Improve Image Security in Combination Method of LSB Stenography and RSA Encryption Algorithm

[1]Dr. Himanshu Arora, [2]Mr. Manish Kumar and [3]Mr. Sanjay Tiwari

[1]Professor, Department of Computer Science & Engineering, Arya College of Engineering & Research Centre, Jaipur

[2]Assistant Professor, Department of Computer Science & Engineering, Arya Institute of Engineering & Technology, Jaipur

[3]Assistant Professor, Department of Computer Science & Engineering, Arya Institute of Engineering Technology & Management, Jaipur

dr.himanshuarora17@gmail.com, mukhijakumar@gmail.com, sanjay76tiwari@gmail.com

Abstract

Images are the most well-known methods of correspondence utilized in different fields, such as clinical, research, mechanical, military and more. In the period of data innovation, the most fundamental part of data trade and correspondence is the Internet. With the headway of data innovation and the web, computerized media has gotten one of the most notable information move devices, however it actually faces various difficulties including confirmation issues, furthermore change, copyright assurance. Stenography and cryptography are the most popular technique of image or data security. In cryptography asymmetric RSA algorithm is one of the best algorithms to use for image encryption purpose. It is very difficult for unauthorized person to get the data from RSA encrypted data. In stenography LSB technique is most popular and secure to hide an image in an image. So, in this paper, present the improve image security technique in combination method of LSB stenography and RSA encryption algorithm. First hide an image into an image using the LSB technique, after that get the embedded image in which secrete image is hidden into the cover image. So now apply the asymmetric RSA encryption algorithm on the embedded image to get the cover image. Using this method now the security of the secrete image is more improved which is very difficult to unauthorized person to creak it.

Keywords: RSA, LSB, Stenography, cryptography, encryption, image.

1. INTRODUCTION

In the period of data innovation, the most indispensable portion of data trade and correspondence is the Internet. With the headway of data innovation and the web, computerized media has gotten one of the most notable information move apparatuses; however it actually faces various difficulties including confirmation issues, alteration, and copyright insurance. Numerous methods, for example, encryption, confirmation, steganography, and so forth can be utilized to protect the digital information [1].Cryptography has two significant cycles: encryption and decryption. Encryption is the way toward encoding the first message into a message that can't be deciphered as the first, while unscrambling is changing the message that was encoded in the first message. There are two encryption models calculations are symmetric keys and asymmetric keys. A symmetric key uses a common key to encode and decode a message. The asymmetric key uses two keys: the public key and the private key [2].

