SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal of Publications & Informatics Engineering Research
Volume 4, Number 1, October 2019
DOI: https://doi.org/10.33395/sinkron.v3i1.10244
e-ISSN: 2541-2019
p-ISSN: 2541-044X

Digital Signs Security System using AES-Blowfish-RSA Hybrid Cryptography Approach

Christnatalis HS
Universitas Prima Indonesia
Medan, Indonesia
christnatalis@unprimdn.ac.id

Amir Mahmud Husein
University of Prima Indonesia
Medan, Indonesia
amirmahmud@unprimdn.ac.id

Abstract- Increasing application of digital signatures in legitimate authentication of administrative documents in both public and private environments is one of the points of concern, especially the issue of security and integrity of ownership of signatures. Digital signature is a mathematical scheme, which a unit to identify and prove the authenticity of the owner of the message or document. The study aims to analyze security patterns and identification of digital signatures on documents using the RSA-AES-Blowfish hybrid cryptographic method approach for securing digital signatures, while the Kohonen SOM method is applied to identify ownership recognition of signature images. The analysis framework used in this study is each signature will be stored in the form of a digital image file that has been encrypted using hybrid method of AES-Blowfish with the SHA 256 hash function. Process of forming private keys and public keys in the signature image using the RSA algorithm. Authentic verification of the use of digital signatures on the document has 2 (two) stages, the first stage is signature will be valid used on the document if the result of hashing the selected signature image is the same based on the private key and public key entered by the user, while the second stage identification is done using the Kohonen SOM method to validate the similarity of the chosen signature with the ownership of the signature.

Keywords— Hybrid Cryptography; RSA-AES-Blowfish; Digital Signatures; Data Security; Kohonen SOM

I. INTRODUCTION

Generally, digital signatures are mathematical schemes, unitally to identify and authenticate from the owner of a message or document (Suratma & Azis, 2017). One of the main functions of the use of digital signatures is as evidence of an agreement between the first and second parties. Thus, digital signatures can be accounted for quickly.

In Indonesia, digital signatures are regulated in Law Number 11 of 2008 Article 11 Paragraph 1 concerning Information and Electronic Transactions (ITE Law), Government Regulation Number 82 of 2012 Article 52 Paragraphs 1 and 2 concerning Operation of Electronic Systems and Transactions and POJK 77/2016 Article 41 concerning lending and borrowing services based on Information Technology (IT). Signatures play an important role in the business world. Most important documents require signatures as proof of approval. The application of digital signatures as valid proofs in documents is very popular nowadays, this is with the many new startup companies that are building digital signature systems such as PriviID, SignEasy, SignDoc Mobile, HelloSing, SignNow and others. The ease of carrying out various activities using only email, social media accounts, or telephone numbers as identity, actually holds the potential to be used in crime, so that the confidentiality of data, integrity and information security in the era of internet technology is one of the special points of attention, ease of sending data using the internet is very vital and significant for data security (Husein, Wijaya, Tommy, Elhanafi, & Siregar, 2018)

Based on the results of several studies, the application of cryptography in securing digital signatures is capable of producing a high level of security and can be used as authenticating user authentication. In this research, security pattern

SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal of Publications & Informatics Engineering Research
Volume 4, Number 1, October 2019
DOI: https://doi.org/10.33395/sinkron.v3i1.10244
e-ISSN: 2541-2019
p-ISSN: 2541-044X

analysis and identification of digital signatures will be carried out in the Faculty of Technology and Computer Science (*Fakultas Teknologi dan Ilmu Komputer* aka FTIK) of the Universitas Prima Indonesia by applying AES-Blowfish-RSA hybrid cryptography for image security while the Kohonen SOM Neural Network method for identification of signature recognition

