BUKTI KORESPONDENSI ARTIKEL
PADA JURNAL INTERNASIONAL BEREPUTASI

PENGUSUL

Dr. Alamsyah, S.Si., M.Kom / NIDN 0017057409

UNIVERSITAS NEGERI SEMARANG
TAHUN 2022

Yth. Penilai Pada Usulan PAK

Bersama dengan surat ini, saya bermaksud menyertakan bukti bukti korespondensi proses review artikel pada Jurnal Internasional dan Jurnal Terakreditasi Sinta 2 dengan judul:

> Data Hiding Security Using Bit Matching-Based Steganography and Cryptography Without Change The Stego Image Quality, dimuat pada Journal of Theoretical and Applied Information Technology, Vol. 82, No. 1, Desember 2015, p-ISSN : 1817-3195, e-ISSN : 1992-8645, Hal: 106 – 112 (Jurnal Internasional Bereputasi).

Adapun susunan kronologi bukti korespondensi terdiri dari beberapa poin, pada tabel di bawah ini:

No	Tanggal	Aktivitas
1	29 Agustus 2015	Submit manuskrip pertama kali
2	29 Agustus 2015	Pemberian nomor ID manuskrip (Paper ID: 28489-JATIT)
3	14 September 2015	Paper diterima setelah dilakukan peer double blind review
4	14 September 2015	Pemberitahuan hasil internal review diterima dan direkomendasikan ke external review
5	14 September 2015	Pemberitahuan hasil evaluasi external review merekomendasikan paper diterima tanpa revisi.
6	14 September 2015	Pemberitahuan agar paper disesuaikan dengan template yang telah disediakan
7	14 September 2015	Pemberitahuan copyright dokumen yang harus ditandatangani oleh penulis
8	14 September 2015	Pemberitahuan biaya publikasi
9	10 Desember 2015	Publikasi artikel

Demikian, agar dapat menjadi periksa.

Terimakasih

Semarang, 1 Februari 2022

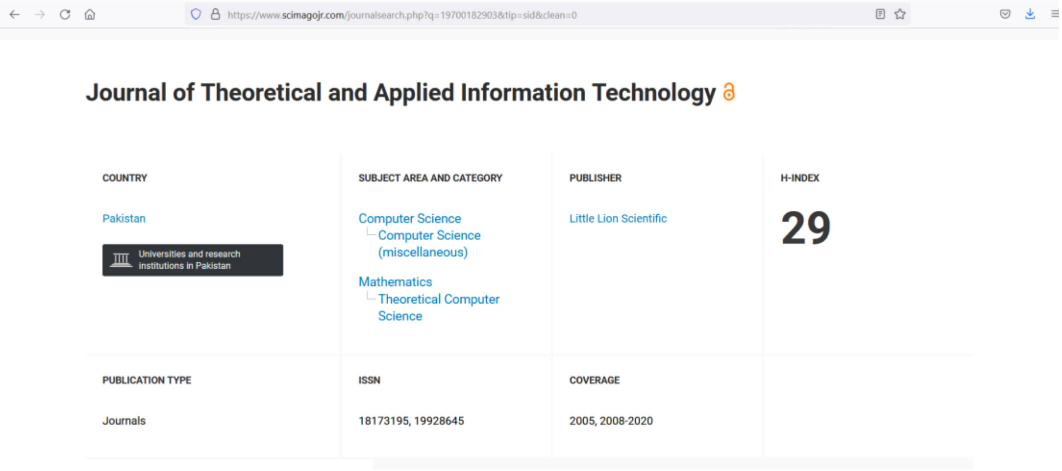
Hormat saya,

Dr. Alamsyah., S.Si., M.Kom

KRONOLOGI KORESPONDENSI PUBLIKASI ARTIKEL PADA JURNAL INTERNASIONAL BEREPUTASI DAN BERFAKTOR DAMPAK

Judul	:	Data Hiding Security Using Bit Matching-Based Steganography and Cryptography Without Change The Stego Image Quality
Jurnal	:	Journal of Theoretical and Applied Information Technology
Volume	:	82
Nomor	:	1
Tanggal Publikasi	:	10 Desember 2015
ISSN (p)	:	1817-3195
ISSN (e)	:	1992-8645
Hal	:	106-112
Penerbit	:	Little Lion Scientific
SJR Jurnal	:	0,15 (2020)
Quartile	:	Q4 (Scopus)
Cite Score	:	1,3
Penulis	:	Alamsyah, Much Aziz Muslim, Budi Prasetiyo

Bukti indexing jurnal:

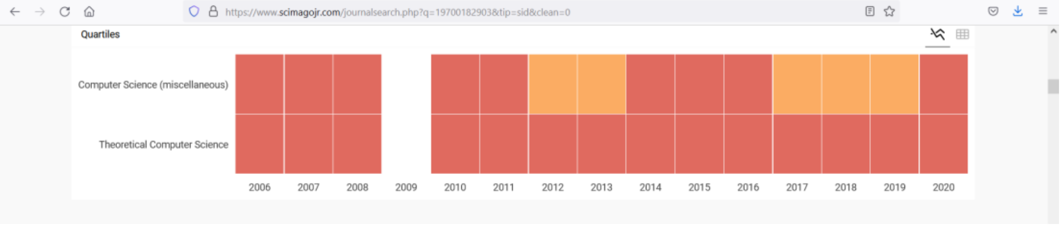


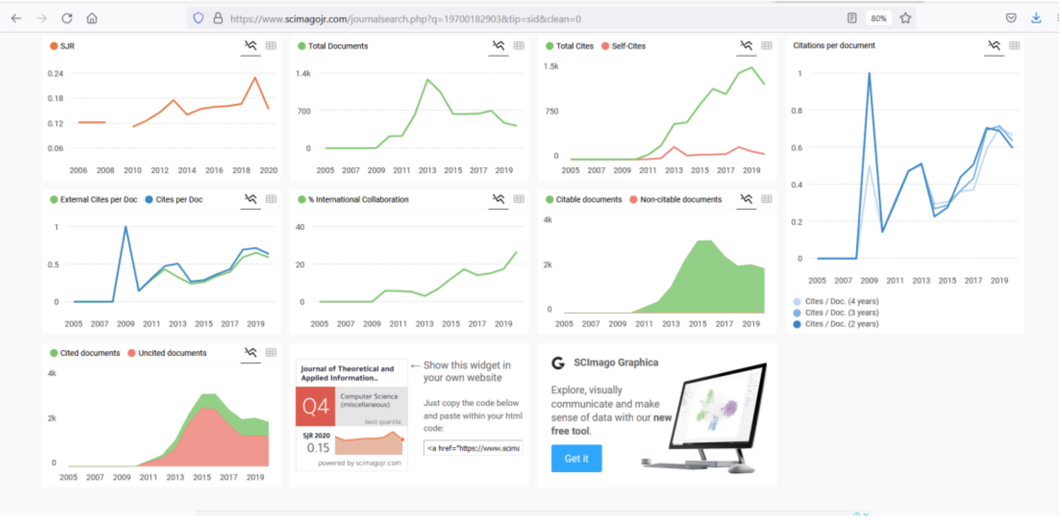
https://www.scimagojr.com/journalsearch.php?q=19700182903&tip=sid&clean=0

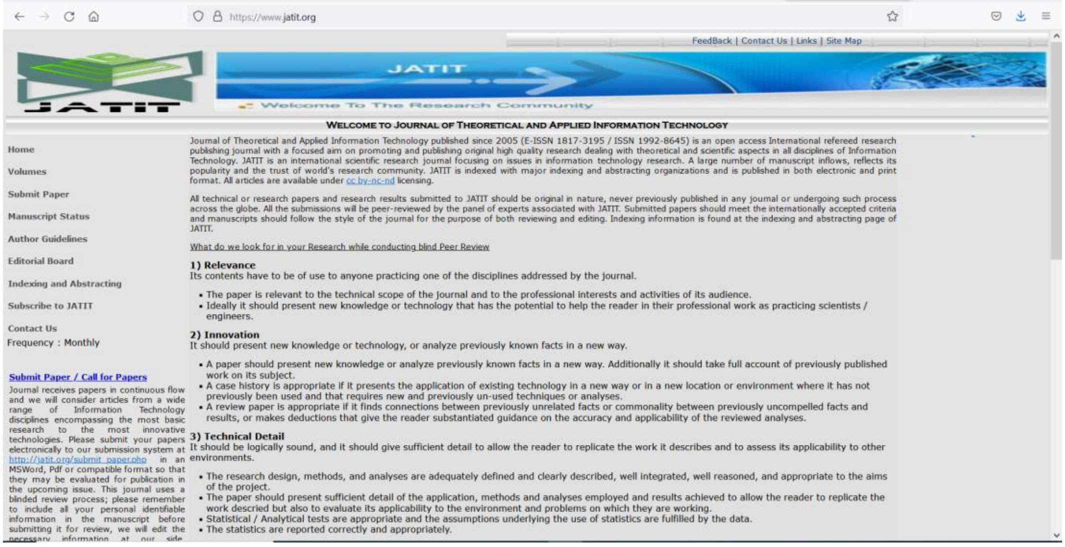
Journal of Theoretical and Applied Information Technology

COUNTRY	SUBJECT AREA AND CATEGORY	PUBLISHER	H-INDEX
Pakistan Universities and research institutions in Pakistan	Computer Science └ Computer Science (miscellaneous) Mathematics └ Theoretical Computer Science	Little Lion Scientific	29

PUBLICATION TYPE	ISSN	COVERAGE
Journals	18173195, 19928645	2005, 2008-2020







WELCOME TO JOURNAL OF THEORETICAL AND APPLIED INFORMATION TECHNOLOGY

Journal of Theoretical and Applied Information Technology published since 2005 (E-ISSN 1817-3195 / ISSN 1992-8645) is an open access International refereed research publishing journal with a focused aim on promoting and publishing original high quality research dealing with theoretical and scientific aspects in all disciplines of Information Technology. JATIT is an international scientific research journal focusing on issues in information technology research. A large number of manuscript inflows, reflects its popularity and the trust of world's research community. JATIT is indexed with major indexing and abstracting organizations and is published in both electronic and print format. All articles are available under cc by-nc-nd licensing.

All technical or research papers and research results submitted to JATIT should be original in nature, never previously published in any journal or undergoing such process across the globe. All the submissions will be peer-reviewed by the panel of experts associated with JATIT. Submitted papers should meet the internationally accepted criteria and manuscripts should follow the style of the journal for the purpose of both reviewing and editing. Indexing information is found at the indexing and abstracting page of JATIT.

What do we look for in your Research while conducting blind Peer Review

1) Relevance
Its contents have to be of use to anyone practicing one of the disciplines addressed by the journal.

- The paper is relevant to the technical scope of the journal and to the professional interests and activities of its audience.
- Ideally it should present new knowledge or technology that has the potential to help the reader in their professional work as practicing scientists / engineers.

2) Innovation
It should present new knowledge or technology, or analyze previously known facts in a new way.

