

LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU PEER REVIEW
KARYA ILMIAH : JURNAL ILMIAH

1. Judul Jurnal Ilmiah (Artikel) : The Proposed Development of Prototype with Secret Messages Model in Whatsapp Chat
2. Jumlah Penulis : 7 orang
3. Penulis Jurnal Ilmiah : Hamdani, H. Ismanto, A. Q. Munir, B. Rahmani, A. Syafrianto, D. Suprihanto, A. Septiarini
4. Status pengusul : Anggota
5. Identitas Jurnal Ilmiah
- a. Nama Jurnal : International Journal of Electrical and Computer Engineering
 - b. ISSN/e-ISSN : 2088-8708
 - b. Volume, Nomor, Edisi (tahun) : Vol 8, No 5: October 2018 (Part II)
 - d. Penerbit : IAES (Institute of Advanced Engineering and Science)
 - e. Halaman/Jumlah halaman : 3843-3851
 - f. Tautan jurnal/artikel : <https://s.id/ci6Hu>
6. Kategori Publikasi Jurnal Ilmiah
- | | |
|---|--|
| √ | Jurnal Ilmiah Internasional Bereputasi |
| - | Jurnal Ilmiah Internasional |
| - | Jurnal Ilmiah Nasional Terakreditasi |
| - | Jurnal Ilmiah Nasional Tidak Terakreditasi |

7. Hasil Penilaian *Peer Review* :

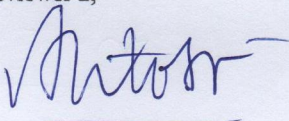
Komponen Yang Dinilai	Nilai Maksimal Jurnal Ilmiah				Nilai Akhir Yang Diperoleh
	Internasional bereputasi	Internasional	Nasional Terakreditasi	Nasional Tidak Terakreditasi	
a. Kelengkapan unsur isi Artikel ilmiah (10%)	4	3	2.5	1	4
b. Ruang lingkup dan kedalaman pembahasan (30%)	12	9	7.5	3	10
c. Kecukupan dan kemutakhiran data/informasi dan metodologi (30%)	12	9	7.5	3	11
d. Kelengkapan unsur dan kualitas penerbit (30%)	12	9	7.5	3	12
Total = (100%)	40	30	25	10	37

Catatan reviewer:

1. Isi artikel ilmiah tidak terindikasi plagiat dan sudah sesuai standar penulisan
2. Ruang lingkup dan kedalaman dalam membahas penelitian sudah cukup
3. Metodologi diuraikan dengan baik dan sudah menggunakan referensi yang ^{baik}
4. Kualitas penerbit sudah sesuai standar

Pangkal Pinang, 8 Februari 2020

Reviewer 2,



Dr. Hadi Santoso, S.Kom., M.Kom.

NIDN. 0225067701

Unit Kerja: Prodi : Sistem Informasi pada

STMIK Atma Luhur

**LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU PEER REVIEW
KARYA ILMIAH : JURNAL ILMIAH**

1. Judul Jurnal Ilmiah (Artikel) : The Proposed Development of Prototype with Secret Messages Model in Whatsapp Chat
2. Jumlah Penulis : 7 orang
3. Penulis Jurnal Ilmiah : Hamdani, H. Ismanto, A. Q. Munir, B. Rahmani, A. Syafrianto, D. Suprihanto, A. Septiartini
4. Status pengusul : Anggota
5. Identitas Jurnal Ilmiah
- a. Nama Jurnal : International Journal of Electrical and Computer Engineering
 - b. ISSN/e-ISSN : 2088-8708
 - b. Volume, Nomor, Edisi (tahun) : Vol 8, No 5: October 2018 (Part II)
 - d. Penerbit : IAES (Institute of Advanced Engineering and Science)
 - e. Halaman/Jumlah halaman : 3843-3851
 - f. Tautan jurnal/artikel : <https://s.id/ci6Hu>
6. Kategori Publikasi Jurnal Ilmiah
- | | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | Jurnal Ilmiah Internasional Bereputasi |
| <input type="checkbox"/> | Jurnal Ilmiah Internasional |
| <input type="checkbox"/> | Jurnal Ilmiah Nasional Terakreditasi |
| <input type="checkbox"/> | Jurnal Ilmiah Nasional Tidak Terakreditasi |

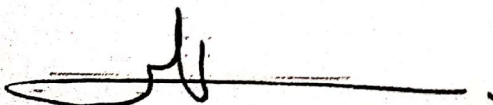
7. Hasil Penilaian Peer Review :

Komponen Yang Dinilai	Nilai Maksimal Jurnal Ilmiah				Nilai Akhir Yang Diperoleh
	Internasional bereputasi	Internasional	Nasional Terakreditasi	Nasional Tidak Terakreditasi	
a. Kelengkapan unsur isi Artikel ilmiah (10%)	4	3	2.5	1	4
b. Ruang lingkup dan kedalaman pembahasan (30%)	12	9	7.5	3	12
c. Kecukupan dan kemutakhiran data/informasi dan metodologi (30%)	12	9	7.5	3	11
d. Kelengkapan unsur dan kualitas penerbit (30%)	12	9	7.5	3	12
Total = (100%)	40	30	25	10	39

Catatan reviewer:

- Kualitas paper sudah baik
 - Pengalaman para penulis sudah cukup baik
 - Nilai akhir yg diperoleh sebagai anggota dibagi 6

Palembang, 11 Rebruari 2020
 Reviewer 1,



Dr. Abdiansah, S.Kom., M.cs.
 NIDN. 0001108401
 Unit kerja: Prodi. Teknik Informatika pada
 Universitas Sriwijaya

Paper 10

by Budi Rahmani

Submission date: 13-Nov-2021 08:37AM (UTC+0700)

Submission ID: 1701303017

File name: Paper_10_10068-31115-1-PB.pdf (1.19M)

Word count: 4695

Character count: 25323

2
**The Proposed Development of Prototype with Secret Messages
Model in Whatsapp Chat**

**Hamdani Hamdani¹, Heru Ismanto², Agus Qomaruddin Munir³, Budi Rahmani⁴, Andri Syafrianto⁵,
Didit Suprihanto⁶, Anindita Septiarini⁷**

^{1,7}Department of Computer Science, Universitas Mulawarman, Samarinda, Indonesia

