iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VII **Month of publication:** July 2018

DOI: http://doi.org/10.22214/ijraset.2018.7037

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VII, July 2018- Available at www.ijraset.com

Research Technique to Authenticate Digital Image Signature Using Cryptography

Prachi R. Nirmal[1], Prof.B.G.Pund[2]
[1, 2]*PG Department of Computer Science & Technology, Hanuman Vyayam Prasarak Mandal, Amravati, Maharashta.*

Abstract: ***Authentication of digital media has been done with the various scheme, one of them is a digital signature. 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. Cryptography is one of the most popular fields of study these days as it is necessary to maintain the confidentiality of the data which is sent over the network. Cryptography is the only powerful tool for achieving high levels of information security in a computer networks environment. Cryptography can support implementation of all these security services, by using various cryptographic techniques, which include among other things conventional secret key algorithms, public-key algorithms, authentication procedures, and different digital signature schemes. Each of these methods has its own shortcomings. A new scheme for evaluating the cryptographic security. so research on digital signatures should be developed to improve its ability to provide security and prove the authenticity of the image. This paper sets out to contribute to the general body of in the area of cryptography application and by a new way of implementing. This paper research a combination of three algorithms to the created digital signature, namely: Rivest – Shamir – Adleman (RSA), Vigenere Cipher and Message Digest 5 (MD 5).By combining these three algorithms, the data security level becomes stronger. This algorithm can protect from image forgery or various image manipulations.***
Keywords: Digital Signature, RSA, Vigenere, MD5, Authentication, Cryptography.

I. INTRODUCTION

In the digital era data is transmitted through internet or machine. Security and communication channel, confidentiality of this data is very important. This in turn has to increases awareness of protection of data and resources. To guarantee authenticity of message is very important. 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.

The purpose of this subject is to provide a practical survey of different Cryptographic algorithm which is used for development of digital signature (DS), study of Digital signature and how this algorithm efficiently used for management of security in digital era.

Cryptography is study of converting original message called plaintext to coded message called cipher text using the process of encryption and decryption A digital signature can be used to determine whether the correct data coming from the sender, then it is necessary to verify.

The digital signature is an authentication technology based on public key cryptography to prevent to be forged and deceived when communicating parties exchange information on the Internet [1]. The RSA cryptographic algorithm is the most widely used in all public-key cryptosystems. It is characterized by high security and easy to implement. Namely, it can be not only used to encrypt the data, but also can be used for identity authentication. Therefore, RSA signature is one of the most common digital signature methods [2].

The advancements in technology and software since the last decade made it easy to copy or alter the contents of digital images. Therefore, image authentication is necessary to verify integrity. Conventionally, image authentication methods can be classified into two groups: digital signature based [6, 7] and watermark-based [8, 9]. In digital signature method a hash file of the image consisting of its features is generated by an algorithm which is further encrypted by the sender's private key before transmission and is used to digitally sign the image. At receiver side the received hash file is decrypted by the user's key and a new hash file of received image is created by the same algorithm and for validation of the signature both hash files are compared, if they match it means no damage has occurred and sender is an authentic user. But if there is a mismatch, it shows that either the tampering is done by an adversary or proper expansion of image is not achieved at the receiver. [5]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VII, July 2018- Available at www.ijraset.com

