Implementation of AES and Partial SHA-1 Image Encryption Algorithm

Sourabh N. Prasad

M.tech Scholor, National Institute of Technical Teacher Training and Research, Bhopal

Abstract- In the present scenario, the world is heading towards the type of communication which is fast, safe and provides better way of communication. Digital communication is far a better than analog communication. Digital communication is used in many fields such as banking, military applications, satellites, railways, airways, online shopping etc. But the actual risk arises with the security of the data (text, image or video) that are stored in the cloud or that we have to transmit or receive via internet. To maintain the integrity, authenticity, and privacy of the data, secure and strong encryption techniques must be adopted. In this dissertation, we will use AES technique (for encryption) and Partial SHA-1 (for digital signature) on a single digital image. AES (Advanced Encryption Standard) is based on the symmetric key algorithm which uses a private key to encrypt and decrypt the image. Partial SHA-1 (Secure Hashing Algorithm -1) is a method that yields a 160-bits message digest which is a 40 words hexadecimal value. AES techniques will encrypt the digital image and Partial SHA-1 will produce the message digest of the original image and then both the encrypted image and message digest is sent to the receiver. Using both these techniques applied on the single image make it formidable and consumes the time of the intruders to decrypt the image. Different performance parameters have been analyzed which are – Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Structural Content (SC), Maximum Difference (MD), Average Difference (AD), Normalized Absolute Error (NAE) and Histogram of the images. The experimental result on the original and the decrypted image shows that the PSNR value is unaffected on the application of low noise but in case of high noise, PSNR value can be affected. The proposed methodology will provide better resistance from the data being hacked.

Keywords- Peak Signal to Noise Ratio, Mean Square Error, Advanced Encryption Standard, Image Encryption, SHA-1, Normalized Absolute Error.

I. INTRODUCTION

In the present scenario, each and everyone is growing their interest in the digital world for faster communication. The Internet is the primary medium through which digital communication is possible. Every person is using the internet on daily basis for communication, transaction, multimedia applications, online shopping and so on. The personal details of the person are also stored in the cloud. There is a high risk that these stored data and communication between two parties can be hacked as the internet can be accessed by anyone. Therefore, there is a need to provide security and integrity to the data (especially to the sensitive data). Cryptography plays a crucial role in hiding the data. Encryption is a cryptographic technique to provide security to the data by encoding the data into an unreadable form. In this technique, the plaintext (message or information) is encoded to form the ciphertext. It can be read by a known receiver only after decryption. The encryption of the data is possible with the help of a key. Only the authorized receiver can decrypt the ciphertext with the key provided by the sender. The intruder will not be able to get the information without the actual key. Apart from this, the authentication of the data is also necessary. Secure Hashing Algorithm is a cryptographic technique which can provide data integrity, data authentication and also confidentiality of the data. In this technique, the whole message or information is converted into hexadecimal values which can be of different size depending upon the type of algorithm adopted. These hexadecimal values can be of size 160 bytes, 256 bytes, 512 bytes and so on. These hexadecimal values are then sent with the data to the receiver. The receiver checks whether the data is authenticated or not. The data authentication means the data which is received by the receiver is coming from a valid or known source. The receiver calculates the hexadecimal value and then compares with the hexadecimal value send by the sender. If both these values are same, the data is accepted otherwise it is discarded. This hexadecimal value is called hash value. The hash value has a unique property that it cannot be reversed. This means that once the hash value of the data is generated then the data cannot be generated by applying the reverse process. In most of the sites, we require username and password, SHA plays a key role to secure the password of the user. It stores the password in form of hash value in its database. Once the user enters the password, it converts the password into the hash value and compares with the hash value stored with the same username. If it is a valid password, the account of the user opens. Different sites are using different hashing algorithm for the data on their site like Google uses SHA256 with RSA encryption technique issued by Google Internet Authority G3 for the security of the data and filehippo uses SHA256 with RSA encryption technique which is issued by Global Sign Cloud SSL CA-G3 for their data.

In this examination an in-depth survey has been conducted which shows the need for a method that will provide a secure transmission between the two parties without the involvement of the intruder/hacker during transmission. The objective of this research is to develop/improve image encryption techniques for secure transmission of the sensitive images. This hybrid image technique will be able to support any format of the image and overcomes hacking of the image during transmission. This research aims at providing image integrity, image security, and image authenticity. With the intent to achieve this forecasted aim, the researcher has identified the following objectives:

- Develop a new hybrid cryptographic technique which is reliable.
- Strongly encrypted data which will overcome the problem of hacking.
- Provide image authenticity and image integrity while storing or transmitting the image.
- Provide a much easier way for encryption and decryption of images.

II. METHODOLOGY

The leakage of sensitive information from the military sector, banks sectors etc. can cause a great loss and this loss cannot be compromised. Therefore, security should be properly maintained during the storing or transmission of the information. This can be achieved by encrypting this information and also converting the information into a form through which the original information cannot be retrieved. So, Symmetric encryption techniques and Hashing encryption techniques should be used in a hybrid manner. This methodology should be implemented in digital systems for faster and safer communication. The techniques used in this methodology are implemented using MATLAB 2013a software. Inside MATLAB, Guide is used for generating the one-click application which is a Windows Standalone Application. Using Guide, Windows Standalone Application is generated which implements these techniques in a hybrid manner.

a. Steps for AES Encryption

- Load the image for encryption.
- Calculate the number of rows and column of the image pixels.
- According to the number of rows and column, make a loop so as to divide the image into 4x4 block matrix (16 bytes or 128 bits).
- The first block and 128 bits sub-key from the key expansion block is loaded to the Add round key block which performs the XOR operation.
- The Block is then, substituted from the SubBytes box subsequently.
- The Block is then subjected to Row Shifting block.
- The output of the Row Shift Block is given to Mix column which performs multiplication of the block matrix with the fixed matrix. (Note: Mix column is not executed in the last round).
- The process from SubBytes to the Add round key (excluding the first Add round key block) is constituted as Round1.
- Again, Add round key process is subjected upon the block matrices and the second sub-key from the key expansion block.
- The Block matrix is subjected to a total of 10 rounds.
- This whole process is for the first block of the image.
- The same process is repeated for each block of the image until the loop is over.

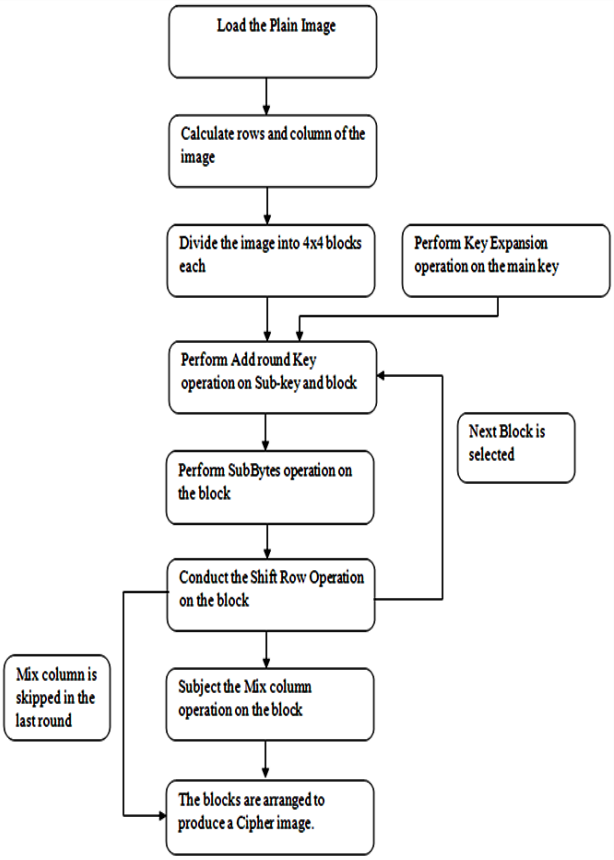


Fig. 2.1 Flowchart of AES Encryption.

b. Partial Secure Hash Algorithm (SHA-1):

Secure Hashing Algorithm-1 or SHA-1 is a non-key cryptographic hash function. Non-key cryptography means a cryptography which does not require a key. The Partial SHA-1 means a part of the image is subjected to the SHA-1 algorithm and the rest of the part of the image is left untouched. The process of Partial SHA-1 is same as the process of SHA-1. SHA-1 takes a variable length input from the user and fabricates a 160-bits (40 words or 20 bytes) hexadecimal value. This hexadecimal value is also known as Hash Value or Message Digest. This algorithm was first designed by NSA (National Security Agency) and

is a standard for U.S. Federal Information Processing. It is an improvement over the SHA-0 algorithm.

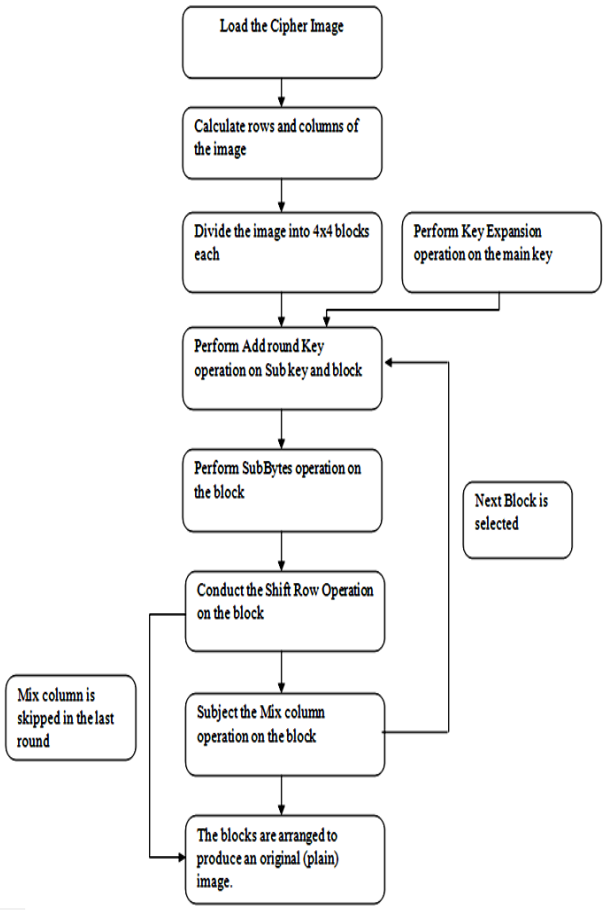


Fig. 2.2 Flowchart of AES Decryption.

The only difference between SHA-1and SHA-0 is a single bitwise rotation in the compression function. Its certification is given by FIPS PUB 180-4, CRYPTREC. The structure of the cipher in SHA-1 is a Merkle-Damgard. The principle of SHA-1 is based on the design of MD5, MD4, and MD2. In SHA-1, the size of the digest is equaled to 160 bits and the size of the block is 512 bits. The block is subjected to a total of 80 rounds in the SHA-1 algorithm. SHA-1 is widely used in protocols such as TLS and SSL, PGP, S/MIME, IPSec, and SSH and found its application in the digital signature, MACs (Message Authentication Codes) and other authentication processes. A good example to show the application of SHA-1 in our day to day life is the login page of the site. If a website is having a login page such as Facebook or Gmail, we have to enter the username and password. When we had created the account in these websites, the username and password of that person are stored in its cloud in form of hexadecimal value.

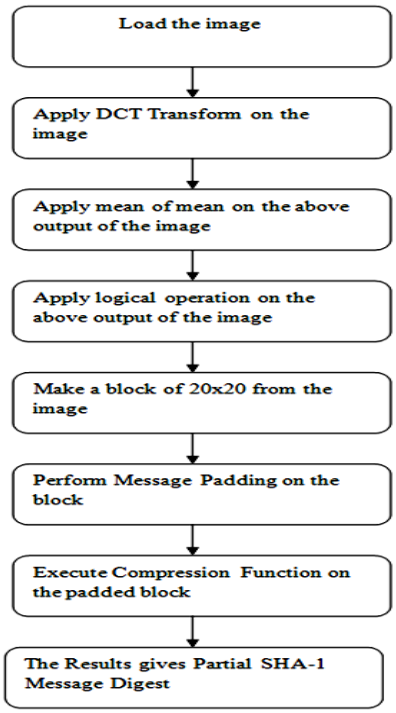


Fig.2.3 Flowchart of Partial SHA-1.

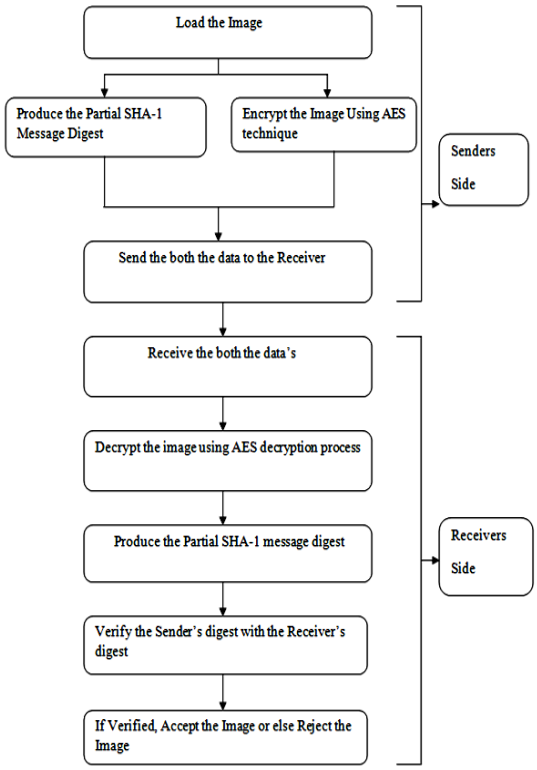


Fig.2.4 Flowchart of the Proposed Methodology.

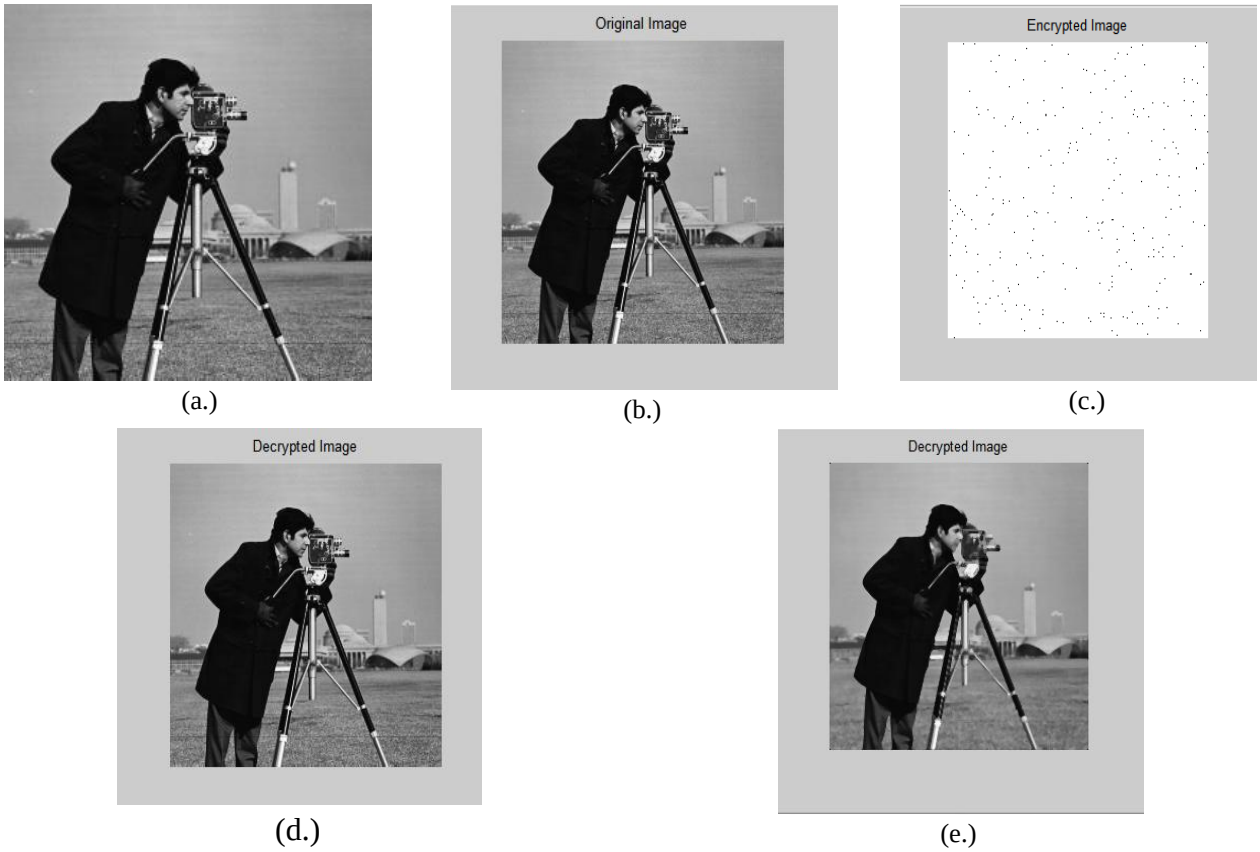
That means Secure hashing algorithm is applied on the username and password of that person. So when he enters the username and password to log in then, the keywords entered by him is first converted into hexadecimal value and checked with the values stored in the website's cloud. If it matches, then the account of that person is opened else error will pop up.

III. SIMULATIONS AND RESULTS ANALYSIS

The performance parameters {like Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Average Difference (AD), Mean Difference (MD), Normalized Absolute Error (NAE), Structural Content (SC), and Histogram analysis} are carried out on different demo image available in the MATLAB 2013b software. These parameters of the adopted methodology are compared with the parameters of the traditional methodology in tabular form. The histogram analysis is done with help of the histogram of the original and the encrypted images. The original images are also displayed in this chapter with their original size. The proposed work is simulated using MATLAB 2013b. At last, the conclusion is drawn from the compared values of the performance analysis.

The Performance Analysis is performed to get the necessary information about the images such as clarity of the image, intensity of the signal with respect to noise, the difference between the original and encrypted images etc. Basically, the endurable amounts of distortion are signified in this analysis. The analysis is carried out using the traditional and proposed approach. The performance analysis is comprised of 8 parameters. They are Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Average Difference (AD), Mean Difference (MD), Normalized Absolute Error (NAE), Structural Content (SC), Normalized Cross Correlation (NCC), and Histogram analysis.

a. Cameraman Image Analysis



(a.) (b.) (c.)

(d.) (e.)

Figure 3.1 (a.) Cameraman Original (256x256) (b.) Cameraman resized (256x256) (c.)Cameraman encrypted (d.) Cameraman Decrypted (e.) Noisy Cameraman decrypted.

These parameters are applied on the 5 five different demo images of MATLAB (Cameraman, Lena, Pepper, Barbara, and Baboon images) using the traditional and proposed approach. The values from traditional approach of these images are compared with the values of proposed approach. The comparison is accomplished on the original and decrypted image as well as on the original and encrypted image using traditional and proposed method. A close and strict examination is done to prove the effectiveness of the proposed method over traditional method.

An image of dimension M x N is considered, in which M= Numbers of rows and N= Number of column of the pixel matrix. Following are the performance parameters:-

The traditional approach and proposed approach are applied on 5 different images of different sizes and formats. The results from these images are well examined and compared with each other on the basis of the above mentioned performance parameters. Also, the images are put into a noisy environment of variance 0.02 and then parameters are calculated for noise. These images are Cameraman.tif (256x256), lena.bmp (512x512),

peppers.png (512x384), Barbara.png (512x512) and baboon.png (512x512).

The tabular form of all the above mentioned performance parameters (i.e. MSE, PSNR, AD, MD, NAE, NCC and Histogram Error) are given below.

Table 1 Performance Estimation of Original and Encrypted Cameraman image.

Parameters	Traditional Approach	Proposed Approach
MSE	$1.46x10^4$	9.6695e+03
PSNR	8.4861	8.2767
AD	103.1637	45.5018
MD	251	254
NAE	0.8818	0.9841
NCC	0.767	0.739
SC	5.8376	0.6972

Table 2 Performance Estimation of Original and Decrypted Cameraman image.

Parameters	Traditional Approach	Proposed Approach
MSE	121.5833	0
PSNR	27.2821	99
AD	7.6728	0
MD	6	0
NAE	0.0711	0
NCC	0.894	1
SC	0.9506	1

Table 3 Performance Estimation of Original and Decrypted Noisy Cameraman image.

Parameters	Traditional Approach	Proposed Approach
MSE	258.7826	125.4224
PSNR	25.1637	27.1471
AD	4.5281	0.4770
MD	177	199
NAE	0.0737	0.0359
NCC	0.753	0.9965
SC	0.9698	1.0024

Table 4 Partial Message Digest of cameraman (20x20).

SHA-1	Traditional Approach	Proposed Approach
Partial Message Digest	6473AE167B0F950439B99 EDE88EC1ADA9847BCA0	E55221C46C8D0B1CED3D 2FDDB7B762B0E040FAC4

b. Lena Image Analysis

The original image of Lena of size 512x512 color image is shown at figure 3.2 (a.). The resized grayscale, encrypted, decrypted image, and noisy decrypted image of lena of 256x256 is shown in figure 3.2(b.), (c.), (d.), and (e.).

The tabular form of all the above mentioned performance parameters (i.e. MSE, PSNR, AD, MD, NAE, NCC and Histogram Error) are given below.

Table 5 Performance Estimation of Original and Encrypted Lena image.

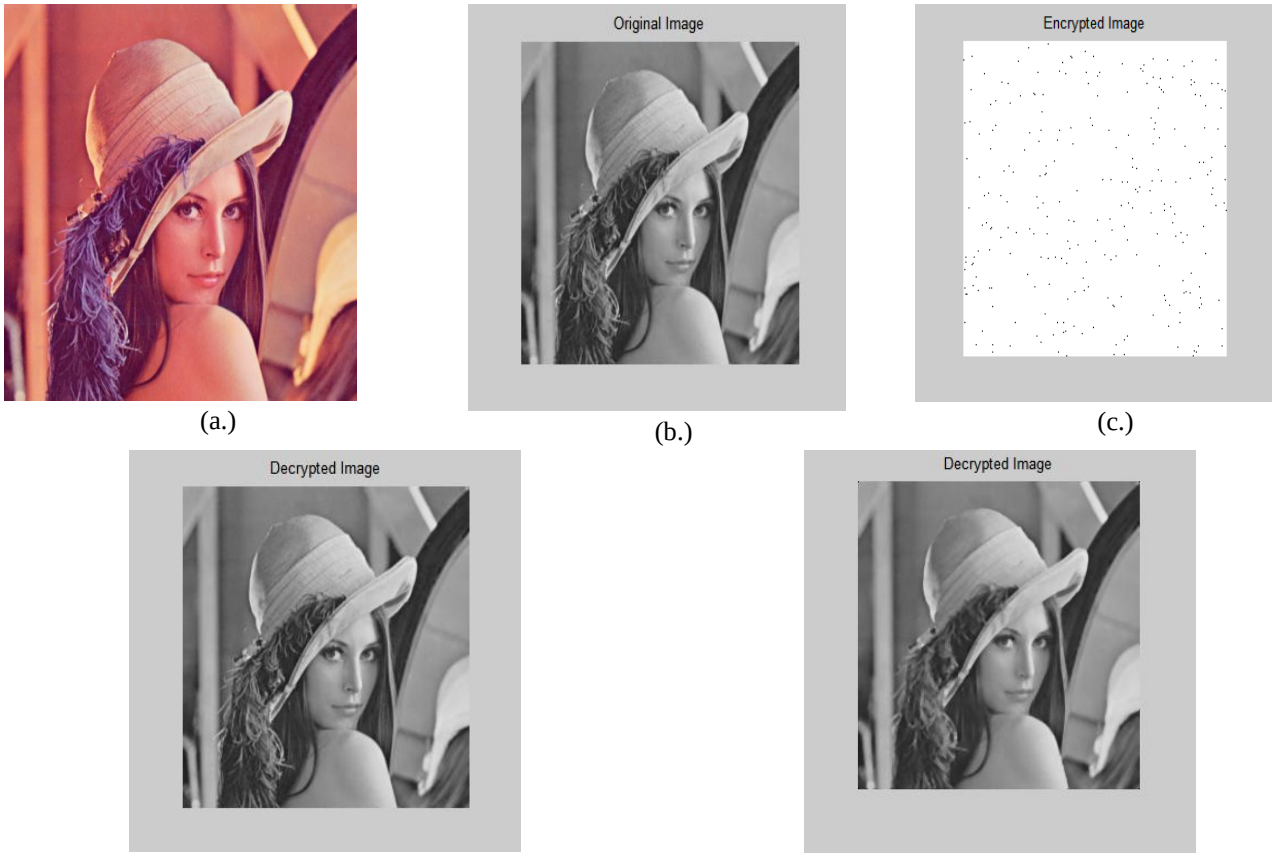
Parameters	Traditional Approach	Proposed Approach
MSE	$1.4158x10^4$	7.6670e+03
PSNR	6.6209	9.2846
AD	108.5365	3.2355
MD	236	223
NAE	0.8749	0.5845
NCC	0.799	0.751
SC	5.9054	0.7290

Table 6 Performance Estimation of Original and Decrypted Lena image

Parameters	Traditional Approach	Proposed Approach
MSE	110.3419	0
PSNR	27.2821	99
AD	6.7177	0
MD	6	0
NAE	0.0620	0
NCC	0.8991	1
SC	0.9520	1

Table 7 Performance Estimation of Original and Decrypted Noisy Lena image

Parameters	Traditional Approach	Proposed Approach
MSE	127.6335	20.1853
PSNR	27.0712	35.0805
AD	4.8764	0.1308
MD	135	162
NAE	0.0788	0.0149
NCC	0.718	0.9975
SC	0.9617	1.0014



(a.) (b.) (c.)

(d.) (e.)

Figure 3.2 (a.) Lena original (512x512) (b.) Lena resized (256x256)(c.) Lena encrypted (d.) Lena Decrypted (e.) Noisy Lena decrypted.

Table 8 Partial Message Digest of Lena (20x20).

