Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5)

Conference Paper · November 2017

DOI: 10.1109/ICON-SONICS.2017.8267827

Atika Sari
Dian Nuswantoro University
68 PUBLICATIONS **313** CITATIONS

De Rosal Ignatius Moses Setiadi
Universitas Dian Nuswantoro Semarang
85 PUBLICATIONS **373** CITATIONS

Eko Hari Rachmawanto
Universitas Dian Nuswantoro Semarang
75 PUBLICATIONS **355** CITATIONS

Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)

Rizky Damara Ardy
Faculty of Computer Science
Dian Nuswantoro University
Semarang, Indonesia
rizky.damara.ardy@gmail.com

Oktaviana Rena Indriani
Faculty of Computer Science
Dian Nuswantoro University
Semarang, Indonesia
oktavianarenaindriani@gmail.com

Christy Atika Sari
Faculty of Computer Science
Dian Nuswantoro University
Semarang, Indonesia
atika.sari@dsn.dinus.ac.id

De Rosal Ignatius Moses Setiadi
Faculty of Computer Science
Dian Nuswantoro University
Semarang, Indonesia
moses@dsn.dinus.ac.id

Eko Hari Rachmawanto
Faculty of Computer Science
Dian Nuswantoro University
Semarang, Indonesia
eko.hari@dsn.dinus.ac.id

Abstract— **Authentication of digital media has been done with the various scheme, one of them is a digital signature. The main reason the technique of digital signature appears on the concerns of people when sending important documents and raises the thought that the file submitted is not changed when it is transmitted and the content is different when received by the recipient of the document. The digital signature attached by the sender to the document can be used as a tool to ensure that the submitted document is authentic or not manipulated. So research on digital signatures should be developed to improve its ability to provide security and prove the authenticity of the image. This paper proposes a combination of three algorithms to the created digital signature, namely: Rivest – Shamir – Adleman (RSA), Vigenere Cipher and Message Digest 5 (MD 5). The proposed method also tested with various attacks to measure the reliability of digital signatures. Various attacks which applied such as blurring, salt, and pepper, Gaussian filters. Based on the attacking result, the smallest change occurred in the blurring attack has a very good PSNR is 86.7532 dB. The experimental result proves the little change of image and filename can affect the validation result. Then, it can be concluded that the proposed method suitable for image authentication.**

Keywords— Digital Signature, RSA, Vigenere, MD5, Authentication, Cryptography

I. INTRODUCTION

In the present, the internet has become a major needs. Almost everyone uses the internet in their daily lives, whether for educational, business, entertainment, and much more [1]. However, along with the rapid development of the Internet, security issues are also more complex. One such security problem is the data theft and data forgery. Data transfer on the internet can be intercepted and changed by the unauthorized person [2]. One way to prevent this is to create a unique sign that ensures that the data are authentic. Cryptography has been used as a method of securing data [3] [4]. For it can be used one of the network security technology called digital signature.

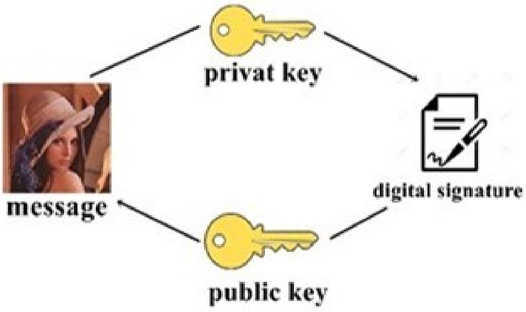

Fig. 1. Commonly process of Digital signature

A digital signature can be used to determine whether the correct data coming from the system, then it is necessary to verify. Digital signatures must have the same functions as conventional signatures, which can guarantee authentication, integrity, and non-repudiation [5]. Digital signatures in their implementation combine two algorithms at once, namely hash function algorithms and public key algorithms [6]. The hash function algorithm is used to form the message digest of a document (text), and the public key algorithm used to encrypt the message digest [7]. The main process in digital signature scheme consists of two processes namely signing (signature) and verification and can show in Fig. 1. The signing process is done by converting a message or document into its message digest and encrypting it using a public key algorithm. As for the verification process used to compare the decrypted message received (ciphertext).

