Journal of Innovative Image Processing (JIIP) (2019)
Vol.01/ No. 01
Pages: 20-30
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2019.1.003

A SECURE STEGANOGRAPHY CREATION ALGORITHM FOR MULTIPLE FILE FORMATS

Mr. R. Vinothkanna,
Department of ECE, Vivekanandha College of Technology for Women,
Namakal, India.
Email id: rvinothkannaphd@gmail.com

Abstract: The technological advancements in the information sharing and the development of many techniques to make the information conveyance easy necessitate a protection methodology that could prevent the personal information that is transmitted from being hacked. Some of the protection methods that have emerged are the cryptography, steganography, watermarking, digital signature etc. As steganography is a popular method of transmitting the covered secret information in order to avoid hacking and the misuse due to its major attributes such as the security, capacity and the robustness. This paper puts forward cryptography incorporated steganography (CICS) to provide a highly secure steganography algorithm for the files of the multiple formats, The performance analysis of the method and the measurement of the parameters such as the PSNR and the SSIM are done to ensure the efficiency of the proffered method.

Keywords: Steganography, Cryptography, RSA, PSNR, SSIM, Capacity, Security and Robustness

1. INTRODUCTION

The evolution of the internet and the advancement in the field of the information and communication has made necessary of the information security, The cryptography, steganography, water marking and many more methods are been put into utilization for protecting the information from the illegal usage and destruction[5]. The steganography could be defined as the art of concealing a data into another data for the purpose of securing the information. Steganography being an ancient method of concealing the information's that are to be kept secret is a Greek word with the meaning "Covered Writing" [1] Though the steganography is utilized in the securing the images similar to the cryptography ,unlike cryptography the steganography doesn't mix –up the information's but just hides the information's . The cryptography seals the information present inside a message alone but he steganography totally hides the presence of the message [2] the major attributes of the steganography in hiding the information compared to the water marking is the capacity, security and the robustness where the capacity states the amount of information that could be hidden, the security is the level of the secureness provided against the eaves

ISSN: 2582- 4252

Journal of Innovative Image Processing (JIIP) (2019)
Vol.01/ No. 01
Pages: 20-30
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2019.1.003

dropping and the robustness is the measure of withstanding capability of the system before it is broken [4]. The figure below shows some of the collection of the secret communications used in maintaining the information security.

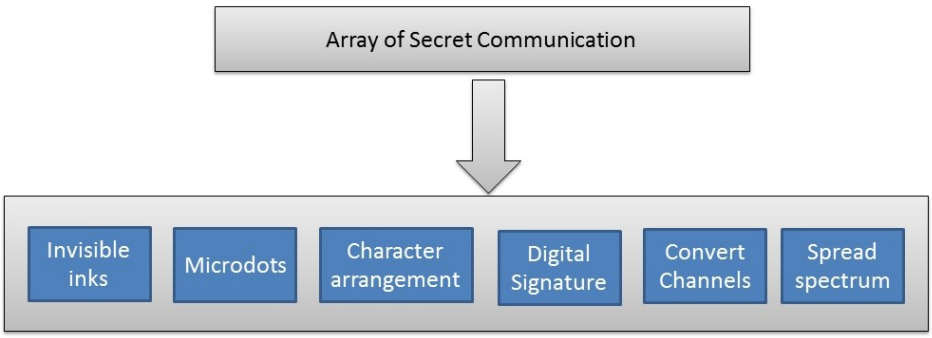

Fig .1 Collection of secret communication

The steganography is viewed as the art and the science for maintaining the secrecy in the transmitted information. [6]. There are steganography are available in all file (text, image, audio and video) formats. some of the well-known steganography are that are predominant in maintaining the secrecy of the messages are the least significant bit, linear feedback shift register , DCT , DWT , CWT etc. the fig.2 shows the example of an image steganography used in securing the information.

ISSN: 2582- 4252

Journal of Innovative Image Processing (JIIP) (2019)
Vol.01/ No. 01
Pages: 20-30
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2019.1.003

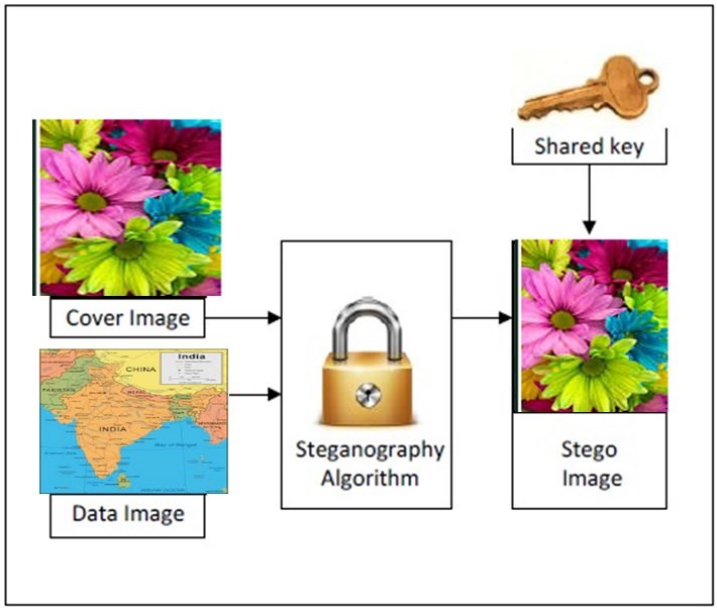

Fig. 2 Image steganography

The paper also put forwards a highly secure steganography algorithm for protecting the information in the multiple image formats. Utilizing the RSA encryption along with the steganography the proposed method presents a more protected and a concealed form of information eluding the illegal hacking, and the misuse.

The remaining of the paper is organized with the related works in the part two, the proposed work in part three, the results in part four and the conclusion in part five.

2. RELATED WORKS

Johnson et al [1] the author presents the discussion on the how to conceal the information that are in the image formats using the steganography software. Anderson, et al [2] the author provides the clarified statement about the capabilities of the steganography by exploring the limits of the steganography theory and providing the overview of the ancient and the modern techniques available in the steganography along with the attacks they are subjected to. Crandall, et al [3], the author presents some valuable notes on the steganography by demonstrating the various methods for diminishing the effect of the hidden message on the cover text. Provos, et al [4] the paper puts forward a discussion on the prevailing steganography and the latest research developments in it along with

ISSN: 2582- 4252

Journal of Innovative Image Processing (JIIP) (2019)
Vol.01/ No. 01
Pages: 20-30
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2019.1.003

the survey of the different detection algorithms and their practical applications. Morkel et al [5] the author has put his effort in elaborating the "overview of the image steganography it usage and its strategies Sadek,et al [6] the paper is the comprehensive review of the latest developments in the steganography, presenting the review of the related attacks with the strategies of the steg-analysis Shiu et al [7], the author provides the method in securing the personal information leakage by proposing a" text based steganography" for the social media communication. Jiang, et al [8] the author proposes the "LSB based quantum image steganography algorithm for the purpose of hiding the information's that are liable of being hacked. Ansari et al [9] the author presents the performance analysis of the various image steganography's with the various methods of the cover media and the embedding domains. Piper, et al [10], Saxena et al [11], explains the utilization of the parallel algorithm for protecting the information that are conveyed Subasree, et al [12], the paper put forwards a novel protocol for securing the information' using the HCA (hybrid-cryptography algorithm) by providing a ECC for the encryption and the dual-RSA for the authentication Gura et al [13], the author presents the combined cryptographic hardware that utilizes the SECG curves + the RS A-1024 +RSA -2048 for a MC for the reduction of the number of memory access. Gupta et al [14], the paper exploits the algorithm of RSA ("Rivet, Shamir, and Adelman"), DHA ("Diffie Hellman Algorithm") and the LSB ("Least Significant Bit") steganography for concealing the information. Sun et al [15] the paper provides the security analysis of the dual/twin RSA ("Rivet, Shamir, and Adelman"),, in the types against the conventional RSA ("Rivet, Shamir, and Adelman"), the table.1 shown below gives the details of the application of the steganography and their limitations. Wang, et al [16] the paper elaborates "file encryption and decryption using the standard RSA"

Applications	Limitations
Confidential Communication and secret data storing	Misuse by terrorist
Protection of data modification	Misuse by attackers
Access control system for digital content distribution	Data theft
Media data base system	Results with potential dangers if created on ill intentions.

ISSN: 2582- 4252

Journal of Innovative Image Processing (JIIP) (2019)
Vol.01/ No. 01
Pages: 20-30
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2019.1.003

Table .1 Limitations and application of Steganography [9]

3. PROPOSED WORK

The proposed work concentrates on the secured transmission of the image of multiple formats, by hiding them under a cover image. So the paper incorporates the cryptography into the steganography to enhance the capacity, security and the robustness of the information transfer.

3.1. CRYPTOGRAPHY INCORPORATED STEGANOGRAPHY (CICS)

The proposed method, utilizes the dual "Rivet, Shamir, and Adelman" [11][15] to encrypt the original images, the encrypted images are covered under the cover image/stego images[9] to protect the data and maintain its data integrity. The algorithm of the CICS is cryptography incorporated steganography is presented in the paper. The fig.3 below shows the flow diagram of the cryptography incorporated steganography.

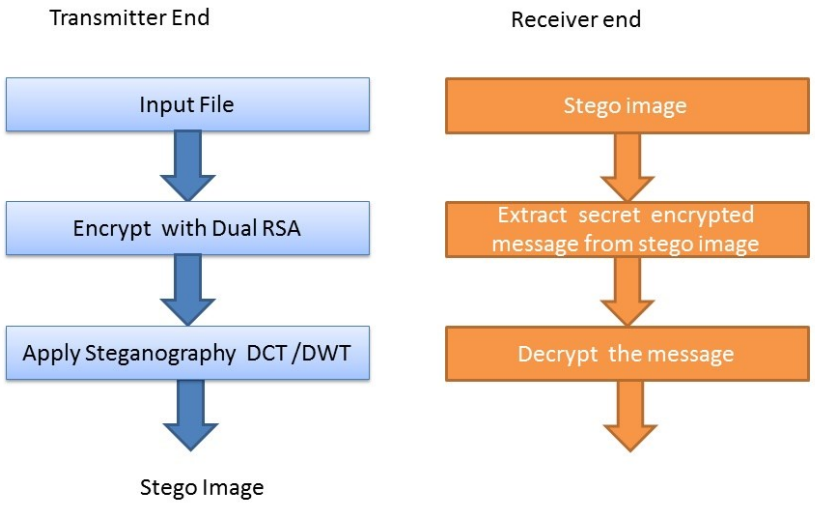

Fig .3 Flow in the Procedure of CICS

ISSN: 2582- 4252

Journal of Innovative Image Processing (JIIP) (2019)
Vol.01/ No. 01
Pages: 20-30
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2019.1.003

3.2. STEPS IN THE TRANSMITTER PART

The step in the transmitter side initiates with selecting a grey image as the image to cover the original image that has to be transmitted. The original image in the next stage is converted into an encrypted form applying the dual RSA Small d [15]. The "Dual RSA" uses the same public and the private exponent for the two different RSA occurrences. The difference is significant in the "blind signatures and the authentication". The encryption of the dual- Rivet, Shamir, and Adelman resembles the encryption in the "standard Rivet, Shamir, and Adelman" [11] [16] the following algorithm details the steps involved in key generation for the dual RSA.

Step 1: Pick a random number 'k' and 'l' of $bit_{size} = M_n$ and $\frac{M}{2-M_n}$ respectively, if multiplication of the two selected numbers added with one ($R = (k * l) + 1$) should result with the prime, otherwise select the next prime.

Step 2: pick another two number randomly $x\ and\ y$ of bit_{size} that is equal to $\frac{M}{2-M_n}$ and M_n respectively and perform the same calculation as in step one by alternating the number ($R1 = kx + 1\ and\ R2 = xy + 1$) to find whether it is Prime.

Step 3: select an Exponent (E) that is private such that its GCD generated is equal to 1.

Step 4: Enumerate the encryption key using the "Rivet, Shamir, and Adelman" equation($1 + s_1(R-1)(R2-1)$).

Step 5: N_1= RR1, N_2= R1R2, s_2= y, Where the s_1 is the randomly selected element.

The encryption with the "dual RSA" is followed by the application of the steganography based on the DCT/DWT that is suitable for variety of image formats. The former separates the encrypted message into 8*8 pixels and embed it by altering the high or the middle frequency and the latter segregates the encrypted pixels into four sub-bands (LL, HL, LH, and HH) and manipulates the information by scanning them in the vertically , horizontally. Once the images are embedded the stego images with the information covered inside another information is generated in the transmission side and send to the receiver end. The frequency domain method usage enables to have highly resistant to vulnerabilities compared to the spatial domain method.

3.3. STEPS IN THE RECEIVER PART

In the receiver side the "stego information" received in the receiver side is subjected to feature extraction to extract the encrypted information, the encrypted information extracted is subjected to the dual RSA decryption that relies on the "RSA-CRT" method. The RSA-CRT fundamentally developed to have a speedy decryption. The decryption

ISSN: 2582- 4252

Journal of Innovative Image Processing (JIIP) (2019)
Vol.01/ No. 01
Pages: 20-30
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2019.1.003

method using the RSA-CRT manipulates the dual factors $f_1 = D^{ER} \left| R \right|$ and $f_2 = D^{ER1} \left| R1 \right|$, the original information can be acquired by combining the two factors utilizing the Chinese remainder theorem. Applying the Dual-RSA decryption the original information is retrieved using the private key by the authorized receiver at the receiver end.

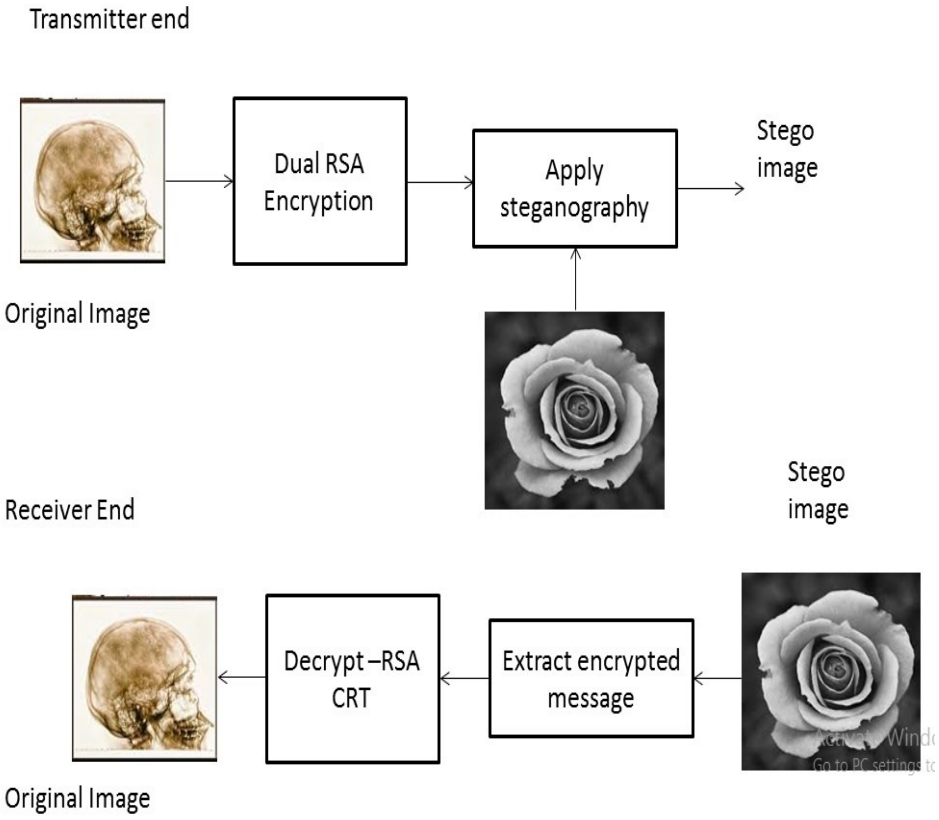

Fig.4 CICS Information Transmission and Reception

The Fig.4 above shows the information transmission through the CICS secure transmission, the proposed methodology is well –suited for confidential information transfer in the field of medicine and research.

4. RESULT ANALYSIS

ISSN: 2582- 4252

Journal of Innovative Image Processing (JIIP) (2019)
Vol.01/ No. 01
Pages: 20-30
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2019.1.003

The performance analysis of the proposed method by implementing in the MATLAB and the measuring the peak signal to noise ratio and the structural similarity index shows the competence of the CICS method against the conventional steganography methodologies. The fig. 5 below shows the percentage of the PSNR, SSIM observed in the conventional and the CICS method.

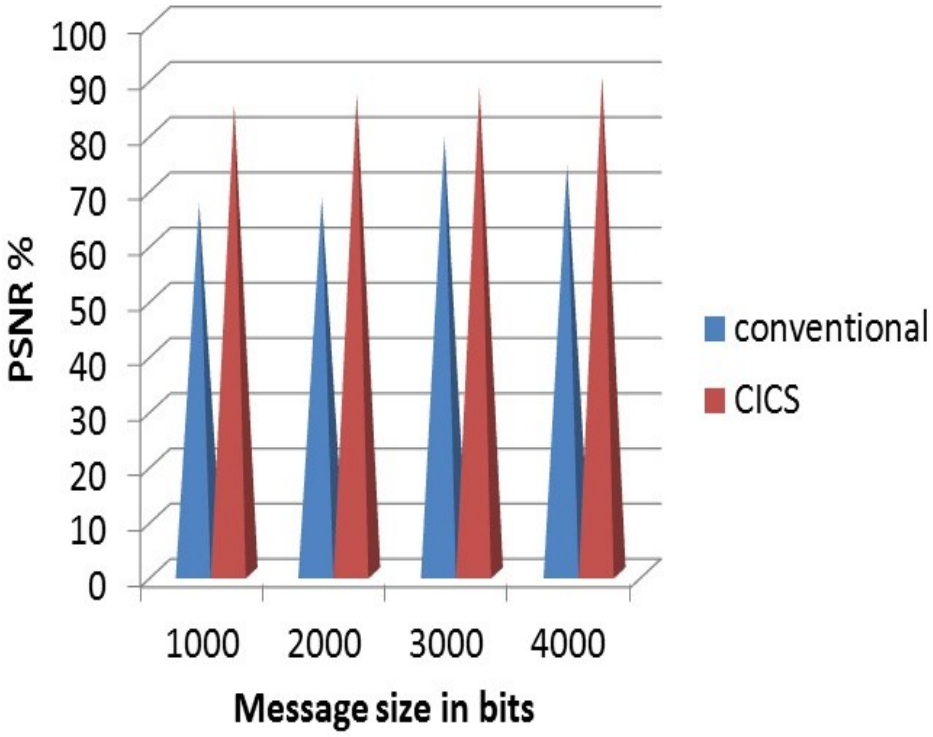

Fig .5 PSNR

The fig.6 shows the SSIM percentage of the proposed and the conventional steganography .The results obtained shows the competence of the CICS method against the conventional steganography.

ISSN: 2582- 4252

Journal of Innovative Image Processing (JIIP) (2019)
Vol.01/ No. 01
Pages: 20-30
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2019.1.003

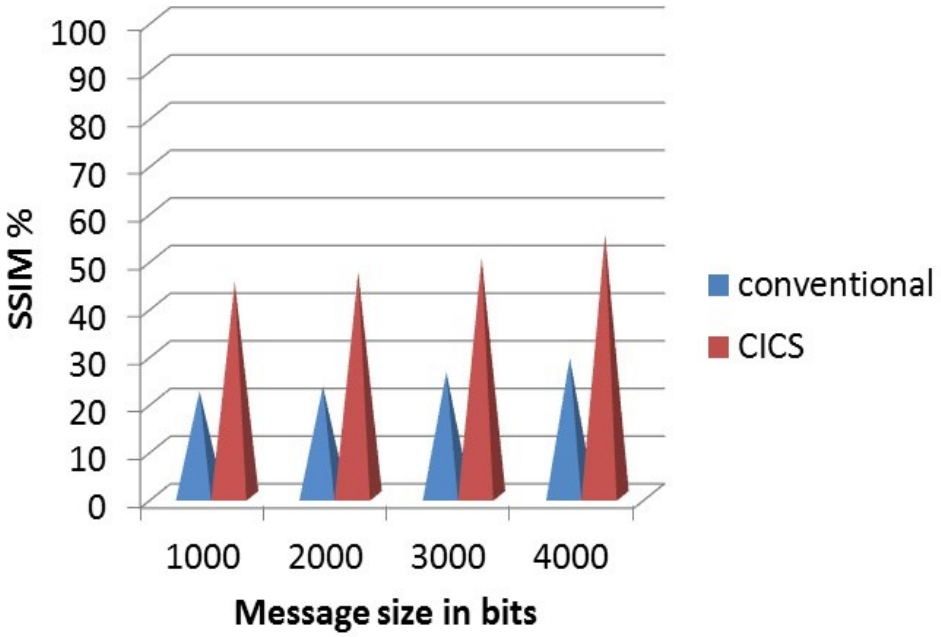

Fig.6 SSIM

5. CONCLUSION

The paper proposes the cryptography incorporated steganography (CICS) to provide a highly secure information transmission. By engaging the cryptography based encryption utilizing the DUAL-RSA enables in having the less memory utilization and speedy decryption process. The encryption is followed by the DCT/DWT based steganography to cover the encrypted information, in the receiver side the encrypted information's are extracted and decrypted using the RSA-CRT to retrieve the original image in the receiver side with a higher capacity, security and robustness. The performance analysis of the CICS by implementing it in the MATLAB, and measuring the values of PSNR and SSIM ensures the efficiency of the CICS against the conventional steganography. In future the paper is to proceed with the implementation of the CICS in the medical field for confidential information transfer for the patients.

ISSN: 2582- 4252

Journal of Innovative Image Processing (JIIP) (2019)
Vol.01/ No. 01
Pages: 20-30
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2019.1.003

References

[1] Johnson, Neil F., and Sushil Jajodia. "Exploring steganography: Seeing the unseen." *Computer* 31, no. 2 (1998): 26-34.

[2] Anderson, Ross J., and Fabien AP Petitcolas. "On the limits of steganography." *IEEE Journal on selected areas in communications* 16, no. 4 (1998): 474-481.

[3] Crandall, Ron. "Some notes on steganography." *Posted on steganography mailing list* (1998): 1-6.

[4] Provos, Niels, and Peter Honeyman. "Hide and seek: An introduction to steganography." *IEEE security & privacy* 1, no. 3 (2003): 32-44.

[5] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." In *ISSA*, pp. 1-11. 2005.

[6] Sadek, Mennatallah M., Amal S. Khalifa, and Mostafa GM Mostafa. "Video steganography: a comprehensive review." *Multimedia tools and applications* 74, no. 17 (2015): 7063-7094.

[7] Shiu, Hung-Jr, Bor-Shing Lin, Bor-Shyh Lin, Po-Yang Huang, Chien-Hung Huang, and Chin-Laung Lei. "Data hiding on social media communications using text steganography." In *International Conference on Risks and Security of Internet and Systems*, pp. 217-224. Springer, Cham, 2017.

[8] Jiang, Nan, Na Zhao, and Luo Wang. "LSB based quantum image steganography algorithm." *International Journal of Theoretical Physics* 55, no. 1 (2016): 107-123.

[9] Ansari, Arshiya Sajid, Mohammad Sajid Mohammadi, and Mohammad Tanvir Parvez. "A comparative study of recent steganography techniques for multiple image formats." *International Journal of Computer Network and Information Security* 11, no. 1 (2019): 11.

[10] Piper, Fred. "Cryptography." *Encyclopedia of Software Engineering* (2002).

[11] Saxena, Sapna, and Bhanu Kapoor. "An efficient parallel algorithm for secured data communications using RSA public key cryptography method." In *2014 IEEE International Advance Computing Conference (IACC)*, pp. 850-854. IEEE, 2014.

[12] Subasree, S., and N. K. Sakthivel. "Design of a new security protocol using hybrid cryptography algorithms." *IJRRAS* 2, no. 2 (2010): 95-103.

[13] Gura, Nils, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz. "Comparing elliptic curve cryptography and RSA on 8-bit CPUs." In *International workshop on cryptographic hardware and embedded systems*, pp. 119-132. Springer, Berlin, Heidelberg, 2004.

[14] Gupta, Shailender, Ankur Goyal, and Bharat Bhushan. "Information hiding using least significant bit steganography and cryptography." *International Journal of Modern Education and Computer Science* 4, no. 6 (2012): 27.

[15] Sun, Hung-Min, Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek. "Dual RSA and its security

ISSN: 2582- 4252

Journal of Innovative Image Processing (JIIP) (2019)
Vol.01/ No. 01
Pages: 20-30
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2019.1.003

analysis." *IEEE Transactions on Information Theory* 53, no. 8 (2007): 2922-2933.

[16] Wang, Suli, and Ganlai Liu. "File encryption and decryption system based on RSA algorithm." In *2011 International Conference on Computational and Information Sciences*, pp. 797-800. IEEE, 2011.

ISSN: 2582- 4252