SHA-1	Traditional Approach	Proposed Approach
Partial Message Digest	FEF17F5C022DC60BC6A8 8E744D98F9BEFF6F73CD7	D22EEE5C5E5B642FF6EE FF696DC243E8240499E8

IV. CONCLUSION AND FUTURE SCOPE

The result drawn from the analysis is much more efficient, easy and time saving in comparison to the traditional method of encryption. Both the techniques involved in this research work are fairly good in their part of work of encryption but when combining both these techniques on a same image in a windows application, gives a much more promising output and also removes the limitation of both the techniques.

- The value of PSNR, NCC, and SC are more in the case of proposed method as compared to the traditional method.
- The values of MD, AD, MSE, and NAE are low in case of proposed method in comparison to traditional method.
- The statistical analysis of the Histogram error is clearly shows that the proposed output gives much better results than traditional output.

As there is always a possibility in the improvement of any method or technique, the same will stand with this research too. The objectives mentioned are successfully met by the researcher but there is always a hope of improvement which are:-

- More security can be enhanced using the hybrid structure of RIPEMD, TIGER, RSA, SHA-2, SHA-3 etc.
- The security of the windows application can be enhanced by the use of password for entering the application.
- Cloud environment can be used using the internet, instead of using the handles as a structure in the application to store the data.

REFERENCES

[1]. K. GaneshKumar, D.Arivazhagan “Generating Digital Signature based on new cryptographic scheme for user

authentication and security" 1-5, Indian Journal of science and technology vol7(S6), Oct.2014.

[2]. Ms. Pranoti Panchal "Mobisecure using DSA" Vol.6, no.8, International Journal of Advanced Research in Computer science, Nov-Dec 2015.

[3]. Eman Salim, Ibrahim Harba "Secure data encryption through a combination of AES, RSA, and HMAC" Vol.7, no.4, 1781-1785, 2017, Engineering, Technology and applied science research.

[4]. Jan Mohammad Najar, Shahid Bashir Dar "A new design of a Hybrid encryption algorithm" International Journal of Engineering and Computer Science, ISSN: 2319-7242, Vol. 3, Issue 11, Nov. 2014.

[5]. Raeed K. Ibraheem, Roula AJ. Kadhim, Ali SH. Alkhalid "Anti-collision Enhancement of a SHA-1 digest using AES encryption by LABVIEW" IEEE 2015, 978-1-4673-6636-6/15.

[6]. Chaitya B. Shah, Drashti R. Panchal "Secure Hashing Algorithm -1" International Journal for Advanced research in Engineering and technology, Vol.2, issue X, oct.2014, ISSN 2320-6802.

[7]. Cheng Xiao-Hui, Deng Jian-Zhi "Design of SHA-1 algorithm based on FPGA" 2010 IEEE, 978-0-7695-4011-5/10.

[8]. Raeed K. Ibrahim, Ali SH. Hussain, Roula A. Kadhim "Implementation of SHA-1 by LABVIEW" IJCSMC, Vol.4, Issue 3, March 2015, pg.61-67.

[9]. Priyanka Vadhera, Bhumika Lall "Review paper on secure hashing algorithm and its variants" IJSR, ISSN (online): 2319-7064, Impact Factor (2012):3.358, Vol.3, Issue 6, June 2014, pg. 629-632.

[10]. M. Sreerama Murty, D. Veeraiah, A. Srinivas Rao "Digital Signature and Watermarking methods for image authentication using cryptography analysis" International Journal (SIPIJ), vol.2, no.2, june 2011.

[11]. Rizky Damara Ardy, Oktawana Rena Indriani, Christy Atika Sari, De Rosal Ignatius Moses Setaidi, Eko Hari Rachmawants "Digital Image Signature using Triple Protecttion Cryptosystem (RSA, VIGENERE AND MD5)", Research gate.net, conference paper, Nov. 2017.

[12]. Prasanth SP, Gowtham B "AES and DES using secure and dynamic data storage in Cloud", IJCSMC, vol.3, issue 1, Jan.2014, pg.401-407.