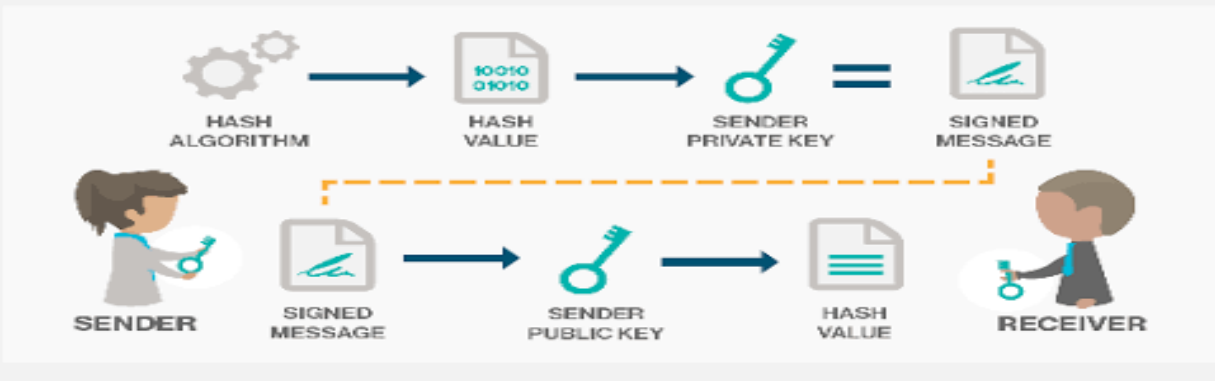


Fig.1 Process of Digital Signature

II. LITERATURE REVIEW

The research presents a set of experiments using a genetic algorithm to develop solutions to a Vigenere alphabetic code [10]. A Vigenere code replaces each character in the plain text with a new character generated by adding the value of a character in the corresponding place in a "keyword". The genetic algorithm uses the number of characters in valid English words as the measure of a solution's fitness; breeding is accomplished by simple crossover and mutation consists of random variations of a single keyword position.

In this paper presents a fair comparison between RSA and Modified RSA algorithm along with time and security by running several encryption and decryption setting to process data of different sizes [11]. The efficiency of these algorithms was considered based on key generation speed and security level. The texts of different sizes were encrypted and decrypted using RSA and modified RSA algorithms.

In this research they proposed a four-prime Chinese Remainder Theorem (CRT)-RSA digital signature algorithm [12]. We used the Hash function SHA512 to make message digest. We optimized large number modular exponentiation with CRT combining in Montgomery algorithm.

The another research presents a reliable and simple method for authenticating the content of a paper document by implementing an on paper digital signature[13]. This method randomly selects the words at random positions of the document along with critical content and creates on paper digital signature. This method employs an online document verification system and the unauthorized access is denied by the user authentication mechanism.

This research is presented to determine the safety of digital images[14], especially for a company logo using vigenere cipher algorithm through the application that created because so far we know only vigenere algorithm method used for the security of data in text form only. the final results of this study focuses on securing data in the form of a digital image for the company logo showed a significant result that the image of the once encrypted to be safe and successful, and decrypted to its original shape in accordance with the original digital image by using vigenere cipher.

Analyses the security risks of the hashing algorithm MD5 in password storage and discusses different solutions [15], such as salts and iterative hashing. We propose a new approach to using MD5 in password storage by using external information, a calculated salt and a random key to encrypt the password before the MD5 calculation. We using key stretching to make the hash calculation and using XOR cipher to make the final hash value

A. The System Cryptographic

1) *Digital signature:* A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. Digital signatures are a standard element of most cryptographic protocol suites, and are commonly used for cases where it is important to detect forgery or tampering. The authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key.
2) *Vigenere cryptography:* The Vigenère Cipher was adapted as a twist on the standard Caesar cipher to reduce the effectiveness of performing frequency analysis on the ciphertext. The cipher accomplishes this using uses a text string (for example, a word) as a key, which is then used for doing a number of alphabet shifts on the plaintext. Similar to the Caesar Cipher, but instead of performing a single alphabet shift across the entire plaintext, the Vigenère cipher uses a key to determine several different shift amounts across the entirety of the message[18].