II. Literature Review

Pattern recognition is one of the fields of research that is quite popular because it can be useful for various purposes such as identification of signatures (Husein, AM, & Harahap M, 2017). In general there are two approaches used for hand identification namely offline and online (Randika, K S., 2014), Neural Network (NN) method (Mukherjee, et all, 2017), Kohonen SOM (Harahap, M., Husein, A M., Darma, A., 2017), back-propagation (Kedia, S., Monga, Er., G, 2017) was proposed by many researchers to identify digital signatures, but the security of digital signature images is one technique which can be applied to avoid misuse in crime. Cryptography is one of the techniques used to secure and guarantee the confidentiality of data (Bhuvaneshwari, 2016), the application of cryptography to secure digital signatures has been proposed by many researchers, such as (Sanger, 2015) proposing RSA and Hash MD5 cryptographic algorithms for the security mechanism of digital signatures in digital data exchange, (Suratmat & Aziz, 2017) uses the QR Code with the Advanced Encryption Standard (AES) method for securing digital signatures that function as authentication of the leader's signature as well as verifying rival documents for the collection of legal goods, (Fauzan & Paulus, 2018) using the SHA-256 algorithm as a digital signature, the AES algorithm as file encryption, and the RSA algorithm as an asymmetric key in the distribution of files and digital signatures.

An undisclosed message is called a plaintext (meaning clear text that can be understood), while an encoded message is called a ciphertext (meaning encoded text). The process of encoding plaintext into ciphertext is called encryption and the process of reversing ciphertext into plaintext is called decryption.

1. Symmetry Cryptography

Symmetry cryptography is often called the classical cryptographic algorithm because it uses the same key for the encryption and decryption process (Ariyus, 2010). This algorithm has been around for more than 4000 years. When sending messages using this algorithm, the recipient of the message must be notified of the key of the message in order to describe the message sent (Diedrich, 2012). The security of messages that use this algorithm depends on the key. If the key is known to someone else, that person will be able to encrypt and decrypt the message. Key symmetry algorithms include:

a. Data Encryption Standard (DES)
b. RC2, RC4, RC5, RC6
c. International Data Encryption Algorithm
d. Advanced Encryption Standard
e. One Time Pad (OTP).
f. A5, etc.

2. Cryptography Asymmetry

Asymmetric algorithms are often also called public key algorithms, meaning that the keywords used to do encryption and decryption are different. In the key asymmetry algorithm is divided into two parts, namely:

a. Public key: a key that can be known by everyone.
b. Secret key (private key): a key that is only known by the owner of the key. These keys are related to each other. With public keys anyone can encrypt the message but cannot decrypt it. Only people who have a secret key can decrypt the message. The asymmetry algorithm can send messages more safely than the symmetry algorithm. Public key algorithms include:
    1. Digital Signature Algorithm (DSA).
    2. RSA
    3. Diffie-Hellman
    4. Elliptic Curve Cryptography
    5. Quantum Cryptography

III. Proposed Method

1. Proposed Model

Our study proposing hybrid AES and Blowfish methods, these two symmetrical methods will increase the time for encryption and decryption in patient medical record data taken from a database with portable document file format (PDF). In Figure 1 and Figure 2 is an illustrative framework for the hybrid cryptographic and decryption processes that we propose. The encryption of digital signatures uses SHA 256 while the process of generating private keys and public keys uses two approaches, namely the RSA method.

SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal of Publications & Informatics Engineering Research
Volume 4, Number 1, October 2019
DOI: https://doi.org/10.33395/sinkron.v3i1.10244
e-ISSN: 2541-2019
p-ISSN: 2541-044X

The main purpose of applying the model for data security for this signature is to facilitate the process of approving correspondence documents within the University of Indonesia, especially the Information Engineering Study Program, where officials who have the authority to approve documents have stored their signature data with cryptographic techniques.