- A paper should present new knowledge or analyze previously known facts in a new way. Additionally it should take full account of previously published work on its subject.
- A case history is appropriate if it presents the application of existing technology in a new way or in a new location or environment where it has not previously been used and that requires new and previously un-used techniques or analyses.
- A review paper is appropriate if it finds connections between previously unrelated facts or commonality between previously uncompelled facts and results, or makes deductions that give the reader substantiated guidance on the accuracy and applicability of the reviewed analyses.

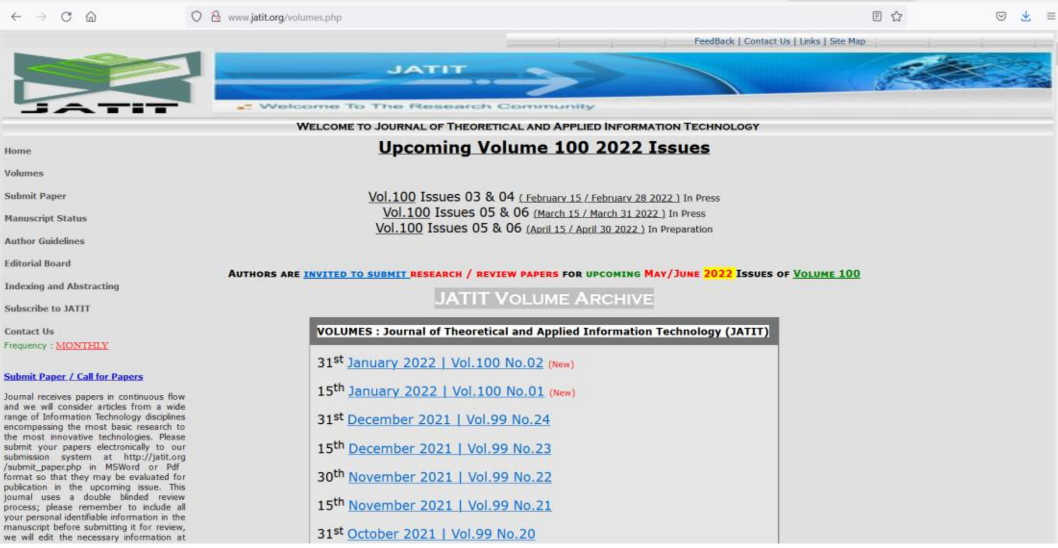
3) Technical Detail
It should be logically sound, and it should give sufficient detail to allow the reader to replicate the work it describes and to assess its applicability to other environments.

- The research design, methods, and analyses are adequately defined and clearly described, well integrated, well reasoned, and appropriate to the aims of the project.
- The paper should present sufficient detail of the application, methods and analyses employed and results achieved to allow the reader to replicate the work descried but also to evaluate its applicability to the environment and problems on which they are working.
- Statistical / Analytical tests are appropriate and the assumptions underlying the use of statistics are fulfilled by the data.
- The statistics are reported correctly and appropriately.

Frequency : Monthly

Submit Paper / Call for Papers

Journal receives papers in continuous flow and we will consider articles from a wide range of Information Technology disciplines encompassing the most basic research to the most innovative technologies. Please submit your papers electronically to our submission system at http://jatit.org/submit_paper.php in an MSWord, Pdf or compatible format so that they may be evaluated for publication in the upcoming issue. This journal uses a blinded review process; please remember to include all your personal identifiable information in the manuscript before submitting it for review, we will edit the necessary information at our side



Welcome to Journal of Theoretical and Applied Information Technology

Upcoming Volume 100 2022 Issues

Vol.100 Issues 03 & 04 (February 15 / February 28 2022) In Press
Vol.100 Issues 05 & 06 (March 15 / March 31 2022) In Press
Vol.100 Issues 05 & 06 (April 15 / April 30 2022) In Preparation

Authors are invited to submit research / review papers for upcoming May/June 2022 Issues of Volume 100

JATIT Volume Archive

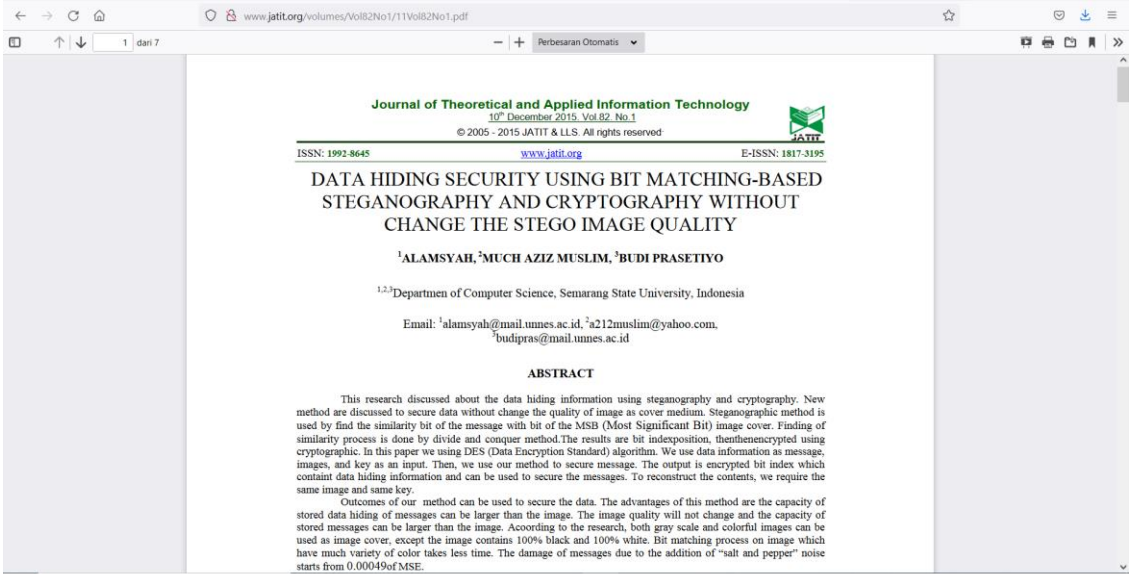
VOLUMES : Journal of Theoretical and Applied Information Technology (JATIT)

31st January 2022 | Vol.100 No.02 (New)
15th January 2022 | Vol.100 No.01 (New)
31st December 2021 | Vol.99 No.24
15th December 2021 | Vol.99 No.23
30th November 2021 | Vol.99 No.22
15th November 2021 | Vol.99 No.21
31st October 2021 | Vol.99 No.20

Frequency : MONTHLY

Submit Paper / Call for Papers

Journal receives papers in continuous flow and we will consider articles from a wide range of Information Technology disciplines encompassing the most basic research to the most innovative technologies. Please submit your papers electronically to our submission system at http://jatit.org /submit_paper.php in MSWord or Pdf format so that they may be evaluated for publication in the upcoming issue. This journal uses a double blinded review process; please remember to include all your personal identifiable information in the manuscript before submitting it for review, we will edit the necessary information at



Journal of Theoretical and Applied Information Technology
10th December 2015. Vol.82. No.1
© 2005 - 2015 JATIT & LLS. All rights reserved·

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DATA HIDING SECURITY USING BIT MATCHING-BASED STEGANOGRAPHY AND CRYPTOGRAPHY WITHOUT CHANGE THE STEGO IMAGE QUALITY

[1]ALAMSYAH, [2]MUCH AZIZ MUSLIM, [3]BUDI PRASETIYO

[1,2,3]Departmen of Computer Science, Semarang State University, Indonesia

Email: [1]alamsyah@mail.unnes.ac.id, [2]a212muslim@yahoo.com,
[3]budipras@mail.unnes.ac.id

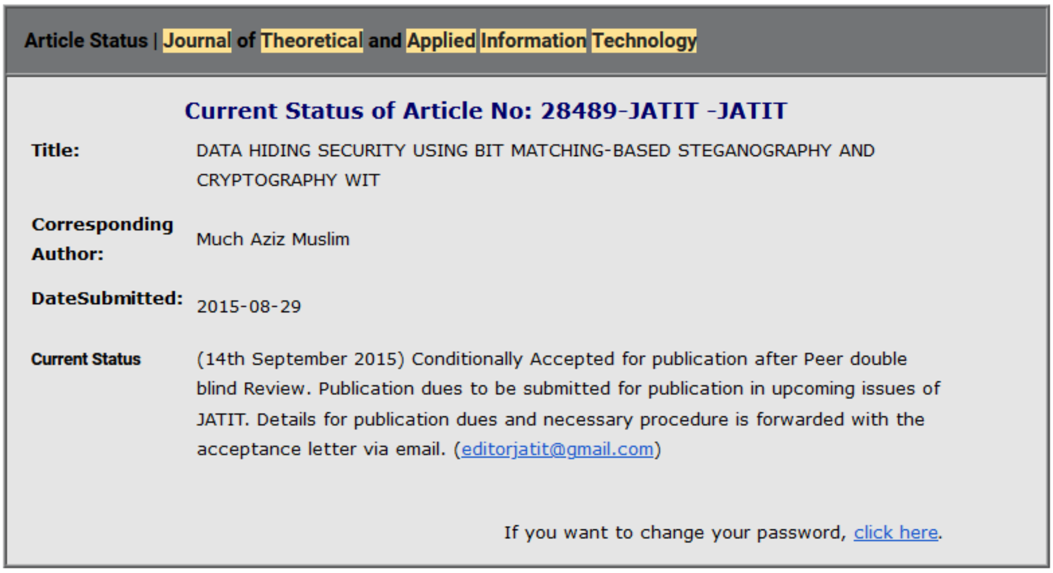
ABSTRACT

This research discussed about the data hiding information using steganography and cryptography. New method are discussed to secure data without change the quality of image as cover medium. Steganographic method is used by find the similarity bit of the message with bit of the MSB (Most Significant Bit) image cover. Finding of similarity process is done by divide and conquer method.The results are bit indexposition, thenthenencrypted using cryptographic. In this paper we using DES (Data Encryption Standard) algorithm. We use data information as message, images, and key as an input. Then, we use our method to secure message. The output is encrypted bit index which containt data hiding information and can be used to secure the messages. To reconstruct the contents, we require the same image and same key.

Outcomes of our method can be used to secure the data. The advantages of this method are the capacity of stored data hiding of messages can be larger than the image. The image quality will not change and the capacity of stored messages can be larger than the image. Acoording to the research, both gray scale and colorful images can be used as image cover, except the image contains 100% black and 100% white. Bit matching process on image which have much variety of color takes less time. The damage of messages due to the addition of “salt and pepper” noise starts from 0.00049of MSE.