²Department of Informatics Engineering, Universitas Musamus, Merauke, Indonesia

³Department of Informatics Management, Universitas Respati Yogyakarta, Yogyakarta, Indonesia

⁴Department of Informatics, STMIK Banjarbaru, Kalimantan Selatan, Indonesia

⁵Department of Informatics Engineering, STMIK El Rahma, Yogyakarta, Indonesia

⁶Department of Electrical Engineering, Universitas Mulawarman, Samarinda, Indonesia

7
Article Info

Article history:

Received May 28, 2018

Revised Aug 12, 2018

Accepted Aug 19, 2018

Keyword:

Chatting
Message
Secret
Security
WA

ABSTRACT

Development of prototype at data security through secret messages is needed for disguising the messages sent in smartphone chatting application, WhatsApp (WA) Chat. We propose a model to disguise a plaintext message which is first encrypted by cryptosystem to change the plaintext message to ciphertext. Plaintext or plainimage entering the smartphone system is changed into encrypted text; receiver then can read the message by using similar key with the sender. The weakness of this proposal is the message random system is not planted directly in the chatting application; therefore message removing process from cryptosystem to WA application is still needed. The strength of using this model is the messages sent will not be easily re-encrypted by hacker and can be used at client computing section.

3
Copyright © 2018 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Hamdani Hamdani⁸,
Departement of Computer Science,
Faculty of Computer Science and Information Technology,
Universitas Mulawarman⁴²,
Jalan Penajam, Kampus Gunung Kelua, Samarinda 75123, East Kalimantan, Indonesia.
Email: hamdani@fkti.unmul.ac.id

1. INTRODUCTION

It is believed that there is a flaw in the existing prototype in WhatsApp (WA) system known by hacker to re-encrypt the messages sent through our smartphone, hence additional development of the application system is needed to suit secondary security in sending and receiving secret messages through social chatting system [1]-[3].

Chatting based communication has been done by many people of smartphone users because of its effectiveness and efficiency [2], [4]-[6]. Communication by chatting is a form of the most effective textual communication used [4], e.g. the textual conversation using the smartphone by social media, chatting with WA, telegram, etc [3], [5], [7]. Writing secret message is a way needed to secure data sent through an Internet connection, thus except the sender and receiver knowing the content of the message, there will be nobody who knows and realized that there is a secret message sent in that message [8].

Plaintext and plainimage sent through chatting application are not fully secured, so a model is needed to modify the additional message in the process of sending plaintext that can be encrypted [9]. Then, there is a possibility of an attack by the hacker to re-encrypt the message sent to the receiver [10], [11]. As a consequence, the sender and receiver of the secret message are supposed to design a proposed model based

on need and encryption method they know, so the message sent and received will be limited by encrypted text personally [12].

Chatting model done individually or in the group does not have any security guarantee to the receiver, yet the plaintext sent through operator server is fragile of hacker attack [10], [11]. Plaintext and plainimage saved in the operator server can be a weakness of the application users who feel secure but in fact there are many hacker attacks achieving textual information saved in the server [13]-[15], so an additional network control software is needed [16].

The steps of sending message through mobile is based on message demand and authentication from mobile A to mobile B [8]. This technique can use secret sharing technique using mobile SMS confirmation method as shown in Figure 1. Model shown in Figure 1 is less effective to be applied in smartphone application system because the message sent through smartphone is a long text, images and multi-participant. The example of multi-participant text sending in a chat room is shown by Figure 2.

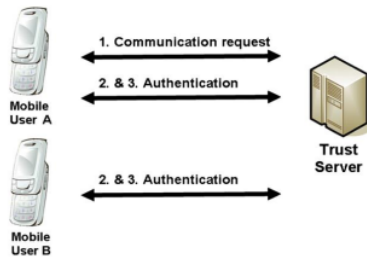


Figure 1. The authentication flowchart [8]



Figure 2. Abstracted chat client user interface, including examples of user, system, and action messages [5]

Figure 2 shows a chatting process in a group in a textual application. This plaintext is likely dangerous to be attacked by outsider trying to achieve those information through smartphone. In WA is already using end-to-end encryption, but we need to provide additional system outside the WA system, so users feel confident that the messages sent are not be tapped by the attackers. Next, our research focuses on how to disguise messages sent through chatting application in smartphone system used by many users nowadays. The plaintext sent will be encrypted, thus the text saved in the operator server will not be easily re-encrypted by the attackers. The text saved can be text [25, 7] or images [18]. Development of a model of secret messages through WA voice as in the crypt analysis of two pads in case of compressed speech [19].

2. RELATED WORK

In the development of the proposed model there are several related studies directly or indirectly, so some prior research is needed to produce a prototype suitable for the security needs of the next secret message. In [20] developing message authentication with a correlated setup for sending messages as done by Bob and Alice. Meanwhile, [21] analyzed the recently-proposed block cipher using cellular automata (CA) and the self-invertible function. This paper performs insecurity analysis of the cipher, because of its conjugate nature.

The results of this study also found the decryption process without knowledge of the secret key so it needs to be fixed. In [8] developing a secret-key cipher based on a non-linear structured code with the distinguishing feature that its error generator is implemented by a non-linear combination of code words of two linear complementary codes. In [2] developing a practical reputation system for pervasive social chatting with Mobile Ad Hoc Network (MANET) on smartphone. In this study [22], a general attack scenario was given in order to conduct security analyses of chaos based crypto systems with proposed cryptanalysis of a new image encryption algorithm so it can be used in the MANET.

In the proposed algorithm, the secret key detected between sender and receiver was used in the calculation of system parameters of chaotic map group. In [1] perform a social graph based text mining framework for chat log investigation for presents a unified social graph based text mining framework. Further, it needs to be made for secure group-based mobile chat protocol [23]. For example, huge mobile

applications (M-APPs) created for the mobile communication services which are not only for voice services, but also for social networking services. Meanwhile, [24] worked on for visual cryptography can do unscrambled [13] Human Visual System (HVS).

