0.0038	0.9993	0.061644
V6	71.99	0.006	0.9999	0.07746
V7	70.58	0.0043	0.9996	0.065574
V8	71.23	0.0043	0.9995	0.065574
V9	70.47	0.0032	0.9992	0.056569
V10	72.29	0.0034	1	0.05831
V11	70.51	0.0069	0.9994	0.083066
V12	70.91	0.0078	0.9998	0.088318
V13	72.74	0.0028	0.9994	0.052915
V14	71.29	0.0057	0.9997	0.075498

3.2.2 Hiding capacity

Hiding Capacity shows the largest quantity of secret data that can be embedded in the video without being noticed. the proposed model is capable of embedding large numbers of data since a small video size contains large numbers of frames so the data is divided on all the frames. Moreover, the larger number of objects being tracked, the more hiding space inside one frame. In Table 7, the video number and the frame are the same but the size of the embedding data varied.

As shown in Table 7, the hiding capacity reached 16KB in only one frame without causing distortion to the frame which can be shown in histogram analysis.

Table 7
Evaluation of Hiding Capacity on one frame of the first video of Kitti Dataset

Videos	Capacity	MSE	RMSE	PSNR	SSIM
V1	2K	0.0053	0.072801	72.87	0.9999
V1	4K	0.0059	0.076811	72.05	0.9999
V1	8K	0.0062	0.07874	71.95	0.9999
V1	16K	0.0067	0.081854	71.84	0.9996

Figure 5 shows the histogram of the tracked object in the original frame without embedding data compared to the histogram of the tracked object after embedding 2KB, 4KB, 8KB and 16 KB of data in only one frame respectively. As shown from the histograms, there aren’t any differences between the histograms graphs especially after increasing the capacity of the embedded message.

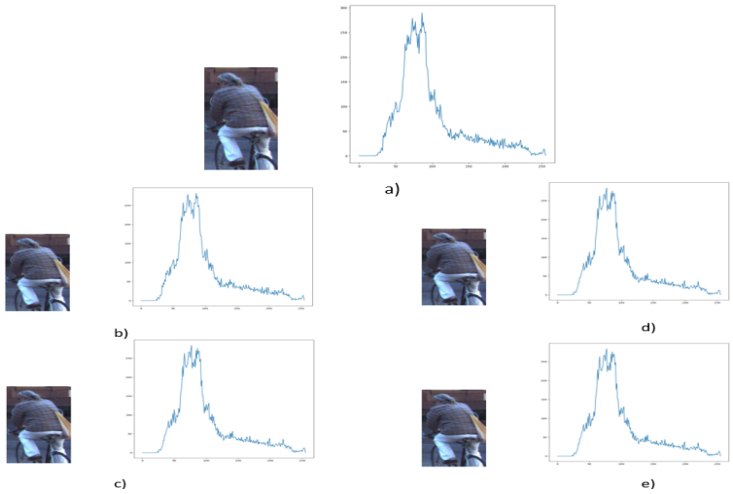

Fig. 5. a) Histogram of the tracked object without embedding data & the Histogram of the tracked object with: b) 2KB of embedded data, c) 4KB of embedded data, d) 8KB of embedded data, e) 16KB of embedded data

Moreover, Figure 6 shows the reconstruction of the frame and the histogram of the original full frame compared to the histogram of the full frame after embedding 2KB, 4KB , 8KB and 16KB of data. The histogram displays no visible differences between the original frame and the stego frame making it hard for the attacker to notice.

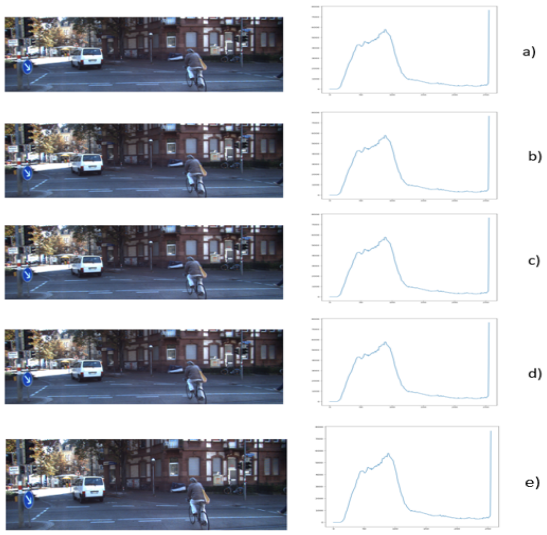

Fig. 6. a) Histogram of the full frame without embedding data & Histogram of the full frame with: b) 2KB of embedded data, c) 4KB of embedded data, d) 8KB of embedded data, e) 16KB of embedded data

Table 8, compared our proposed technique with previous techniques [27,28]. Our proposed Model achieved 71.358 db in PSNR and average of 0.00435, 0.999738 in MSE and SSIM respectively when embedding 1000 characters. Songul *et al.,* [27] used Genetic Algorithm and LSB to embed medical records into DICOM Images achieving around 66 db PSNR and 0.01 in terms of MSE

embedding 1000 characters as well, while Mostafa A. *et al.,* [28] used DES to encrypt the data into the wavelet frequency domain achieving higher PSNR reaching 70 db. The proposed Model achieved 2% improvement in PSNR terms, moreover, 5% and 9 % improvement in terms of SSIM and RMSE Respectively surpassing the previous state of arts.

Table 8
Evaluation of hiding 1000 characters compared to previous state of art

State of Art	PSNR	MSE	SSIM	RMSE
Karakus and Avci's [27]	66.4055	0.01488	0.15408	0.12198
M.A. Ahmad *et al.,* [28]	70.9528	0.00526	0.95372	0.07254
Proposed Model	72.368	0.00435	0.999738	0.06595

4. Conclusions

IoMT and security are two important topics that are closely related. The security of medical records is very important in IoMT because medical records contain sensitive and personal information about patients, such as their health conditions, diagnoses, treatments, prescriptions, and test results. If these records are compromised by hackers, they can cause serious consequences, such as Privacy violations, Identity theft, and Data manipulation, Therefore, it is essential to protect the medical records in IoMT from unauthorized access and tampering. To ensure the safety of medical records, this paper proposed a CryptoStegno model based on video Steganography. Rather than embedding data throughout the whole frame, the StrongSort technique was used to track multiple objects in each frame providing a high capacity for embedding large amounts of data without causing noise or noticeable disturbance to the original frame. AES steganography technique was also used to provide high security to the embedded medical data. High imperceptibility was achieved with an average PSNR of 68.7 dB for the considered video dataset. Moreover, the proposed model was also tested on embedding multiple data sizes such as 2KB, 4KB, and 8KB to ensure its capability to hide a large capacity of data. The performance of the model was tested by objective metrics as well as subjective metrics such as Histogram analysis. A Frame could carry up to 16KB of data without showing any distortion in the histogram values compared to the original frame which makes our model special in imperceptibility and hiding capacity metrics.

Acknowledgement
This research was not funded by any grant.

References
[1] Ashfaq, Zarlish, Abdur Rafay, Rafia Mumtaz, Syed Mohammad Hassan Zaidi, Hadia Saleem, Syed Ali Raza Zaidi, Sadaf Mumtaz, and Ayesha Haque. "A review of enabling technologies for Internet of Medical Things (IoMT) Ecosystem." *Ain Shams Engineering Journal* 13, no. 4 (2022): 101660. https://doi.org/10.1016/j.asej.2021.101660

[2] Somasundaram, R., and Mythili Thirugnanam. "Review of security challenges in healthcare internet of things." *Wireless Networks* 27, no. 8 (2021): 5503-5509. https://doi.org/10.1007/s11276-020-02340-0

[3] Parveen, R., M. Nabi, F. A. Memon, S. Zaman, and M. Ali. "A review and survey of artificial neural network in medical science." *Journal of Advanced Research in Computing and Applications* 3, no. 1 (2016): 7-16.

[4] Dwivedi, Ruby, Divya Mehrotra, and Shaleen Chandra. "Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review." *Journal of oral biology and craniofacial research* 12, no. 2 (2022): 302-318. https://doi.org/10.1016/j.jobcr.2021.11.010

[5] Hireche, Rachida, Houssem Mansouri, and Al-Sakib Khan Pathan. "Security and privacy management in Internet of Medical Things (IoMT): a synthesis." *Journal of Cybersecurity and Privacy* 2, no. 3 (2022): 640-661. https://doi.org/10.3390/jcp2030033

[6] Binbusayyis, Adel, Haya Alaskar, Thavavel Vaiyapuri, and M. J. T. J. O. S. Dinesh. "An investigation and comparison of machine learning approaches for intrusion detection in IoMT network." *The Journal of Supercomputing* 78, no. 15 (2022): 17403-17422. https://doi.org/10.1007/s11227-022-04568-3

[7] Manickam, Pandiaraj, Siva Ananth Mariappan, Sindhu Monica Murugesan, Shekhar Hansda, Ajeet Kaushik, Ravikumar Shinde, and S. P. Thipperudraswamy. "Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare." *Biosensors* 12, no. 8 (2022): 562. https://doi.org/10.3390/bios12080562

[8] NBC. "Hackers post detailed patient medical records from two hospitals to the dark web." https://www.nbcnews.com/tech/security/hackers-post-detailed-patient-medical-records-two-hospitals-dark-web-n1256887

[9] Medibank. "Cybercrime updates and support." https://www.medibank.com.au/health-insurance/info/cyber-security/timeline

[10] Utama, Sunariya, and Roshidi Din. "Performance Review of Feature-Based Method in Implementation Text Steganography Approach." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 28, no. 2 (2022): 325-333. https://doi.org/10.37934/araset.28.2.325333

[11] Devi, V. Anjana, I. Bhuvaneshwarri, C. Santhosh Kumar, V. Chandrasekar, V. Kalaichelvi, E. Anitha, and Jogendra Kumar. "Reliable and Secure Data Transfer in IoT Networks using Knight-Tour and PHLSB Method." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 32, no. 2 (2023): 107-118. https://doi.org/10.37934/araset.32.2.107118

[12] Noroozi, E., S. M. Daud, and A. Sabouhi. "A Security Enhanced Robust Image Hiding Algorithm from Digital Signature."

[13] Du, Yunhao, Zhicheng Zhao, Yang Song, Yanyun Zhao, Fei Su, Tao Gong, and Hongying Meng. "Strongsort: Make deepsort great again." *IEEE Transactions on Multimedia* (2023). https://doi.org/10.1109/TMM.2023.3240881

[14] Veeramani, Balaji, John W. Raymond, and Pritam Chanda. "DeepSort: deep convolutional networks for sorting haploid maize seeds." *BMC bioinformatics* 19 (2018): 1-9. https://doi.org/10.1186/s12859-018-2267-2

[15] Muttaqin, Khairul, and Jefril Rahmadoni. "Analysis and design of file security system AES (advanced encryption standard) cryptography based." *Journal of Applied Engineering and Technological Science (JAETS)* 1, no. 2 (2020): 113-123. https://doi.org/10.37385/jaets.v1i2.78

[16] Aslam, Muhammad Adnan, Muhammad Rashid, Farooque Azam, Muhammad Abbas, Yawar Rasheed, Saud S. Alotaibi, and Muhammad Waseem Anwar. "Image steganography using least significant bit (lsb)-a systematic literature review." In *2022 2nd International Conference on Computing and Information Technology (ICCIT)*, pp. 32-38. IEEE, 2022. https://doi.org/10.1109/ICCIT52419.2022.9711628

[17] Geiger, Andreas, Philip Lenz, Christoph Stiller, and Raquel Urtasun. "The kitti vision benchmark suite." *URL http://www. cvlibs. net/datasets/kitti* 2, no. 5 (2015): 1-13.

[18] Goyette, Nil, Pierre-Marc Jodoin, Fatih Porikli, Janusz Konrad, and Prakash Ishwar. "Changedetection. net: A new change detection benchmark dataset." In *2012 IEEE computer society conference on computer vision and pattern recognition workshops*, pp. 1-8. IEEE, 2012. https://doi.org/10.1109/CVPRW.2012.6238919

[19] Milan, Anton, Laura Leal-Taixé, Ian Reid, Stefan Roth, and Konrad Schindler. "MOT16: A benchmark for multi-object tracking." *arXiv preprint arXiv:1603.00831* (2016).

[20] Xue, Yongjie, and Zhiyong Ju. "Multiple pedestrian tracking under first-person perspective using deep neural network and social force optimization." *Optik* 240 (2021): 166981. https://doi.org/10.1016/j.ijleo.2021.166981

[21] Zhang, Yifu, Chunyu Wang, Xinggang Wang, Wenjun Zeng, and Wenyu Liu. "Fairmot: On the fairness of detection and re-identification in multiple object tracking." *International Journal of Computer Vision* 129 (2021): 3069-3087. https://doi.org/10.1007/s11263-021-01513-4

[22] Dendorfer, Patrick, Aljosa Osep, Anton Milan, Konrad Schindler, Daniel Cremers, Ian Reid, Stefan Roth, and Laura Leal-Taixé. "Motchallenge: A benchmark for single-camera multiple target tracking." *International Journal of Computer Vision* 129 (2021): 845-881. https://doi.org/10.1007/s11263-020-01393-0

[23] Dendorfer, Patrick, Hamid Rezatofighi, Anton Milan, Javen Shi, Daniel Cremers, Ian Reid, Stefan Roth, Konrad Schindler, and Laura Leal-Taixé. "Mot20: A benchmark for multi object tracking in crowded scenes." *arXiv preprint arXiv:2003.09003* (2020).

[24] Zhou, Xingyi, Vladlen Koltun, and Philipp Krähenbühl. "Tracking objects as points." In *European conference on computer vision*, pp. 474-490. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-58548-8_28

[25] Sun, Peize, Jinkun Cao, Yi Jiang, Rufeng Zhang, Enze Xie, Zehuan Yuan, Changhu Wang, and Ping Luo. "Transtrack: Multiple object tracking with transformer." *arXiv preprint arXiv:2012.15460* (2020).

[26] Cao, Jinkun, Jiangmiao Pang, Xinshuo Weng, Rawal Khirodkar, and Kris Kitani. "Observation-centric sort: Rethinking sort for robust multi-object tracking." In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 9686-9696. 2023. https://doi.org/10.1109/CVPR52729.2023.00934

[27] Karakus, Songul, and Engin Avci. "A new image steganography method with optimum pixel similarity for data hiding in medical images." *Medical hypotheses* 139 (2020): 109691. https://doi.org/10.1016/j.mehy.2020.109691

[28] Ahmad, Mostafa A., Mourad Elloumi, Ahmed H. Samak, Ali M. Al-Sharafi, Ali Alqazzaz, Monir Abdullah Kaid, and Costas Iliopoulos. "Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images." *Alexandria Engineering Journal* 61, no. 12 (2022): 10577-10592. https://doi.org/10.1016/j.aej.2022.03.056