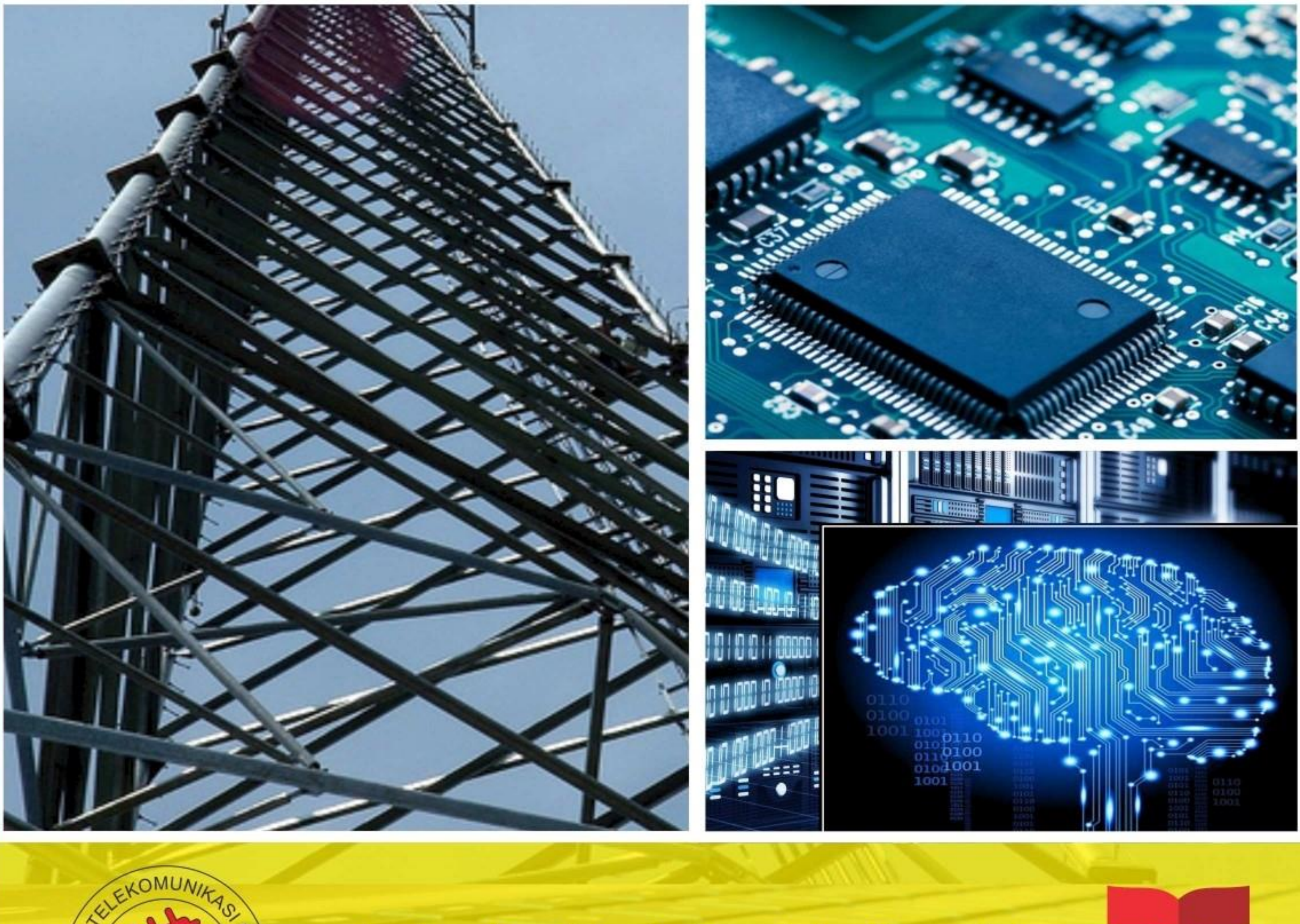
ISSN : 2085-3688 | e-ISSN : 2460-0997

JURNAL INFOTEL

INFORMATICS TELECOMMUNICATION ELECTRONICS

Volume 14, Number 02 May 2022



Lembaga Penelitian dan Pengabdian Masyarakat
Institut Teknologi Telkom Purwokerto

JURNAL INFOTEL

Informatics, Telecommunication, and Electronics

Volume 14, Number 2 May 2022

DESCRIPTION AND POLICY

About Jurnal INFOTEL

Jurnal INFOTEL is a scientific journal published by Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) of Institut Teknologi Telkom Purwokerto, Indonesia. It was firstly published in 2009 for a printed version and for online version in 2012. The aims of Jurnal INFOTEL are to disseminate research results and to improve the productivity of scientific publications. Jurnal INFOTEL is published quarterly in February, May, August, and November. **Starting in 2018, Jurnal INFOTEL uses English as the primary language.**

Focus and Scope

Jurnal INFOTEL covers the field of informatics, telecommunications, and electronics. We receive **original research articles and any review papers.** Jurnal INFOTEL is published quarterly in **February, May, August and November** with the scopes and focus of the research areas that are:

Informatics: including Software Engineering, Information Technology, Information System, Data Mining, Multimedia, Mobile Programming, Artificial Intelligence, Computer Graphic, Computer Vision, Augmented/Virtual Reality, Games Programming.

Telecommunications: including Modulation and Signal Processing, Information Theory and Coding, Antenna and Wave Propagation, Wireless and Mobile Communication, Radio Communication, Satellite Communication, Fiber Optic, Network, and System.

Electronic: including Microelectronic System, VLSI Design, Biomedical Instrument, Embedded System, Robotic, Communication Electronic, Optoelectronic, Internet of Things, Analogue and Digital Control, Intelligent Control, Adaptive System, System Identification.

Peer Review Policy

Each article that goes to the editor will be selected in advance on the scope and feasibility by the editorial board. Then, the articles will be sent to peer reviewer and will go to the next selection by **Blind Preview Process**. Reviewers do not know the identity of the authors, and authors do not know the identity of reviewers either. Each submitted paper will be reviewed by at least two peer-reviewers. After that, the articles will be returned to the authors to revise. The reviewing process will consider novelty, objectives, method, scientific impact, conclusion, and references.

Open Access Policy

This journal is an open access journal which provides free access to the full text of all published articles without charging readers or their institutions for access. Readers have the right to read, download, copy, distribute, print, search, or link to the full texts of all articles in Jurnal INFOTEL. This journal provides immediate open access to its content on the principle that makes the research freely available to the public supports a greater global exchange of knowledge.

Registration Process

Due to security issues, the registration process in Jurnal INFOTEL is conducted by sending author's data such as full name and academic degree, email, and institutional affiliation to email **infotel@st3telkom.ac.id**. Author's account will be created by Admin. Account details, namely username and password, will be sent to Authors. The Authors, then are welcomed to submit their paper(s) afterward.

Online Submission

If you have already got the Username/Password for Jurnal INFOTEL, go to log in at: http://ejournal.st3telkom.ac.id/index.php/infotel/login

Copyediting and Proofreading

All accepted papers will be checked with Copyediting and Proofreading process. We also use Grammarly application to improve the grammar quality of the articles.

Accreditation

Jurnal INFOTEL has been accredited by Ministry of Research, Technology and Higher Education as an online Scientific journal in Indonesia with accreditation number: 200/M/KPT/2020, December 23, 2020.

Indexing

Jurnal INFOTEL has been listed and indexed by Google Scholar, Open academic journals index, Crossref, ResearchBib, Bielefeld Academic Search Engine (BASE), ROAD: The Directory of Open Access Scholarly Resources, Directory of Open Access Journal (DOAJ), Neliti, Indonesia One Search, Garba Rujukan Digital (Garuda), Science and Technology Index (SINTA), Index Copernicus International (ICI).

Mailing Address

Jurnal INFOTEL office:
Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Institut Teknologi Telkom Purwokerto (IT Telkom Purwokerto)
D.I Panjaitan Street No. 128 Purwokerto, Indonesia
Telp. 0281-641629
Email: infotel@st3telkom.ac.id
Website:
http://ejournal.st3telkom.ac.id/index.php/infotel

ISSN : 2085-3688; e-ISSN : 2460-0997

JURNAL INFOTEL

Informatics, Telecommunication, and Electronics

Volume 14, Number 2 May 2022

Publisher

Lembaga Penelitian dan Pengabdian Masyarakat (LPPM)
Institut Teknologi Telkom Purwokerto

Editor-in-Chief

Advisory Board

Associate Editor

Editorial Board

Managing Editor

JURNAL INFOTEL

Informatics, Telecommunication, and Electronics

Volume 14, Number 2 May 2022

PREFACE FROM EDITOR-IN-CHIEF

Jurnal INFOTEL is a scientific journal published by Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) of Institut Teknologi Telkom Purwokerto, Indonesia. It covers the field of Informatics, Telecommunications, and Electronics. The aims of Jurnal INFOTEL are to disseminate research results and to improve the productivity of scientific publications. Starting in Volume 10 Number 1, 2018, Jurnal INFOTEL uses English as the primary language.

Jurnal INFOTEL is indexed by national and international indexer such as Neliti, Indonesia One Search, Garba Rujukan Digital (Garuda), Science and Technology Index (SINTA), Google Scholar, Open academic journals index, Crossref, ResearchBib, Bielefeld Academic Search Engine (BASE), ROAD: The Directory of Open Access Scholarly Resources, Directory of Open Access Journal (DOAJ), Index Copernicus International (ICI).

In this issue, nine papers are published by 25 authors from 8 institutions in Indonesia. Three papers related to Informatics topics. Two papers related to Telecommunication topics. One paper is about Electronics topic.

We would like to thank our Associate Editors, Editorial Boards, Reviewers, and Authors. We hope that Jurnal INFOTEL can contribute to the progress of scientific publications in Indonesia and in the world.

Purwokerto, May 2022

Editor-in-Chief

JURNAL INFOTEL
Informatics, Telecommunication, and Electronics
Volume 14, Number 2 May 2022

TABLE OF CONTENT

JURNAL INFOTEL
Informatics - Telecommunication - Electronics
Website Jurnal : http://ejournal.st3telkom.ac.id/index.php/infotel
ISSN : 2085-3688; e-ISSN : 2460-0997

Secure protection for covid-19 infographic using blockchain and discrete cosine transform-singular value decomposition (DCT-SVD) watermarking

Muhammad Fajar Sidiq[1*], Akbari Indra Basuki[2], Didi Rosiyadi[2], Iwan Setiawan[2], Yusnan Hasani Siregar[3], Sriyadi[4]
[1] Department of Informatics. Institut Teknologi Telkom Purwokerto
[2] Research Center for Informatics. National Research and Innovation Agency
[3] Research Center for Appropriate Technology, National Research, and Innovation Agency
[4] Faculty of Engineering and Informatics, Bina Sarana Informatika University
[1] Jalan D.I. Panjaitan No. 128, Purwokerto 53147, Indonesia
[2] Jalan Cisitu No. 21/154 D, Bandung 40135, Indonesia
[3] Jl. KS Tubun No 5, Subang 41211 , Indonesia
[4] Jl. Kamal Raya No.18, Jakarta 11730, Indonesia
*Corresponding email: fajar@ittelkom-pwt.ac.id

Received 24 December 2021, Revised 29 March 2022, Accepted 13 April 2022

Abstract — Covid-19 infographics have a crucial role in mitigating the covid-19 pandemic by conveying the complex Covid-19 information in a form of a simple yet understandable image. However, keenly to contribute to mitigating Covid-19, numerous parties and agencies had released Covid-19 infographics that might contain incorrect or inaccurate information. To prevent such recurrent, this paper proposed an authentication system by using a blockchain-based authorization service that lets the authority guarantee the correctness and validity of the infographics in a transparent manner. We proposed smart contract-based watermarking requests and approval management that let anyone track the watermarking process. To prevent unauthorized infographic fabrications, we use the discrete cosine transform and singular value decomposition (DCT-SVD) method considering its robustness against various attacks. We deployed and evaluated the smart contract on Ethereum test networks (Ropsten, Rinkeby, Goerli, and Kovan) to compare the efficiency and the ease of use. The result showed that the test networks have similar efficiency while the Ropsten and Goerli have better ease of use. The watermark validation service is accessible via a web-based interface for anyone to check the validity of the infographic's watermark.

Keywords – Infographic, Protection, Covid-19, Watermarking, Blockchain, smart contract

I. INTRODUCTION

The Covid-19 pandemic has a severe impact on the world economy and people's psychology [1, 2]. The World Bank records that there has been a sharp increase in extreme poverty particularly in developing countries. The phenomenon is the direct consequence of the business and employments downturn that results in reduced working hours, reduced wages, and workers laid-off [3].