One of the commonly used hash function algorithms is Message- Digest 5 (MD5) [8]. In this study, the results of MD5 are used as key and message on the method of the Vigenere cipher. Vigenere cipher is a type of compound alphabetic cipher that applies alphabetic poly substitution method and belongs to a symmetric key category where the key used for the encryption process is the same as the key used for the decryption process. Then the encryption result of Vigenere cipher is made as the plain text of RSA cryptography algorithm (Rivest-Shamir-Adleman). The RSA algorithm is chosen because it is the first algorithm suitable for digital signatures that use public key encryption [9]. It can guarantee the privacy and authenticity of digital data [6]. The result of RSA encryption in the form of decimal value is then converted into a hexadecimal. The hexadecimal of RSA in here as a digital signature.

II. Related Research

According to research from [6], using digital signatures for digital image authentication. The one where the Hash of the original image is taken and encrypted with the RSA method. It has been successfully implemented using Lena image. The results of the experiments show that with RSA use has high security and is able to authenticate images.

Based on a research paper entitled a modified RSA Algorithm to enhanced digital security [9]. By comparing RSA and modified RSA algorithms simultaneously to process data of different sizes, it was generated that the RSA Key Generated Modem algorithm was faster and could increase security twice. As for RSA algorithm in terms of speed of encryption and decryption faster than Modified RSA algorithm.

In another research [10], many of the protocol security and encryption technologies have adopted from the RSA algorithm. RSA cryptographic algorithms are the most widely used in all public key cryptosystems. It is characterized by high security and easy to implement. That is, it may not only be used to encrypt data, but it can also be used for identity authentication.

Other results of research [5], it shows by RSA digital signature method using a new scheme to generate the private key and public key by using the concept of "Strong Prime". The digital signature of RSA by using different 256, 512, 1024, 2048, 4096, and 8192 different keys. Shows that the computational time required to generate private keys and public keys using the primary key generation normally records a slight variation of time for small to medium key sizes, as opposed to strong primary key generation. But the time for the key generation of Strong Prime is significantly less than the traditional Prime for keys larger than 4096.

In a study conducted by Aditi Saraswat et al [11], the Vigenere cryptographic algorithm was used. Vigenere is one of the polyalphabetic techniques. The polyalphabetic cipher technique is one of the most commonly used and safe ciphers for replacement. The polyalphabetic cipher technique overcomes the weakness of the monoalphabetic technique in which each message character is converted to the same cipher character so it is very susceptible by using frequency analysis. In this technique, each Vigenere character will change depending on the key character. From the above-related research, we can conclude that by using RSA digital signature method for image authentication can be implemented and generate a high-security level. So to optimize its security in this paper the RSA algorithm is combined with Vigenere and MD5.

III. Literature Study

A. Rivest-Shamir-Adleman (RSA)

RSA is an asymmetric cryptography algorithm. This algorithm is the first algorithm most appropriate for signing and encryption and one of the first major cryptographic discoveries with a public key [12]. In this method, there are three main parts: key generation, encryption, and decryption process.

1) Key generation

In RSA algorithm, encryption and decryption process need a public key and private key. Here are the steps to generate the public and private key on RSA algorithm:

Step 1: Generate two prime number p and q, where $p \neq q$.

Step 2: Calculate p and q using Eq. 1-3:

$$n = p \times q \tag{1}$$

$$\emptyset(n) = (p-1) \times (q-1) \tag{2}$$

$$k = \emptyset(n) + 1 \tag{3}$$

Step 3: Factor the value of k to get coprime value, so the first-factor use for e and the second factor is the value of d.

Step 4: Our public key is $[e, n]$ for the sender and pair private key is $[d, n]$ for the receiver.

2) Encryption

To encrypt the sender message (M) using a public key $[e, n]$ that has been generated at key generation process To generate the cipher using Eq. 4.

$$c = (m^e) \: mod \: n \tag{4}$$

Where c is an element of the cipher $(c \in C)$, m is an element of the message $(m \in M)$, e is the public key and n can show at Eq.1.

3) Decryption

To decrypt the cipher (C), from receiver use the private key $[d, n]$. Below is decryption process. Use Eq.5 to perform the decryption process.

$$m = (c^d) \: mod \: n \tag{5}$$

Where, m is an element of the message $(m \in M)$, c as an element of the cipher $(c \in C)$, d is the private key. While n obtained from Eq.1.