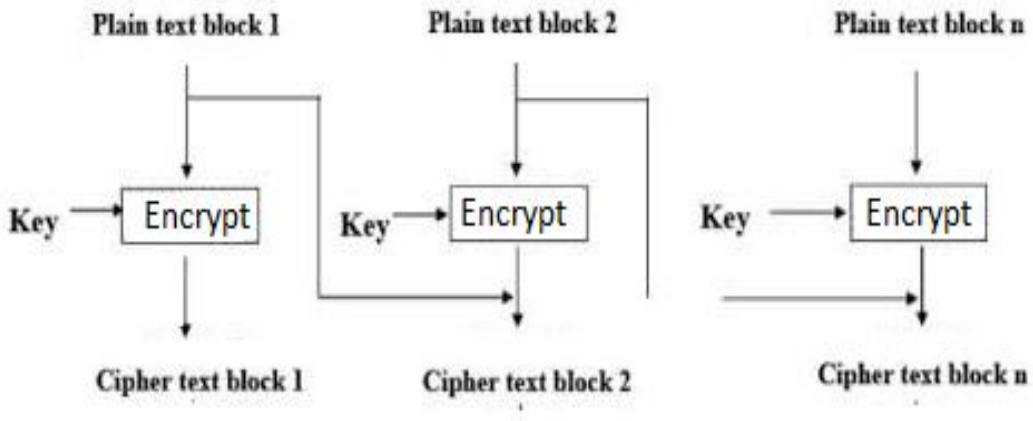


Fig:2 Vigenere cryptography Technique

B. 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 [16].

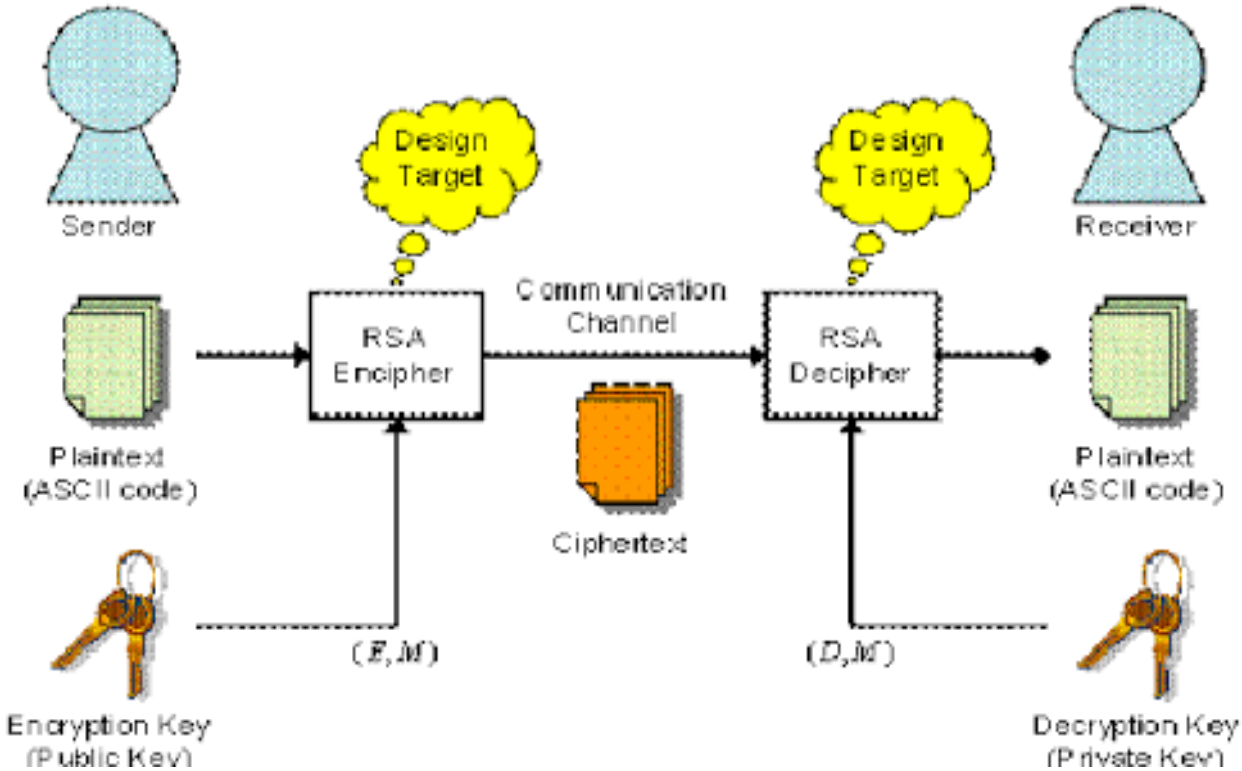


Fig:3 Workimg of RSA Algorithm

C. Message- Digest 5 (MD5)

MD5 is the most popular hash function that produces 128bit hash value or 16 Char. MD5 generally use for check integrity of a file. Cycle shift operation, modular addition and bitwise Boolean operation. 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 [17].