The effect of coaching and feedback on online chats in this case also found in the study [25]. Coaching occurred before each chat, and feedback was provided immediately afterwards. The findings suggest that over time, the frequency of higher-order thinking will increase more in a group that receives coaching and feedback than in a group that does not receive coaching and feedback. In addition, the findings suggest that the Community of Inquiry framework has benefits [22] and its use in course design, facilitation, and assessment to include serving as a guide to coaching [25]. New steganography algorithm to conceal a large amount of secret message using hybrid adaptive neural networks with modified adaptive genetic algorithm [26]. Meanwhile, a high capacity text steganography scheme based on LZW compression and color coding [27]. [15]

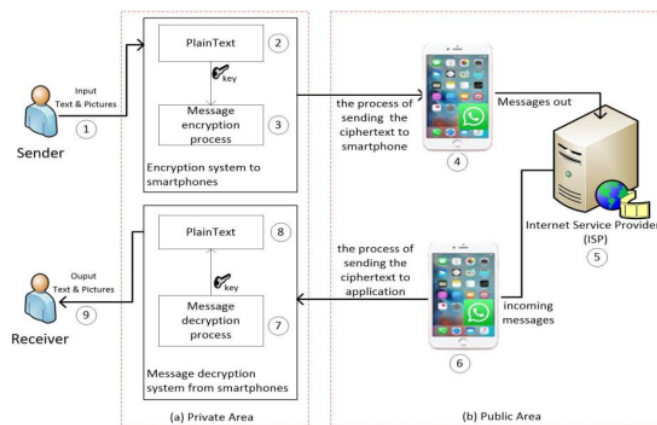
The steganographic system thus embeds secret content in cover media (like text, image, audio, and video) so that its existence is not detected to an eavesdropper. Impostor Detection Through Chat Analysis also done by [3] for verify the identity of the person on the basis of his writing style. In this case we also need a model that can integrate the system in sending text. Some other research results such as [3] [14] and [23].

In [28] an encryption algorithm with an error detection technique and technique has been successfully verified and synthesized using Xilinx by Spartan-3E FPGA. [14] present a scheme which allows an arbitrary 2-qubit quantum state teleportation between two remote parties with control of many qubits in a network, while on [23] using Mobile Chat (MC) and Mobile Chat System (MCS) for services plays a very important role in current social networking. Thus, both the Secure End-to-End Secure Mobile Chat (SE2E-MC) scheme and Secure Group-based Mobile Chat (SG-MC) scheme are provided the suitable solutions. The design and implementation of secure chatting application with end to end encryption [29] and combining steganography and cryptography on android platform to achieve a high-level security [30].

3. PROPOSED METHOD

Data security model is needed to encrypt client message before sending through the provider service, thus the message has been encrypted when it is received by the server. Plaintext and plainimage sent to the other users will not be easily read with application such as WA before decrypted to plaintext. In this method, we prepare some material consisting of cryptography model such as vigenere cipher and transposition to encrypt the message sent and to smartphone as sender and receiver.

In this case, we try to do encryption by using vigenere model, transposition and web service for testing whether the messages we sent can be encrypted in the smartphone system. Meanwhile, we use web service for integrating data from client in the smartphone so that the message written in the client application can be accepted by WA chat system. This method is proposed to secure textual message and images sent through chatting system hence the users of chatting application feel more secured. The steps of proposed model in developing prototype with secret message model as shown in Figure 3 we are working on is used for message sending process written by sender and then received by others.



2 Figure 3. Proposed method of chat messages security in (a) private area to (b) public area

In Figure 3 we can see the process in (a) private area and (b) public area in a proposed method consisting of sender (1) as the secret message sender. Sender (1) fill in the textual data or images as plaintext which is then encrypted before sending so that the message sent to the smartphone is in the form of ciphertext. The message is then sent to the providers (2) plaintext as the origin, (3) step for message encryption process (MEP) then sent to the chatting system in the smart phone (4) receive encrypted message to send to receivers through providers. (5) ISP only receive message than cannot be read the originality and then sent to the receivers as the destination (6).

The receiver (6) of encrypted message then input the encrypted message into cryptosystem in the smartphone to be encrypted (7) by message decryption process (MDP) based on private key of the sender key, thus the origin text as the plaintext (8) will be returned in the receiver system (9). Receiver (9) receives the message in the form of ciphertext which is next will be decrypted to see the original message. It can be seen that the message sent from the sender to the receiver through provider is a cryptography method encrypted message. In the proposed method we are working on, there are some methods in building prototype of secret message in chatting. They are:

51

3.1. Message encryption and decryption with vigenere cipher model

Vigenere Cipher is a polyalphabetic substitution cipher algorithm. It means, for every similar letter in a plaintext is not substituted by a letter but another letter based on the key used to encrypt. Vigenere Cipher is the simple form of polyalphabetic substitution code [31]. Vigenere Cipher is very well-known because it is very easy to understand and implement [32]. Vigenere Cipher can be seen on Figure 4.

a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 4. Vigenere cipher square method [32]

To perform Vigenere cipher encryption, draw a downward vertical line from the plaintext in the vigenere square. Then draw an across line from the key letter to the right. The letter at the intersection shows the ciphertext letter with addition [31]. Mathematically, the encryption process is expressed as follow (1):

$$C_i = (P_i + K_r) \text{ mod } 26 \quad (1)$$

Decryption is done oppositely by drawing across line from key letter to the chipertext letter, then draw a vertical line from ciphertext letter to the plaintext letter with subtraction [31]. The decryption process can be written mathematically as follow (2):

$$C_i = (P_i - K_r) \text{ mod } 26 \quad (2)$$

where,

- C_i = ciphertext (encryption text)
- P_i = plaintext
- K_r = key

3.2. Message encryption and decryption with transposition model

Transposition model is basically making ciphertext by changing plaintext object-object position without shifting the plaintext object, thus in this technique another character is not needed [33]. Reading the matrix value column by column based on the key used is done to get the ciphertext by using this transposition technique [34]. Chiper example of character transposition technique from “Universitas Mulawarman Samarinda” plaintext and using of frame 9x4 is shown by Figure 5.

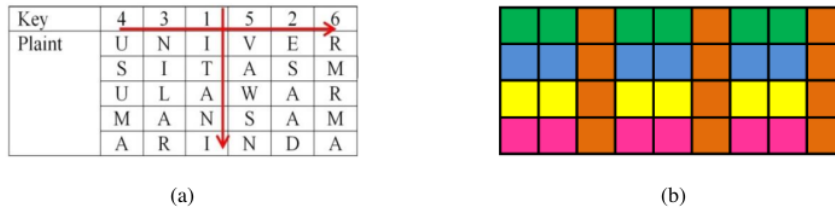


Figure 5. (a) Transposition model and (b) example of frame with 9x4

Plaintext is arranged to the right then downward by “4 3 1 5 2 6” key, so the cipher result will follow the key downward as “ITANI ESAAD NILAR USUMA VAWSN RMRMA”. Encryption for data disguising by using key is known as encryption process. The key used is alphanumeric (a-z, A-Z, 0-9). Figure 6 shows the encryption and decryption process as shown in Figure 7 at frame 9x4 pixel.

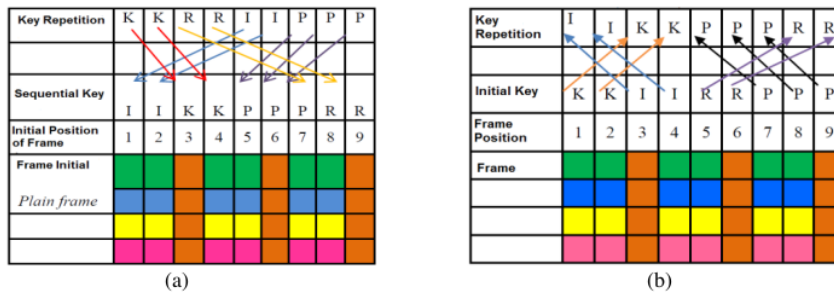


Figure 6. Process of vertical in frame (a) horizontal encryption (b) horizontal decryption

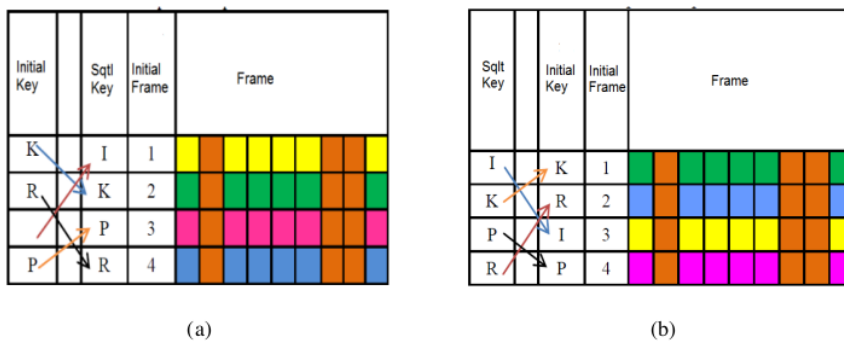


Figure 7. Process of vertical in frame (a) vertical encryption and (b) vertical decryption

Figure 6 shows a process of encryption and decryption horizontally, meanwhile Figure 7 shows the process vertically. This model is used to jumble the number of pixel in the images so it cannot be easily recognized when it is encrypted and can be recognized when it is decrypted.

3.3. Integration with web service model

In this step we carry out data integration by using web service to achieve secret message through sender and receiver in which architecture is oriented in doing service producing different solution in business logic with various application [15]. Web service technology combines the message sent through WhatsApp (WA) web to be disguised. The model of architecture in the web service is shown in Figure 8:

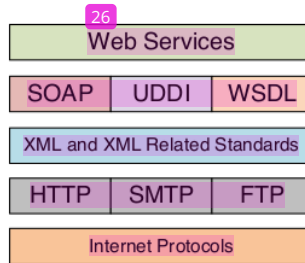


Figure 8. Web services building blocks [15]

3.4. Autentification model

An authentication system with a correlated setup is a pair of algorithms (MAC, VER) for a source space S , a message space M and a distribution P_{xyz}^n over $X^n \times Y^n \times Z^n$, specified as follows [20].

- Setup (1^n). Initially, C is taken from $X^n \times Y^n \times Z^n$ according to P_{xyz}^n . Alice receives X^n , Bob receives Y^n and Oscar receives Z^n .
- Authentication $MAC(X^n, S)$. Upon $S \in S$, Alice uses her secret key X^n to run algorithm MAC to generate a message $M = MAC(X^n, S)$.
- Verification $VER(Y^n, M)$. Upon $M \in M$, Bob uses his secret key Y^n to run algorithm VER to compute $S^- = VER(Y^n, M) \in S \cup \{\perp\}$, where $S^- = \perp$ means that Bob accepts S^- as an authenticated source state while $S^- = \perp$ means a reject.

3.5. Security model

An authentication system (MAC, VER) with a correlated setup for source space S . distribution P_{xyz}^n $X^n \times Y^n \times Z^n$ is t -order secure if the following holds. If user attack doesn't attack, then $\Pr(S^- = S | S = S) = S$ $X^n \times Y^n \times Z^n$ is t -order secure if the following holds [20].

- Authentication attack has only a negligible success probability in n in the following attack:
- After seeing messages $M_1, \dots, M_{(\leq t)}$ from sender to receiver, attacker constructs a new message M^* such that $VER(Y^n, M^*)$ is distinct from \perp, S_1, \dots, S_t , where S_i is the source state in M_i .

4. RESULTS AND DISCUSSION

4.1. Implementation result

We recognize that the WA system already has end to end encryption. However, we need to propose other systems outside the system to give the WA users more confidence in the messages they send. Our research focuses on encrypting and decrypting text and images in the secret message through chatting to be applied in WA application and has successfully tested in android system application, thus the text will be first encrypted before sending to the WA application. The implementation of the secret message is shown in Figure 9.

Figure 9 shows our test results for sending secret messages into private and group chats. The result of encryption process of sentence THIS PLAINTEXT is done by using key sonysonys, i.e. Text for T is encrypted to key S and so on, as the result the step of encryption can be seen as follows:

$$(T + S) \bmod 26 = (19 + 18) \bmod 26 = 11 = L \rightarrow (\text{applied to all text})$$

This step is applied to all letters in encryption. Ciphertext is resulted as follows:

Plaintext : THIS PLAINTEXT
 Key : sony sonysonys
 Ciphertext : LVVQ HZNGFHRVL

To find plaintext result in decryption, this step is applied:

$$(L - S) \bmod 26 = (11 - 18) \bmod 26 = 19 = T \rightarrow (\text{applied to all text})$$

The result of message decryption can be seen as follows:

Ciphertext : LVVQ HZNGFHRVL
 Key : sony sonysonys
 Plaintext : THIS PLAINTEXT

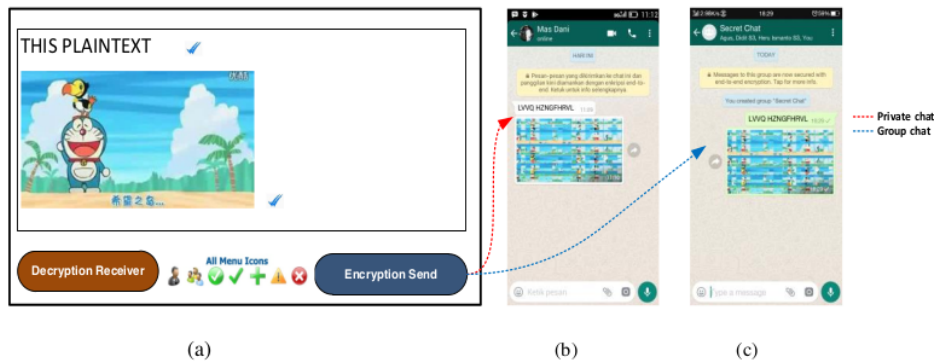


Figure 9. (a) Implementation of plain text and picture to WhatsApp in (b) private and (c) group secret chat

4.2. Discussion result

There are some weaknesses we need to improve in the model we are working on. For instance, how to not separate secret message system and WA so that the model developed does not need to carry out two steps of the process; message sent encryption and message received decryption in the system and sending a message to the WA system. We assume it is more practical and safe to have the model separately with the WA so that users do not need to encrypt the message they do not intend to if it does not require a secret thing.

5. CONCLUSION

The model developed has produced a new prototype in chatting application to add secret message as text security. The model can be used by users of the application in their smartphone. As the result, users will be more secure in using social chatting application than before. In the next research, we are trying to integrate the prototype into social chatting application in web so that the model can be used immediately and embedded in WA system.

REFERENCES

- [1] T. Anwar and M. Abulaish, "A Social Graph based Text Mining Framework for Chat Log Investigation", *Digit. Investig.*, vol. 11 (21), 4, pp. 349-362, Dec. 2014.
- [2] Z. Yan, *et al.*, "A Practical Reputation System for Pervasive Social Chatting", *J. Comput. Syst. Sci.*, vol. 79, no. 5, pp. 556-572, Aug. 2013.
- [3] S. Shrivastava and P. Singh, "Impostor Detection through Chat Analysis", *Procedia Comput. Sci.*, vol. 89, pp. 540-548, 2016.

- 34
- [4] F. A. B. H. Ali and S. M. Aydah, "Development of Prototype Chat System Using Mobile Platform for Disable 31 ple", *Procedia - Soc. Behav. Sci.*, vol. 57, pp. 33-39, Oct. 2012.
- [5] D. C. Uthus and D. W. Aha, "Multiparticipant Chat Analysis: A Survey", *Artif. Intell.*, vol. 199-200, pp. 106-121, 8 June 2013.
- [6] E. Hatfield and R. L. Rapson, "From Pen Pals to Chat Rooms: The Impact of Social Media on Middle Eastern Society", *Springer*, 18 vol. 4, p. 254, January 2015.
- [7] T. Sutikno, et al., "WhatsApp, Viber and Telegram: Which is the Best for Instant Messaging?," *Int. J. Electr. 40 Input. Eng.*, vol. 6, no. 3, pp. 909-914, 2016.
- [8] V. C. da Rocha and D. L. de Macedo, "A Secret-Key Cipher based on a Non-Linear Structured Code", *Comput. Commun.*, vol. 22, pp. 758-761, 1999.
- [9] M. Caboara, et al., "Lattice Polly Cracker cryptosystems", *J. Symb. Comput.*, vol. 46, no. 5, pp. 534-549, 9 May 2011.
- [10] B. Pumama and a. H. H. Rohayani, "A New Modified Caesar Cipher Cryptography Method with LegibleCiphertext 47 m a Message to Be Encrypted", *Procedia Comput. Sci.*, vol. 59, no. Iccsci, pp. 195-204, 2015.
- [11] A. M. Yousef, "Cryptanalysis of a Quadratic Knapsack cryptosystem", *Comput. Math. with Appl.*, vol. 61, no. 4, pp. 7261-1265, Feb. 2011.
- [12] S. Oukili and S. Bri, "High Throughput FPGA Implementation of Data Encryption Standard with Time Variable Sub-Keys", *Int. J. Electr. Comput. Eng.*, vol. 6, no. 1, pp. 298-306, 2016.
- [13] X. Sun, "A Scheme of Concealment and Transmission of Secret Information in Text Files", *Phys. Procedia*, vol. 27, pp. 1365-1368, 2012.
- [14] Z. Zhang, "Controlled Teleportation of an Arbitrary n-qubit Quantum Information using Quantum Secret Sharing 38 Classical Message", *Phys. Lett. A*, vol. 352, no. 1-2, pp. 55-58, Mar. 2006.
- [15] 44 Moradian, "Integrating Web Services and Intelligent Agents in Supply Chain for Securing Sensitive Messages", in *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems*, 28 771-778, 2008.
- [16] I. Alsmadi and D. Xu, "Security of Software Defined Networks: A Survey", *Comput. Secur.*, vol. 53, pp. 79-108, 16 tember 2015.
- [17] L. D. Singh and K. M. Singh, "Implementation of Text Encryption using Elliptic Curve Cryptography", *Procedia Comput. Sci.*, vol. 54, no. 1, pp. 7292, 2015.
- [18] J. Zarepour-Ahmadabadi, et al., "An Adaptive Secret Image sharing with a new Bitwise Steganographic Property", *Inf. Sci. (Ny)*, vol. 369, pp. 467-480, 25 mber 2016.
- [19] L. A. Khan, et al., "Crypt Analysis of Two Time Pads in Case of Compressed Speech", *Comput. Electr. Eng.*, vol. 37, no. 4, pp. 559-569, July 2011.
- [20] S. Jiang, "On message authentication with a correlated setup", *Inf. Process. Lett.*, vol. 116, no. 4, pp. 289-293, April 2016. 35
- [21] J. Sung, et al., "Cryptanalysis of an Involutional Block Cipher using Cellular Automata", *Inf. Process. Lett.*, vol. 104, no. 5, pp. 183-185, Nov. 2007. 33
- [22] F. Özkaynak and A. B. Özer, "Cryptanalysis of a new Image Encryption Algorithm based on Chaos", *Opt. - Int. J. Light Electron Opt.*, 45 127, no. 13, pp. 5190-5192, July 2016. 46
- [23] H.-C. Chen, et al., "A Secure group-based Mobile Chat Protocol", *J. Ambient Intell. Humaniz. Comput.*, vol. 7, 36 5, pp. 693-703, Maret 2016.
- [24] A. V. Dahat and P. V. Chavan, "Secret Sharing based Visual Cryptography Scheme Using CMY Color Space", *Procedia Comput. Sci.* 13 ol. 78, pp. 563-570, 2016.
- [25] D. S. Stein, et al., "From 'Hello' to Higher-Order Thinking: The Effect of Coaching and Feedback on Online 5 ats", *Internet High. Educ.*, vol. 16, pp. 78-84, January 2013.
- [26] 5 N. El-Emam and R. A. S. AL-Zubidy, "New steganography algorithm to conceal a large amount of secret message using hybrid adaptive neural networks with modified adaptive genetic algorithm," *J. Syst. Softw.*, vol. 86, no. 6, pp. 1465-1432 June 2013.
- [27] A. Malik, et al., "A high Capacity Text Steganography Scheme based on LZW Compression and Color Coding", *Eng. Sci. Technol. an Int. J.*, pp. 3 11, August 2016.
- [28] T. Narendra Babu, et al., "Implementati 50 of High Security Cryptographic System with Improved Error Correction and Detection Rate using FPGA", *Int. J. Electr. Comput. Eng.*, vol. 6, no. 2, pp. 602-610, 2016.
- [29] A. H. Ali and A. M. Sagheer, "Design and Implementation of Secure Chatting Application with end to end Encryption", *J. Eng. Appl. Sci.*, vol. 12, no. 1, pp. 156-160, 2017.
- [30] S. H. Ahmed, et al., "Combining Steganography and Cryptography on Android Platform to Achive a High-Level 12 urity", *J. Eng. Appl. Sci.*, vol. 12, no. 17, pp. 4448-4452, 2017.
- [31] A. Bhateja and S. Kumar, "Genetic Algorithm with Elitism for Cryptanalysis of Vigenere Cipher", in *Issues and Challenges in Intelligent 20 mputing Techniques (ICICT), 2014 International Conference on*, 2014, pp. 373-377.
- [32] A. Saraswat, et al., "An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure 30 nunication", *Procedia - Procedia Comput. Sci.*, vol. 92, pp. 355-360, 2016.
- [33] B. H. Krishna, et al., "Multiple Text Encryption, Key Entrenched, Distributed Cipher using Pairing Functions and Transposition Ciphers", in *This full-text paper was peer-reviewed and accepted to be presented at the IEEE 11 PNET 2016 conference*, 2016, pp. 1059-1061.
- [34] M. Jain and S. K. Lenka, "Secret Data Transmission using Vital Image Steganography over Transposition Cipher", in *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on*, 2016, pp. 1026-1029.

BIOGRAPHIES OF AUTHORS



Dr. Hamdani is a lecturer and a researchers at Department of Computer Science in Universitas Mulawarman, Indonesia. He obtained his ¹⁷achelor degree of Informatics in Universitas Ahmad Dahlan, Indonesia (2002). He obtained his ⁶aster of ⁶omputer Science in Universitas Gadjah Mada, Indonesia (2009) and Ph.D in Computer Science at Department of Computer Science & Electronics in Universitas Gadjah Mada, Yogyakarta, Indonesia (2018). His research interests include decision support systems (DSS), group decision support systems (GDSS), social networks analysis, intelligent system, information security and web engineering. E-mail : hamdani@fkti.unmul.ac.id; dani@ieee.org / Web : <http://odahetam.com>



Heru Ismanto received his bachelor's of Informatics, and Master of Computer Science from Universitas Padjadjaran (1996) and Universitas Gadjah Mada (2009) respectively. Currently he is a lecturer at ⁶epartment of Informatics Engineering, Universitas Musamus, Merauke, Papua and his a Ph.D student at ⁶epartment of Computer Science and Electronics, Universitas Gadjah Mada since 2014. He was interesting in Decision Support System, GIS, e-Government System. Email: heru@unmus.ac.id



Agus Qomaruddin Munir received his bachelor's of Informatics, and ¹⁷aster of Computer Science from Universitas Islam Indonesia (2001) and Universitas Gadjah Mada (2009) respectively. Currently he is a lecture ⁶t Department of Informatics Engineering, Universitas Respati Yogyakarta and his a PhD student at ⁶epartment of Computer Science and Electronics, Universitas Gadjah Mada since 2014. He was interesting in Decision Support System, GIS, e-Government System. Email: agusqnmnr@yahoo.com



Budi Rahmani received his bachelor's of Electrical Engineering, and Master of Informatics from ²³yakarta State University and Dian Nuswantoro University in 2003 and 2010 respectively. Currently he is a PhD student at ⁶epartment of Computer Science and Electronics, Universitas Gadjah Mada since 2014. He was interesting in Embedded System and Robotics. Currently his research focused is computer vision and control system for robot. His other research interests include decision support system using artificial neural network. He can be contacted by email: budirahmani@gmail.com <http://budirahmani.wordpress.com>



Andri Syafrianto is a lecturer and a researches at ⁶epartment of Informatics Engineering in STMIK El Rahma, Yogyakarta and Born April 9th, 1983 in Palembang, Indonesia. He obtained his bachelor degree of Informatics E²⁴ngineering in Universitas Bina Darma Palembang, Indonesia (2005). He obtained his Master of Computer Science in Universitas Gadjah Mada, Indonesia (2010). His research interests include decision support systems (DSS), intelligent system, Information system and Cryptanalysis. Email: andrisyafrianto@gmail.com



Didit Suprihanto is a ²³PhD Student at Department of Computer Science and Electronics Gadjah Mada University and lecturer at Department of Electrical Engineering, Universitas Mulawarman, Samarinda, Indonesia. His research interests include computer networks security, e-Government related issues and security assessment. Email: didit.suprihanto@ft.unmul.ac.id



Dr. Anindita Septiarini was born in Nganjuk, East Java, Indonesia in September 1st 1982. She received her Bachelor degree in Informatic Engineering of ¹⁷ersitas Surabaya, Indonesia in 2005. She received her Master of Computer Science deg⁶e at Universitas Gadjah Mada, Yogyakarta, Indonesia in 2009 and Ph.D in Computer Science at Department of Computer Science & Electronics in Universitas Gadjah Mada, Yogyakarta, Indonesia (2018). She is working as a lecture in the department of Computer Science Universitas Mulawarman, Samarinda, Indonesia since 2009. Her research interest are image processing, pattern recognition and neural network. Email: anindita.septiarini@gmail.com

Paper 10

ORIGINALITY REPORT

25%

SIMILARITY INDEX

1%

INTERNET SOURCES

24%

PUBLICATIONS

1%

STUDENT PAPERS

PRIMARY SOURCES

- 1** Assaad El Makhroufi, Nisrine Chekroun, Noha Tagmouti, Samir El Adib, Naoufal Raissouni. "Improvements in space radiation-tolerant FPGA implementation of land surface temperature-split window algorithm", International Journal of Electrical and Computer Engineering (IJECE), 2021
Publication 2%
 - 2** Goncalo Ribeiro, Marin Grabovschi, Mario Antunes, Luis Frazao. "Ncryptr: A symmetric and asymmetric encryption application", 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), 2019
Publication 1%
 - 3** Narendra Babu T, Fazal Noorbasha, Leenendra Chowdary Gunnam. "Implementation of High Security Cryptographic System with Improved Error Correction and Detection Rate using FPGA", International Journal of Electrical and Computer Engineering (IJECE), 2016
Publication 1%
-

4

Fatih Özkaynak, Ahmet Bedri Özer.
"Cryptanalysis of a new image encryption
algorithm based on chaos", Optik -
International Journal for Light and Electron
Optics, 2016

Publication

1 %

5

Ruili Wang, Wanting Ji. "Computational
Intelligence for Information Security: A
Survey", IEEE Transactions on Emerging
Topics in Computational Intelligence, 2020

Publication

1 %

6

Sholeh, Firdaus Ismail. "White blood cell
segmentation for fresh blood smear images",
2013 International Conference on Advanced
Computer Science and Information Systems
(ICACISIS), 2013.

Publication

1 %

7

Edwin Romeroso Arboleda, Carla Eunice R.
Fenomeno, Joshua Z. Jimenez. "KED-AES
algorithm: combined key encryption
decryption and advance encryption standard
algorithm", International Journal of Advances
in Applied Sciences, 2019

Publication

1 %

8

www.ripublication.com

Internet Source

1 %

9

Dilip Kumar Sharma, Ningthoujam
Chidananda Singh, Daneshwari A Noola,

1 %

Amala Nirmal Doss, Janaki Sivakumar. "A review on various cryptographic techniques & algorithms", Materials Today: Proceedings, 2021

Publication

10

da Rocha, V.C.. "A secret-key cipher based on a non-linear structured code", Computer Communications, 19990525

Publication

11

Giridhar Maji, Sharmistha Mandal, Narayan C. Debnath, Soumya Sen. "Pixel Value Difference Based Image Steganography with One Time Pad Encryption", 2019 IEEE 17th International Conference on Industrial Informatics (INDIN), 2019

Publication

12

Seeven Amic, K.M. Sunjiv Soyjaudah, Heman Mohabeer, Gianeshwar Ramsawock. "Cryptanalysis of DES-16 using Binary Firefly Algorithm", 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech), 2016

Publication

13

Meng-Chuan Tsai, Chia-Wen Tsai. "Applying online externally-facilitated regulated learning and computational thinking to improve

1 %

1 %

1 %

1 %

students' learning", Universal Access in the Information Society, 2017

Publication

14

Shreya Ghosh, Tarique Anwar. "Depression Intensity Estimation via Social Media: A Deep Learning Approach", IEEE Transactions on Computational Social Systems, 2021

Publication

1 %

15

Aruna Malik, Geeta Sikka, Harsh K. Verma. "A high capacity text steganography scheme based on LZW compression and color coding", Engineering Science and Technology, an International Journal, 2017

Publication

1 %

16

Sarala Ghimire, Jae Young Choi, Bumshik Lee. "Using Blockchain for Improved Video Integrity Verification", IEEE Transactions on Multimedia, 2020

Publication

1 %

17

Dyah Apriliani, Taufiq Abidin, Edhy Sutanta, Amir Hamzah, Oman Somantri. "SentiHotel: a sentiment analysis application of hotel services using an optimized neural network", Bulletin of Electrical Engineering and Informatics, 2021

Publication

<1 %

18

Rusydi Umar, Imam Riadi, Guntur Maulana. "A Comparative Study of Forensic Tools for

<1 %

WhatsApp Analysis using NIST
Measurements", International Journal of
Advanced Computer Science and Applications,
2017

Publication

19

Zhang, Z.j.. "Controlled teleportation of an
arbitrary n-qubit quantum information using
quantum secret sharing of classical message",
Physics Letters A, 20060320

Publication

20

Arief Susanto, Tutik Khotimah, Muhammad
Taufik Sumadi, Joko Warsito, Rihartanto ..
"Image encryption using vigenere cipher with
bit circular shift", International Journal of
Engineering & Technology, 2018

Publication

21

Jian Shen, Tianqi Zhou, Chin-Feng Lai, Jiguo Li,
Xiong Li. "Hierarchical Trust Level Evaluation
for Pervasive Social Networking", IEEE Access,
2017

Publication

22

Sajasi, Sara, and Amir Masoud Eftekhari
Moghadam. "A high quality image
steganography scheme based on Fuzzy
Inference System", 2013 13th Iranian
Conference on Fuzzy Systems (IFSC), 2013.

Publication

<1 %

<1 %

<1 %

<1 %

23 Shidik, Guruh Fajar, Azhari ., and Khabib Mustofa. "Evaluation of Selection Policy with Various Virtual Machine Instances in Dynamic VM Consolidation for Energy Efficient at Cloud Data Centers", Journal of Networks, 2015. <1 %
Publication

24 "The Data-Driven Fuzzy System with Fuzzy Subtractive Clustering for Time Series Modeling", International Journal of Innovative Technology and Exploring Engineering, 2020 <1 %
Publication

25 Ali Sadr, Raziye Sadat Okhovat. "Security in the speech cryptosystem based on blind sources separation", Multimedia Tools and Applications, 2014 <1 %
Publication

26 Beznosov, K.. "Introduction to Web services and their security", Information Security Technical Report, 2005 <1 %
Publication

27 Fenxiang Fu, Min Jiang. "Multihop nondestructive teleportation via different nonmaximally entangled channels", Journal of the Optical Society of America B, 2020 <1 %
Publication

28 Hlabishi I. Kobo, Adnan M. Abu-Mahfouz, Gerhard P. Hancke. "A Survey on Software- <1 %

Defined Wireless Sensor Networks:
Challenges and Design Requirements", IEEE
Access, 2017

Publication

29

Lizhi Xiong, Xinwei Zhong, Ching-Nung Yang,
Xiao Han. "Transform Domain-Based
Invertible and Lossless Secret Image Sharing
With Authentication", IEEE Transactions on
Information Forensics and Security, 2021

Publication

<1 %

30

Peppino Fazio, Miralem Mehic, Pavol Partila,
Jaromir Tovarek, Miroslav Voznak. "A New
Mobility Samples Encoding Scheme Based on
Pairing Functions and Data Analytics", 2020
IEEE/ACM 24th International Symposium on
Distributed Simulation and Real Time
Applications (DS-RT), 2020

Publication

<1 %

31

Koray Balci, Albert Ali Salah. "Automatic
Classification of Player Complaints in Social
Games", IEEE Transactions on Computational
Intelligence and AI in Games, 2017

Publication

<1 %

32

"Computational Science and Its Applications –
ICCSA 2020", Springer Science and Business
Media LLC, 2020

Publication

<1 %

33

Muhammad Hanif, Rizwan Ali Naqvi, Sagheer Abbas, Muhammad Adnan Khan, Nadeem Iqbal. "A Novel and Efficient 3D Multiple Images Encryption Scheme Based on Chaotic Systems and Swapping Operations", IEEE Access, 2020

Publication

<1 %

34

Nian Afrian Nuari, Paisal Halim, Syamsiah Badruddin, Taufan Maulamin et al. "Caring of Disabilities Deaf Mute Patient with Talking Devices Application Based on Mobile", International Journal of Engineering & Technology, 2018

Publication

<1 %

35

Ascension Hern Encinas, Angel Mart Rey, J.L. P Iglesias, Gerardo Rodr S, Araceli Queiruga Dios. "Cryptographic Properties of Second-Order Memory Elementary Cellular Automata", 2008 Third International Conference on Availability, Reliability and Security, 2008

Publication

<1 %

36

Kanusu Srinivasa Rao, Mandapati Sridhar. "A Lossless Secret Image Sharing Scheme based on Bit Sharing Visual Cryptography", 2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE), 2018

<1 %

37

Hsing-Chung Chen, Hong Chang, Tzu-Liang Kung, Yung-Fa Huang, Ze-Min Lin, Pei-Chi Yeh, Qiu-Hua Ruan. "Chapter 6 A Secure Color-Code Key Exchange Protocol for Mobile Chat Application", Springer Science and Business Media LLC, 2018

Publication

<1 %

38

Mihai Horia Zaharia, Florin Alexandru Hodorogea. "Research stakeholders identification using an mobile agent's framework", Expert Systems with Applications, 2017

Publication

<1 %

39

Ahmed Taha, Aya S. Hammad, Mazen M. Selim. "A High Capacity Algorithm for Information Hiding in Arabic Text", Journal of King Saud University - Computer and Information Sciences, 2018

Publication

<1 %

40

V.C. da Rocha. "Coding for privacy with burst adaptive permutations", Seamless Interconnection for Universal Services Global Telecommunications Conference GLOBECOM 99 (Cat No 99CH37042) GLOCOM-99, 1999

Publication

<1 %

41

David C. Uthus, David W. Aha. "Multiparticipant chat analysis: A survey",

<1 %

Artificial Intelligence, 2013

Publication

42

Dina Lusiana Setyowati, Swandari Paramita, Riza Hayati Ifroh, Tanti Asrianti, Efi Fitriani, Wahnadita Rahman. "Work readiness during COVID-19 among taxibike online drivers in Samarinda, Indonesia", International Journal of Public Health Science (IJPHS), 2021

Publication

<1 %

43

Sarang Shrivastava, Priyanja Singh, Ranvijay. "Impostor Detection through Chat Analysis", Procedia Computer Science, 2016

Publication

<1 %

44

"Knowledge-Based Intelligent Information and Engineering Systems", Springer Nature, 2008

Publication

<1 %

45

Ilsun You, Jin Li. "Special issue on security and privacy techniques in mobile cloud computing", Journal of Ambient Intelligence and Humanized Computing, 2016

Publication

<1 %

46

Dhivya Ravichandran, Padmapriya Praveenkumar, John Bosco Balaguru Rayappan, Rengarajan Amirtharajan. "DNA Chaos Blend to Secure Medical Privacy", IEEE Transactions on NanoBioscience, 2017

Publication

<1 %

47

Diaz, R. D., L. H. Encinas, and J. M. Masque. "Cryptanalysis of two combinatorial public key cryptosystems", Logic Journal of IGPL, 2015.

Publication

<1 %

48

www.abulaish.com

Internet Source

<1 %

49

Anwar, Tarique, and Muhammad Abulaish. "A social graph based text mining framework for chat log investigation", Digital Investigation, 2014.

Publication

<1 %

50

Subhi R. M. Zeebaree. "DES encryption and decryption algorithm implementation based on FPGA", Indonesian Journal of Electrical Engineering and Computer Science, 2020

Publication

<1 %

51

Mohammed H. Ahmed, Ahmed K Shibeeb, Ahmed H. Mohammed. "Solve Polyalphabetic Cipher Based on Intelligent System", 2021 International Conference on Communication & Information Technology (ICICT), 2021

Publication

<1 %

52

Vishal Sharma, Ilsun You, Ravinder Kumar, Pankoo Kim. "Computational Offloading for Efficient Trust Management in Pervasive Online Social Networks Using Osmotic Computing", IEEE Access, 2017

Publication

<1 %

53

"Innovative Mobile and Internet Services in Ubiquitous Computing", Springer Science and Business Media LLC, 2021

Publication

<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off