B. Vigenere Cipher

A Vigenere cryptosystem is the simple form of polyalphabetic substitution. Compared with monoalphabetic substitution such as Caesar cipher and Shift cipher, Viegener is not so vulnerable to a cipher-breaking, a method called frequency analysis [13]. Encryption and decryption will be given in Eq. 6 and 7.

$$c = (m + k) \: mod \: n \tag{6}$$

$$m = (c - k) \: mod \: n \tag{7}$$

Where:
m = element of message, $m \in M$
c = element of cipher, $c \in C$
k = element of key, $k \in K$
n = max depth value of message

C. Message-Digest 5 (MD5)

MD5 is the most popular hash function that produces 128-bit hash value or 16 Char. MD5 generally use for check integrity of a file. Cycle shift operation, modular addition and bitwise boolean operation [14].

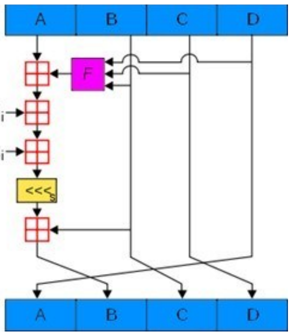

Fig. 2. MD5 main process

For generating message digest MD5 perform two main part, that is padding and compression. Here is the detail of padding and compression process on MD5.

1) Padding

Step 1: The message is added with a number of padding bit until congruent with 448 modulo 512.

Step 2: If the message length is 448 bits, then the message is added with 512 bits to 960 bits. Thus, the length of the padding bits is between 1 and 512.

Step 3: Padding bit consist of “1” bit followed by the remaining “0” bit.

Step 4: Messages that have been given bit padding then added again with 64 bits that state the length of the original message.

Step 5: If the length of the message greater than 264 then length will be used in modulo 264. In other words, if the initial message length is K bit, then 64 bit adds K modulo 264.

Step 5: Once added with 64 bits, the message length now becomes a multiple of 512 bits.

2) Compression

Step 1: MD5 requires 4 buffers each 32 bits long. The total length of the buffer is 4 x 32 bit = 128 bits. These four buffers accommodate intermediate and final results. These four buffers are named A, B, C, and D. Each buffer is initialized with values:

word A: 01 23 45 67
word B: 89 AB CD EF
word C: FE DC BA 98
word D: 76 54 32 10.
These registers are usually called chain variables.

Step 2: The message divided into L block that 512-bit length each block. There are 4 (four) nonlinear functions which are each used in each operation (one function for one block). Eq. 8-11 is used to perform this process.

$$F(X,Y,Z) = (X\&Y)|((\sim X)\&Z) \tag{8}$$
$$G(X,Y,Z) = (X\&Z)|(Y\&(\sim Z)) \tag{9}$$
$$H(X,Y,Z) = X\char`^Y\char`^Z \tag{10}$$
$$I(X,Y,Z) = Y\char`^(X|\sim(Z)) \tag{11}$$

This equation is bitwise operator NOT, XOR, OR and AND. The result will store at variable A, B, C, and D. Main operation process will be shown in Fig.2

IV. Proposed Method

In this section, we will explain about our proposed method, for generating digital signature firstly image hash will encrypt using Vigenere cipher algorithm. The ciphertext of Vigenere will be encrypted using RSA algorithm. The result of RSA encryption is Digital signature of the image. For verification, the digital signature decrypted using RSA and Vigenere cipher algorithm. The result from decryption will compare with a hash of image if match so the image is authentic. For detail explanation author will explain below:

A. Generating Digital Signature (Encryption)

Figure 3 below is a proposed scheme to generate the digital signature:

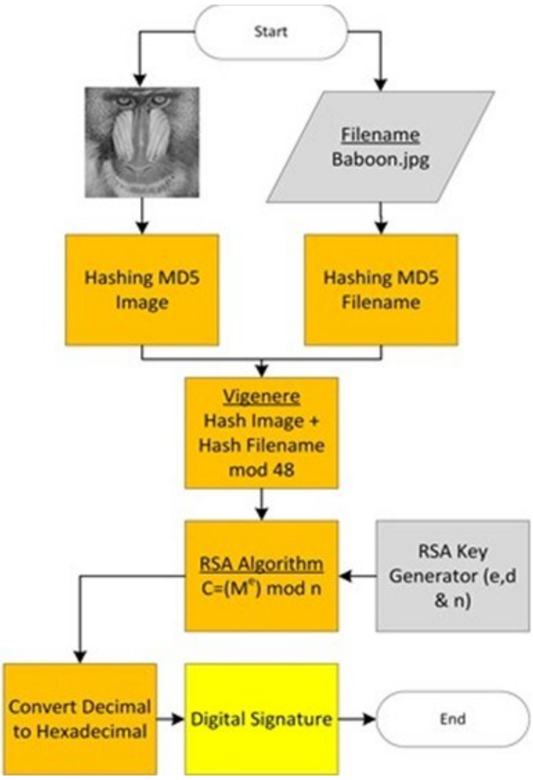

Fig. 3. Proposed Method of Generating Digital Signature

Based on Fig. 3, the input needed is an image, two prime number called prime number 1 (p) and prime number 2 (q). (p) and (q) are for generating a public key (d), a private key

$(e)$and n value of RSA. Here is details explanation of the proposed method for generating digital signatures:

Step 1: Load image.

Step 2: Pre-processing pixel image from matrix $x \times y \times z$ become matrix $1 \times i$ for image pre-processing.

Step 3: Calculate hash pixel of the image that has been processed at step 2 using the MD5 function. The result will be used as plain text Vigenere.

Step 4: Using MD5 function calculate the hash name of the file. Filename message digest will be used as the key of vigenere

Step 5: Encrypt hashing pixel image $(Mvig)$ using Vigenere Algorithm (Eq.7). The value of n at our proposed method is 48, the reason using mod 48 because the result MD5 is ASCII '0' until ASCII 'Z' that have range 43. This process iteration is 32 times because the length of the plaintext is 32 character. After that, the result becomes the RSA message that will encrypt using RSA algorithm.

Step 6: Generating public (e), private key (d) and value (n) of RSA from the input variable (p) and (q), to generate using Eq.1, Eq. 2 & Eq. 3. After that factor the value (k) and get two value, the first-factor store at variable(e) as a public key and the second-factor store at variable (d)as a private key.

Step 7: After generating the public key, RSA using the public key $[e, n]$ to encrypt the message (Eq. 4). This process also doing 32 times iteration.

Step 8: The result RSA encryption will be converted to hexadecimal become the digital signature.

B. *Verification (Decryption)*

Verification stage is required the digital signature image, private key $[d, n]$, d and n for decrypt digital signature on RSA. Here is details step by step verification process:

Step 1: Input the Digital Signature

Step 2: The Digital Signature will convert to decimal from hexadecimal.

Step 3: After converted decrypt using RSA algorithm (Eq. 5). The iteration will occur 32 times, the result become cipher text vigenere

Step 4: Calculate Hash name of the file (N) using MD5 as key Vigenere.

Step 5: Decrypt ciphertext at Step 3 using Vigenere (Eq.7). This calculation will last 32 round.

Step 6: Load the Image

Step 7: Pre-processing pixel image from matrix become matrix

Step 8: Hashing pixel of an image using MD5 to verify on the next step.

Step 9: Compare the result of digital signature decryption at step 5 and hash pixel at step 8, if a match between that two variable that means the image authentic, if not match someone has modified the image or change the name of the image.

To see more clearly about the proposed verification scheme see Fig. 4.

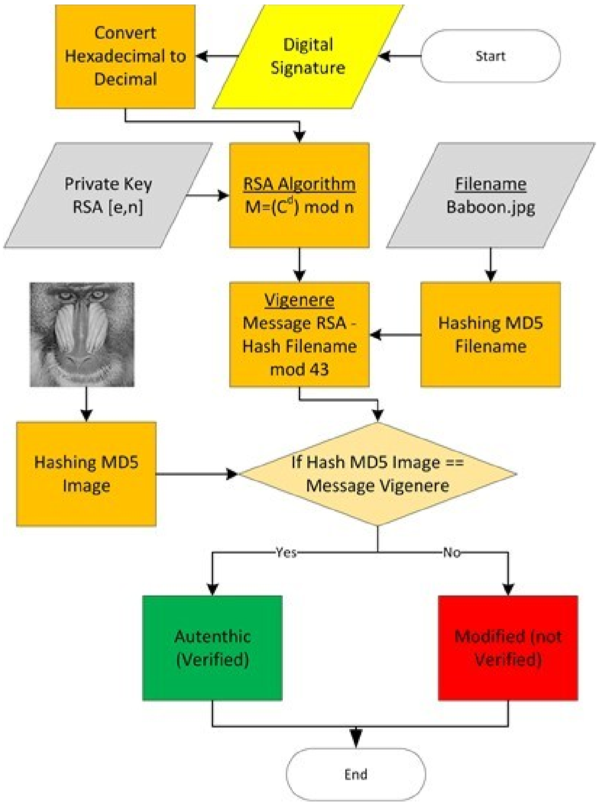

Fig. 4. Proposed Method of Verification Digital Signature

V. EXPERIMENTAL RESULT AND TESTING

In this study used grayscale and true color images with three kinds of extensions, namely: jpg, BMP, and tiff. With image size used 256x256. Fig. 5 shows the image used in this experiment:

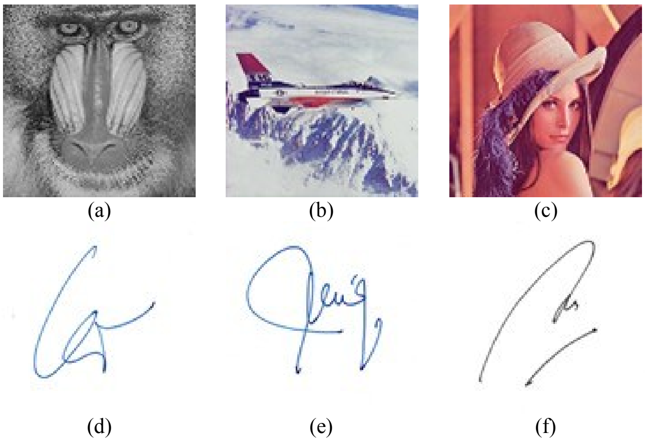

Fig. 5. Image Used for Digital Signature {(a)Babbon.jpg; (b)F16.tiff; (c)Lena.bmp; (d)Signature1.jpg; (e)Signature2.tiff; (f)Signature3.bmp} (a) and (f) is grayscale images, while (b),(c),(d), and (e) is true color images.

It then uses RSA keys along 8 bits for encryption, where the p and q values are ranging from 0-255. The Vigenere key is derived from the hash function. For attack testing the digital signature, using blurring, Gaussian noise and change the file name. PSNR to find out imperceptibility quality of the image. A Higher value of PSNR means little changes with the original image. PSNR calculate using Eq. 12.

$$PSNR = 10\, log_{10} \frac{Max - 1}{MSE} \tag{12}$$

Where, max=2^8

TABLE I. EXPERIMENT RESULT AND ATTACK TEST

Image (Filename)	Digital Signature	Attack	PSNR (Db)	Decrypted (DS)	Hash Image	Verified
Baboon.jpg	FB9:FB9:FB9:37AD: F1D:3C01:6488:5089: 2DE1:7B78:5372:8D7B: 6FA5:41BB:5D97:39A8: 9B2:F1D:5965:69DF: 142A:975:41BB:2DE1: 69DF:68BF:660A:6819: 548B:41BB:69DF:5D97:	Nothing	Inf	**130DEAB8048A6670 D32496D10A009654**	**130DEAB8048A6670 D32496D10A009654**	**Yes**
		Change Filename	Inf	3Z2SFNP;?34T8IV0G CO5W5DAMJ5Z75MU	130DEAB8048A6670 D32496D10A009654	No
		Blurring	74.2544	130DEAB8048A6670 D32496D10A009654	C886637BFBF7F6EC F0DC18E024EE811E	No
		Gaussian Noise	50.2833	130DEAB8048A6670 D32496D10A009654	A5B2000179421872 2587971F73D9C5A5	No
F16.tiff	548B:7B78:142A:68BF: 6FA5:41DB:5B72:FB9: 14B0:7B78:2DE1:41DB: 86BA:41DB:86BA:41DB: 173E:14B0:68BF:41DB: 5372:8D7B:442E:5EB6: 5372:2259:14B0:442E: 86BA:6488:9B2:975:	Nothing	Inf	**EC8491C202CB7CF5 B4C55C265F4DFDF4**	**EC8491C202CB7CF5 B4C55C265F4DFDF4**	**Yes**
		Change Filename	Inf	LE>G:EPHNA?3G2HC <K9>BM?>3KJD6DT;	EC8491C202CB7CF5 B4C55C265F4DFDF4	No
		Blurring	81.4289	EC8491C202CB7CF5 B4C55C265F4DFDF4	56A70A0C38622078 5368D7C08338EDC0	No
		Gaussian Noise	67.8117	EC8491C202CB7CF5 B4C55C265F4DFDF4	4EA7585BD7576D4A 1D79D8BF4A29166D	No
Lena.jpg	210:2259:173E:7B78: 2DE1:69DF:86BA:41DB: F1D:548B:210:9B2: 142A:42CB:5D97:6488: 39A8:7B78:68BF:8D7B: 39A8:5D97:6FA5:8C37: 39A8:5D97:2DE1:69DF: 6488:442E:F1D:7DAF:	Nothing	Inf	**A9C42494FF9D804B 369B165459C1DAA0**	**A9C42494FF9D804B 369B165459C1DAA0**	**Yes**
		Change Filename	Inf	WM<D;79F3L0E<0TT 5BI?58>K1<@7EA56	A9C42494FF9D804B 369B165459C1DAA0	No
		Gaussian Blurring	83.9911	A9C42494FF9D804B 369B165459C1DAA0	866B3E4EDBEDF854 A542B291DBC2DD5B	No
		Noise	59.0594	A9C42494FF9D804B 369B165459C1DAA0	CA89761C1F8C8628 C2D8B0F9007453DB	No
Signature1.jpg	68BF:5965:5372:142A: 7B78:442E:2DE1:41BB: 6488:7B78:68BF:8C37: 68BF:548B:210:5D97: 8D7B:975:8C37:5089: 5D97:37AD:39A8:5372: 173E:9B2:58F:86BA: 149B:7BF5:41BB:58F:	Nothing	Inf	**62A7BCABD3A1EE03 C6288F17CF8C2CC6**	**62A7BCABD3A1EE03 C6288F17CF8C2CC6**	**Yes**
		Change Filename	Inf	C488D@<6W?44EI95 QTZV8U5GDU6;IA6U	62A7BCABD3A1EE03 C6288F17CF8C2CC6	No
		Blurring	80.6926	62A7BCABD3A1EE03 C6288F17CF8C2CC6	2A9D228E5121E373 89DCC4645F306BF1	No
		Gaussian Noise	48.1648	62A7BCABD3A1EE03 C6288F17CF8C2CC6	5FEC1D614AC8ADD5 486D39FB9FAA76E8	No
Signature2.tiff	2259:68BF:5372:5965: 2259:41DB:14B0:68BF: 5089:5372:5D97:69DF: 5372:9B2:86BA:173E: 6FA5:442E:660A:42CB: 39A8:7DAF:173E:7BF5: 5D97:2259:4031:975: 42CB:5EB6:548B:5965:	Nothing	Inf	**9477903E0E30CC64 6A0E414A7FE4F6E8**	**9477903E0E30CC64 6A0E414A7FE4F6E8**	**Yes**
		Change Filename	Inf	<JFSKEKH9I3MIDFA TCMS10ELQGT;TX<T	9477903E0E30CC64 6A0E414A7FE4F6E8	No
		Blurring	84.4392	9477903E0E30CC64 6A0E414A7FE4F6E8	E80D1378369E72E1 FFBC50BA499EF2B6	No
		Gaussian Noise	52.9360	9477903E0E30CC64 6A0E414A7FE4F6E8	DB3414923A91857D DD19101EE04BCDED	No
Signature3.bmp	8C37:F1D:39A8:7DAF: 5372:5965:F1D:548B: 173E:68BF:41DB:7B78: 442E:7B78:F1D:149B: 7B78:39A8:5372:68BF: 41DB:5EB6:39A8:9B2: 142A:FB9:58F:7B78: 5965:7BF5:5B72:41BB:	Nothing	Inf	**5661E5CEDAA1D140 B5EFD69D80664CCE**	**5661E5CEDAA1D140 B5EFD69D80664CCE**	**Yes**
		Change Filename	Inf	15444T5<>A?D>BGV 117GC96T=06CPNT7	5661E5CEDAA1D140 B5EFD69D80664CCE	No
		Blurring	86.7532	5661E5CEDAA1D140 B5EFD69D80664CCE	A68736878C4D8649 D13FE0BED2CFE26B	No
		Gaussian Noise	52.9360	5661E5CEDAA1D140 B5EFD69D80664CCE	2DDEB595FE6E64C6 FA36A5C60FBB880C	No

VI. CONCLUSION

From the experimental results in Table I, it has been proven that the combination of Vigenere, RSA, and MD5 algorithms has been successfully used for digital signature security. The MD5 combination with hash function gets a better result than hash function only. The combination of this operation is done in the image as well as image file name. Vigenere and RSA are then encrypted. The similarity of MD5, Vigenere and RSA is a symmetric encryption algorithm, so the algorithm is successfully combined. The difference is that MD5 does not require a key to encrypt, while Vigenere and RSA need a key. RSA requires both private and public keys, whereas Vigenere only uses private keys. By combining these three algorithms, the data security level becomes stronger. This algorithm can also protect digital signatures of counterfeiting or from various image manipulations. Although the pixels changed very little, as evidenced by the PSNR value reaching 86.7532 dB, the algorithm successfully detects pixel image changes. Similar to a file name change in the digital signature image. So, if at the time of digital signature transfer process occurs interference that damage or manipulate the file, this algorithm can do the security well.

References

[1] U. Sudibyo, F. Eranisa, E. H. Rachmawanto, D. R. I. M. Setiadi and C. A. Sari, "A Secure Image Watermarking using Chinese Remainder Theorem Based on Haar Wavelet Transform," in International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), Semarang, 2017.

[2] A. Setyono, D. R. I. M. Setiadi, and Muljono, "StegoCrypt Method using Wavelet Transform and One-Time Pad for Secret Image Delivery," in International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), Semarang, 2017.

[3] D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari, "Secure Image Steganography Algorithm Based on DCT," Journal of Applied Intelligent System, vol. 2, no. 1, pp. 1-11, 2017.

[4] E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi and C. A. Sari, "A Performance Analysis StegoCrypt Algorithm based on LSB-AES 128 bit in Various Image Size," in International Seminar on Technology for Technology of Information and Communication (iSemantic), Semarang, 2017.

[5] A. H. Mansour, "Analysis of RSA Digital Signature Key Generation using Strong Prime," International Journal of Computer, vol. 24, no. 1, pp. 28-36, 2017.

[6] S. Alam, A. Jamil, A. Saldhi, and M. Ahmad, "Digital Image Authentication and Encryption using Digital Signature," in International Conference on Advances in Computer Engineering and Applications (ICACEA), Ghaziabad, 2015.

[7] D. Shah, "Digital Security Using Cryptographic Message Digest Algorithm," International Journal of Advance Research in Computer Science and Management Studies, vol. 3, no. 10, pp. 215-219, 2015.

[8] M. C. A. Kioon, Z. Wang and S. D. Das, "Security Analysis of MD5 algorithm in Password Storage," inProceedings of the 2nd International Symposium on Computer, Communication, Control and Automation, Paris, 2013.

[9] S. A. Jaju and S. S. Chowhan, "A Modified RSA Algorithm to Enhance Security for Digital Signature," in International Conference and Workshop on Computing and Communication (IEMCON), Vancouver, 2015.

[10] Z. Xiao, Y. Wang and Z. Jiang, "Research and Implementation of Four-Prime RSA Digital Signature Algorithm," in IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), Las Vegas, 2015.

[11] A. Saraswata, C. Khatria, Sudhakara, P. Thakrala and P. Biswasa, "An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication," in2nd International Conference on Intelligent Computing, Communication & Convergence, Bhubaneswar, 2016.

[12] V. R. Pallipamu, T. R. K, and S. V. P, "Design of RSA Digital Signature Scheme Using A Novel Cryptographic Hash Algorithm," International Journal of Emerging Technology and Advanced Engineering, vol. 4, no. 6, pp. 609-613, 2014.

[13] Q.-A. Kester, "A Cryptosystem Based on Vigenère Cipher with Varying Key," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 1, no. 10, pp. 108-113, 2012.

[14] P. Ora and P. R. Pal, "Data Security and Integrity in Cloud Computing Based on RSA Partial Homomorphic and MD5 Cryptography," in International Conference on Computer, Communication, and Control (IC4), Indore, 2015.