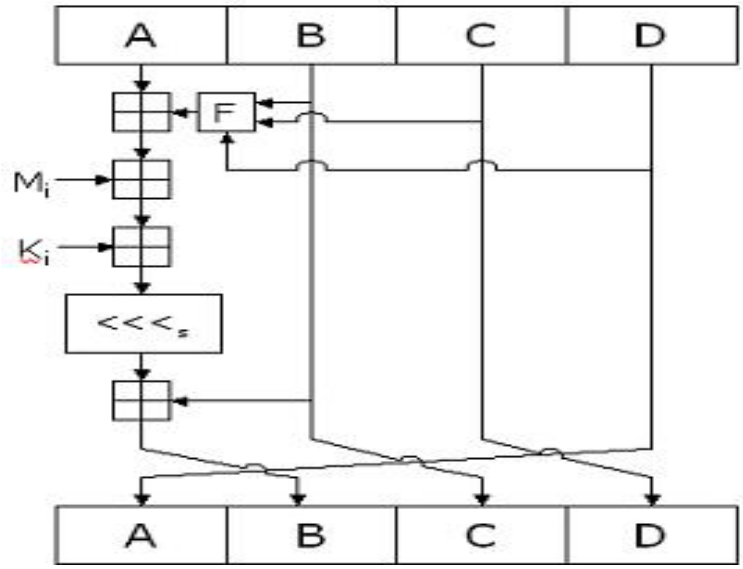


Fig:4 MD5 Algorithm

These are different Cryptographic algorithm used to secure digital image. We research technique to combine these different technologies to protect digital image signature.

D. Cryptographic Technique For Digital Image Signature

Encryption is required to protect data from 3rd party attacks that can arise during the transmission of data. It is a process of making the data unintelligible to all unauthorized parties and only the authorized user can decrypt the data into intelligible form. Hence encryption is necessary for data integrity, privacy and for security purposes.

In this section with the help of different Cryptographic algorithm we analysis technique to generate digital image signature. MD 5 hashing algorithm is used for hashing a image and filename [15]. These image hash and filename is encrypted using Vigenere cipher algorithm. Using MD5 function calculates the hash name of the file. Filename message digest will be used as the key of Vigenere .The ciphertext of Vigenere will be encrypted using RSA algorithm. The result of RSA encryption is the digital signature of the image. The results RSA encryption will be converted to hexadecimal become the digital signature.

For verification, the digital signature decrypted using RSA and Vigenere cipher algorithm. The comparison is being done between these two hash file, if both the files holds the same data it means the sender is authentic and no data has been modified during transmission.

III. CONCLUSION

The purpose of this subject is to study of different Cryptographic algorithm which is used for development of digital signature. Cryptographic algorithm used to secure digital image. We research technique to combine this different technology to protect digital image signature. The MD5 combination with Vigenere gets a better result than hash function only. The combination of this operation is done in the image as well as image filename. By combining these three algorithms, the data security level becomes stronger. This algorithm can protect from image forgery or various image manipulations.

REFERENCE

[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.