RINCIAN KRONOLOGIS SEBAGAI BUKTI KORESPONDENSI ARTIKEL PADA JURNAL INTERNASIONAL BEREPUTASI

Submit manuskrip pertama kali ke jurnal dan mendapatkan ID manuskrip (Paper ID: 28489-JATIT) [29 Agustus 2015]



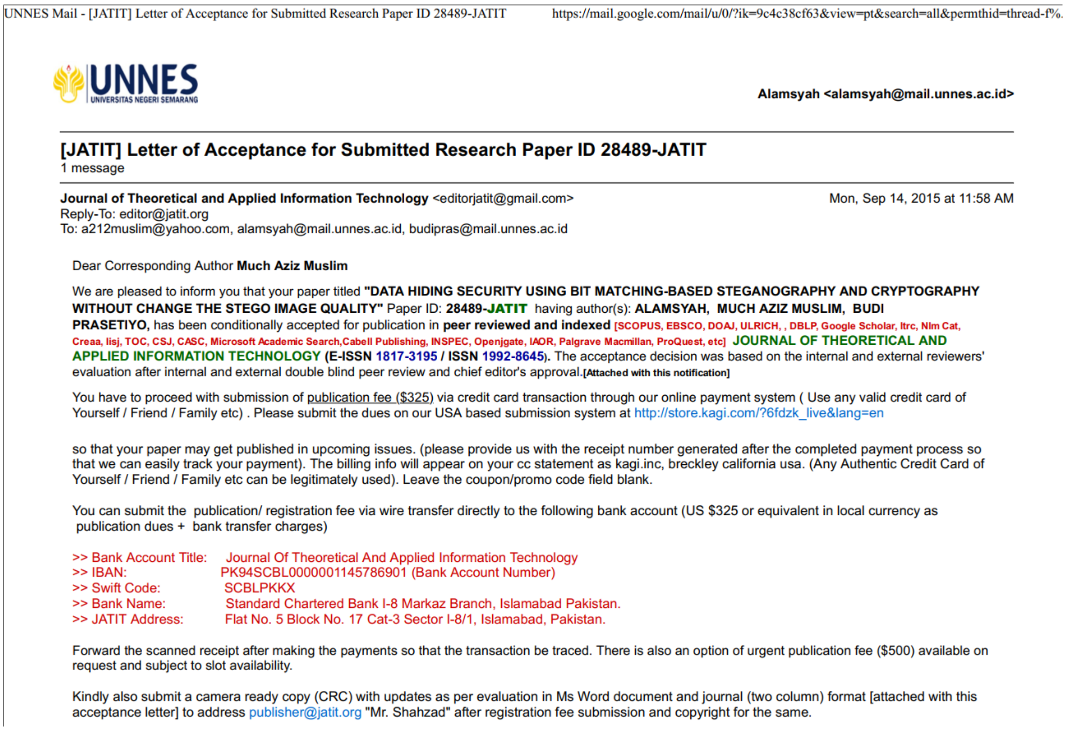
Article Status | Journal of Theoretical and Applied Information Technology

Current Status of Article No: 28489-JATIT -JATIT

Title:	DATA HIDING SECURITY USING BIT MATCHING-BASED STEGANOGRAPHY AND CRYPTOGRAPHY WIT
Corresponding Author:	Much Aziz Muslim
DateSubmitted:	2015-08-29
Current Status	(14th September 2015) Conditionally Accepted for publication after Peer double blind Review. Publication dues to be submitted for publication in upcoming issues of JATIT. Details for publication dues and necessary procedure is forwarded with the acceptance letter via email. (editorjatit@gmail.com)

If you want to change your password, click here.

Paper diterima setelah dilakukan peer double blind review [14 September 2015]



Alamsyah <alamsyah@mail.unnes.ac.id>

[JATIT] Letter of Acceptance for Submitted Research Paper ID 28489-JATIT
1 message

Journal of Theoretical and Applied Information Technology <editorjatit@gmail.com> Mon, Sep 14, 2015 at 11:58 AM
Reply-To: editor@jatit.org
To: a212muslim@yahoo.com, alamsyah@mail.unnes.ac.id, budipras@mail.unnes.ac.id

Dear Corresponding Author **Much Aziz Muslim**

We are pleased to inform you that your paper titled **"DATA HIDING SECURITY USING BIT MATCHING-BASED STEGANOGRAPHY AND CRYPTOGRAPHY WITHOUT CHANGE THE STEGO IMAGE QUALITY"** Paper ID: **28489-JATIT** having author(s): **ALAMSYAH, MUCH AZIZ MUSLIM, BUDI PRASETIYO,** has been conditionally accepted for publication in **peer reviewed and indexed** **[SCOPUS, EBSCO, DOAJ, ULRICH, , DBLP, Google Scholar, Itrc, Nlm Cat, Creaa, Iisj, TOC, CSJ, CASC, Microsoft Academic Search,Cabell Publishing, INSPEC, Openjgate, IAOR, Palgrave Macmillan, ProQuest, etc]** **JOURNAL OF THEORETICAL AND APPLIED INFORMATION TECHNOLOGY (E-ISSN 1817-3195 / ISSN 1992-8645).** The acceptance decision was based on the internal and external reviewers' evaluation after internal and external double blind peer review and chief editor's approval.**[Attached with this notification]**

You have to proceed with submission of publication fee ($325) via credit card transaction through our online payment system (Use any valid credit card of Yourself / Friend / Family etc) . Please submit the dues on our USA based submission system at http://store.kagi.com/?6fdzk_live&lang=en

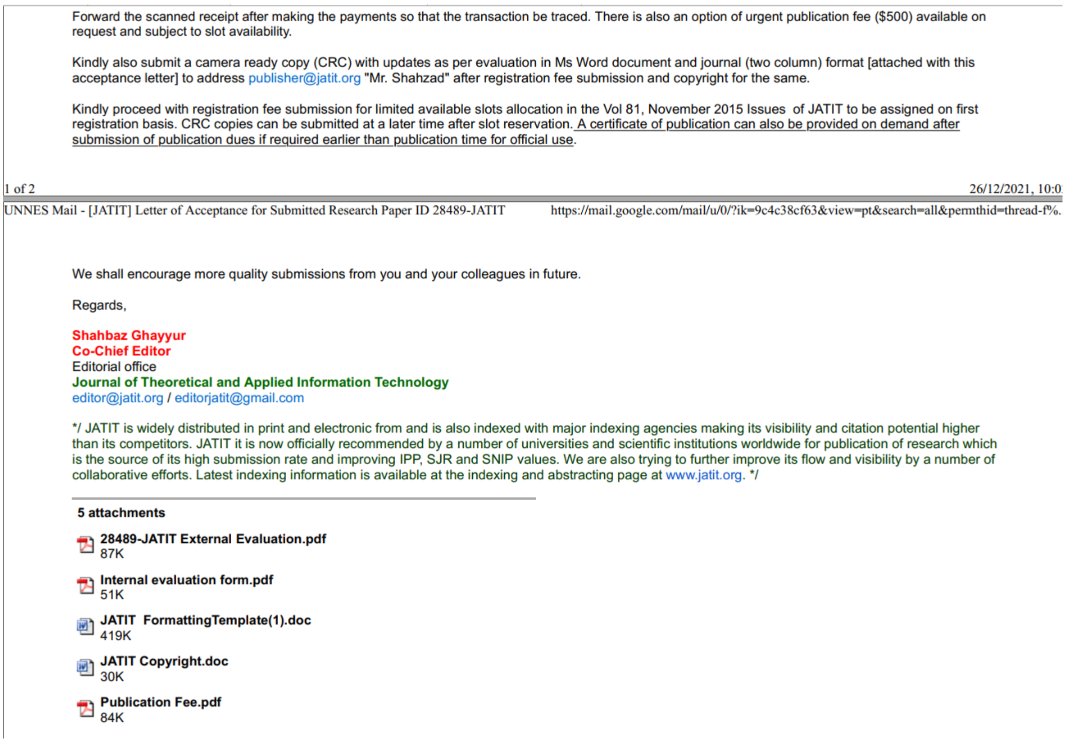
so that your paper may get published in upcoming issues. (please provide us with the receipt number generated after the completed payment process so that we can easily track your payment). The billing info will appear on your cc statement as kagi.inc, breckley california usa. (Any Authentic Credit Card of Yourself / Friend / Family etc can be legitimately used). Leave the coupon/promo code field blank.

You can submit the publication/ registration fee via wire transfer directly to the following bank account (US $325 or equivalent in local currency as publication dues + bank transfer charges)

>> Bank Account Title:	Journal Of Theoretical And Applied Information Technology
>> IBAN:	PK94SCBL0000001145786901 (Bank Account Number)
>> Swift Code:	SCBLPKKX
>> Bank Name:	Standard Chartered Bank I-8 Markaz Branch, Islamabad Pakistan.
>> JATIT Address:	Flat No. 5 Block No. 17 Cat-3 Sector I-8/1, Islamabad, Pakistan.

Forward the scanned receipt after making the payments so that the transaction be traced. There is also an option of urgent publication fee ($500) available on request and subject to slot availability.

Kindly also submit a camera ready copy (CRC) with updates as per evaluation in Ms Word document and journal (two column) format [attached with this acceptance letter] to address publisher@jatit.org "Mr. Shahzad" after registration fee submission and copyright for the same.



Forward the scanned receipt after making the payments so that the transaction be traced. There is also an option of urgent publication fee ($500) available on request and subject to slot availability.

Kindly also submit a camera ready copy (CRC) with updates as per evaluation in Ms Word document and journal (two column) format [attached with this acceptance letter] to address publisher@jatit.org "Mr. Shahzad" after registration fee submission and copyright for the same.

Kindly proceed with registration fee submission for limited available slots allocation in the Vol 81, November 2015 Issues of JATIT to be assigned on first registration basis. CRC copies can be submitted at a later time after slot reservation. A certificate of publication can also be provided on demand after submission of publication dues if required earlier than publication time for official use.

We shall encourage more quality submissions from you and your colleagues in future.

Regards,

Shahbaz Ghayyur
Co-Chief Editor
Editorial office
Journal of Theoretical and Applied Information Technology
editor@jatit.org / editorjatit@gmail.com

*/ JATIT is widely distributed in print and electronic from and is also indexed with major indexing agencies making its visibility and citation potential higher than its competitors. JATIT it is now officially recommended by a number of universities and scientific institutions worldwide for publication of research which is the source of its high submission rate and improving IPP, SJR and SNIP values. We are also trying to further improve its flow and visibility by a number of collaborative efforts. Latest indexing information is available at the indexing and abstracting page at www.jatit.org. */

5 attachments

28489-JATIT External Evaluation.pdf
87K

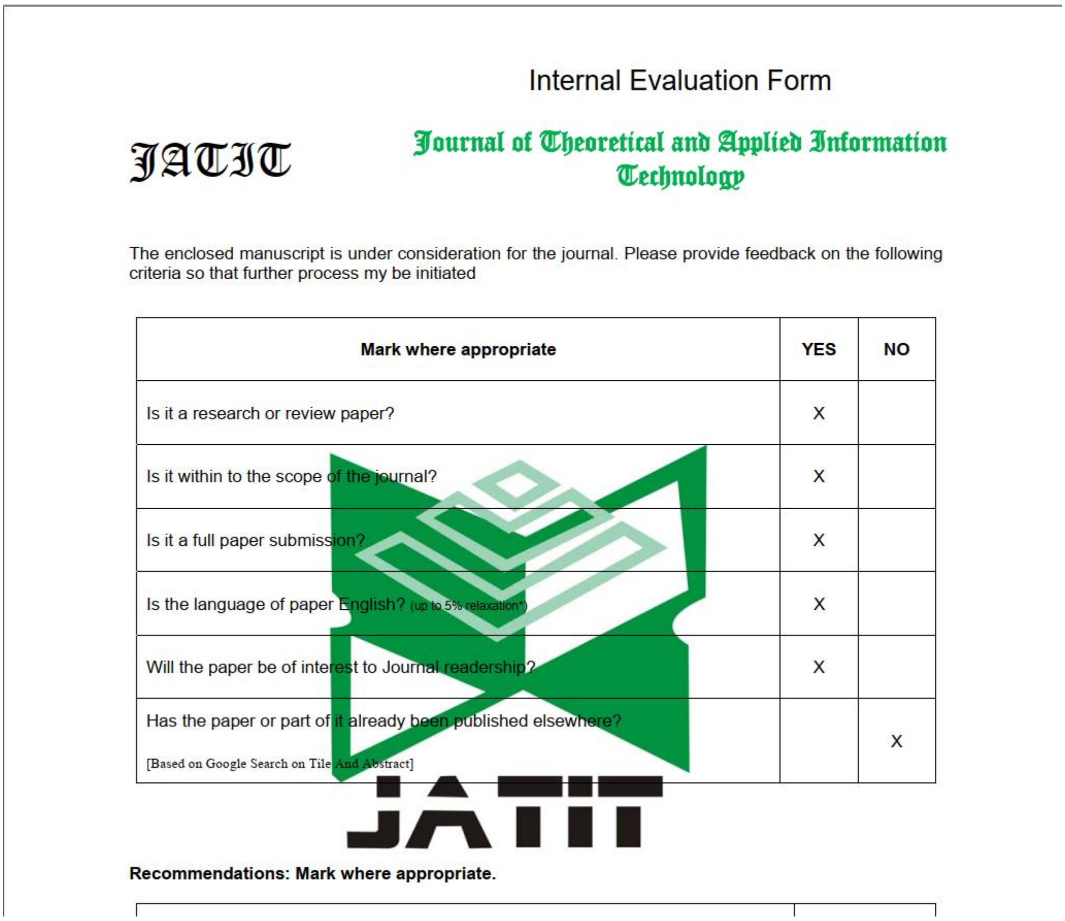
Internal evaluation form.pdf
51K

JATIT FormattingTemplate(1).doc
419K

JATIT Copyright.doc
30K

Publication Fee.pdf
84K

Hasil evaluasi internal review diterima dan direkomendasikan ke external review.



Internal Evaluation Form

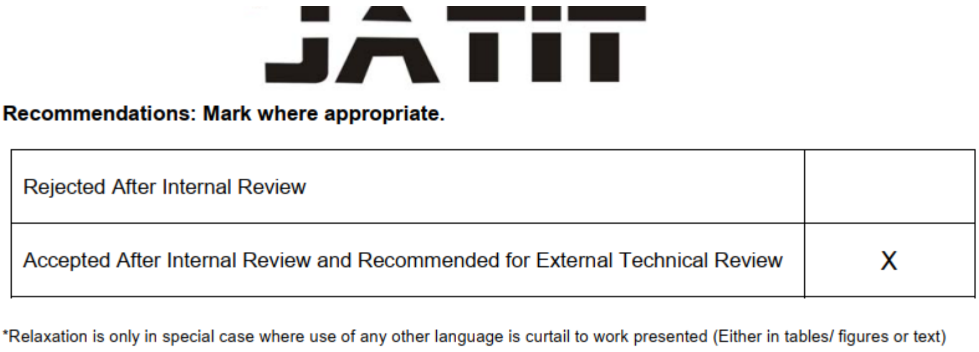
JATIT

Journal of Theoretical and Applied Information Technology

The enclosed manuscript is under consideration for the journal. Please provide feedback on the following criteria so that further process my be initiated

Mark where appropriate	YES	NO
Is it a research or review paper?	X	
Is it within to the scope of the journal?	X	
Is it a full paper submission?	X	
Is the language of paper English? (up to 5% relaxation*)	X	
Will the paper be of interest to Journal readership?	X	
Has the paper or part of it already been published elsewhere? [Based on Google Search on Tile And Abstract]		X

Recommendations: Mark where appropriate.

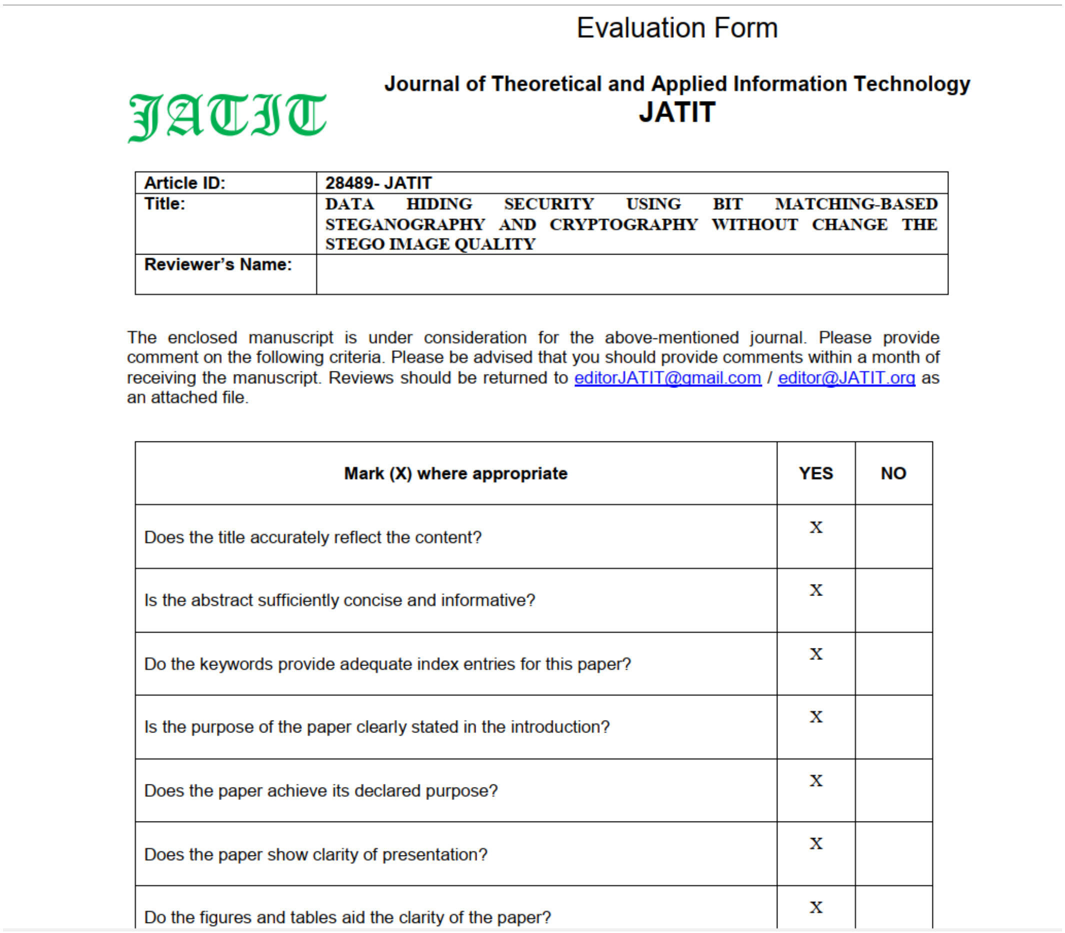


Recommendations: Mark where appropriate.

Rejected After Internal Review	
Accepted After Internal Review and Recommended for External Technical Review	X

*Relaxation is only in special case where use of any other language is curtail to work presented (Either in tables/ figures or text)

Hasil evaluasi external review merekomendasikan paper diterima tanpa revisi.



Evaluation Form

JATIT

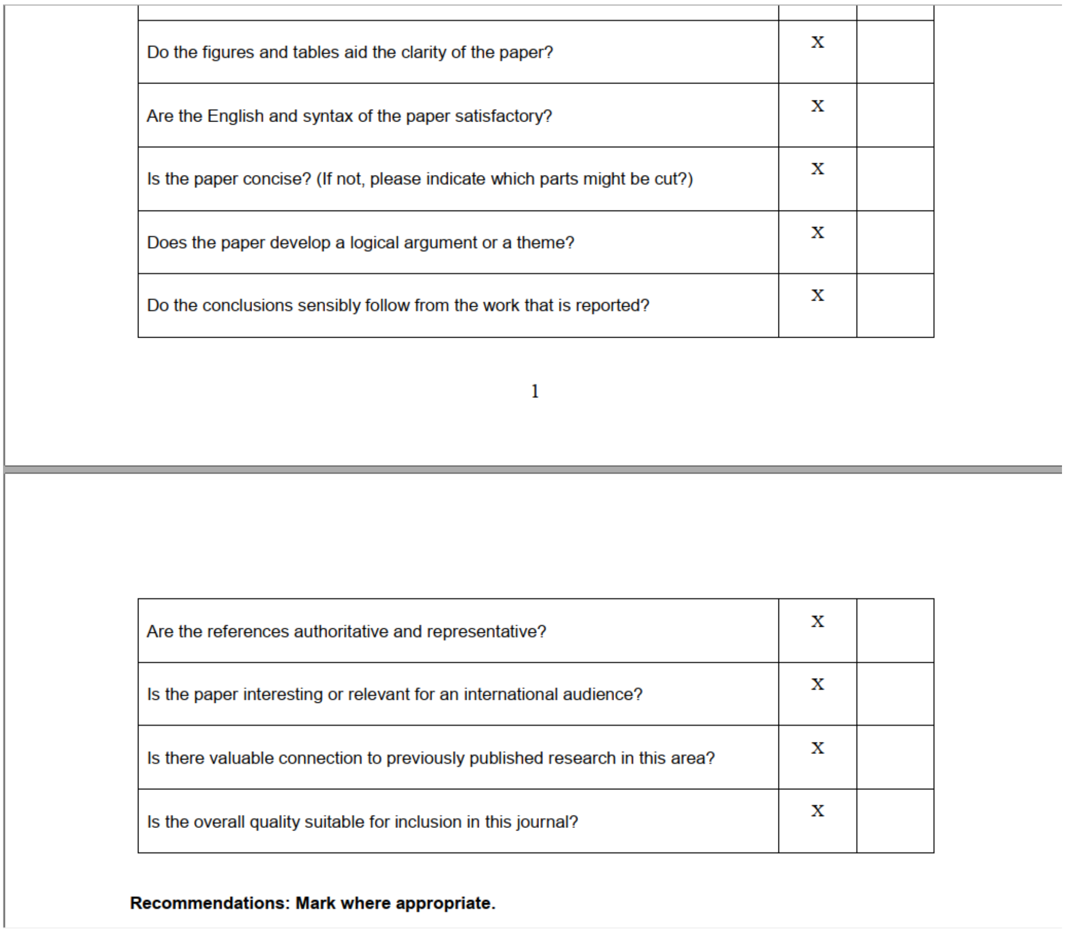
Journal of Theoretical and Applied Information Technology

JATIT

Article ID:	**28489- JATIT**
Title:	**DATA HIDING SECURITY USING BIT MATCHING-BASED STEGANOGRAPHY AND CRYPTOGRAPHY WITHOUT CHANGE THE STEGO IMAGE QUALITY**
Reviewer's Name:	

The enclosed manuscript is under consideration for the above-mentioned journal. Please provide comment on the following criteria. Please be advised that you should provide comments within a month of receiving the manuscript. Reviews should be returned to editorJATIT@gmail.com / editor@JATIT.org as an attached file.

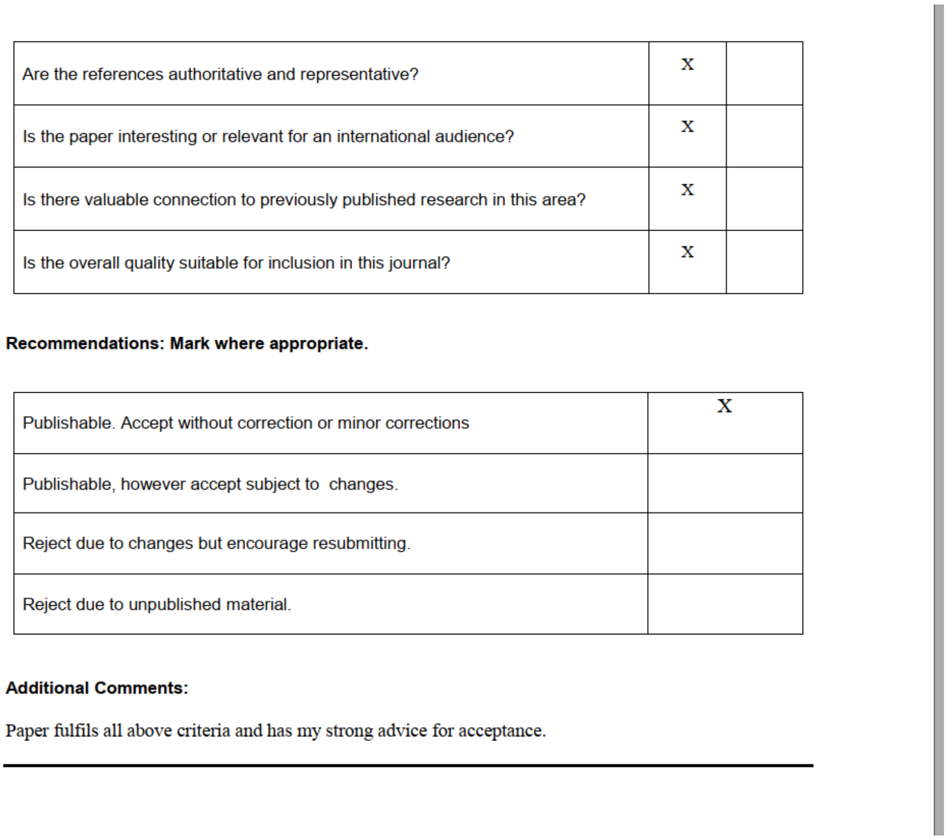
Mark (X) where appropriate	**YES**	**NO**
Does the title accurately reflect the content?	X	
Is the abstract sufficiently concise and informative?	X	
Do the keywords provide adequate index entries for this paper?	X	
Is the purpose of the paper clearly stated in the introduction?	X	
Does the paper achieve its declared purpose?	X	
Does the paper show clarity of presentation?	X	
Do the figures and tables aid the clarity of the paper?	X	



Do the figures and tables aid the clarity of the paper?	X	
Are the English and syntax of the paper satisfactory?	X	
Is the paper concise? (If not, please indicate which parts might be cut?)	X	
Does the paper develop a logical argument or a theme?	X	
Do the conclusions sensibly follow from the work that is reported?	X	

Are the references authoritative and representative?	X	
Is the paper interesting or relevant for an international audience?	X	
Is there valuable connection to previously published research in this area?	X	
Is the overall quality suitable for inclusion in this journal?	X	

Recommendations: Mark where appropriate.



Are the references authoritative and representative?	X	
Is the paper interesting or relevant for an international audience?	X	
Is there valuable connection to previously published research in this area?	X	
Is the overall quality suitable for inclusion in this journal?	X	

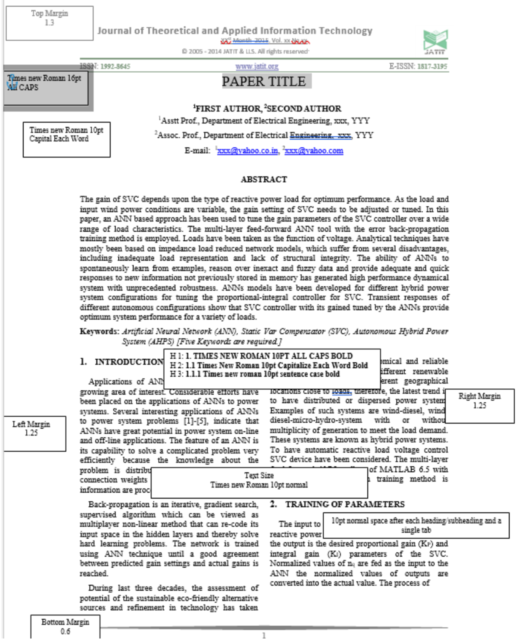
Recommendations: Mark where appropriate.

Publishable. Accept without correction or minor corrections	X
Publishable, however accept subject to changes.	
Reject due to changes but encourage resubmitting.	
Reject due to unpublished material.	

Additional Comments:

Paper fulfils all above criteria and has my strong advice for acceptance.

Paper disesuaikan dengan template yang telah disediakan



Top Margin
1.3

Journal of Theoretical and Applied Information Technology
XXth Month 2015. Vol. xx No.xx
© 2005 - 2014 JATIT & LLS. All rights reserved·

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Times new Roman 16pt
All CAPS

PAPER TITLE

[1]FIRST AUTHOR, [2]SECOND AUTHOR

[1]Asstt Prof., Department of Electrical Engineering, xxx, YYY

[2]Assoc. Prof., Department of Electrical Engineering, xxx, YYY

E-mail: [1]xxx@yahoo.co.in, [2]xxx@yahoo.com

Times new Roman 10pt
Capital Each Word

ABSTRACT

The gain of SVC depends upon the type of reactive power load for optimum performance. As the load and input wind power conditions are variable, the gain setting of SVC needs to be adjusted or tuned. In this paper, an ANN based approach has been used to tune the gain parameters of the SVC controller over a wide range of load characteristics. The multi-layer feed-forward ANN tool with the error back-propagation training method is employed. Loads have been taken as the function of voltage. Analytical techniques have mostly been based on impedance load reduced network models, which suffer from several disadvantages, including inadequate load representation and lack of structural integrity. The ability of ANNs to spontaneously learn from examples, reason over inexact and fuzzy data and provide adequate and quick responses to new information not previously stored in memory has generated high performance dynamical system with unprecedented robustness. ANNs models have been developed for different hybrid power system configurations for tuning the proportional-integral controller for SVC. Transient responses of different autonomous configurations show that SVC controller with its gained tuned by the ANNs provide optimum system performance for a variety of loads.

Keywords: *Artificial Neural Network (ANN), Static Var Compensator (SVC), Autonomous Hybrid Power System (AHPS) [Five Keywords are required.]*

H 1: **1. TIMES NEW ROMAN 10PT ALL CAPS BOLD**
H 2: **1.1 Times New Roman 10pt Capitalize Each Word Bold**
H 3: **1.1.1 Times new roman 10pt sentence case bold**

1. INTRODUCTION

Applications of ANN growing area of interest. Considerable efforts have been placed on the applications of ANNs to power systems. Several interesting applications of ANNs to power system problems [1]-[5], indicate that ANNs have great potential in power system on-line and off-line applications. The feature of an ANN is its capability to solve a complicated problem very efficiently because the knowledge about the problem is distribu connection weights information are proc

Back-propagation is an iterative, gradient search, supervised algorithm which can be viewed as multiplayer non-linear method that can re-code its input space in the hidden layers and thereby solve hard learning problems. The network is trained using ANN technique until a good agreement between predicted gain settings and actual gains is reached.

During last three decades, the assessment of potential of the sustainable eco-friendly alternative sources and refinement in technology has taken

omical and reliable ifferent renewable erent geographical locations close to loads, therefore, the latest trend i to have distributed or dispersed power system Examples of such systems are wind-diesel, wind diesel-micro-hydro-system with or withou multiplicity of generation to meet the load demand. These systems are known as hybrid power systems. To have automatic reactive load voltage control SVC device have been considered. The multi-layer of MATLAB 6.5 with training method is

Text Size
Times new Roman 10pt normal

Left Margin
1.25

Right Margin
1.25

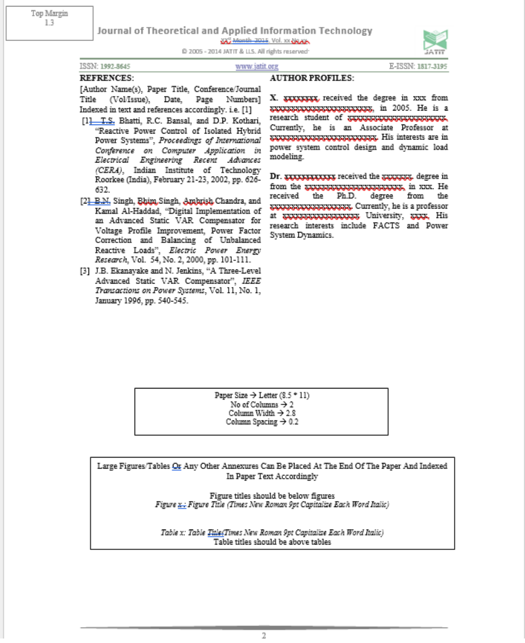
2. TRAINING OF PARAMETERS

The input to reactive power the output is the desired proportional gain (K_P) and integral gain (K_I) parameters of the SVC. Normalized values of n_q are fed as the input to the ANN the normalized values of outputs are converted into the actual value. The process of

10pt normal space after each heading/subheading and a single tab

Bottom Margin
0.6

1



Top Margin
1.3

Journal of Theoretical and Applied Information Technology
XXth Month 2015. Vol. xx No.xx
© 2005 - 2014 JATIT & LLS. All rights reserved·

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFRENCES:

[Author Name(s), Paper Title, Conference/Journal Title (Vol/Issue), Date, Page Numbers] Indexed in text and references accordingly. i.e. [1]

[1] T.S. Bhatti, R.C. Bansal, and D.P. Kothari, "Reactive Power Control of Isolated Hybrid Power Systems", *Proceedings of International Conference on Computer Application in Electrical Engineering Recent Advances (CERA)*, Indian Institute of Technology Roorkee (India), February 21-23, 2002, pp. 626-632.

[2] B.N. Singh, Bhim Singh, Ambrish Chandra, and Kamal Al-Haddad, "Digital Implementation of an Advanced Static VAR Compensator for Voltage Profile Improvement, Power Factor Correction and Balancing of Unbalanced Reactive Loads", *Electric Power Energy Research*, Vol. 54, No. 2, 2000, pp. 101-111.

[3] J.B. Ekanayake and N. Jenkins, "A Three-Level Advanced Static VAR Compensator", *IEEE Transactions on Power Systems*, Vol. 11, No. 1, January 1996, pp. 540-545.

AUTHOR PROFILES:

X. xxxxxxxx received the degree in xxx from xxxxxxxxxxxxxxxxxxxxxxx, in 2005. He is a research student of xxxxxxxxxxxxxxxxxxxxxxx. Currently, he is an Associate Professor at xxxxxxxxxxxxxxxxxxxxxxx. His interests are in power system control design and dynamic load modeling.

Dr. xxxxxxxxxxxx received the xxxxxxx degree in from the xxxxxxxxxxxxxxxxxxxxxx, in xxx. He received the Ph.D. degree from the xxxxxxxxxxxxxxxxxxx. Currently, he is a professor at xxxxxxxxxxxxxxxxxx University, xxxx. His research interests include FACTS and Power System Dynamics.

Paper Size → Letter (8.5 * 11)
No of Columns → 2
Column Width → 2.8
Column Spacing → 0.2

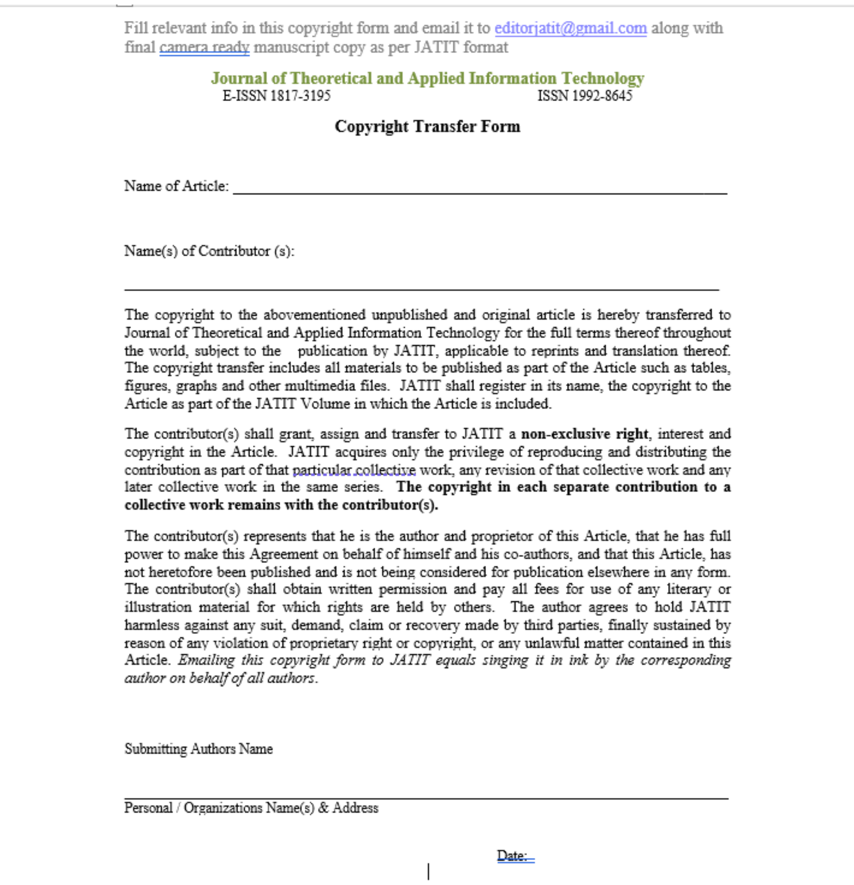
Large Figures/Tables Or Any Other Annexures Can Be Placed At The End Of The Paper And Indexed In Paper Text Accordingly

Figure titles should be below figures
Figure x.: Figure Title (Times New Roman 9pt Capitalize Each Word Italic)

Table x: Table Title(Times New Roman 9pt Capitalize Each Word Italic)
Table titles should be above tables

2

Copyright dokumen yang harus ditandatangani oleh penulis



Fill relevant info in this copyright form and email it to editorjatit@gmail.com along with final camera ready manuscript copy as per JATIT format

Journal of Theoretical and Applied Information Technology
E-ISSN 1817-3195 ISSN 1992-8645

Copyright Transfer Form

Name of Article: ______________________________________

Name(s) of Contributor (s):

____

The copyright to the abovementioned unpublished and original article is hereby transferred to Journal of Theoretical and Applied Information Technology for the full terms thereof throughout the world, subject to the publication by JATIT, applicable to reprints and translation thereof. The copyright transfer includes all materials to be published as part of the Article such as tables, figures, graphs and other multimedia files. JATIT shall register in its name, the copyright to the Article as part of the JATIT Volume in which the Article is included.

The contributor(s) shall grant, assign and transfer to JATIT a **non-exclusive right**, interest and copyright in the Article. JATIT acquires only the privilege of reproducing and distributing the contribution as part of that particular collective work, any revision of that collective work and any later collective work in the same series. **The copyright in each separate contribution to a collective work remains with the contributor(s).**

The contributor(s) represents that he is the author and proprietor of this Article, that he has full power to make this Agreement on behalf of himself and his co-authors, and that this Article, has not heretofore been published and is not being considered for publication elsewhere in any form. The contributor(s) shall obtain written permission and pay all fees for use of any literary or illustration material for which rights are held by others. The author agrees to hold JATIT harmless against any suit, demand, claim or recovery made by third parties, finally sustained by reason of any violation of proprietary right or copyright, or any unlawful matter contained in this Article. *Emailing this copyright form to JATIT equals singing it in ink by the corresponding author on behalf of all authors.*

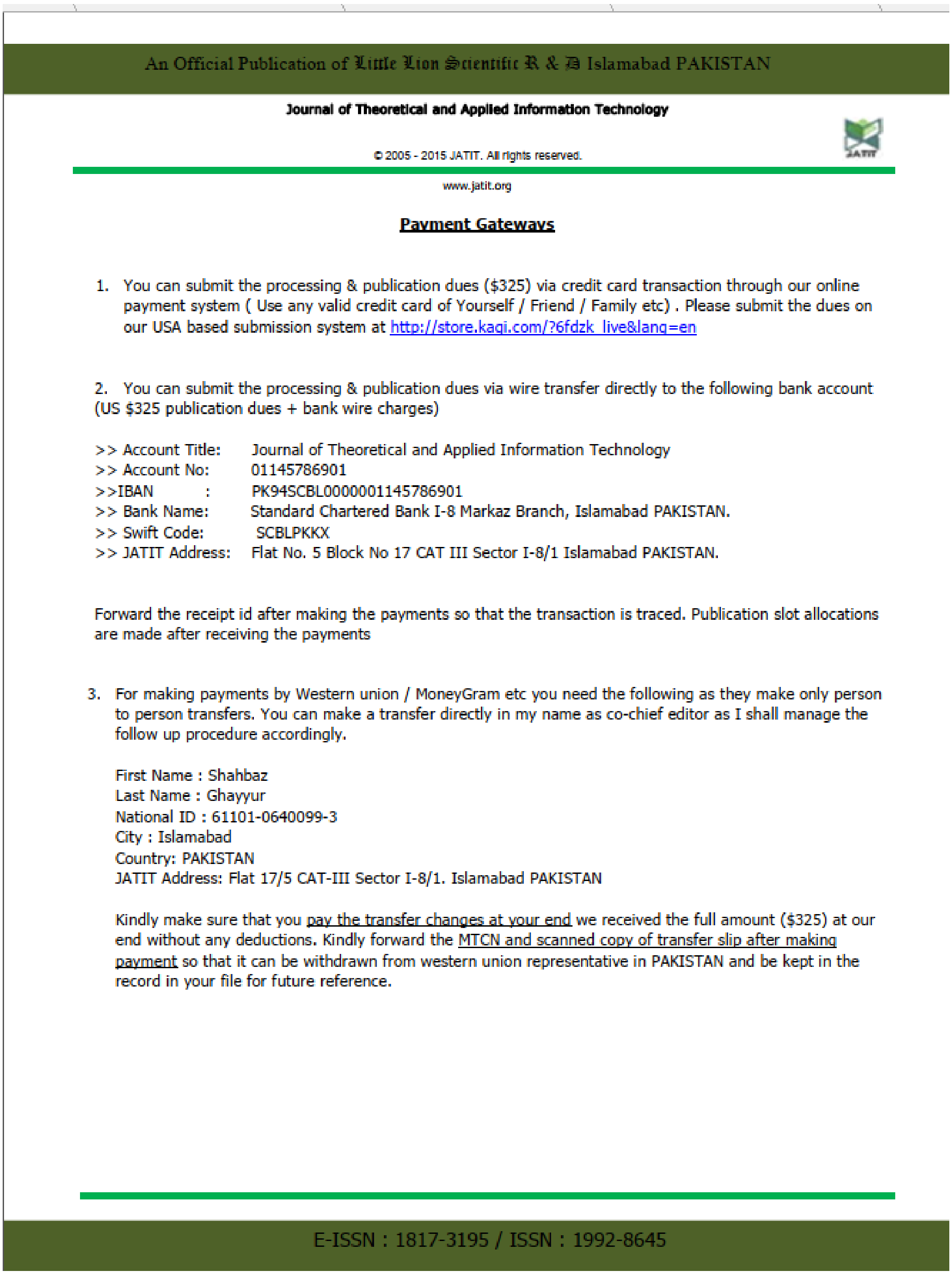
Submitting Authors Name

____

Personal / Organizations Name(s) & Address

Date:

Biaya publikasi.



An Official Publication of Little Lion Scientific R & D Islamabad PAKISTAN

Journal of Theoretical and Applied Information Technology

© 2005 - 2015 JATIT. All rights reserved.

www.jatit.org

Payment Gateways

1. You can submit the processing & publication dues ($325) via credit card transaction through our online payment system (Use any valid credit card of Yourself / Friend / Family etc) . Please submit the dues on our USA based submission system at http://store.kagi.com/?6fdzk_live&lang=en

2. You can submit the processing & publication dues via wire transfer directly to the following bank account (US $325 publication dues + bank wire charges)

>> Account Title:	Journal of Theoretical and Applied Information Technology
>> Account No:	01145786901
>>IBAN :	PK94SCBL0000001145786901
>> Bank Name:	Standard Chartered Bank I-8 Markaz Branch, Islamabad PAKISTAN.
>> Swift Code:	SCBLPKKX
>> JATIT Address:	Flat No. 5 Block No 17 CAT III Sector I-8/1 Islamabad PAKISTAN.

Forward the receipt id after making the payments so that the transaction is traced. Publication slot allocations are made after receiving the payments

3. For making payments by Western union / MoneyGram etc you need the following as they make only person to person transfers. You can make a transfer directly in my name as co-chief editor as I shall manage the follow up procedure accordingly.

First Name : Shahbaz
Last Name : Ghayyur
National ID : 61101-0640099-3
City : Islamabad
Country: PAKISTAN
JATIT Address: Flat 17/5 CAT-III Sector I-8/1. Islamabad PAKISTAN

Kindly make sure that you pay the transfer changes at your end we received the full amount ($325) at our end without any deductions. Kindly forward the MTCN and scanned copy of transfer slip after making payment so that it can be withdrawn from western union representative in PAKISTAN and be kept in the record in your file for future reference.

E-ISSN : 1817-3195 / ISSN : 1992-8645

Publikasi Artikel [10 Desember 2015]

DATA HIDING SECURITY USING BIT MATCHING-BASED STEGANOGRAPHY AND CRYPTOGRAPHY WITHOUT CHANGE THE STEGO IMAGE QUALITY

[1]ALAMSYAH, [2]MUCH AZIZ MUSLIM, [3]BUDI PRASETIYO

[1,2,3]Departmen of Computer Science, Semarang State University, Indonesia

Email: [1]alamsyah@mail.unnes.ac.id, [2]a212muslim@yahoo.com,
[3]budipras@mail.unnes.ac.id

ABSTRACT

This research discussed about the data hiding information using steganography and cryptography. New method are discussed to secure data without change the quality of image as cover medium. Steganographic method is used by find the similarity bit of the message with bit of the MSB (Most Significant Bit) image cover. Finding of similarity process is done by divide and conquer method.The results are bit indexposition, thenthenencrypted using cryptographic. In this paper we using DES (Data Encryption Standard) algorithm. We use data information as message, images, and key as an input. Then, we use our method to secure message. The output is encrypted bit index which containt data hiding information and can be used to secure the messages. To reconstruct the contents, we require the same image and same key.

Outcomes of our method can be used to secure the data. The advantages of this method are the capacity of stored data hiding of messages can be larger than the image. The image quality will not change and the capacity of stored messages can be larger than the image. Acoording to the research, both gray scale and colorful images can be used as image cover, except the image contains 100% black and 100% white. Bit matching process on image which have much variety of color takes less time. The damage of messages due to the addition of “salt and pepper” noise starts from 0.00049of MSE.

Keywords: bit index, bit matching, cryptography, divide and conquer, MSB, steganography.

1. INTRODUCTION

These recent years, the human need for information is increasing. In the midst of rapid development of information technology, the internet is no longer providing secure information. The development of search-engine coupled with the development of virus, bugs, spam and hackers who can steal confidential data [1]. To solve this problem, various ways have been developed to improve data security, such as cryptography and steganography. For example, [2] using steganography Techniquesin the study of Distributed XML.

Steganography is the art and science of hiding data in other media as a cover in order to makethe data looks sketchy [3]. Cryptography is the art and science of maintaining the confidentiality of data [4]. In cryptography, the original data is converted into another form that can not be read. The combination of steganography and cryptography can simultaneously increase the security of the data [5].

Method for combining steganography and cryptography has been developed. In general, the mostly used technique is message encrypting first (cryptography), then hiding it into media cover (steganography)[6]. However, the embedding process can affect the quality of the cover media. A data hiding method by improved LSB substitution process is proposed by [7]. The quality of stego-image can be greatly improved with low computational complexity.

Efforts to minimize the quality changes of cover image can be done by embedding the data in the least significant bit. Changes in the quality of cover is invisible [8], but the embedding of cover into the least bit tends to make the cover prone to robust. Robust resistance can be done by embedding the data in the first bit (most significant bit), but it will change the quality of the cover and it will look suspicious. Primitive structural method was proposed by [9] for improve capacity text steganography can be embed. Each bit of secret text will be placed at corresponding place in the cover text.

Other studies conducted by [10] developed a new way of merger steganography and cryptography without changing the media cover. The technique is performed by matching the message bits on the cover, and then continue the process of encryption (cryptographic). One well-known cryptographic algorithms since 1977 and became a worldwide standard is the Data Encryption Standard (DES) .

This research willcombine steganography and cryptography without changing the media cover. The steganography method used is a method based on bit matching in the first bit (most significant bit) and the cryptographic method used is the DES algorithm.

2. REVIEW OF LITERATURE

Various methods have been developed for data security. In general,the techniques use this encrypting themes sage first (cryptographic process), and then embedding it into theme diacover (steganography process)[6].

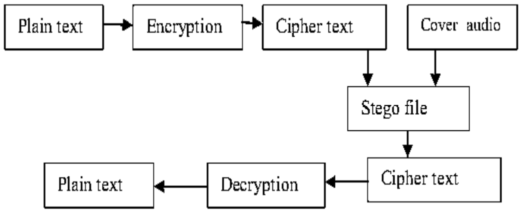


Figure 1.Combination Of Steganography And Cryptography[6].

Combination technique is not only limited as shown inFigure1. Research [11] examines two approach estosecure steganography mediacover (image). Securing steganography imageis done by encrypting. The first method, steganography image is directly encrypted with S-DES, the result is a ciphertext. The second method, the image is encrypted then ciphertext from encryption will be embedded ona nother image.

One of the easiest methods of steganography is LSB (Least Significant Bit). The procedure to perform this method is to embedthe least bit at each pixel with the message bits. Terminology LSB is reviewed by [12]. The LSB embedding will change the bit value, but it will be invisible, so that the third party does not know the existence of the secret message behind the media cover [7].

The use of LSB on the combination of steganography and cryptography was done in a research conducted by[12]. The process consists of three stages, namely encryption, steganography and decryption. Encryption and decryption is done with DES algorithm (Data Encryption Standard). The use of LSB can minimize the image quality changes, but the capacity of messages that can be accommodated is due to the size of the image. Kekre, et al. [13] conducted a LSB steganography study to increase the messages capacity with PVD approach (Pixel value differencing). LSB insertion is based on comparison of the MSB bit value. If the value of the first 4 MSB bits is "1”, then embed it on the last 4 bits. If the first 3 bits MSB is " 1 ", then embed it on the last 3 bits. If the first 2 MSB bit is " 1", then embedit on the last 2 bits. If the value is outside the criteria, then the embedding is done on the last bit (least).

Image quality is an important component in steganography. Challita and Farhat [10] developed another way to combine both steganography and cryptography without changing the image quality. The technique is performed by matching the message bits on the cover, the results is in the form of bit position index. Index is then encrypted. The output is bit index ciphertext.

Bit matching is done by divide and conquer[14] that consist of three processes, namely divide, conquer, and combine. Arrangement of long bits is splitting it into two smaller parts (divide), then match each section (conquer). The results of each part of the solution then combined into a total solution (combine).

3. RESEARCH METHOD

Solving a problem begins with the development of software in the process of combining steganography and cryptography used Agile Method as seen in Figure 2.

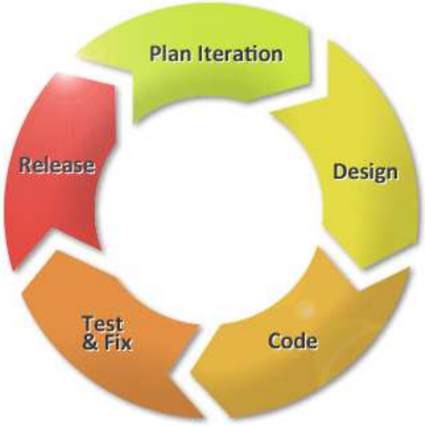


Figure 2. Agile Method

Agile method is methodology development of software based on short-term development system that require adaptation rapidly than the developer to changes of any form [15].The step of method: planning, design, code, test & fix, and release.

The combination of stego-crypto in this caserequired 4 processes, they are bit matching, encryption, decryption and reconstruction. The details are as follow.

3.1. Matching Bit

In this study the method of matching is done with divide and conquer[14]. The matching bit process is as follows.

Input: secret message and image
Output: secret bit position

Procedure:
Step 1: Convert the message and image in binary.

Step 2: Put the value of MSB image.

Step 3: Perform the matching messages on MSB image. If the bit message is contained in the MSB image, then proceed to save the position of the bit index. Index saving consists of index position of the first (start) and the position index of the last bit (end). If the matching process does not occur, continue the process step 4 as follows.

Step 4: Divide the message into two parts of equal length of the left (L [i]) and right (R [i]).

Step 5: Repeat the same steps as instep 4), with L [i] and R [i] as input. If all the bit message are contained in the image, the matching process is completed and continue to step 6). If not, repeat step 3) with L [i] and R [i] as any step .

Step 6: Keep all bit index from matching results.

Step 7: The output is a vector that contains the index structure of bit position.

3.2. *Encryption*

Secret bit position then encrypted by cryptography algorithm (DES) shown at Figure 3.

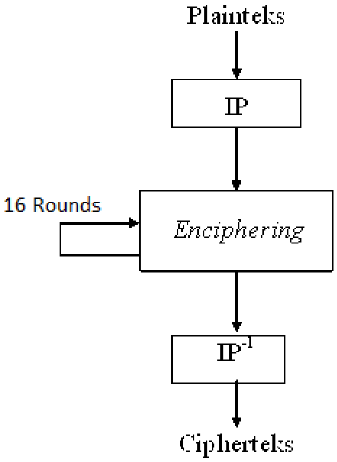


Figure 2a..Des Algorithm

The ecryption process is as follows.
Input: secret bit position (plaintext) and key.
Output: chipertext of bit position.

Procedure:
Step 1: Broke the 64-bit plaintext into L (32 bit) R (32 bit).

Step 2: Perform initial permutation (IP).

Step 3: Encrypt in 16 rounds (enchipering). Internal locks on each different lap.

Step 4: Invert the initial permutation (IP^{-1}).

3.3. *Decryption*

The decryption process is as follows.
Input: chipertext of bit position and key
Output: Plaintext.

Decryption of the ciphertext is the inverse of the encryption process. DES uses the same algorithm for encryption and decryption. In the process of decryption, the key sequence used is the inverse one namely K16, K15, ...,K1. For each round of 16, 15, ...,1, the output a teach round of deciphering is

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i).$$

3.4. Reconstruction

Reconstruction aims to restore the message to its original form.
Input: text file (that consists of bit and image index location)
Output: composition of bit meggase.

Procedure:
Step 1: Convert the image in binary form and take the bit of MSB image.

Step 2: Read the contents of two index vectors. The first index is a bit's early position (start) and the second index is the bit's end position (end).

Step 3: Taking the value of bit image based on step 2).

Step 4: Repeating the process step 2) and step 3) until the last index position.

Step 5: The composition of the bits will create an output in the form of bit message

3.5. Combination Steganography and Cryptography

3.5.1.Overview

Combination of steganography and cryptography in this research consists of two main processes: embedding and extraction which is generally shown in Figure 4.

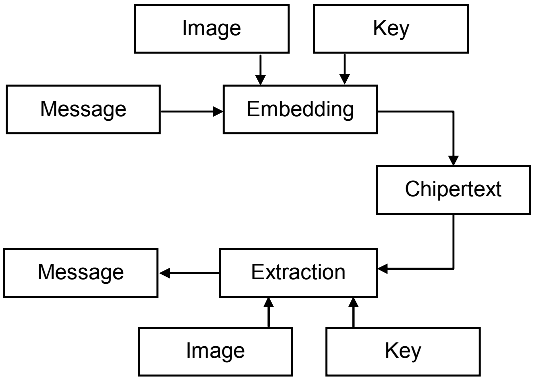


Figure 4.Overview The Combination Of Steganography And Cryptography

Embedding process (Figure 5) consists of bit matching and encryption, the result is ciphertext. Extraction process (Figure 6) consists of decryption and reconstruction; the results are in the form of a message.

3.5.2. Embedding Process

Embedding process aims to generate bit index position as shown in the Figure 5.

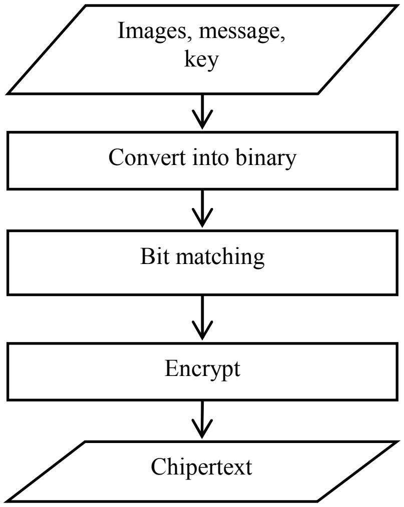


Figure 5.Embedding Process

Input: secret messages, images, andkey.
Output: ciphertext.

Algorithm of embedding steps as follows.
Step 1: Read input information: images, messages, and key.

Step 2: Convert the message and image in binary form.

Step 3: Match the bit message with the bit of MSB image. The same bit positions are stored in the bit vector index.

Step 4: Encrypt the bit vector index with DES algorithm.

Step 5: The output is ciphertext. The ciphertext contains a bit vector that has been encrypted.

3.5.3. Extraction process

Extraction process as shown in the Figure 6 store the message to its original for min order to maintain the original contents.

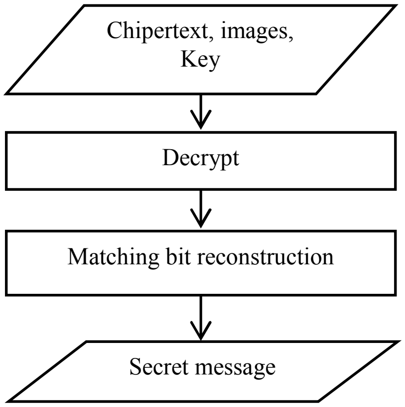


Figure 6.Extraction Process

Input: ciphertext vector, a key, and image.
Output: original message.

Algorithm of extraction process steps are as follows.

Step 1: Input key, ciphertext vector, and image.

Step 2: Decrypt the vector with the key, the decrypted plain text is in the form of bit index.

Step 3: Do a message reconstruction by matching bit of MSB image based on bit index vector.

Step 4: The output isthe message.Finish.

4. RESULTS AND DISCUSSIONS

The result is application programs of stego-crypto which has developed using the programming language MATLAB R2009 a then use it forsecure the data.

Experiment 1: Testing the image color

Selecting the secret messages in file transfer.txt. Then Choosing a cover imageJet.bmp (Figure 7).

Figure 7. Cover Image

Typing key as the encryption key for DES, for example key: 1234567.The output of embedding is bit index position (Figure 8).

```
vÀáÞhsÂ«A°9üª  ànÕsm7-y4fé>>²å  # ¶i<`~¡*Z
g?.a¦«¥¦è~Ã\p+|Í$I3M"Ú_x6¶zø±ä-U2¿ï^«üu¥Dy
VhIOvA0ÊFÁ];p¢f<ú4½ëaK«ø:XkÄ+m{ú7zè/8(
\GêéªZ~µ}êË  0k{     Ü|DHÛZ  é£[;ÿÅÀu/¶äN
§oKqÂð¨¤.Ð#¥ûR#á¢'ø¦þX  kMO{ªÛý¤;®iùröÂ
8,ÐýXUjD  ®G[Ü®{<y6WLõwÝåXô¤á71F|6D
Oxo LóÛy¥ÅÀ  îhi*7}GÑ>ñ,yX8È8äY5ÆÛMñ
7ºçdÅ<pdÄ×v£¢`äi]J¦÷H±áL*<«¡¡dÆÎg|_Aª4±k¡
æGäñýjÛê0uX³¹x=IÊ Kï¬·L=?óK×úR¦zZV\dÝr°ê
èJ!¶ÂP  fta[)a¼ç     ÷Fæú·»ÝzÒäíÒS¯
³Ë$8õùÔþUÖ#És
```

Figure 8. Encrypted bit index.

Experiment 2: Experiment in Different Size Resolution

The application was also tested with different image sizes, ranging from 512px, 256px, 128px, to 64px. The test result (Table 1 and 2) shows that the larger the image resolution, the longer the bit matching process will take. The bit matching time of "Jet" is 0.729 sec.

Table1.The test results embedding process

Image	Resolution (px)	Embedding time ('s)		
		Matching	Encrypt	Total
"Jet"	512 x 512	2,038	12,186	14,713
	256 x 256	0,567	11,341	12,095
	128 x 128	0,221	10,714	11,039
	64 x 64	0,089	10,734	10,902
	Average	0,729	11,244	12,187

Table 2.The test results reconstruction process

Image	Resolution (px)	Reconstruction ('s)		
		Decrypt	Recons-truction	Total
"Jet"	512 x 512	10,564	0,181	10,900
	256 x 256	11,099	0,267	11,574
	128 x 128	10,704	0,183	11,503
	64 x 64	10,575	0,179	10,946
	Average	10,736	0,203	11,231

Experiment 3: Testing with Giving Noise

Noise 'salt and pepper' was given to the image in the next embedding process. The image was given noise 'salt and pepper' with standard deviation, d=0.001; 0.005, 0.01; 0.05. The image has been given a noise then tested in the extraction process store cover the messages. Then computing then PSNR that can computed by:

$$PSNR = 20.\log_{10}\frac{R}{MSE}$$

Where R is the maximum fluctuation in the input image data type.R=255. Then, MSE computing by as follows.

$$MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left|f(x,y)-g(x,y)\right|^2$$

where f(x,y) and g(x,y) denote pixel value of original and the reconstructed image at the position (x,y), respectively. The Test results with Noise shown in the Table 3.

Table3.The Test Results With Noise

Citra	Salt & pepper (d)			
	d	MSE	PSNR	Message
"Jet"	0,001	0,00014	61,398	Fine- readable
	0,005	0,00056	55,936	Fine- readable
	0,01	0,00123	52,807	Fine- readable
	0,05	0,00515	46,077	Damage-readable
"Lenna"	0,001	0,00030	34,987	Fine- readable
	0,005	0,00140	28,435	Fine- readable
	0,01	0,00310	25,014	Damage-readable
	0,05	0,01400	18,282	Damage-readable
"Pepper"	0,001	0,00010	67,295	Fine- readable
	0,005	0,00483	50,094	Damage-readable
	0,01	0,00094	57,320	Damage-readable
	0,05	0,00483	50,094	Damage-readable
"Baboon"	0,001	0,00013	67,773	Fine- readable
	0,005	0,00049	60,369	Damage-readable
	0,01	0,00091	57,660	Damage-readable
	0,05	0,00494	50,410	Damage-readable

Test results of message reconstruction on a black and white image with the addition of salt & pepper noise remains good. Messages can be read, but there was one image which was damaged. While most of the colorful images were damage, except the image of "Jet" and "Lenna" which only suffer from a little damage. Both “jet” and “lenna” images have the highest MSE value 0.014. Damage to colorful image occurred from 0.00049 MSE on image "Baboon" which incidentally has a fairly simple color variations. The result of message reconstruction will produce the changed message as well.

5. CONCLUSION

Step of hiding data security in this study consists of two processes. First, the embedding process which includes the process of matching the same bit thenencrypt it. Secondly, the extraction process which includes the decryption process then construct bit position to restore the message.The advantages of this method are the capacity of stored data hiding of messages can be larger than the image. the image quality will not change and the capacity of stored messages can be larger than the image

The experiment with addition noise to the image causes some changes in the message content. In the black and white image, the changes are not significant, while in the colorful imagethe message content changes a lot. Damage occurred on the addition of salt and peper noise start from MSE 0.00049.

6. REFERENCES

[1] Kautzar, M.G., 2007, *Studi Kriptografi Mengenai Triple DES and AES*, ITB, Bandung.

[2] Memon, A. G., Khawaja, S. & Shah, A., 2008, Steganography: A New Horizon for Safe Communication Through XML. *Journal of Theoretical and Applied Information Technology (JATIT), 4*, 187-202.

[3] Provos, N., and Honeyman, P., 2003, Hide and Seek: An Introduction to Steganography, *IEEE Security & Privacy Vol. 1(3)*, 32-44.

[4] Schneier, B., 1996, *Applied Cryptography 2nd Edition*, Wiley & Sons. Inc., New York.

[5] Krenn, R., 2004, *Steganography and Steganalysis*, Whitepaper.

[6] Raphael and Sundaram, A.J., and Sundaram, V., 2011, Cryptography and Steganography – A Survey, *International Journal Comp. Tech. Applied Vol. 2 (3)*, 626-630.

[7] Sharma, V. K., Shrivastava, V., 2012, A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection, *Journal of Theoretical and Applied Information Technology (JATIT) Vol. 36 No.1*, 1-8.

[8] Chan, C. K., and L.M. Cheng, 2004, Hiding Data in Images by Simple LSB Substitution, *Pattern Recognition Vol. 37(3)*, 469–474.

[9] Roslan, N. A., Mahmod, R., Udzir, N. I., and Zurkarnain, Z. A, 2014, Primitive Structural Method for High Capacity Text Steganography, *Journal of Theoretical and Applied Information Technology (JATIT),Vol. 67 No.2.*

[10] Challita, K., andFarhat, H., 2011, Combining Steganography and Cryptography: New Directions, *International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1)*, 199-208.

[11] Narayana, S., and Prasad, G., 2010, Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions, *Signal & Image Processing: An International Journal (SIPIJ) Vol. 1(2)*, 60-73.

[12] Sharp, T., 2001, An implementation of Key-based Digital Signal Steganography, *Proc. Information Hiding Workshop Vol. 2137, Springer LNCS*, 13–26.

[13] Kekre, H.B., Archana A., and Pallavi N.H., 2012, Comparison between the basic LSB Replacement Technique and Increased Capacity of Information Hiding in LSB's Method for Images, *International Journal of Computer Applications (0975 – 8887) Vol .45 (1)*, 33-38.

[14] Cormen, T.H., Leiserson C.E., Rivest R.L., and Stein D., 2009, *Introduction to Algorithms, Third Edition*, The MIT Press, England.

[15] Gandomani, T.J., H. Zulzalil, A.Z.A. Ghani & A.A.MD. Sultan. 2013. Important Considerations For Agile Software Development Methods Governance. *Journal of Theoretical and Applied Informations Technology (JATIT),* Vol. 55 No. 3.