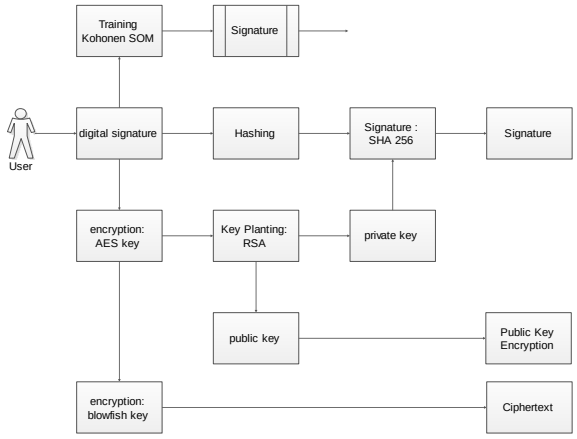

Figure 1. The Proposed Model for Signature Encryption

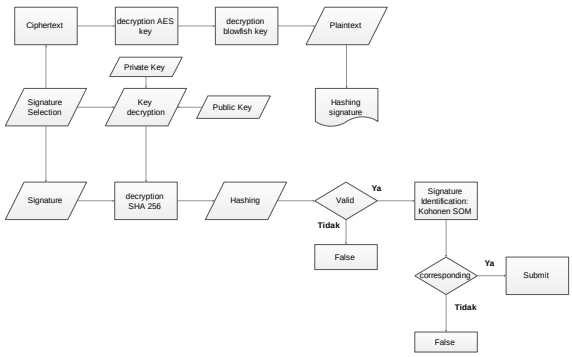

Figure 2. The Proposed Model for Signature Description

2. Data obtained

The process of entering the signature using a pen designed in the application then for each signature will be extracted its characteristics. From the example the signature will be stored in the database then training will be conducted. The signature sampling process is a total of 500 samples obtained from 100 different people from which each person took 3 different signatures. Some examples of data are shown in the following table:

Table 1. Signatures Dataset

IV. RESULT AND DISCUSSION

The stages of the signature security method use the flow of analysis as shown below:

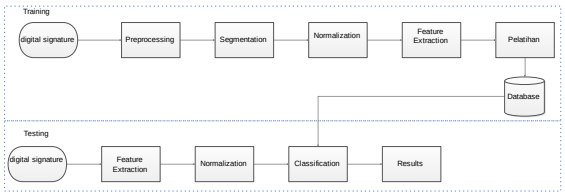

Figure 4. Analysis Stages of the Model

The dataset to be identified is the signature pattern character, where the data acquisition of the signature image for training and testing with a ratio of 75:25. For training data, 500 signatures from 100 respondents were used, where each respondent was taken with 5 signatures. While for testing needs, the image of the signature will be 300 signatures were used, also from 100 these respondents assuming each respondent was taken with 3 signatures.

SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal of Publications & Informatics Engineering Research
Volume 4, Number 1, October 2019
DOI: https://doi.org/10.33395/sinkron.v3i1.10244
e-ISSN: 2541-2019
p-ISSN: 2541-044X

Each signature will be encrypted using AES and Blowfish method where the SHA 256 hashing function is applied to integrity, the private key generation method and the public key uses RSA method. The results of the encryption process are shown in table 2 below.

Table 2. Signature Encryption Results

User	Signature (size)	Encryption Runtime (t)		
		BF	AES	AES-BF
User 1	372.67	124.22	165.89	244.22
User 2	367.33	122.44	164.11	242.44
User 3	424.00	141.33	183.00	261.33
User 4	214.67	71.56	113.22	191.56
User 5	142.00	47.33	89.00	167.33
User 6	185.33	61.78	103.44	181.78
User 7	426.67	142.22	183.89	262.22
User 8	230.00	76.67	118.33	196.67
User 9	179.33	59.78	101.44	179.78
User ..	296.67	98.89	140.56	218.89

The next stage is the process of identifying signatures using the Kohonen SOM approach. From the signature data, the preprocessing process is carried out, that is, the signature taken is processed first to be equalized in size and converted to a gray scale. At this stage, starting from taking pictures of signatures directly entered by online respondents in an application designed with pen facilities to facilitate the making of signatures. Then the results of the respondent's signature will be stored in a database that is limited to a 16x16 pixel size box, then proceed with the preprocessing process.

Preprocessing consists of 2 (two) main stages, namely cropping and scaling. This preprocessing stage is needed because each signature image does not have the same location and size so it is necessary to uniform the signature image data from differences in location and size so that the results of preprocessing can be used as input at the feature extraction stage.

Feature extraction process using the PCA approach. The PCA method basically rotates a set of points around the average in order to adjust to the main component, this method moves the variance as much as possible by using linear transformation into several dimensions.

The feature extraction results will be used as Kohonen SOM input parameters by determining the threshold value $\theta = 0.5$. Learning rate used is $\alpha = 0.2$. The initial weight chosen is w1 = 0.1 and w2 = 0.1. Maximum Epoh = 100, the error value is obtained from ty value.

This artificial neural network training serves to teach patterns of existing signatures so that the network is expected to recognize new character patterns that are given. The last step is the stored weight.

In table 3 is the weighting stage that will be used in SOM kohonen, the value of n (t) is a learning rate for testing the identification of digital signature with a value of 0.6. The results of the training using the two approaches can be seen in table 4 and figure 1 graph results

Table 3. Testing Results

No	User	Signature	epoch	Time (t)	Accuracy
1	User 1	5	100	0.98	95%
2	User 2	5	100	0.06	90%
3	User 3	5	100	0.54	95%
4	User 4	5	100	0.65	91%
5	User 5	5	100	0.48	98%
6	User 6	5	100	0.43	92%
7	User 7	5	100	0.90	89%
8	User 8	5	100	0.10	92%
9	User 9	5	100	0.52	90%
..	..	..	..	..	..
100	User 11	5	100	0.43	89%

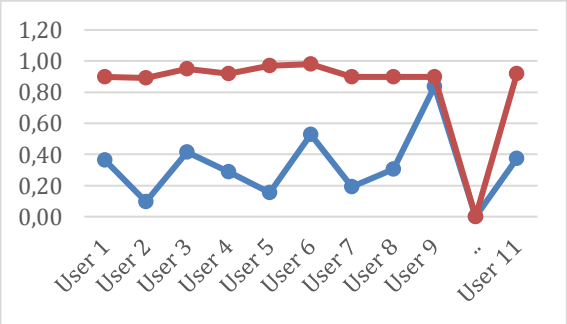

Figure 5. Graphs of Training Results

In table 3 is a table of test results conducted on 100 respondents where data signature data that has been encrypted will be done the classification process uses SOM Kohonen to identify the ownership of signatures, the next step is the process of identifying the image classification of signatures after the encryption process.

SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal of Publications & Informatics Engineering Research
Volume 4, Number 1, October 2019
DOI: https://doi.org/10.33395/sinkron.v3i1.10244
e-ISSN: 2541-2019
p-ISSN: 2541-044X

Table 5 Test Results

No	User	Signature	Iteration	Time (t)	Accuracy
1	User 1	3	10	0.69	94%
2	User 2	3	10	0.22	93%
3	User 3	3	10	0.07	94%
4	User 4	3	10	0.61	93%
5	User 5	3	10	0.81	95%
6	User 6	3	10	0.36	92%
7	User 7	3	10	0.82	91%
8	User 8	3	10	0.20	95%
9	User 9	3	10	0.12	92%
..	..	..	..	..	..
100	User 11	3	10	0.30	95%

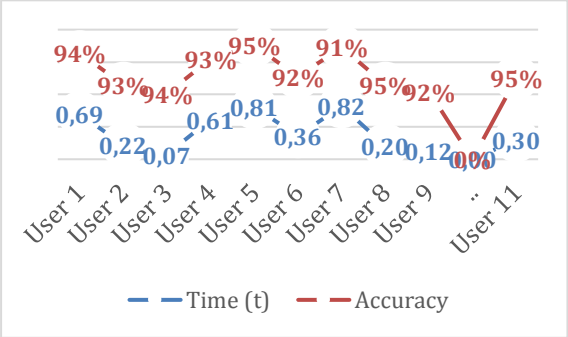

Figure 6. Test Results Graph

V. Conclusion and Suggestion

Based on the results of testing the digital signature data security process using the AES-Blowfish-RSA hybrid cryptographic approach, the initial process can be described as taking a signature image using an application developed to facilitate data storage, AES-Blowfish-RSA hybrid encryption processes are performed on the image to maintain integrity of signature images to avoid misuse, the testing process is carried out with 100 respondents with 5 signature images each then image testing is performed. After the encryption process is carried out the next step is the process of applying the Kohonen SOM method for identification, from the training results the accuracy is quite high at 98% with a time of 0.48 seconds, but at the testing stage there is a significant change in accuracy that is equal to 94% with a time of 0.16, from these results, the efficiency of the testing process time is faster than the training process, but we still need to evaluate methods to improve testing accuracy by considering the computational time efficiency for the next testing process.

VI. Acknowledgment

Thank you to:

1. Kemenristekdikti who has provided assistance in the form of financial support.
2. Universitas Prima Indonesia, which has provided motivational support and facilities.
3. Student majoring in Informatics Engineering at Prima Indonesia University as a partner, giving a dataset.

VII. References

Husein, A M., Bayu, A W, Tommy, Andi, M E, and Siregar, R., 2018, *Performance analysis of AES-Blowfish hybrid algorithm forsecurity of patient medical record data*, IOP Conf. Series: Journal of Physics: Conf. Series 1007 (2018) 012018, doi:10.1088/1742-6596/1007/1/012018.