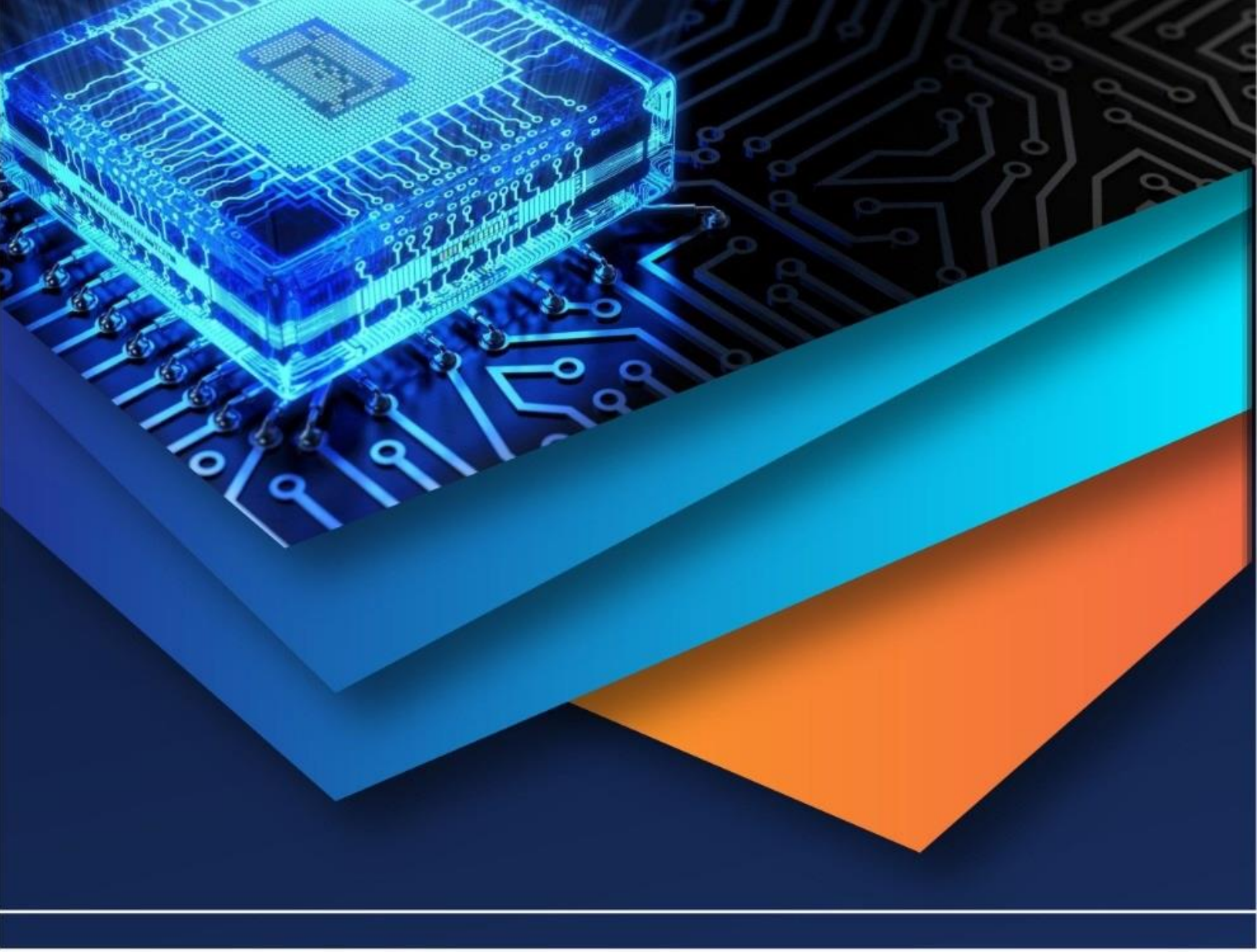
[2] A. Setyono, D. R. I. M. Setiadi, and Muljono, “StegoCrypt Method using Wavelet Transform and One-Time Pad for Secret Image Delivery,” in International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), Semarang, 2017.

[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] Manpreet Singh , Harpreet Kaur , Ajay Kakkar,” Digital signature verification scheme for image authentication”, 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS),Dec 2015.

[6] Marc Schneider and Shih-Fu Chang, "A robust content based digital signature for imageauthentication," IEEE conjerence on Image Processing, pp.227-230, Sep. 1996.
[7] Ching-Yung Lin and Shih-Fu Chang, "Robust digital signature for multimedia authentication," iEEE Circuits and Systems Magazine, vol.3, no.4, pp.23-26, Jan. 2003.
[8] Ping Wah Wong and Nasir Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," iEEE Transactions on image Processing, voLlO, no.IO, pp.1593-160 I, Oct. 2001.
[9] Di Xiao and Jian Jin, "A reversible two-level image authentication scheme based on chaotic fragile watermark," 9th international Conference and Expo on Emerging Technologies jor a Smarter World (CEWiT), pp.I-6, Nov. 2012.
[10] C. F. Jones, M. Christman," Genetic algorithm solution of Vigenere alphabetic codes", IEEE Mountain Workshop on Soft Computing in Industrial Applications, June 2001.
[11] Sangita A. Jaju, Santosh S. Chowhan," A Modified RSA algorithm to enhance security for digital signature", International Conference and Workshop on Computing and Communication (IEMCON),Oct 2015.
[12] Zhenjiu Xiao, Yongbin Wang, Zhengtao Jiang," Research and implementation of four-prime RSA digital signature algorithm", IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS),July 2015
[13] Sajan Ambadiyil, V B Vibhath, V. P. Mahadevan Pillai," Performance analysis and security dependence of on paper digital signature using random and critical content", International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Oct 2016
[14] Yana Aditia Gerhana, Entik Insanudin, Undang Syarifudin, Mohammad Rizal Zulmi," Design of digital image application using vigenere cipher algorithm", 4th International Conference on Cyber and IT Service Management, April 2016.
[15] Mary Cindy Ah Kioon, ZhaoShun Wang and Shubra Deb Das," Security Analysis of MD5 algorithm in Password Storage," Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation (ISCCCA-13), 2016.
[16] 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.
[17] Q.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.
[18] Quist-Aphetsi Kester," A cryptosystem based on Vigenère cipher with varying key," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10, December 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY