Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 11, November -2017

Improved Method For A Secure Image Cryptography Based On RSA And DES Algorithm And LSB Steganography Technique

[1]Yamunesh Goswami, [2]Anuj Bhargava, [3]Prashant Badal

[1]*Dept. of ECE, S.R.C.E.M College, Gwalior (India)*
[2]*Dept. of ECE, S.R.C.E.M College, Gwalior (India)*
[3]*Dept. of ECE, S.R.C.E.M College, Gwalior (India)*

Abstract— *Now a day's security is one of the major problem facing all over the world. To protect facts into the unrecognizable form diverse technique are used for records hiding like steganography and cryptography techniques have been advanced. This paper also introduces new methods wherein cryptography and steganography are blended to encrypt the data as well as to cover the statistics in some other medium through image processing (IP). This paper securing the image by way of encryption is completed by RSA and DES algorithm. The encrypted picture can be hiding in some other image by way of the use of LSB strategies so that the secret's message exists. The decryption can be done by the same key using DES and RSA algorithm.*

Keywords—*Image steganography, DES, RSA.*

I. INTRODUCTION

In this modern era, where technology is developing at fast pace and each day new developments are made, security is of utmost priority. [1] The data needs to be kept secure and safe so that it could be accessed only by the authorized personnel and any unauthorized user cannot have any access of that data. Data sharing is increasing as thousands of messages and data is being transmitted on internet everyday from one place to another. The protection of data is prime concern of the sender. The need is that correct data should be sent but in a secret way that only the receiver should be able to understand the message. At first procedure of cryptography turned into invented to send mystery messages over locations. In cryptography the message turned into encoded in every other message in a blanketed way such that handiest the sender and receiver knew the manner to decrypt it [2].A cryptographic key was used to decode the message that was known only by the authorized persons. The limitation of cryptography was that other person came to know that the message had a hidden text in it and so the probability of message being decoded by other person increased. To overcome this limitation the technique of steganography was introduced.

The word steganography belongs to Greek language. In Greek the steganography stands for "covered writing". The first of all steganography was used in Greece. They use to enter the message on a wooden tablet and then apply wax on it to hide the written data. The technique of steganography was far better than cryptography as in it the data was hidden in image. The image was then sent over internet. It had advantage over cryptography as now the middle person does not come to know whether data is hidden in the image or not. The data could only be decrypted from image by the authorized person as he knows the phenomenon to decode it and had the authorized key with him that was required to decode the data. The security and the reliability of data transmission also improved with invention of steganography as now no other person could change the sent data. The main application fields of steganography are:

- Copyright Protection
- Feature Tagging
- Secret Communication
- Use by terrorists
- Digital Watermarking

Digital steganography is a technique designed to secure a via hiding that message inside every other item so that it can be saved secret from all and sundry except the intended recipient.

Steganography strategies may be separated into two corporations: Visible and invisible, the visible steganography is used if steganography is supposed to be seen by human eyes, For example, a emblem inserted into corner of an picture.

While the invisible steganography is embedded into more than a few image through sophisticated algorithms and is secreted to human eyes.[3]

II. RELATED WORK

Ramadhan J. Mstafa et. al(2016) —Over the past few decades, the art ofzz secretly embedding and communicating digital data has gained enormous attention because of the technological development in both digital contents and communication. The imperceptibility, hiding capacity, and toughness next to attacks are 3 main necessities that some video steganography way should get into thought. In this, a tough and protected video steganographic algo inside the DWT and DCT domain names is to be based on Multiple Object Tracking known as MOT algo and Error Correcting Codes this is called (ECC) is being proposed. Primarily, motion-based MOT algorithm be implemented resting on host videos to differentiate the regions of attention in moving objects. After that, the process of data hiding is being performed by concealing top secret message into DWT and DCT coefficients of each and every motion regions in video depending on center masks. Our experimental outcome exemplify that suggested algo not only improves capacity of embedding and imperceptibility although it also enhances its safety and robustness by encoding the secret message and withstanding against various attacks.[4]

Alavi Kunhu et.al (2016) In this paper, we recommend a new blind color video watermarking way for copyright safety of multimedia color films through the use of index mapping concept. The inventiveness in obtainable approach consists in crafty a hybrid Discrete Wavelet Transform (DWT) and Discrete Cosine Transform also recognized as (DCT) based distortion caused all the way through watermarking be assess by way of peak signal to sound ratio (PSNR) along with correspondence structure index measure (SSIM) and robustness within antagonism to different types of attacks have been assessed using StirMark. The proposed video watermarking algo provide improved imperceptibility within harmony by way of human visual system and offers advanced toughness in opposition to signal processing attacks.[5]

Ch.Sathi Raju et.al (2016) Compression is serious trouble in applications of capsule endoscopy. In this paper hybrid DCT compression method and DWT compression method is being employed to capitalize advantages of together techniques. The approach entails in generating shade statistics of the white band and slender band pictures in an intermediate layout and then generating the decompressed image. The quality of decompressed image is being evaluated in conditions of mean square error (MSE), signal to noise ratio known as (SNR) and PSNR.[6]

N.V.Lalitha et.al (2016) steganography is method of embedding information into signal in a technique that is complex to remove.here , a dynamic capacity of audio watermarking system is used to establish data and take away them via singular value decomposition also known as (SVD). With help of SVDbased algor and by income of lifting wavelet transform recognized as (LWT), discrete cosine transform (DCT)and DWT . DCT-SVD, DWT-SVD, DWT-DCT-SVD, LWT-DCTSVD methods are developed. It be observed so as to by growing the quantization levels signal-to-noise ratio (SNR) value decreases exponentially which leads to deformation in the original signal. It is moreover observed with the aim of robustness is also greater than before by applying dissimilar malicious attacks like resampling, echo addition, cropping, additive white gaussian noise (AWGN), and signal subtraction to enclosed signal with the aim of doesn't perturb novel signal and mine image. [7]

Shashi Mehrotra Seth, et al. (2011) In the research paper diverse experimental elements are analyzed. Based at the text files used and the experimental end result was concluded that DES set of rules consumes least encryption time and AES algorithm use least reminiscence usage, Encryption time differs in case of AES algorithm and DES set of rules. RSA devour extra encryption time and memory usage is likewise very high but output byte is least in case of RSA algorithm.[8]

Aman Kumar, et al. (2012) In the studies paper discussed that DES is secret key based totally set of rules suffers from key distribution and key settlement troubles. But RSA consumes big amount of time to carry out encryption and decryption operation It had been also determined that decryption of DES algorithm is better than different algorithms in throughput and much less energy intake. [9]

Ammad Ul Isla et al. (2016) in this paper The rapid development of data communication in modern era demands secure exchange of information. Steganography is recognized way intended for hiding information as of unauthorised access. Invisibility, capacity of payload, and PSNR security and toughness are key challenges to steganography. In this, an original image stegnography way based on majority significant bits (MSB) of pixels is proposed. Bit No. 5 is used to store the secret bits based on the difference of bit No. 5 and 6 of cover image. If the difference of bit No. Five and 6 is

dissimilar from mystery facts bit then the fee of bit no. Five is modified. The consequences state that the proposed technique ensures sizable enhancements in sign to noise ratio. Usually, hackers focus on the LSB bits for top secret data mining but proposed method utilizes MSB bits that create it more protected from illegal access. Furthermore, the offered approach is not simplest relaxed, however computationally green as properly [10]

III. USING TECHNIQUES ARE LSB, DES, RSA

a. LSB

The Least Significant Bit (LSB) is one of the essential techniques in spatial domain photograph steganography. LSB is the bottom big bit inside the byte value of a photograph pixel. The LSB based picture steganography embeds the name of the game in least good sized bits of pixels values of the quilt photograph. It exploits the truth that the level of precision in lots of picture formats is a long way greater than that perceivable through average human imaginative and prescient. Therefore, an altered image with moderate versions in hues might be indistinguishable from the unique via a human being, simply by looking at it. In LSB approach just four byte of pixels are sufficient to hold one message byte. Rest of bits in the pixel remains the equal.[11]

b. DES (Data Encryption standard)

In this research paintings, the name of the game information or file is encrypted before embedding in a cover report. We have in comparison DES, AES and RSA encryption method to encrypt records or document. Let us describe the algorithms separately. [12]

1) DES: .Data Encryption standard (DES) specifically followed by means of employer for protection products. Algorithm layout for encryption and decryption machine has been performed with equal key. These algorithm procedures the subsequent steps. DES accepts an enter of sixty four-bit lengthy plaintext and 56-bit key (eight bits of parity) and convey output of sixty four bit block. The plaintext block has to shift the bits spherical. The 8 parity bits are eliminated from the key through subjecting the critical component to its Key Permutation. The plaintext and key will processed through following

A. The key is cut up into 28 halves

b. Each 1/2 of the key is shifted (rotated) by one or two bits, depending at the spherical.

C. The halves are recombined and challenge to a compression permutation to reduce the important thing from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.

D. The rotated key halves from step 2 are utilized in subsequent spherical. E. The records block is cut up into 32-bit halves.

F. One half is challenging to a variety permutation to growth its length to forty eight bits.

G. Output of step 6 is unique-OR'ed with the 48-it compressed key from step 3.

H. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.

I. Output of step 8 is difficult to a P-box to permute the bits.

J. The output from the P-container is specific-OR'ed with different half of the facts block.

K. The two records halves are swapped and grow to be the next round's input.

c. RSA (Rivest Shamir Aldeman)

RSA is the maximum usually used public key encryption set of rules. RSA computation occurs with integers modulo n = p*q. [12] It calls for keys of at least 1024 bits for suitable safety. Keys of period 2048 bit offer extremely good safety. Widely used for relaxed communication channel and for authentication to identification provider. RSA is simply too sluggish for encrypting big volumes of information. But it's miles drastically used for key distribution Following steps are observed in RSA to generate the public and private keys

1. Conisder two large high numbers p and q such that p~=q. 2.Compute n=p*q

3. Compute φ (pq) = (p-1)*(q-1)

4. Consider the general public key k1 such that gcd (φ (n), k1) =1; 1<k1< φ (n)

5. Select the personal key k2 such that k2*okay mod φ (n) =1 Encryption and Decryption are carried out as follow Encryption: Calculate cipher text C from plaintext P such that C=P ^k1 mod n Decryption :

P=C^k2 mod n=P^k1k2 mod n

IV. PROPOSED METHODOLOGY

The proposed scheme is implemented in Matlab platform the use of preferred cryptography and steganography set of regulations. DES-RSA hybrid cryptography is used alongside LSB photograph steganography. Figure 1. Shows the working of proposed statistics protection scheme. Select an genuine photograph. Apply canny aspect detection on unique photo. Encrypt and cover textual content rub down using RSA and DES. Open encrypted massage. Decrypt textual content using RSA & DES. Calculate PSNR and MSE.

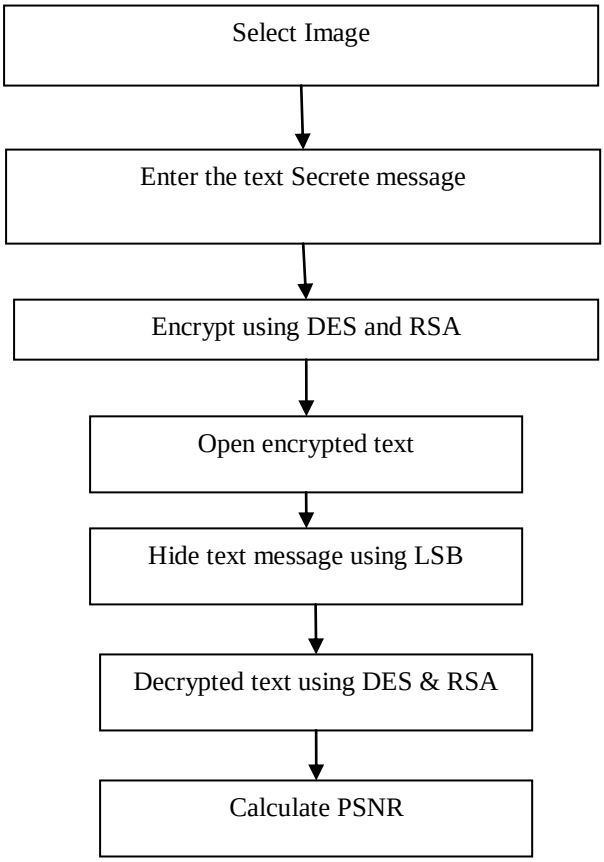

Fig 1: Flow chart of propose work

Proposed Algorithm

Step1: Select an original picture.
Step 2: Enter the textual content Secrete message
Step 3: Encrypt the usage of RSA. And DES
Step 4: Open encrypted rub down.
Step 5. Hide text message using LSB in to cover picture
Step 6: Decrypt text the usage of DES & RSA.
Step 7: Calculate PSNR.

V. RESULT ANALYSIS

Fig. 2 image dataset

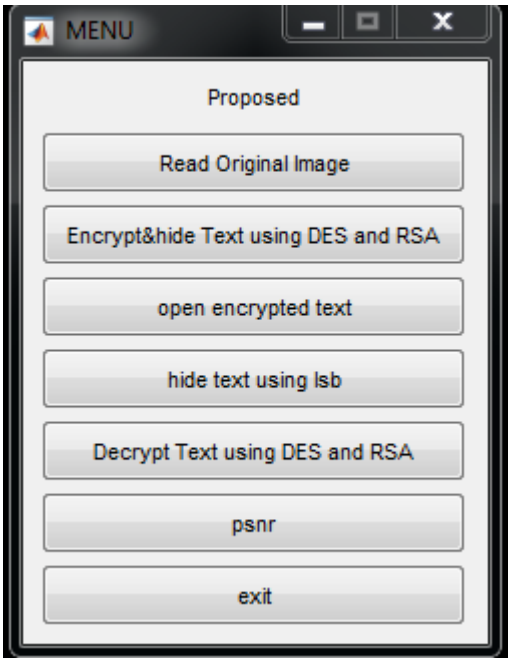

Fig. 3. first run the code and open the menu bar.

Fig. 4.Read original image.

```
Enter the message: i love my india
```

Text 1. Enter the message for hiding into original image using DES and RSA algorithm

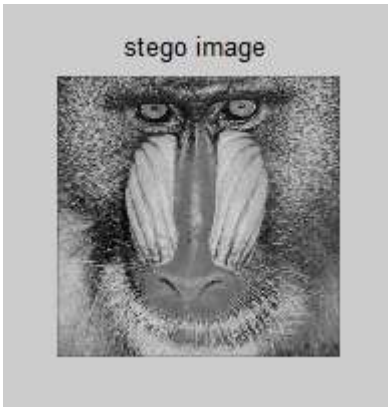

Fig. 5. Hide message into image.


```
Decrypted Message is: i love my india
```

Text. 2. Decrypt, encrypted message using DES and RSA algorithm

Table1.Comparison between base and Proposed PSNR

Base PSNR	Propose PSNR
16.8509	22.4361

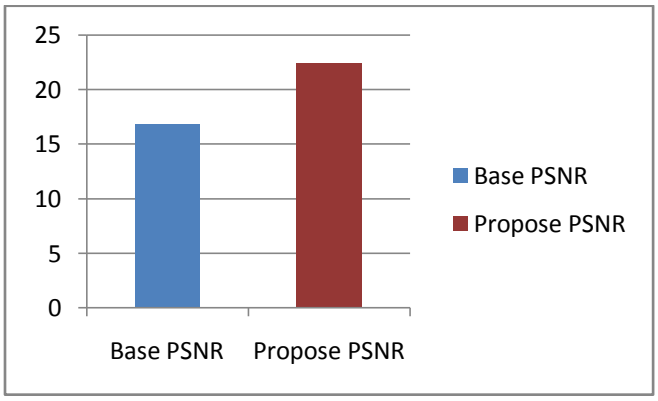

Fig. 6. Graph 1 Comparison between base PSNR and Proposed PSNR

Base MSE	Propose MSE
0.5946	0.022

Table2. Comparison between base and Proposed MSE

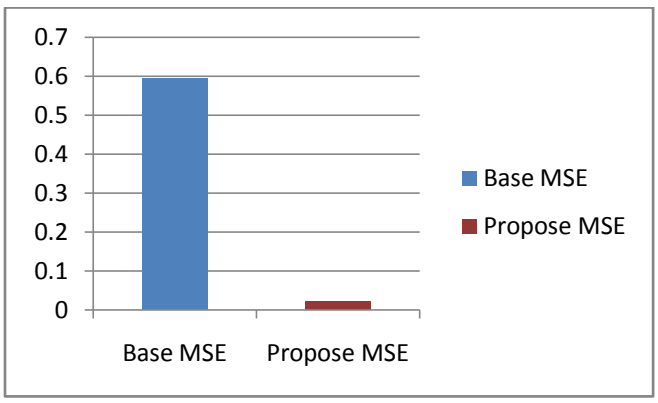

Fig. 7. Graph 2 Comparison between base MSE and Proposed ME

CONCLUSION

In the proposed approach the power of DES-RSA hybrid increase the extent of safety compared to the existing technique where simplest DES is used. In this approach the message is encrypted with a DES and the keys of DES are over again encrypted with a RSA then the hybrid of each ciphertext is hidden inner a photo using LSB photograph steganography.

Steganography, mainly shared with the cryptography is a stronger tool which permits replacing records secretly. With the fast growth of digital era and internet, steganography has incredibly advanced masses in a beyond few years. It will take a look at the information of the attacker about every cryptography and steganography. If an attacker is able to extract information from picture then he has to crack the hybrid cryptography then best he's going to get the proper records. A result of proposed approach shows that the encryption time is better than the triumphing method. It gives a extra protection in assessment to the triumphing one. Brute pressure assault in this technique can be very difficult to use as there may be use of RSA for DES key. In future exceptional steganography strategies may be used with hybrid cryptography for more protection.

REFERENCES

[1] Ashadeep Kaur* , 2Rakesh Kumar, 3Kamaljeet Kainth, "Review Paper on Image Steganography". International Journal of Advanced Research in Computer Science and Software Engineering. Volume 6, Issue 6, June 2016 ISSN: 2277 128X

[2] Anil Kumar, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", IJARCSSE, Volume 3, Issue 7, July 2013, pp 363-372

[3] P. Kruus, C. Scace, M. Heyman, and M. Mundy., A survey of steganography techniques for image files . Advanced Security Research Journal. [On line], 5(1), (2003), pp. 41-52.

[4] Ramadhan J. Mstafa1 ,Khaled M. Elleithy1 and Eman Abdelfattah2, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC" , 2169-3536 (c) 2016 IEEE

[5] Alavi Kunhu, Nisi K, Sadeena Sabnam, Majida A, Saeed AL-Mansoori, "Index Mapping based Hybrid DWT-DCT Watermarking Technique for Copyright Protection of Videos Files" , 978-1-5090-4556-3/16/$31.00 ©2016 IEEE.

[6] Ch.Sathi Raju, D.V.Rama Koti Reddy, "On Compression Characteristics of White Band and Narrow Band Images Using Hybrid DCT and DWT" , 978-1- 4788-7225 -8/15/$31.00©2015 IEEE.

[7] N.V.Lalitha, P.Vara Prasad, S.UmaMaheshwar Rao, S.UmaMaheshwar Rao , "Performance Analysis of DCT and DWT Audio Watermarking based on SVD" ,978-1-5090-1277-0/16/$31.00 ©2016 IEEE

[8] Shashi Mehrotra Seth, Rajan Mishra "Comparative Analysis Of Encryption Algorithms For Data Communication" IJCST Vol. 2, Issue 2, June 2011 I S N : 2 9 - 4 3 (P r i n t) | I S S N : 0 9 7 6 - 8 4 9 1 (On l i n e)www. i j c s t. c o m

[9] Aman Kumar , Dr. Sudesh Jakhar , Mr. Sunil Makkar "comparative analysis between DES and RSA algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[10] Ammad Ul Islam1 , Faiza Khalid2 , Mohsin Shah2 , Zakir Khan2 , Toqeer Mahmood3 , Adnan Khan2 , Usman Ali2 , Muhammad Naeem4, "An Improved Image Steganography Technique based on MSB using Bit Differencing" , 978-1-5090-2000-3/16/$31.00 ©2016 IEEE.

[11] Deepika Dongre, Rina Mishra, "A Review on Edge Based Image Steganography
International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321.8169Volume: 2 Issue: 9 2862 - 28

[12] B. Padmavathi1 , S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique" International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064. Volume 2 Issue 4, April 2013

