ISO 9001:2008
Reg. No. : RQ91/3688

MUSLIM ARTS COLLEGE

THIRUVITHANCODE-629174, KANYAKUMARI DISTRICT
TAMILNADU.

National Conference on

Inter disciplinary Research through New Age Information Technology (IRNAIT-2023)

2023, February 24, Friday

Certificate

This is to certify that Prof. / Dr. / Mr. / Mrs.

Dr. P. Raajan, Associate Professor,
Muslim Arts College, Thiruvithancode.

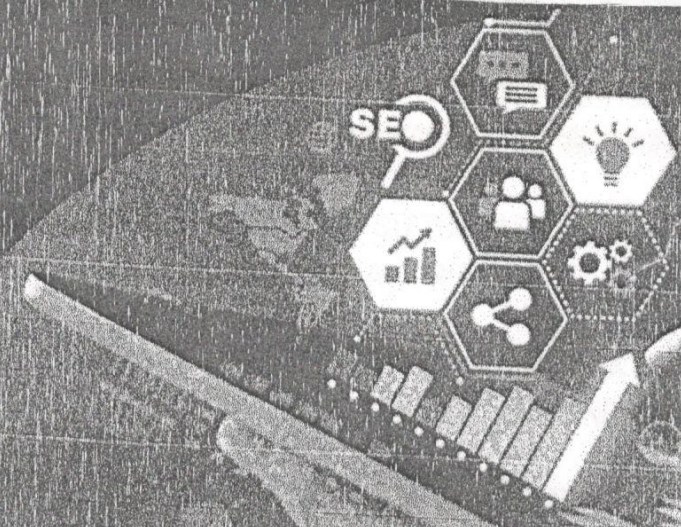
has ~~participated~~ / ~~Best paper~~ / presented a paper entitled

Tamper Detection and ECDH-DSA-FYS-Tiger Based User Authorization in Blockchain for Securing IoMT Data

in the National Conference on "Inter disciplinary Research through New Age Information Technology" held on 24th February 2023, organized by the P.G and Research Department of Computer Science, Muslim Arts College, Thiruvithancode, Kanyakumari-629174, Tamil Nadu, India.

Lion Dr H. Mohamed Ali	Dr G. Edwin Sheela	Dr. P. Raajan
Chief Patron	Patron	Organizing Secretary

Research Trends in information Technology



Dr. RAAJAN PAULRAJ

MUSLIM ARTS COLLEGE
(Affiliated to Manonmaniam Sundaranar University, Tirunelveli)
Thiruvithancode, Kanyakumari District.

Published by

Tamilsuvadi

182, First Middle Street, Thiyagaraja Nagar,
Tirunelveli-627 011.
Cell : 95979 22250.
www.booksha.in

Disclaimer:

The findings/views/opinions expressed in the book are solely those of the authors and do not necessarily reflect the views of the publisher.

Book Name	:	RESEARCH TRENDS IN INFORMATION TECHNOLOGY
Author Name	:	Dr.P Raajan
Toatal Pages	:	700
Rate	:	Rs. 1550/-
First Edition	:	2023
ISBN No	:	ISBN 978-81-962277-1-5

தமிழ்ச்சுவடி

Tamilsuvadi

182, First Middle Street, Thiyagaraja Nagar,
Tirunelveli-627 011.
Cell : 95979 22250. www.booksha.in

IRNAIT-029.
TAMPER DETECTION AND ECDH-DSA-FYS-TIGER-BASED USER AUTHORIZATION IN BLOCKCHAIN FOR SECURING IoMT DATA

Y.JANI
Reg. No.;21213092342009,
Research Scholar,
Department of computer science
Muslim Arts college, Thiruvithancode affiliated to Manonmaniam Sundaranar University,
Abishekapatti, Tirunelveli -627012, Tamil Nadu, India
E-mail: janijaanu05@gmail.com

Dr. P.RAAJAN
Associate Professor,
Department of Computer Science,
Muslim Arts College, Thiruvithancodeaffiliated to Manonmaniam Sundaranar University,
Abishekapatti,
Tirunelveli- 627012, Tamil Nadu, India
E-mail: raajanp99@gmail.com

Abstract:

IoMT is playing vital role in providing medical services instantaneously. In IoMT, sensitive data are shared via centralized service providers, which arises security concerns. Several works have been developed with blockchain to solve security issues, yet less focus was given to tamper detection in shared IoMT data. Hence, in this article, an OLES-LWT-based watermark for tamper detection is proposed. Initially,a patient login into hospital website with credential information provided during registration and booksan appointment with doctor. Online consultation happens atthe scheduled time, and the IoT-sensed image will be shared. To detect tampering inIoT Image, watermark image by fusion of hospital icon, department icon, and signature with a time stamp image is embedded in the IoTimage and stored in the cloud. Meanwhile, for user authorization,FYS-Tiger hashing and role-

based access policy with a digital signature in blockchain is introduced. On the other hand, the doctor downloads data after successful login, signature verification, and hashcode matching processes. Then,the watermark will be removed at the doctor's side for tampering detection. The performance of the proposed model is proven with better outcomes of experimental results.

Keywords: **Internet of Medical Things (IoMT), Blockchain, authorization, Watermarking, Odd-Log-Even-Scaling-based Lifting Wavelet Transform (OLES-LWT).**

1. INTRODUCTION

The advancement of IoT is projected towards transforming the medical sector as well as compel the growth of IoMT(Ogundokun et al., 2021).IoMT is an assortment of health care systems to provide secure transmission of health-related data between smart devices, which help remotely located doctors, and healthcare-providers, to collect and analyze health data electronically(Garg et al., 2020). Although IoMT provides more services, it is also equally important to protect patient's data that is generated from various healthcare systems(Quasim et al., 2020) as healthcare data requires a high-level of security and privacy(Tanwar et al., 2020). To solve security and privacy issues, symmetric and asymmetric cryptographic techniques were developed(Ghubaish et al., 2021). Still, cryptographic techniques failed to give security to patients' data due to exploitation of public key parameters. One possible solution to solve this issue relies on Blockchain technology-based authentication of users.

Blockchain technology is a tamper-proof digital ledger with secure Peer-to-Peer communication feature(Bhattacharjya et al., 2022). Blockchain is extremely secure as it is immune to modification of data. One of the most important properties of blockchain is that it is a distributed ledger(Swetha et al., 2020). Also, blockchain is a decentralized technology that solves setbacks of centralized architectures' such as network users do not clearly view how the information they generated will be used(Bataineh et al., 2022). More research was developed based on blockchain technology to preserve privacy of patient's data. However, these schemes often use interplanetary file system, which relies on Hash Table for data storage and sharing, leading to high data retrieval latency(Nguyen et al., 2021). Moreover, various Attribute-based authentication techniques were developed to create access policies in block chain. Although various authentication mechanisms have been developed to protect patients' data, most of them are cost-ineffective, or face scalability issues(Fotopoulos et al., 2020). Also, less importance was given to detection of tampering in received patients' data. Hence, to solve these problems, an OLES-LWT watermarked image-based IoMT-data tamper detection is proposed in this research.

1.1 Problem definition

The securing of healthcare data with existing works in IoMT environment has certain limitations such as,

- In existing works, no importance was given to prevent malicious modifications to the shared medical image.
- In existing system, confidentiality is low in distributed healthcare networks.
- In existing system, attribute-based access policy relied on centralized authorities which caused privacy issues.

By considering the above problems, the contributions of proposed model are,

- The OLES-LWT watermark image-based tamper detection is proposed to detect the modifications on shared IoT images.
- To solve confidentiality and privacy problems, the ECDH-DSA with FYS-Tiger-based user authorization in blockchain is introduced.

The rest of this article is organized as follows; Section 2 describes related works of proposed model. Section 3 describes proposed methodologies. Section 5 discusses experimental results. Section 5 concludes the paper.

2. RELATED WORKS

(Nishi et al., 2022)presented a framework for electronic healthcare data security with blockchain and smart contracts. The presented framework utilized Etherium network to store patient data. The framework revealed that the developed system facilitated secure transfer of patient medical records. However, Ethereumneededmore resources, which create scalability issues in IoMT.

(Abbas et al., 2021)suggested a Blockchain-assisted Secure Data Management Framework (BSDMF) for health information on IoMT. In BSDMF, blockchain guaranteed data transmission security between linked nodes. Experimental results revealed a high accuracy ratio, which proved efficacy of the suggested framework. Still, with less than 20 patients, the BSDMF could not provide sufficient trust.

(Zulkifl et al., 2022) demonstrated a framework for the adaptive security of healthcare IoTs. The framework was developed based on fuzzy logic and hyperledger blockchain to achieve Authentication, Authorization, and Audit logs. Defined comparison unveiled reliability of the demonstrated model. Yet, fuzzy rules created with human knowledge make the model less reliable.

(Veeramakali et al., 2021) implemented a secure healthcare framework with Optimal Deep Learning-based Secure Blockchain (ODLSB) model. ODLSB leveraged orthogonal particle swarm optimization algorithm for secret sharing of medical images. Presented approach attained the highest accuracy during model validation. Yet, with compression technique in ODLSB model, quality of data could deteriorate when decompressed at the receiver end.

(Mohan et al., 2022) developed blockchain for secure data handling in IoMT. Data confidentiality was ensured via a double-encryption mechanism. Experimental outcomes revealed that the developed model performed well with minimum transaction speed. However, double encryption and Proof of Work consensus algorithm could make time inefficient in IoMT.

(Hao et al., 2022) investigated a secure data-sharing scheme in cloud-assisted IoMT. The sharing scheme was developed with proxy re-encryption and key blinding techniques. Performance evaluation demonstrated security of the scheme. But, with communication overhead problem, the scheme could not be applicable to larger distributed network.

(Kumar et al., 2022) deployed robust authentication protocol for IoMT-based Cloud-Healthcare Infrastructure (CHI). To ensure the security of CHI, an authentication and key agreement were formed. The comparative analysis revealed that deployed scheme was lightweight in terms of computation. But, they relied on third-party services and centralized architecture, which caused security threats.

3. PROPOSED IOMT DATA TAMPER DETECTION AND USER AUTHENTICATION METHODOLOGIES

Medical image watermarking is considered as one of the possible solutions to detect tampering with received file. Thus, OLES-LWT watermarked image-based IoMT data tamper detection with FYS-TIGER hashing for user authorization is proposed. The framework of the proposed approach is given in figure 1,

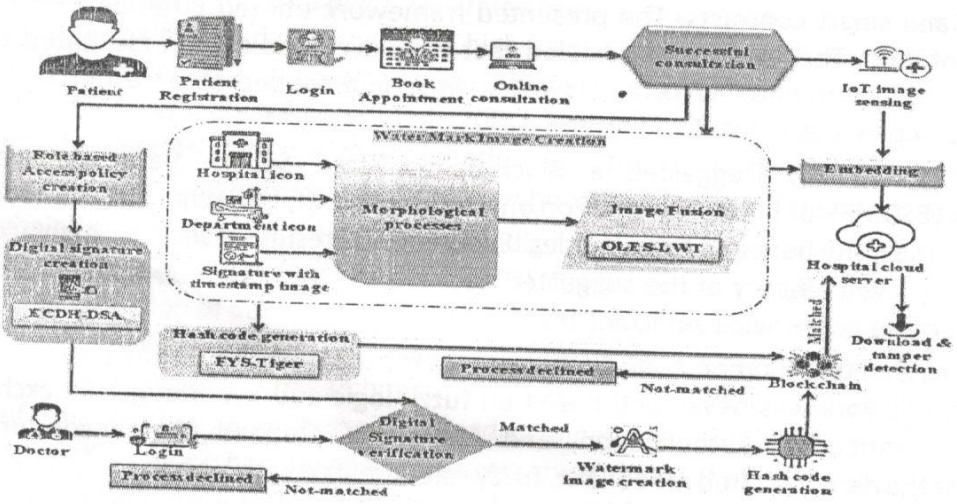


Figure 1: Block representation of the proposed model

3.1 Registration and login

Initially, patient registers their details such as user ID, password on hospital website. After successful registration, patient P logs into the hospital website using user ID, and password. If the user ID, and password of P gets matched with the details given during the registration, P is considered as authorized user and can further proceed with processes on the website.

3.2 Booking appointment and online consultation

After successful login of P, P can book an appointment with doctor (D) of the

corresponding hospital (H) using patient ID, Doctor ID, and Timestamp. After booking an appointment, consultation will be done and after successful consultation, IoT image sensing takes place. During IoT sensing image (S), a watermark image is generated by P.

3.3 Watermark image

The watermark image is formed by fusion of morphologically processed hospital icon, department icon, and doctor signature with time-stamp images using the OLES-LWT technique.

Hospital Icon (H): To obtain watermark image, initially, H is processed with morphological erosion and dilation process. The morphological process uses a small template called Structuring Element (SE) (E), which determines the number of pixel to be added or removed in H.

The E eroded and dilated with H to obtain image (HI_{er}, HI_{dil}) as,

$$HI_{er} = HI \ominus E \quad (1)$$

$$HI_{dil} = HI \bullet E \quad (2)$$

Where, $\ominus, \bullet$ depicts erosion and dilation operator.

After erosion and dilation are performed, obtained HI_{er} and HI_{er} are combined with XOR operation as,

$$HI_{image} = HI_{er} \oplus HI_{dil} \quad (3)$$

Here, H_{image} depicts the combined HI_{er} and H_{dil} image, $\oplus$ is XOR operation.

Department Icon (D): The D is processed with morphological opening and closing process to remove small objects and holes in D with SE (ρ) as,

$$DI_{open} = (DI \ominus \rho) \bullet \rho \quad (4)$$

$$DI_{close} = (DI \bullet \rho) \ominus \rho \quad (5)$$

Then, morphological opening and closing images (D_{open}, D_{close}) are combined to generate image D_{image} as,

$$DI_{image} = DI_{open} \oplus DI_{close} \quad (6)$$

Signature with timestamp *(ST)*: Next, doctor's digital signature with time-stamp image *(ST)* is processed with morphological thinning and thickening to remove and grow selected foreground pixels, which uses hit-and-miss transform *(T)* and SE *(e)* as,

$$ST_{thin} = ST - T(ST, e) \quad (7)$$

$$ST_{thick} = ST \cup T(ST, e) \quad (8)$$

Where, ST_{thin}, ST_{thick} is morphologically thinnedand thickened *(ST)* image, and $-$ depicts logical subtraction.

Then ST_{thin} and ST_{thick} are combined to produce an image (ST_{image}) as,

$$ST_{image} = ST_{thin} \oplus ST_{thick} \quad (9)$$

3.3.1 Image fusion

The obtained images H_{image}, D_{image} and ST_{image} are fused with OLES-LWT approach to obtain a watermark image.Lifting Wavelet Transform (LWT) is considered as it factorizes discrete wavelet transforms with reduced steps, but LWT has the disadvantage of end distortion and frequency aliasing in pixels. To solve this problem Odd Log Even Scaling (OLES) is introduced in LWT technique.

Split: Initially, H_{image} is split into odd and even (H_{odd}, H_{even}) sequences with OLES as,

$$H_{even} = 2\left(\frac{H - \overline{H}}{\sigma}\right)$$
$$H_{odd} = K_B \log(2.H + 1) \quad (10)$$

K_B, σ signifies Boltzmann constant and standard deviation.

Prediction and Updation: Then high-frequency component $(l(H_{image}))$ prediction and low-frequency component $(l(H_{image}))$updationare obtained by,

$$h(H_{image}) = H_{odd} - \alpha(H_{even}) \quad (11)$$

$$l(H_{image}) = H_{even} + \Delta(h(H_{image})) \quad (12)$$

$\alpha(\ ), \Delta(\ )$indicates prediction and updation operation which acts as the high pass and low pass filters. Thus coefficients set $(C)$of H_{image} is viewed as,

$$C = \{h(H_{image}), l(H_{image})\} \quad (13)$$

Similarly, coefficient sets for D_{image} and ST_{image} is obtained with OLES-LWT as $(Z)$and (X) which contains its corresponding high-frequency and low-frequency components.

Finally, coefficients are fused to obtain fused coefficient image $(\lambda(W))$ as,

(14)

Here, $\otimes$ is coefficient fusion operator. By applying inverse OLES-LWT on the $\lambda(W)$, the watermark image W is obtained.

Pseudo-code of proposed OLES-LWT

Input: Images H_{image}, D_{image} and ST_{image}

Output: watermark image (W)

Begin

Initialize LWT functions, $K_B, \alpha(\ ), \Delta(\ )$ and $\otimes$

For image $(H\ )$ **do**

Perform splitting (H_{odd}, H_{even}) via OLES

Predict odd samples with $\alpha(H_{even})$

Update even samples

Repeat For DI_{image}, ST_{image}

End For

Determine C, Z, X

Apply $\lambda(W) = C \otimes Z \otimes X$

Perform inverse OEEE-LWT

Return W

End

Watermark embedding: This obtained W is then embedded on the IoT sensed image (S) and uploaded on hospital cloud server.

3.5 Hashcode generation

For fused image (W), a hashcode is generated and stored in blockchain using Fishers Yates Shuffled–Tiger (FYS-Tiger) hashing algorithm. Tiger hashing was considered due to its design efficiency of 64-bit processors, but it has setback of pseudo-collision due to eight 64-bit words division of message. To solve this issue, Fisher Yates Shuffling (FYS) technique is included in Tiger Hashing algorithm.

The pixels in image (W), is extracted as bits and then bits are converted to eight 64-bit word and then shuffled with FYS as,

(i) Create a temporary array $(t[\ ])$ and store the eight 64-bit words in it and give a value of $(1,2,..,8)$ to each word.

(ii) Select a random value w from $(1,2,..,8)$ and store corresponding word of $t[\ ]$ in the end of a new array $(n[\ ])$ and delete the word from $t[\ ]$.

(iii) Then repeat the process (ii) until all words in $t[\ ]$ is deleted. By doing this process, shuffled array of words $n[w_0, w_1, .., w_7]$ or $n[w_i], i = 0,1,..,7$ is obtained.

This array of words is then converted to hash values as,

State update transformation: Tiger hashing starts from fixed three words, which are updated in three passes. In each round, one 64-bit word w_i used to update three state variables $\beta, \delta, \varepsilon$ which are considered as initial hash value (λ_0). Thus, save operation in tiger hashing is performed as,

$$\begin{cases} \beta = w_0 w_0 \\ \delta = w_1 w_1 \\ \varepsilon = w_2 w_2 \end{cases} \quad (15)$$

Key scheduling: After save operation, key scheduling is performed, in which inversion operation is carried out to prevent sparse attack. Thus key scheduling is given as,

$$\begin{cases} \lambda_0(\beta,\delta,\varepsilon) \\ \nabla_1(\beta,\delta,\varepsilon) \\ k \\ \nabla_2(\beta,\delta,\varepsilon) \\ k \\ \nabla_3(\beta,\delta,\varepsilon) \end{cases} \quad (16)$$

Where, $\nabla_1, \nabla_2, \nabla_3$ defines compression operation, and k depicts the key scheduled.

Compression: The compression operation undergoes eight rounds as,

$$\partial(\ ), mul \quad (17)$$

Where, $\partial(\ ), mul$ signifies rounding operation and arithmetic multiplication. Then the output hash value is obtained in feed-forward stage as,

$$\begin{cases} \beta_{(1)} \oplus = \beta \\ \delta_{(1)} - = \delta \\ \varepsilon_{(1)} + = \varepsilon \end{cases} \quad (18)$$

Where, $\beta_{(1)}, \delta_{(1)}, \varepsilon_{(1)}$ is the output 192 bits hashvalue. This hashcode is then stored in blockchain.

3.6 Role-based access policy

When sensed image (S) is shared via cloud, a role-based access policy is created in block chain. Role-based access control policies represent the rights of users in terms of roles to access S. A role-based access control policy is created for D and digitally signed with the ECDH-DSA algorithm and then added to block chain.

3.6.1 Digital signature creation

The role-based access control policy is digitally signed with the ECDH-DSA technique. The Digital Signature Algorithm (DSA) is selected in the proposed model as it provides more message integrity. But, revoking a compromised key is impossible in DSA, which allowed

malicious actors to impersonate user privacy without any method of confirmation. To solve this problem, Elliptic Curve Diffie Hellman (ECDH) is used for secret key generation in DSA.

Key generation: Initially, private and public keys are generated on patient and doctor side is generated with Elliptic Curve Cryptography during the P and D registration from elliptic curve equation,

$$q^2 = p^3 + a.p + b \tag{19}$$

Where, p,q denotes p and q-axes respectively, a,b are constant values, in elliptic curve a predefined generator point (g) is taken and multiplied random integers (i.e., private keys) (μ,ω) to generate points in curve as,

$$k_P, k_D \tag{20}$$

Here, k_P, k_D are the public keys generated at P and D side. With μ,ω,k_P,k_D, a shared secret key (s) is generated with theDiffie Hellman technique as,

$$s = (k_D)^{\mu} \bmod g = (k_P)^{\omega} \bmod g \tag{21}$$

Where, $(k_D)^{\mu} \bmod g, (k_P)^{\omega} \bmod g$ are computed at the patient's and doctor's side respectively.

Signature generation: Then, a signature for user $(i.e\, D)$ identity (ϖ) is generated with DSA technique using a random integer (τ) and $SHA-1(\varpi)$ as,

$$\left.\begin{aligned} \zeta &= k_D \bmod h + s \\ t &= \tau^{-1}(\hbar + \mu.\zeta) \bmod h \end{aligned}\right\} \tag{22}$$

Where, $h,\hbar$ defines random constant and $SHA-1(\varpi)$ resultant integer value. (ζ,t) is the signature for identity (ϖ).

3.7 Data access

The registered doctor D, accesses S by successfully logging in to the hospital server. Then after, the digital signature and hashcode verification on blockchain, D can successfully retrieve S from cloud.

Signature verification: When D access S, then the access policy will be validated by signature verification as,

The $SHA-1(\varpi)$ is performed and integer $(\hbar)$ is generated at the doctor's side. Next, computes the following steps,

$$\left.\begin{aligned} y &= t^{-1} \bmod h \\ z_1 &= \hbar.y \bmod h \\ z_2 &= (\zeta - s).y \bmod h \end{aligned}\right\} \tag{23}$$

Where, y, z_1, z_2 are computation parameters. The signature is accepted and can access S if,

$$\xi = \hat{k}_D \bmod h = \zeta \qquad (24)$$

Where, $\hat{k}_D$ is integer value computed for k_D. And if $\xi \neq \zeta$, the access of S by D will be rejected.

Hashcode verification: After signature verification, watermark image is created at the doctor's side using the OLES-LWT. Then,the hashcode for the corresponding fused image is generated and matched with the $\beta_{(1)}, \delta_{(1)}, \varepsilon_{(1)}$ in the blockchain. If generated hashcode gets matched, the S will be downloaded from the cloud.

3.8 Tamper detection

After S is downloaded by D, the watermark will be removed. If the watermark is completely removed, then it is considered as non-tampered and will be analysed by D. Else, if the watermark cannot be removed completely, it is regarded as tampered data and D asks P to resend the data.

4. RESULTS AND DISCUSSIONS

In this section, experimental outcomes of proposed approaches are evaluated in comparison with baseline approaches. The experiments are performed on the working platform of PYTHON, with synthetically generated datasets.

4.1 Performance analysis

Here, performance of the proposed framework is analyzedin three segments namely Image fusion, Hash Code Generation (HCG), and digital signature.

4.1.1 Performance analysis of image fusion

In this subdivision, experimental results based on entropy and fusiontime of watermark image are discussed in comparison with the LWT and Wavelet Transform (WT) techniques.

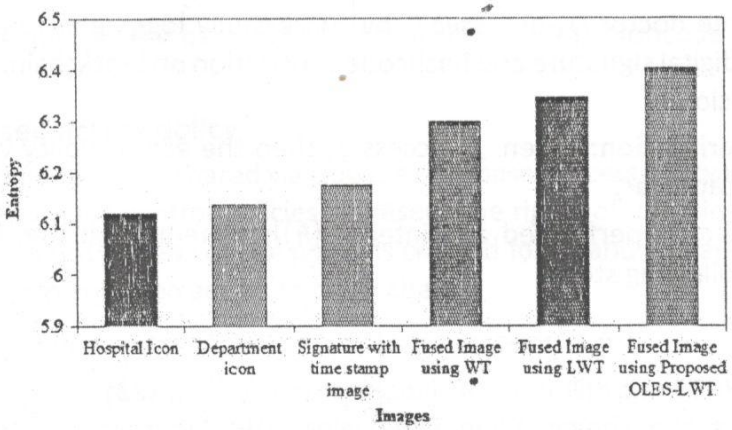


Figure 2: Entropy results of fused images

A system with a higher entropy value depicts that the fused image contains more detailed information. From figure 2, it is evident that entropy of OLES-LWT (6.4033) is higher than baseline LWT and WT techniques. This shows that fusion of H_{image}, D_{image} and ST_{image} gives a better watermark than existing techniques.

Table 1: Fusion time results

Algorithms	Fusion time (ms)
Proposed OLES-LWT	298
LWT	381
WT	437

Table 1 unveils fusion time of H_{image}, D_{image} and ST_{image} images, in which the proposed OLES-LWT approach takes 139ms and 83ms lesser than WT and LWT respectively during image fusion. This shows that with OLES-LWT in the proposed framework, watermark image is obtained faster than other techniques.

4.1.2 Performance analysis of hashcode generation

The experimental analysis of HCG time of the proposed FYS-Tiger is discussed in this segment in comparison with prevailing hashing algorithms of Tiger, Message Digest-5 (MD5), SWIFFT, and SHA-512.

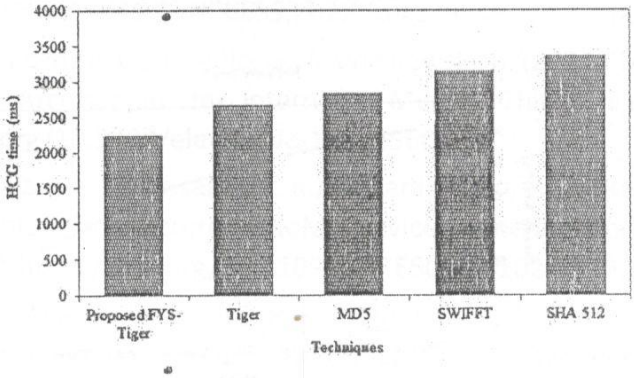


Figure 3: Results of HCG time

From Figure 3, it can be seen HCG is performed in less time with Tiger hashing during the experimental analysis of existing algorithms. But, with FYS in Tiger hashing, HCG time was reduced by 446ms. This shows that FYS-Tiger hashcodes are generated in IoMT environment.

4.1.3 Performance evaluation of digital signature

In this phase, digital signature generation and verification times of the proposed ECDH-DSA technique areanalyzed in comparison with baseline Elliptic Curve DSA (ECDSA), DSA, Rivest-Shamir-Adlemann (RSA) and Boneh–Lynn–Shacham (BLS).

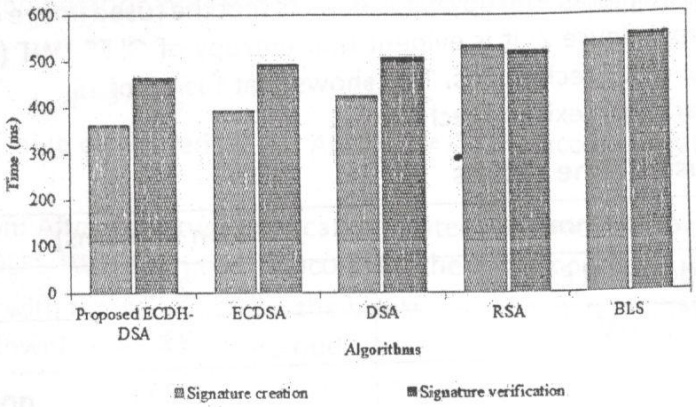


Figure 4: Signature creation and verification time outcomes

Figure 4 unveils experimental outcomes of digital signature creation and verification times, in which ECDSA and DSA performed signature creation and verification in less than that of RSA and BLS. Yet, with ECDH key-generation in DSA technique, the proposed ECDH-DSA takes 361ms and 464ms only for signature creation and verification processes. Thus, it is concluded that ECDH-DSA gives better performance in the proposed architecture.

4.2 Comparative analysis

In this section, security level of the proposed framework is compared with the works with security as an objective, such as (Abbas et al., 2021), (Veeramakali et al., 2021), and (Kumar et al., 2022).

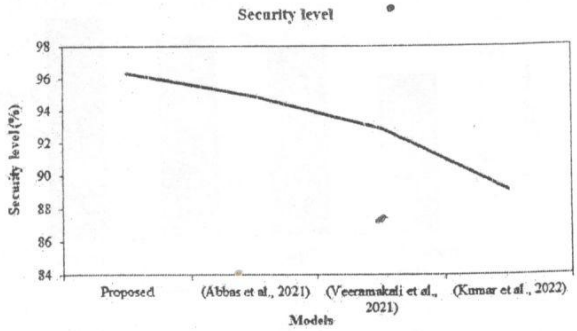


Figure 5: comparative analysis with security level

The comparative analysis of security level of proposed and existing models of (Abbas et al., 2021), (Veeramakali et al., 2021), and (Kumar et al., 2022) are shown in figure 5, where (Kumar et al., 2022) model attained less security by using centralized architecture. But, with watermarking and ECDH-DSA with FYS-Tiger-based user authentication in blockchain, the proposed model attained the highest security level of 96.34% in IoMT environment. Also, even with blockchain technology,models of (Abbas et al., 2021) and (Veeramakali et al., 2021) attained 1.54% and 3.57% less security than the proposed model. Thus, it is verified that proposed model is suitable for securing data in IoMT.

5. CONCLUSION

In this article, a novel tampering detection and ECDH-DSA with Fys-Tiger-based blockchain verification in IoMT is proposed. Here, to generate a watermark image, a fused image is formed with hospital icon, department icon, and digital signature with a time-stamp image using OLES-LWT technique. Then, proposed approaches are experimentally analyzed with baseline techniques to prove reliability of the proposed model. During fusion image analysis, proposed OLES-LWT attained higher entropy (6.4033) and less fusion time (298ms). Also, HCG, signature generation, and verification times of the proposed techniques are less than state-of-the-art techniques. Finally, security analysis proved the objective of proposed model by providing high security in IoMT environment.In this work, IoMT data tamperingdetection is concentrated. In the future, the appropriate technique can be introduced to avoidtampering with IoMT data.

REFERENCES

1. Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2021). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and Ubiquitous Computing. https://doi.org/10.1007/s00779-021-01583-8
2. Bataineh, M. R., Mardini, W., Khamayseh, Y. M., & Yassein, M. M. B. (2022). Novel and Secure Blockchain Framework for Health Applications in IoT. IEEE Access, 10, 14914–14926. https://doi.org/10.1109/ACCESS.2022.3147795
3. Bhattacharjya, A., Kozdrój, K., Bazydło, G., & Wisniewski, R. (2022). Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical-Things. Electronics, 11(16). 1-19. https://doi.org/10.3390/electronics11162560
4. Fotopoulos, F., Malamas, V., Dasaklis, T. K., Kotzanikolaou, P., & Douligeris, C. (2020). A Blockchain-enabled Architecture for IoMT Device Authentication. 2ndIEEE Eurasia Conference on IOT. https://doi.org/10.1109/ECICE50847.2020.9301913
5. Garg, N., Wazid, M., Das, A. K., Singh, D. P., Rodrigues, J. J. P. C., & Park, Y. (2020). BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment. IEEE Access, 8, 95956–95977. https://doi.org/10.1109/ACCESS.2020.2995917
6. Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2021). Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. IEEE Internet of Things Journal, 8(11), 8707–8718. https://doi.org/10.1109/JIOT.2020.3045653
7. Hao, J., Tang, W., Huang, C., Liu, J., Wang, H., & Xian, M. (2022). Secure Data Sharing With Flexible User Access Privilege Update in Cloud-Assisted IoMT. IEEE Transactions on Emerging Topics in Computing, 10(2), 933–947. https://doi.org/10.1109/TETC.2021.3052377

8. Kumar, V., Mahmoud, M. S., Alkhayyat, A., Srinivas, J., Ahmad, M., & Kumari, A. (2022). RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure. Journal of Supercomputing, 78(14), 16167–16196. https://doi.org/10.1007/s11227-022-04513-4
9. Mohan, D., Alwin, L., Neeraja, P., Lawrence, K. D., & Pathari, V. (2022). A private Ethereum blockchain implementation for secure data handling in Internet of Medical Things. Journal of Reliable Intelligent Environments, 8(4), 379–396. https://doi.org/10.1007/s40860-021-00153-2
10. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain. IEEE Internet of Things Journal, 8(14), 11743–11757. https://doi.org/10.1109/JIOT.2021.3058953
11. Nishi, F. K., Shams-E-Mofiz, M., Khan, M. M., Alsufyani, A., Bourouis, S., Gupta, P., & Saini, D. K. (2022). Electronic Healthcare Data Record Security Using Blockchain and Smart Contract. Journal of Sensors. https://doi.org/10.1155/2022/7299185
12. Ogundokun, R. O., Awotunde, J. B., Adeniyi, E. A., & Ayo, F. E. (2021). Crypto-Stegno-based model for securing medical information on IOMT platform. Multimedia Tools and Applications, 80(21–23), 31705–31727. https://doi.org/10.1007/s11042-021-11125-2
13. Quasim, M. T., Algarni, F., Radwan, A. A. E., & Alshmrani, G. M. M. (2020). A Blockchain-based Secured Healthcare Framework. 2020 International Conference on Computational Performance Evaluation. https://doi.org/10.1109/ComPE49325.2020.9200024
14. Swetha, M. S., Pushpa, S. K., Muneshwara, M. S., & Manjunath, T. N. (2020). Blockchain enabled secure healthcare Systems. IEEE International Conference on Machine Learning and Applied Network Technologies. https://doi.org/10.1109/ICMLANT50963.2020.9355970
15. Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 1-13. https://doi.org/10.1016/j.jisa.2019.102407
16. Veeramakali, T., Siva, R., Sivakumar, B., Senthil Mahesh, P. C., & Krishnaraj, N. (2021). An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. Journal of Supercomputing, 77(9), 9576–9596. https://doi.org/10.1007/s11227-021-03637-3
17. Zulkifl, Z., Khan, F., Tahir, S., Afzal, M., Iqbal, W., Rehman, A., Saeed, S., & Almuhaideb, A. M. (2022). FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs. IEEE Access, 10, 15644–15656. https://doi.org/10.1109/ACCESS.2022.3149046

★★★