The severity of the pandemic has moved anyone to share the effort in mitigating the pandemic. The main purpose is to educate the people on how to properly inhibit the spreading of the Covid-19 virus. These phenomena increase infographic dissemination to the mass aiming to inform and educate society. Infographic is the most preferable medium since it can convey complex information in a simple and yet easily fathomable by the mass [4]. The infographic can teach people about general knowledge related to Covid-19 up to technical detail such as how to wear the mask properly [5].

Nevertheless, the phenomena lead to the enormous release of the Covid-19 infographic to the public. Numerous agencies and media had issued their version of the Covid-19 infographic [6]. While it might be a good sign, it possesses potential threats in how to guarantee the accuracy and correctness of the infographic. Moreover, based on the study in [7], most people are unaware of the credibility of the information source. In social media, most people will likely treat equally the information shared by any bystanders to the official release of the World Health Organization (WHO).

To solve this problem, the government must step in to guarantee infographic correctness and authenticity. We define three possible actions that can be taken by the government as follow.

a) Providing a trusted authentication system to handle the infographic registration.
b) Providing an intrinsic authentication system using image watermarking.
c) Providing a verification service to verify infographic validity.

By providing an intrinsic authentication system such as image watermarking, it will prevent anyone to consume unauthorized infographics. Anyone can extract the watermarking to verify whether the infographic has been approved by the authority or not.

Nonetheless, single control of the infographic might rise an authoritarian behavior, i.e., unfair or discrimination on the watermarking request. For pubic transparency, any request to authenticate the infographic alongside its approval must be shared with the public. The user must know the exact progress of their request such as whether it has been approved for watermarking, or how they can download the watermarked result.

Considering the authentication system will determine the infographic validity, the system integrity must be proven to the mass. Thus, the infographic watermarking must be approved by both parties; the authority and content creators, under public monitoring. Likewise, it acts as double-layer protection for watermarking service. Even though the attacker has breached the authority server and forcefully assigned the watermarking, anyone can verify that the watermarking violated the standard procedure of two-side approval since it lacks the content creator's approval.

Several works have dealt with image watermarking as a service, such as in buyer and seller scenario [8-10]. They proposed secure and privacy preserving technique using homomorphic encryption. Nonetheless, the works did not offer traceability to track watermarking requests and approvals. Other works do provide the traceability by using blockchain to record the transaction [11-13]. However, those works treat the watermarking process one-sidedly without offering two-faction authentication. In case the watermarking server is compromised, the attacker will have full control of the entire watermarking process.

This study aims to solve the aforementioned problem by proposing a transparent and trusted watermarking service for the Covid-19 infographic by using blockchain smart contract and image watermarking. We use smart contracts to ensure the transparency of the watermarking process while discrete cosine transform and singular value decomposition (DCT-SVD) watermarking is used to secure infographic validity. We offer two-side verification to prevent watermarking abuse by the authority or any attacker to take control the watermarking service. The proposed system is accessible via a web-based service for public requests.

We present the research method in section II, followed by the result and discussion in sections III and IV. At last, the conclusion is available in section V.

II. RESEARCH METHOD

A. DCT-SVD Watermarking

The DCT-SVD watermarking embeds noise-tolerant information into the image (I) for future verification that an image has been approved by the authority. We use DCT-SVD watermarking due to its robustness against various image manipulation attacks [14, 15].

The computation of watermark embedding can be described as follow. First, the image is converted into frequency domain using direct cosine transform (DCT) (1). The SVD operation then can be applied into the transform data to retrieve the orthogonal matrices (U) and (V^T) and singular value (S) of the image (2). The watermark embedding is run by adding the watermark data (W_S) into the singular value of the image (3). Where the watermark data is the scaled version of the singular value of the watermark image.

$$c(r,s) = \alpha(r) \cdot \alpha(s) \sum_{x,y=0}^{N-1} \sum \{ f(x,y) \cdot cos\left[\frac{(2x+1)\pi r}{2N}\right] \cdot \cos\left[\frac{(2y+1)\pi x}{2N}\right] \} \quad (1)$$

$$I = U_I S_I V_I^T \quad (2)$$

$$S_{WI} = S_I + \alpha S_W \quad (3)$$

$$I' = U_I S_{WI} V_I^T \quad (4)$$

The watermarked image (I') can be constructed by applying inverse DCT-SVD operations. First, we swap the singular value of the image using the newly generated singular value (3). Next, the inverse SVD can be computed using (4) to form image representation in frequency domain. At last, to convert the image into spatial domain, an inverse DCT (5) is applied to the data.

$$f(x,y) = \sum_{x,y=0}^{N-1} \sum \{ \alpha(r) \cdot \alpha(s) \cdot c(r,s) \; cos\left[\frac{(2x+1)\pi r}{2N}\right] \cdot \cos\left[\frac{(2y+1)\pi x}{2N}\right] \} \quad (5)$$

Upon being released to social media or instant messaging, an image might be attacked by the adversaries by modifying the image. To verify whether an image has a valid watermark or not, we can extract the watermark form the image and compare the structural similarity of the extracted watermark with the original watermark.

In our works, we use non-blind watermarking where the original image is used to extract the embedded watermark. The extraction follows the step of watermark embedding by breaking down the SVD of the possibly attacked image $I"$ within frequency domain using DCT-SVD operation. The proces will yields three matrices U_{WI}, S_{WI}, and V_{WI}^T. The singular value of the extracted watermark (W') can be computed using (6). It subtracts the singular value of watermarked image with the singular value of the original image. Finally, the extracted watermark can be reconstructed using (7), by multiplying the extracted singular value with the orthogonal matrices of the watermark image (U$_W$, V$_W^T$).

$$S_{W'} = S_{WI} - S_I \quad (6)$$

$$W' = U_W \, S_{W'} V_W{}^T \quad (7)$$

The mean structural similarity index (MSSIM) determines whether the extracted watermark has close similarity to the original watermark. Equation (8) shows how to compute the MSSIM value of the extracted watermark. Higher similarity value indicates the resemblance of the extracted watermark with the original one.

$$SSIM\ (x,y) = [l(x,y)^{\alpha}]\big[c(x,y)^{\beta}\big][s(x,y)^{\gamma}]$$

$$= \frac{(2\mu_x\mu_y + C_1)(2\sigma_x\sigma_x + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

$$MSSIM\ (x,y) = \frac{1}{M}\sum_{j=1}^{m} SSIM(x_j, y_j) \quad (8)$$

Besides the MSSIM value, peak signal to noise ratio (PSNR) value is usually used to measure the infographic quality after watermarking additions. The lower the PSNR value the higher image degradation due to watermarking process. Equation (9) formulates the PSNR computation while equation (10) show how to compute the MSE.

$$PSNR = 10\ \log_{10}\left(\frac{255^2}{MSE}\right) \quad (9)$$

$$MSE = \frac{1}{MN\ \sum_{x=1}^{M}\sum_{y=1}^{N}(I_{x,y} - J_{x,,y})} \quad (10)$$

B. Blockchain and Smart Contract

Blockchain is a distributed system that stores a chain of block containing list of transactions. The chain of block or called the ledger (L) records sequences of blocks such that $L = \{b_1, b_2, b_3, \dots\ b_n\} |\ b_i \,\epsilon\, B$. Every block ($b$) contain N-transactions where each transaction (T) can be modelled as $T = (A_s, A_D, G_L, G_P, V\ , D\ )$. The A_s andA_D refers to the source and destination address of the transaction. The $G_L$and G_P correspond to gas limit and gas price of the transaction. Finally, V and D represent the transaction value and extra data carried by the transaction.

Blockchain has immutable property since the data or the chain of block are stored by all of the participants that run the same blockchain application. To alter the data, the attacker must breach and modify the data from $50\,\% + 1$ of the nodes that widely spread across the globe.

Smart contract is a unique address that contains a program. It can be run by any account by sending a transaction to the address. A smart contract transaction (T_{SC}) is unique transaction where the extra data field (D) contains the function name (F) and its parameters (P) that callable by anyone. The contract can be programmed to only accept addresses by specifying the address directly within the smart contract or by dynamically inserted via a smart contract function. Upon the smart contract transaction being recorded into a new valid block, the miners will run the function (F) and the final state will be updated.

A smart contract transaction has two kinds of successful status, a systemic and logical one. The systemic status indicates whether the transaction has been recorded into a new valid block or not. Whereas the logical status indicates whether the function being called have met the requirement or not. A particular function (F_i) might be designed to be run only by the smart contract creator. Thus, other accounts that send a transaction to call this function (F_i) might successfully get the transaction being recorded into the blockchain. However, it has transaction logical status fail (access error). In this case, the function F_i is not being executed by the miners since it does not meet the function requirements.

The main advantage of blockchain is public verifiability. Anyone can run a blockchain node to participate in securing blockchain systems using a distributed system. Those who do not run blockchain nodes can monitor the transaction and smart contract execution by using blockchain explorer services such as Etherscan [16].

C. System Design

The block diagram of the system can be depicted as Fig. 1. The system contains three main elements: the smart contract, cloud storage, and the watermarking server. The smart contract serves as the logging tool to keep track of the watermarking request in a transparent manner. The smart contract records only the URL and the hash value of the image, while the encrypted image is being stored in the cloud storage.

The watermarking server has two roles. First, it computes image watermarking based on the request being recorded in the smart contract. Second, it computes watermarking validation in case there is a request for infographic verification.

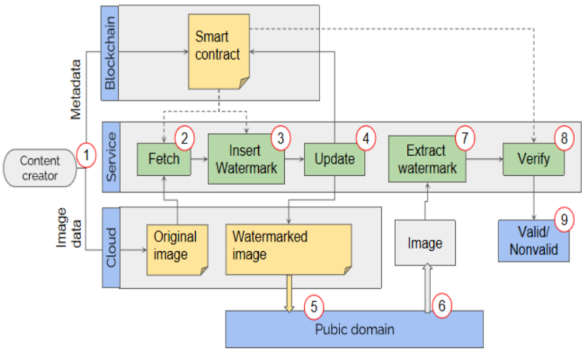


Fig.1. Block diagram of the system

The working sequence of the system can be described as follow (Fig. 1).

a) The creator of the infographic submit the request to the smart contract (Step-1)
The request contains a tuple of data that describe the infographic/content as follow:
1) The hash value of the infographic,
2) The URL containing the Encrypted infographic, and
3) Admin ID (optional).
The infographic creator must upload the encrypted version of the infographic to the cloud storage prior to sending the request to the smart contract. The data is encrypted using the admin's public key that is recorded in the smart contract.
b) The watermarking server regularly fetches a new watermarking request and downloads the infographic based on the provided URL (Step-2). Next, the server will decrypt the infographic for further process.
c) Upon decrypting the infographic, the server embeds the watermarking to the infographic using the DCT-SVD method (Eq. 1 - 5).
d) The server uploads the watermarked infographic to the cloud storage and updates the URL to the smart contract (Watermarked URL) (Step-4). The watermarked infographic is encrypted using the creator public key which is stored in the smart contract.
e) The creator might disseminate the watermarked infographic to the internet via social media, instant messaging, or other media (Step-5).
f) For infographic validity checking, anyone might send the request by uploading the intended infographic to the watermarking server (Step-6).
g) The server, upon receiving the request will extract the watermark by using the DCT-SVD method (Step-7).
h) The server then compares the metadata with the one stored in the smart contract and computes the MSSIM (6) to determine whether the infographic is valid or not based on the similarity value (Step-8).

D. Watermarking Contract

The smart contract aims to preserve the transparency of the watermarking request and its approval mechanism, i.e., prevents one-sided rejection by the authority. Considering the watermarking request has been recorded in the blockchain, it can act as temporal evidence regarding who is the real owner of the infographics.

The smart contract also serves as an immutable look-up table for watermarking validation. The user who requests infographic authentication will receive the record number of the infographics alongside their similarity values. The requester can cross-check the result given by the validation server with the data stored in the smart contract.

The class diagram of the smart contract is shown in Fig. 2. The green colors represent static data while the blue ones correspond to dynamics that store watermarking-related data. The yellow colors indicate the user status.

The infographic data is stored as a Content class that consists of 5 records, namely the index, hash, URLs, and admin id. The index refers to the ID number of the infographic. The hash contains the hash value of the original image for conflict resolution. The two URLs correspond to the web addresses of the encrypted infographic and the encrypted watermarked version. The last record represents the ID number of the watermark provider (Admin). Watermarking requester might choose their preferred and trusted authority independently from another user.

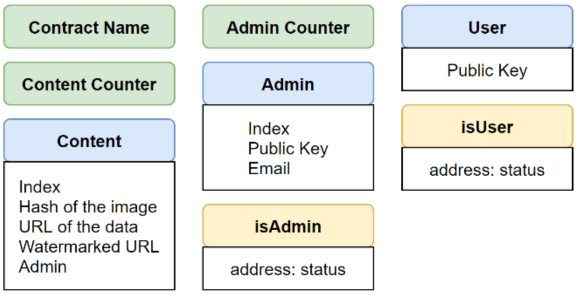


Fig.2. Class diagram of the smart contract

Considering the infographic image and its watermarked result have big sizes (megabytes), it cannot be stored in the blockchain. Thus, it must be stored into off-chain storage indicated by the URLs records. To keep the data secret between the requester and the authority, we use asymmetric cryptography to encrypt the infographic data. To achieve it, the public key of the authority and the user must be exposed to in the smart contract. Thus, the communicating party can deliver the data in a secret way using those public keys.

E. Watermaking Server

The watermarking server provides two main services: infographic watermarking (Fig. 3) and infographic validation (Fig. 4).

The watermarking process involved the smart contract and cloud storage coordination (Fig. 3). The status of watermarking request is stored in smart contract. Meanwhile the image data is stored in cloud storage in encrypted format. The design is to accommodate the limited storage capacity of the blockchain transaction. The watermarking server periodically read the smart contract status for a new watermarking request.

Upon detecting new watermarking request, there are five steps for the server to generate a valid watermarked image. First, it downloads the infographic from the cloud storage using the link sent by the content creator via smart contract transactions. Second, it decrypts the image using the server's private key. In the next step, the server embeds the watermark data into the infographics. Fourth, the server uploads the watermarked infographic to the cloud server. At last, the server update status and the URL of the result into the smart contract.

The requester or content creator will retrieve the watermarked infographic by reading the status of the smart contract. Upon receiving the URL of the result, the infographic creator can download the watermarked version.

In watermarking validation scenario (Fig. 4), anyone can submit untrusted infographics to the webserver for validation request. First, the watermarking server will populate the watermarking request and apply the watermarking accordingly. Second, the validation server uses DCT-SVD parameters stored in the smart contract to check its validity. The validity is determined by the MSSIM value. If the MSSIM value is high or close to 1 (one), it indicates that the watermark data embedded nto the infographic image are still similar to the original watermark data. Thus, it can be concluded that the infographic contain valid watermark.

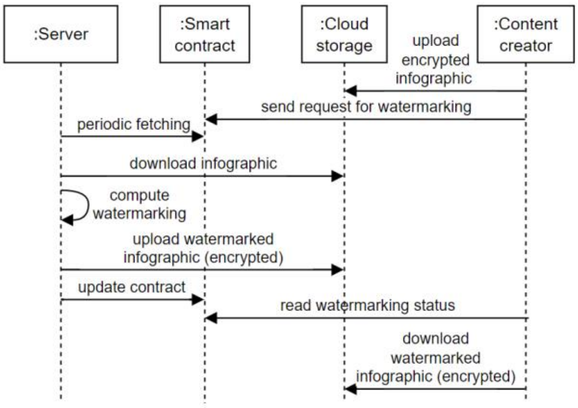


Fig.3. Sequence diagram of the infographic watermarking request

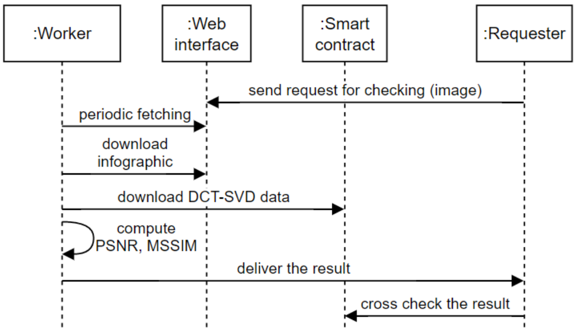


Fig.4. Sequence diagram of the infographic validation using two-factor verification

The verification consists of two factors, intrinsic verification by referring to the embedded watermark and extrinsic verification by referring to the smart contract data. First, the server will extract the embedded watermark by comparing the submitted image with the original one submitted by the requester. After retrieving the watermark image, the server computes the structural similarity index of the extracted watermark compared to the original watermark.

At last, the server delivers the result to the user containing three data: 1) the content ID and smart contract address, 2) the MSSIM value of the extracted watermark, and 3) the validation status, either valid or invalid.

III. RESULT

A. DCT-SVD Watermarking

We implemented DCT-SVD watermarking (1 - 5) using python and the source code is available at [17]. Fig. 5 shows the tested images that consist of the original image (info5_ori.png), watermark data (satgas.png) and the result or the watermarked image (info5.png).

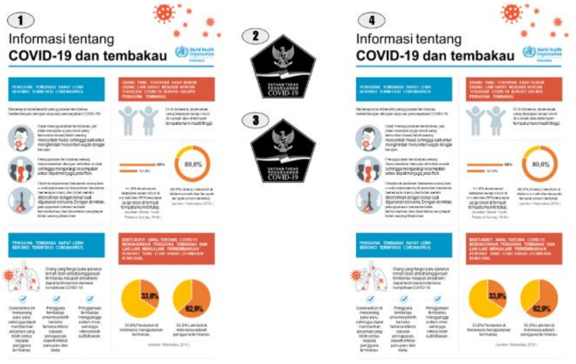


Fig.5. From left to right, 1) Original image, 2) embedded, 3) extracted watermark image, and 4) the result or the watermarked image.

For evaluation, we tested the watermarking quality by observing the original image and the watermarked image correspond to the PSNR, and similarity index (MSSIM). The results are depicted in Table 1. The PSNR values > 60 indicated that image quality is still preserved, even though extra watermark data has been embedded. Meanwhile, the MSSIM value is close to 1 indicating that watermark data is similar to the original form. It can be embedded and extracted successfully without losing significant data in the process.

Table 1. Watermarking quality

Parameter	Value
PSNR	66.56885716426036
MSSIM	0. 9999817

B. Blockchain-driven Watermarking

We implemented the smart contract using solidity and the source code is available at [18]. We tested the smart contract to do five main functions: deploy the contract, add admin, add user, add content, and set the watermark.

We run the experiment on four Ethereum test networks namely Ropsten, Rinkeby, Goerli, and Kovan. The parameters to send the blockchain transaction are presented in Table 2. The admins refer to the watermarking authority while the creator refers to the infographic creator. We use Google drive to deliver the infographics and watermarked results between the creator and authority. For the infographic image, we use the image available at the content URL and the watermarking result will be available at watermarking URL. Both images are encrypted using RSA public keys that are stored in the smart contract.

Table 2. Experiment parameters

Parameter	Value
Admin1	0xa5C64A61D225Bc5614a2CE5fAc81926438e93844
Admin2	0x1C49AA3FEAb57bc27Ad79F0De64862786766F611
Creator1	0x5F380aC8878881f9bf846A066911D4e38fF57BA0
Content URL	gdrive: 1sxOPdIqV3-50rbR9fFxTiSkKra7px-2e
Watermark URL	gdrive: 1YDFqhgycNIWkrfSOv3cgzTS3FvHmzAPw
Image hash	2d4e998045c70a422549943f9d0d8b6c1de9c23c98c733cecfe32dc922920cad6a5d025de338bf05f5993caee3cba94847bf9fc52335e6a0967b3df385748453

Table 3. Experiment Scenarios

Transaction	Function	Value
Deploy	Sender	Admin1
	Name	"Infographic Watermarking"
Add Admin	Sender	Admin1
	New admin	Admin2
Add User	Sender	Admin1
	New user	Creator1
Add Content	Sender	Creator1
	Image hash	Image hash*
	URL Content	Content URL*
	Admin Id	1
Set Watermark	Sender	Admin1
	URL wmark	Watermark URL*
	index	1

*) The value refers to the Table 2

Table 3 describes the testing scenario for the smart contract. Each transaction has a sender that sends the contract transaction to the blockchain network. The sender calls the respective function by embedding the function parameters into the transaction. As a result, we have deployed the contract to each of the test networks as shown in Table 4.

The goal of using blockchain is to maintain the transparency of the watermarking process. Everyone can monitor the watermarking transactions, either for request or approval, by scanning the transaction from the respective blockchain explorer. The blockchain explorer for the Ethereum test network can be accessed using the format of "https://<name of network>.etherscan.io", where the name of the network refers to the test network field in Table 3.

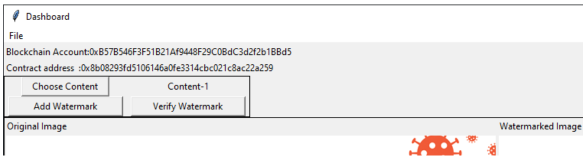
Table 4. Deployment Result

Test Network	***The addresses of the deployed contract***
ropsten	0xb34848064D59BaFa5CAac21b7E9bF3Ecd8c969FF
rinkeby	0x2f05c02F3529665c6a4A25941305A10b178A43F0
goerli	0xA3CEFc93C69053694C69b08255f1c87bA628fa9B
kovan	0xb34848064D59BaFa5CAac21b7E9bF3Ecd8c969FF

C. Watermarking Server

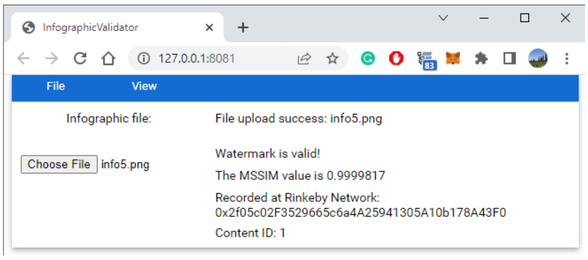
We developed the watermarking server based on python using Remi library for the webserver and Tkinter library for the dashboard. Fig. 6 shows the dashboard for the user interface of the watermarking authority. The program must be run manually to assign the watermarking to the infographic. The program automatically downloads the watermarking request from the smart contract and populates the infographic into the internal database.

The authority must inspect the request manually for content incorrectness or inaccuracies lies within the infographic. The "choose content" button only displays the unauthorized request. If the infographic passes manual verification, the authority can embed the watermark by using the "add watermark" button. The "verify watermark" button acts as a testing purpose to compare the watermarked version with the original infographic. After local verification, the watermarking result will be updated accordingly. The program will upload the watermark version to Google drive and send “set watermark” transaction to the smart contract.



Dashboard
File
Blockchain Account:0xB57B546F3F51B21Af9448F29C0BdC3d2f2b1BBd5
Contract address :0x8b08293fd5106146a0fe3314cbc021c8ac22a259

Fig.6. Dashboard for the watermarking server



Infographic file: info5.png

File upload success: info5.png

Watermark is valid!

The MSSIM value is 0.9999817

Recorded at Rinkeby Network: 0x2f05c02F3529665c6a4A25941305A10b178A43F0

Content ID: 1

Fig.7. Web-based validation for infographic and its result.

Fig. 7 depicts the webserver that runs the infographic validation service. The user can upload the intended infographic for validation using “Choose File” button. Upon receiving the uploaded infographic, the server will extract the watermarking image, and compute the MSSIM. At last, it informed the user regarding the status of the infographic that consists of three records: 1) the verification status, 2) the MSSIM value of the embedded watermark, and 3) if the infographic is valid, the address of the smart contract and content Id of the watermarking request.

IV. DISCUSSION

The discussion covers the efficiency and ease of use of the proposed method on different Ethereum test networks.

Fig. 8 depicts the total gas usage of smart contract transactions from the four test networks. The total gas usage is exactly the same since the data send by the transaction is the same (Table 3). The gas used by a smart contract transaction depends on the bytes representation of the transaction data. In Ethereum, a zero-byte costs less gas than non-zeros. Fig. 8 shows two transactions that carry different data that result in different gas usage by the transaction. As a recap, all of the test networks have exactly similar efficiency in terms of transaction fee or Ethers’ consumption.

Besides the efficiency, the affecting factor of using Ethereum test networks is its ease of use. Table 5 accounts for the comparison of the test network in terms of how the user receives free Ethers for sending any transactions.

Rinkeby test network has the highest daily free ether compared to other test networks. However, the Rinkeby faucet requires social media account such as Twitter and Facebook which is less convenient.

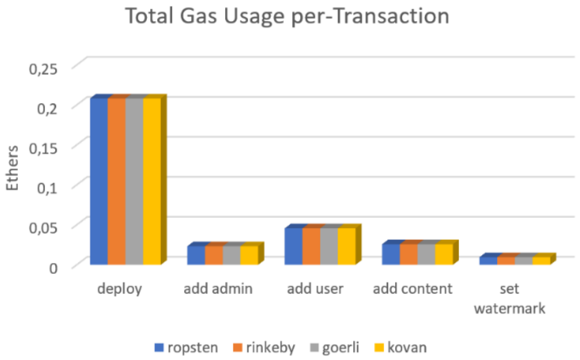


Fig.8. Comparison of Total gas usage by the Test Networks

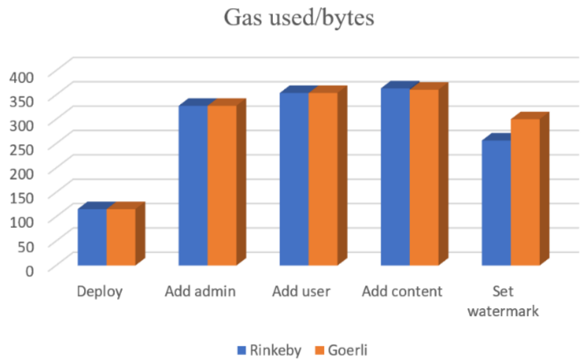


Fig.9. Gas usage over different data value

Table 5. Ease of Use Comparison

Test network	Daily Ethers	User Access	URL
ropsten	0.3	Account address	https://faucet.ropsten.be
	1.0	Account address	https://faucet.metamask.io
rinkeby	7.5	Twitter/ Facebook	https://faucet.rinkeby.io
goerli	1.0	Twitter/ Facebook	https://faucet.goerli.mudit.blog
	0.05	Account address	https://goerli-faucet.slock.it/
kovan	0.0014	Twitter, github, gitlab	https://gitter.im/kovan-testnet/faucet
	0.0014	Account address	https://ethdrop.dev

A more flexible scheme is offered by Ropsten and Goerli networks that provide both, account address and social media access, to receive free Ethers. The received ethers are smaller compared to the Rinkeby network but the amount is sufficient to send one infographic watermarking request at a daily rate (Fig. 8).

The Kovan network has smaller free daily ether available for the user. It makes the Kovan network the less attractive option to deploy the smart contract. The free Ethers of 0.0014 per day is far lesser compared to 0.2 ethers for contract deployment (Fig. 9).

All in all, Ropsten and Goerli networks if the most preferred option while Rinkeby networks come at second. The Kovan is not preferred as it takes time to accumulate ether to send a smart contract transaction.

V. CONCLUSSION

This paper presented a protection system to ensure Infographic integrity and validity by using a smart contract and DCT-SVD watermarking. The DCT-SVD ensure the practical implementation of watermarking by using singular value addition. It also retains the image quality indicated by the high value of PSNR and MSSIM. Meanwhile, the smart contract provides transparent watermarking request management that enables public monitoring. Anyone can trace the process by observing the process from blockchain explorer.

We have tested the system on four different Ethereum test networks, namely Ropsten, Rinleby, Goerli, and Kovan. The most preferred option is to use Ropsten and Goerli network that lets the watermarking requester receive free Ethers by using only the account address. The Rinkeby network is more suitable for frequent watermarking requests since it offers higher free ethers on daily basis. The Kovan network is the least option to implement the proposed system.

REFERENCES

[1] A. Atalan, “Is the lockdown important to prevent the covid-19pandemic? effects on psychology, environment and economy-perspective,”Annals of medicine and surgery, vol. 56, pp. 38–42,2020.

[2] A. Haleem, M. Javaid, and R. Vaishya, “Effects of covid-19pandemic in daily life,”Current medicine research and practice,vol. 10, no. 2, p. 78, 2020.

[3] W.Bank,“2020-yearinreview:Theimpactofcovid-19in12charts,”Oct.2021.[Online].Available: https://blogs.worldbank.org/voices/2020-year-review-impact-covid-19-12-charts

[4] J. J. Otten, K. Cheng, and A. Drewnowski, “Infographics andpublic policy: using data visualization to convey complex infor-mation,”Health Affairs, vol. 34, no. 11, pp. 1901–1907, 2015.

[5] M. Egan, A. Acharya, V. Sounderajah, Y. Xu, A. Mottershaw,R. Phillips, H. Ashrafian, and A. Darzi, “Evaluating the effect ofinfographics on public recall, sentiment and willingness to useface masks during the covid-19 pandemic: a randomised internet-based questionnaire study,”BMC public health, vol. 21, no. 1,pp. 1–10, 2021.

[6] C. Jerome, S.-H. Ting, and Y. Podin, “Getting the messageacross: Examining malaysia’s covid-19 public service announce-ment (psa) infographics,”International Journal of Business andSociety, vol. 22, no. 1, pp. 194–212, 2021.

[7] E. K. Vraga and L. Bode, “Addressing covid-19 misinformationon social media preemptively and responsively,”Emerging infec-tious diseases, vol. 27, no. 2, p. 396, 2021.

[8] Deng, M., Bianchi, T., Piva, A., & Preneel, B. (2009, September). An efficient buyer-seller watermarking protocol based on composite signal representation. In Proceedings of the 11th ACM Workshop on Multimedia and Security (pp. 9-18).Re

[9] Seong, T. Y., Kwon, K. C., Lee, S. H., Moon, K. S., & Kwon, K. R. (2014). DCT and Homomorphic Encryption based Watermarking Scheme in Buyer-seller Watermarking Protocol. *Journal of Korea Multimedia Society*, *17*(12), 1402-1411.

[10] Rial, A., Deng, M., Bianchi, T., Piva, A., & Preneel, B. (2010). A provably secure anonymous buyer–seller watermarking protocol. IEEE Transactions on Information Forensics and Security, 5(4), 920-931

[11] Meng, Z., Morizumi, T., Miyata, S., & Kinoshita, H. (2018, July). Design scheme of copyright management system based on digital watermarking and blockchain. In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC) (Vol. 2, pp. 359-364). IEEE.

[12] Dwivedi, A. D. (2019). A scalable blockchain based digital rights management system. Cryptology ePrint Archive.

[13] Frattolillo, F. (2020). A watermarking protocol based on Blockchain. Applied Sciences, 10(21), 7746.

[14] D. S. Chandra, “Digital image watermarking using singularvalue decomposition,” inThe 2002 45th Midwest Symposium onCircuits and Systems, 2002. MWSCAS-2002., vol. 3. IEEE, 2002,pp. III–III.

[15] D . Rosiyadi, S.-J. Horng, P. Fan, X. Wang, M. K. Khan, andY. Pan, “Copyright protection for e-government document im-ages,”IEEE MultiMedia, vol. 19, no. 3, pp. 62–73, 2011.

[16] Etehreum, “Ethereum (eth) blockchain explorer,” Oct. 2021.[Online]. Available: https://etherscan.io/

[17] *“DCT-SVD.py” Dec. 2021 [Online]. Available at* https://github.com/DSRGBRIN/Image-Watermarking/blob/main/codes/hints/DCT-SVD.py

[18] *“SecuringInfographic-Vicochain.sol” Oct. 2021 [Online]. Available at* https://github.com/ DSRGBRIN/SecuringInfographic/blob/main/Solidity/ VICoChain.sol

JURNAL INFOTEL

Informatics, Telecommunication, and Electronics

Volume 14, Number 2 May 2022

PEER REVIEWERS ACKNOWLEDGEMENT

We, as editors of Jurnal INFOTEL, would like to thank the reviewers who have taken time, effort and thought to provide reviews and assessments of articles in the Jurnal INFOTEL. These reviews and assessments have a good impact on improving the quality of articles published in this Journal. The followings are the reviewers :

Dwi Ely Kurniawan, S.Pd., M.Kom.

Politeknik Negeri Batam, Indonesia

Email : dwialikhs@polibatam.ac.id

Google Scholar ID : zHpp5s0AAAAJ

Scopus ID : 57200983756

Dr. Arta Moro Sundjaja., S.Kom., S.E., MM

Universitas Bina Nusantara, Indonesia

Google Scholar ID : Bob96GEAAAAJ

Scopus ID : 55858212100

Daniel Yeri Kristiyanto, S.Kom., M.Si., M.Kom

Institut Teknologi Telkom Purwokerto

Google Scholar ID : qvtc8_EAAAAJ

Scopus ID :

Prof. Dr. Eng. Retno Supriyanti, S.T.,M.T

Universitas Jenderal Soedirman, Indonesia

Google Scholar ID : vUJQJu4AAAAJ

Scopus ID : 24332824200Fahrul Agus

Farah Zakiyah Rahmanti, S.ST., M.T.

Institut Teknologi Telkom Surabaya, Indonesia

Google Scholar ID : 0RiyjfoAAAAJ

Scopus ID : 56027742300

Rafina Destiarti Ainul, S.ST.,M.T

Universitas Surabaya, Indonesia

Google Scholar ID : yYCxvPsAAAAJ

Scopus ID : 57189387798

Dr. Wahyu Pamungkas, S.T., M.T.

Institut Teknologi Telkom Purwokerto, Indonesia

Google Scholar ID : UyMg3zQAAAAJ

Scopus ID : 57203096241

Eko Fajar Cahyadi, S.T., M.T.

Institut Teknologi Telkom Purwokerto

Google Scholar ID : H9l4TIMAAAAJ

Scopus ID :

H. Arief Goeritno, S.T., M.T.

Universitas Ibn Khaldun Bogor, Indonesia

Google Scholar ID : H06e6fQAAAAJ

Scopus ID : 57194647547

JURNAL INFOTEL

Informatics, Telecommunication, and Electronics

Volume 14, Number 2 May 2022

GUIDELINES FOR AUTHOR

A. General Guidelines

General guidelines for writing in JURNAL INFOTEL are as follows :

- Written in English
- The length of submitted paper is at least 6 pages and no more than 12 pages. If the number of pages more than 12 will incurred extra charges
- Make sure that your paper is prepared using the Manuscript Template and Copyright Transfer Form when if it accepted
- At least 15 references with 80% coming from the original research article (Journal)

B. Guidelines for The Manuscript Body Text

Scientific articles will be published in the JURNAL INFOTEL must follow the rules of writing on the paper body. The rules follow the pattern of IMRAD (Introduction, Method, Result, and Discussion) added the last section is conclusion section.

Title : The title should be concise and indicate the identity of the subject, the research objectives, and keywords.

Author name : The author's name without academic degrees and not preceded by the word "by" followed by the name of the institution, address of institution and contact email.

Abstract : Abstract should describe the entire content of the article with maximum of 250 word. It is not allowed references to figures and tables. it is written in a straightforward, concise, and must include:

- Background (optional, one or two sentence)
- Research objective
- Method
- Result
- Conclusion

Keyword : Use keywords can describe the content of article. It is written in 3 to 5 words.

Introduction : Basically, in the introduction provides general background research, literature review (state of the art), originality of research (gap analysis), and research objectives. In the literature review, there are at least five articles reviewed briefly that can justify the novelty of the research.

Method : In the methods section provides a summary of the methods used, such as the subjects studied, tools and materials used, model or design used, sampling technique, the measured variable, analysis and statistical models used.

Result : In the results section contains the presentation of the results of research can be illustrated using tables or figures to clarify the presentation of the results verbally. The data presented is data that is processed, not raw data.

Discussion : material discussion mainly concerned, whether the results are consistent with the hypothesis or not, and put forward the argument.

Conclusion : write the conclusions of the research that has been done and future works. The conclusion must answer the purpose of the study or hypothesis. Write the conclusion briefly and clearly. Do not discuss again at the conclusion. Do not use Bullet / Numbering.

Style referral source citations in Jurnal INFOTEL using **IEEE style**. It is advisable to use a reference management software such as **Mendeley, EndNote, Zotero** and others.

Jurnal Penelitian dan Pengembangan INFOTEL
Sekretariat :

KANTOR LPPM
SEKOLAH TINGGI TEKNOLOGI TELEMATIKA TELKOM PURWOKERTO
Jl. D.I. Panjaitan No. 128 Purwokerto 53157
Telp. 0281 641629 | Fax. 0281 641630 | Email : infotel@st3telkom.ac.id | Homepage : ejournal.st3telkom.ac.id

9 772085 368009