Husein, A M, Harahap, M., 2017, Pengenalan Multi Wajah Berdasarkan Klasifikasi Kohonen SOM Dioptimalkan dengan Algoritma *Discriminant Analysis* PCA, QUERY: Jurnal Sistem Informasi, Volume: 01, Number: 02, pp 33-39, ISSN 2579-5341.

Husein, A M., Harahap, M., 2017, Penerapan Metode Distance Transform Pada *Kernel Discriminant Analysis* Untuk Pengenalan Pola Tulisan Tangan Angka Berbasis *Principal Component Analysis*. Sinkron, Vol 2, No 2, pp 31-36, e-ISSN:2541-2019, p-ISSN:2541- 044X.

Randika, K S., 2014, *Online and Offline Signature Verification: A Combined Approach*, International Conference on Information and Communication Technologies, doi: 10.1016/j.procs.2015.02.089.

Mukherjee, A., Priya, K., Pandit, M., & Bhattacharya, D., 2017, *Use of Auto Associative Network for signature recognition*, International Journal of Current Engineering and Technology, E-ISSN:2277–4106.

Harahap, M., Husein, A M., Darma, A., 2017, Identifikasi Tanda Tangan Dengan Kohonen SOM berbasis *Principal Component Analysis*. Seminar Nasional APTIKOM (SEMNASTIKOM), pp 333-337.

Journal of Publications & Informatics Engineering Research
Volume 4, Number 1, October 2019
DOI: https://doi.org/10.33395/sinkron.v3i1.10244
e-ISSN: 2541-2019
p-ISSN: 2541-044X

Kedia, S., Monga, Er., G, 2017, *Static Signature Matching Using LDA and Artificial Neural Networks*, International Journal of Advance Research, Ideas and Innovation in Technology, 245-248, Volume3, Issue3, ISSN: 2454-132X.

Ghosh, S N et al., 2015, *Performance Analysis of AES, DES, RSA And AES-DES-RSA Hybrid Algorithm for Data Security*, International Journal of Innovative and Emerging Research in Engineering Volume 2, Issue 5, 83-88.

Bhuvaneshwari M, Tenmozhi S. 2016, *A VLSI architecture for security based stenographic processor with AES algorithm*. International Journal of Electrical and Computer Engineering; pp 1–6.

Suratma, P G., Azis, A., 2017. Tanda Tangan Digital Menggunakan QR Code Dengan Metode *Advanced Encryption Standard*. Techno, Volume 18 No. 1, pp 059-068, ISSN 1410 – 8607.

Fauzan, A M., Paulus, E., 2018, A Framework to Ensure Data Integrity and Safety, Journal of Computing and Applied Informatics (JoCAI) Vol. 02, No. 1, pp 1-11, ISSN: 2580-6769.

Shaikh, A. P., Kaul, V., 2014, *Enhanced Security Algorithm using Hybrid Encryption and ECC*, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 3; PP 80-85.

Kadam, K G., Khairnar, V., 2015, *Hybrid RSA-AES Encryption for Web Services*, International Journal of Technical Research and Applications", Special Issue 31(September, 2015), PP. 51-56.

Behl, R., Sehgal, G., Kumar, M., Gupta, P., Garg, S., 2015, *Experimental comparison between Hybrid RSA-AES and RSA algorithms in IP security*, IJMTER, 588-594.

Kumar B., Boaddh., and Mahawar, L., 2016, *A hybrid security approach based on AES and RSA for cloud data*, International Journal of Advanced Technology and Engineering Exploration", Vol 3(17), 43-49.

Mohammed, H. R., Al-Taee, E. J. A. R., 2015, *Signature Identification and Recognition using Elman Neural Network*, European Journal of Scientific Research, ISSN 1450-216X/1450-202X Vol. 131 No 2.

Daqrouq, K., Sweidan, H., Balamesh, A. & Ajour, M. N., 2017, *Off-Line Handwritten Signature Recognition by Wavelet Entropy and Neural Network*, Entropy 2017, 19, 252; doi:10.3390/e19060252.

Por, L. Y., Beh, D., Ang, T. F., Ong, S. Y., 2013, "An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm", The International Arab Journal of Information Technology, Vol. 10, 51-60