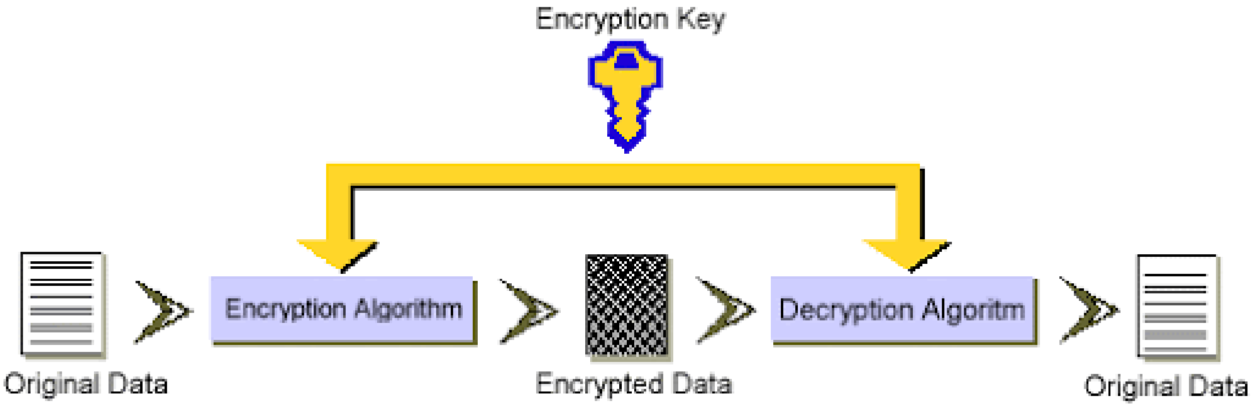

Fig 1 : Symmetric Key Cryptography

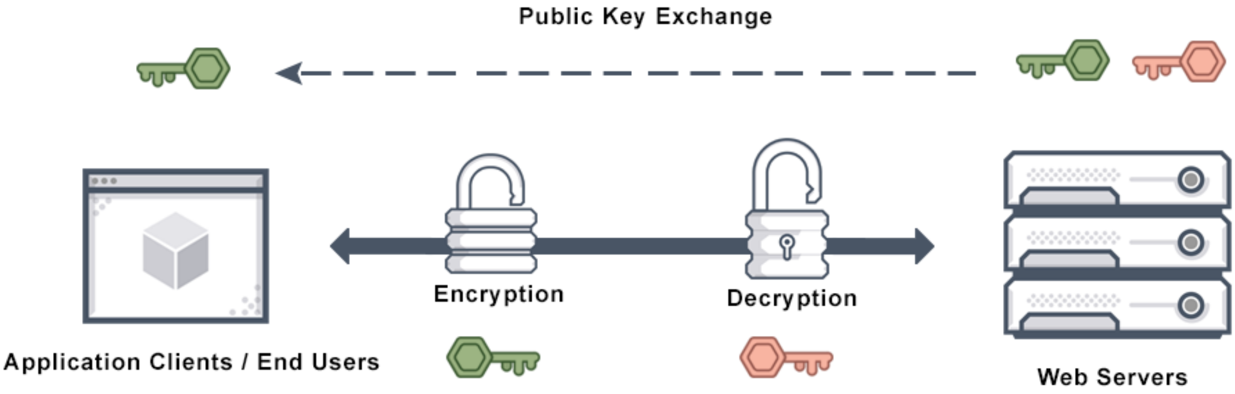

Fig 2 : Asymmetric Key Cryptography

Today, mainstream researchers have seen extraordinary enthusiasm for data encryption to shield important data from undesirable person. Subsequently, different encryption algorithms have been utilized in computerized data encryption to accomplish this objective, for example, DES, GA, AES, RSA algorithms, and so on [3]. Encryption is a kind of picture security technique that gives a protected method to move and store pictures over the Internet. Security is the essential worry of any framework to protect the respectability, privacy and credibility of the picture. Despite the fact that encryption is a powerful way, it likewise represents a security issue if information with grey scale is increasingly various [4]. Steganography is a secret communication technique that is done by infusing the secret information into picture, sound and video records. In picture Steganography, the measurable properties of the picture must be protected in the wake of veiling the secret information in the picture. There are mainly three types of Steganography image, video and audio Steganography [5,6]. In image or picture steganography, the statistical properties of the picture must be maintained after masking the secret data in the image. LSB and PVD are the most popular steganography techniques [6].

2. RSA ENCRYPTION ALGORITHM

The RSA algorithm is the one of the most popular and large used for public key encryption approach. The advanced mark is an approval framework that permits the sender of the message to attach the code as a computerized signature. Customarily, the high level imprint is molded by taking the hash of the message and encoding the message with the ender's private key. This imprint guarantees the source and genuineness of the message [2]. RSA is one of the most normally utilized algorithms for computerized picture security or advanced picture encoding. Encryption is probably the most straight forward approaches to ensure data and pictures through correspondence. In an encoded picture, nobody can see the original information or picture in it. To show the original picture or information, you can utilize the disentangling method to get the first picture from the encoded picture [7].

3. LSB STEGANOGRAPHY TECHNIQUE

The information covered up in the picture is isolated into two domains, specifically the frequency and spatial domain. In the domain of frequency, the data is veiled by first changing the cover data. The broadly utilized techniques are SVD, DWT and DCT. In the domain of spatial, the secret data is embedded straightforwardly by changing the pixel estimation of the spread picture. LSB and MSB are the most famous methods in spatial domain [8]. Least Significant Bit Replacement (LSB) is a notable steganographic plot, in which the LSBs in the spread picture are supplanted with secret information bits to get the steganographic picture [9] . It has the upsides of a high payload, great visual indistinctness and extraordinary simplicity of usage. In any case, in the replacement for LSB, the inclusion pixels with even qualities are not changed or expanded by 1, while the opposite is valid for pixels with odd qualities [10].

4. PROPOSED DESIGN TECHNIQUE

In proposed design technique to improve image security of the secrete image first hide the secrete image into the cover image after that get the embedded image that is seen similar as the cover image but it consist of secrete image. After get the embedded image apply the RSA encryption algorithm on it and get the encrypted image that is totally differ then the original and secrete image. Hence using the two layer of security improved the image security in combination method of LSB stenography and RSA encryption algorithm.

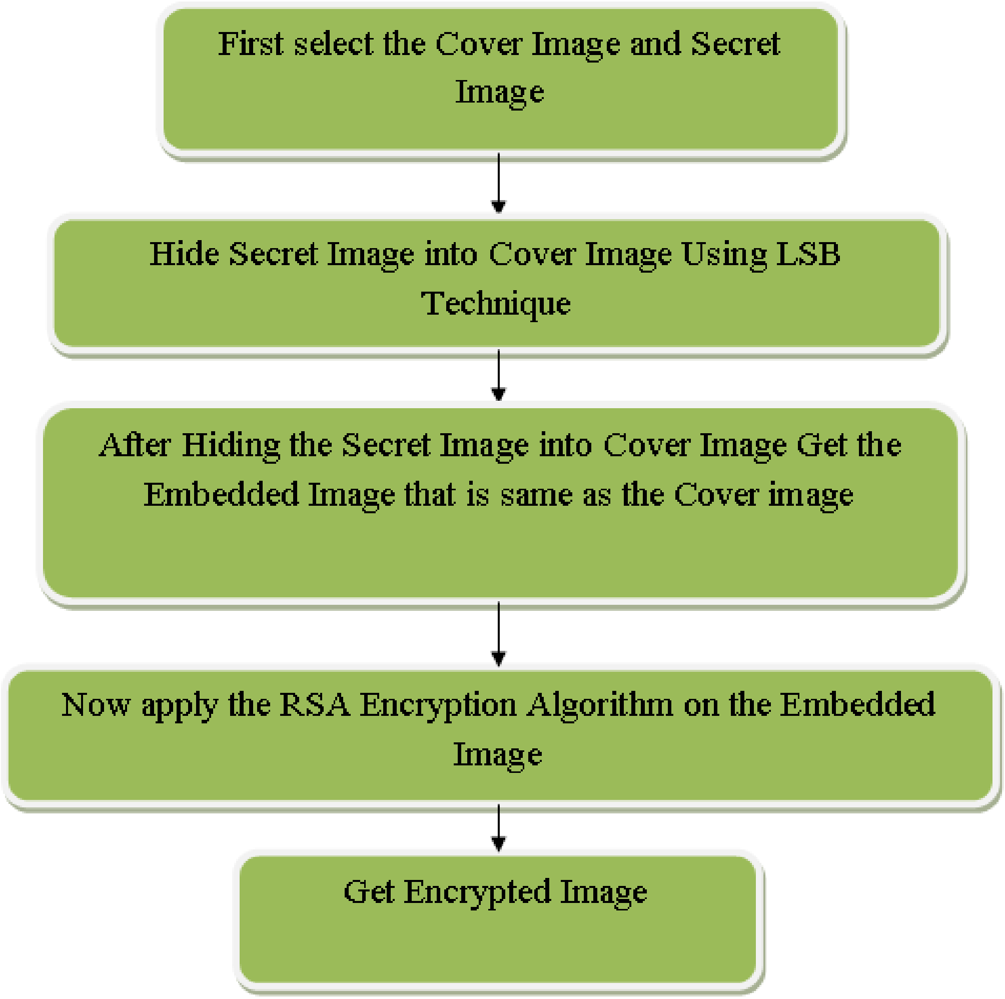
First select the Cover Image and Secret Image
Hide Secret Image into Cover Image Using LSB Technique
After Hiding the Secret Image into Cover Image Get the Embedded Image that is same as the Cover image
Now apply the RSA Encryption Algorithm on the Embedded Image
Get Encrypted Image

Fig 3 :Flow Chart of Proposed Design Implementation

In Fig 4 and Fig 5 shown the cover image tiger and secret image of rear coin respectively, now hide the secret image into the cover image using LSB technique and get the embedded image that is same as the cover image tiger, shown in Fig 6. Now apply the RSA encryption algorithm on it and get the encrypted image that is totally differ then the original image which is shown in Fig 7. To analysis the security levels of the shown the histogram of cover image and encrypted image is shown in the Fig 8 and Fig 9 respectively.

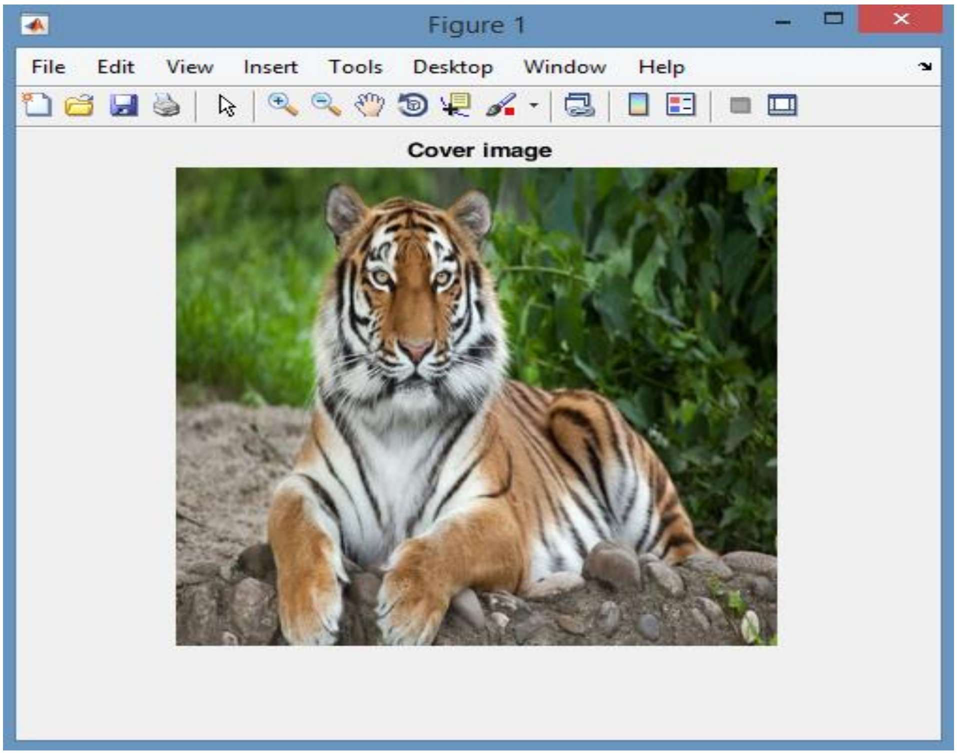

Fig 4 :Cover Picture of The Tiger

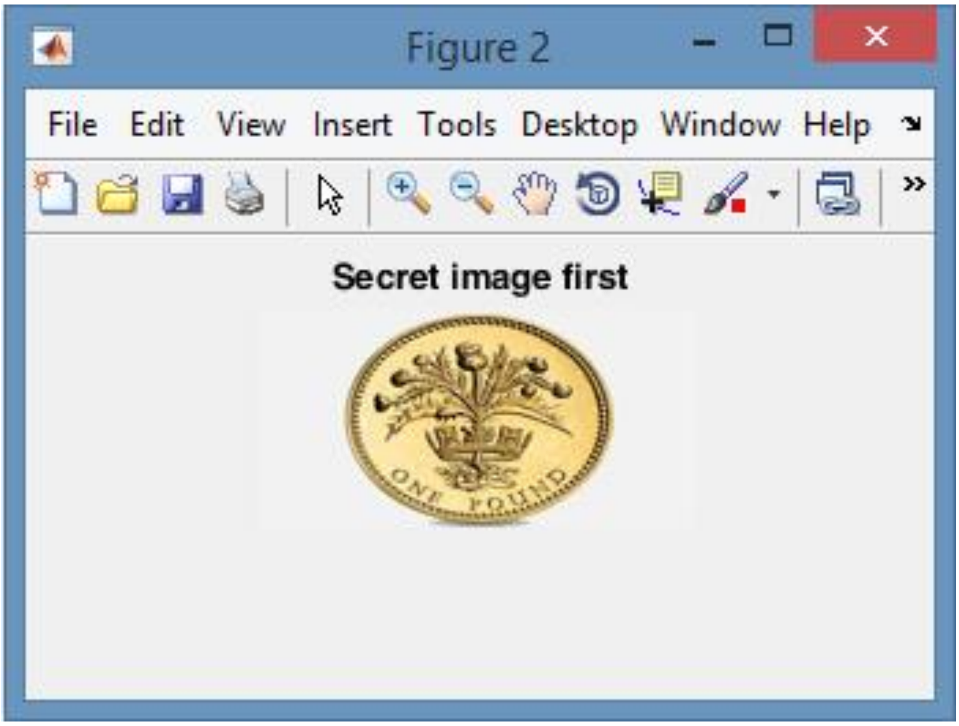

Fig 5 :Secret Picture of The Rear Coin

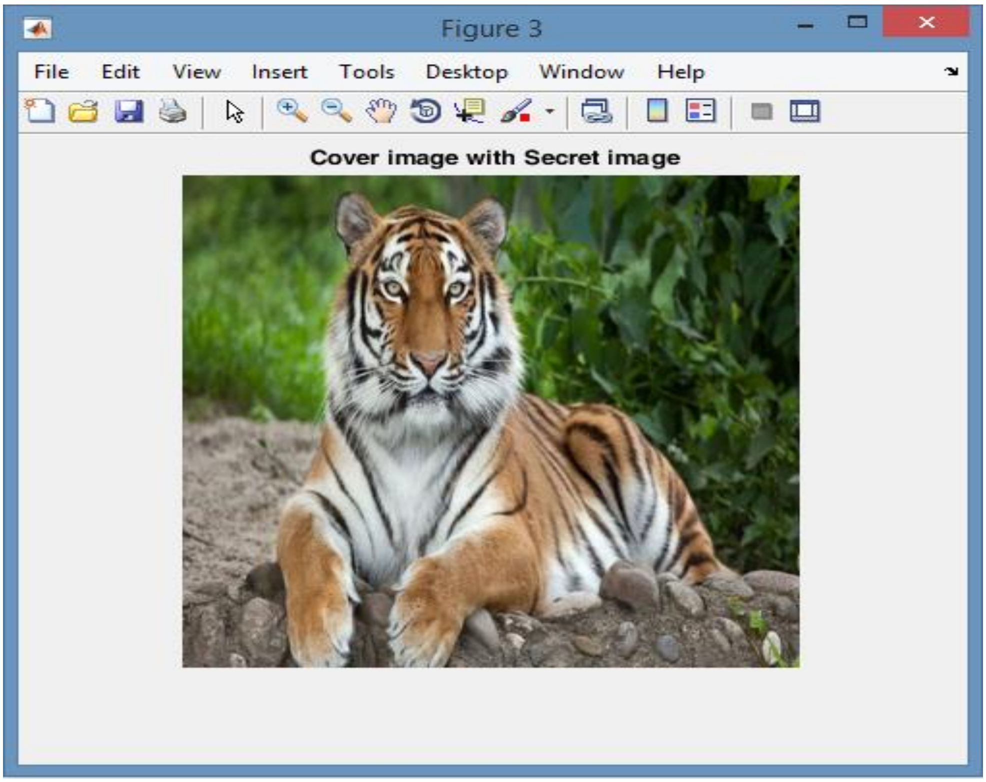
Figure 3
File Edit View Insert Tools Desktop Window Help
Cover image with Secret image

Fig 6 : Embedded Picture

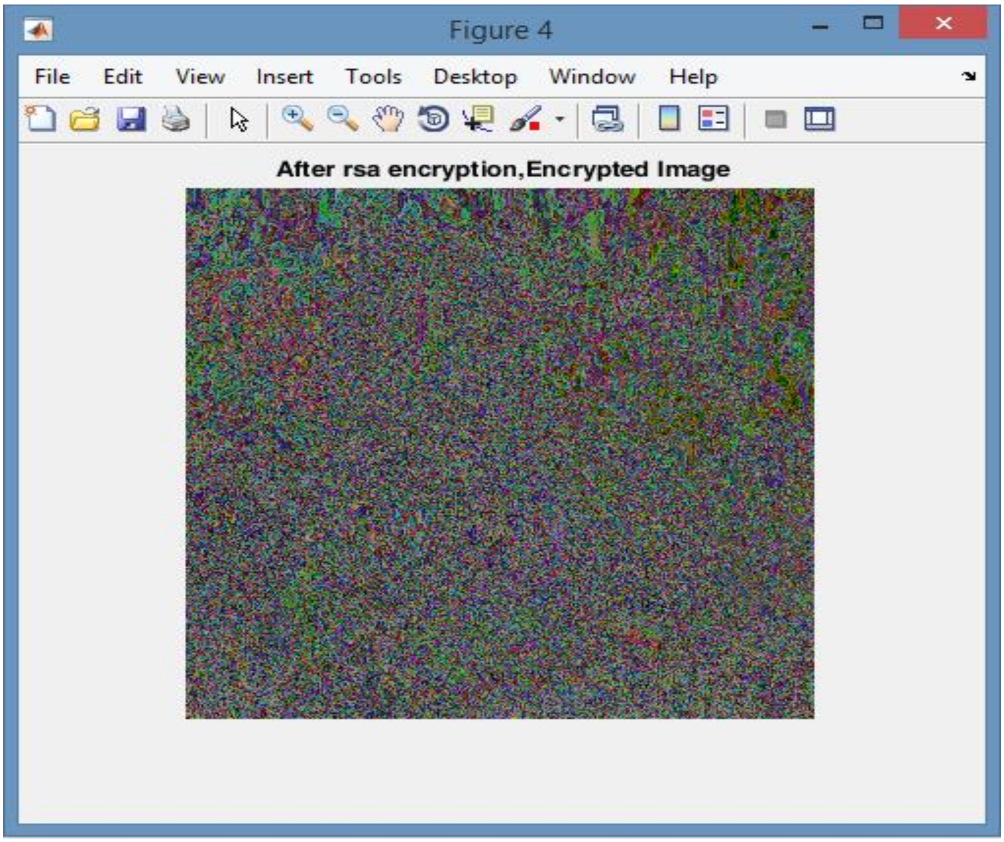
Figure 4
File Edit View Insert Tools Desktop Window Help
After rsa encryption,Encrypted Image

Fig 7 :Encrypted Picture

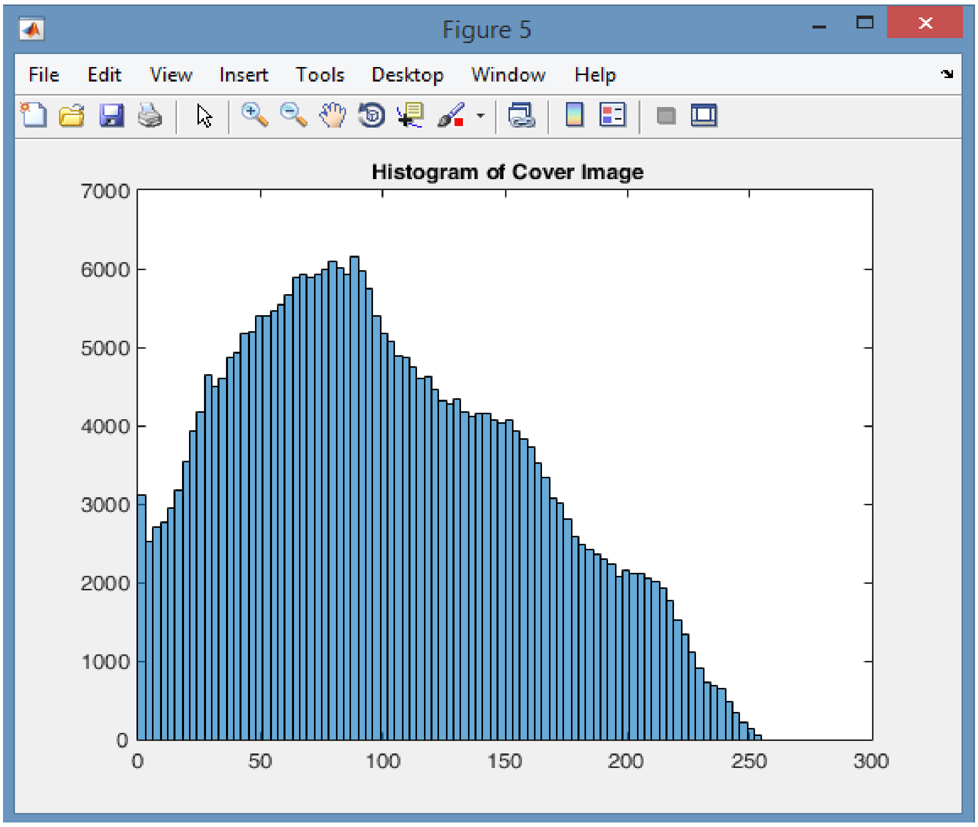

Fig 8 :Histogram of Cover Image

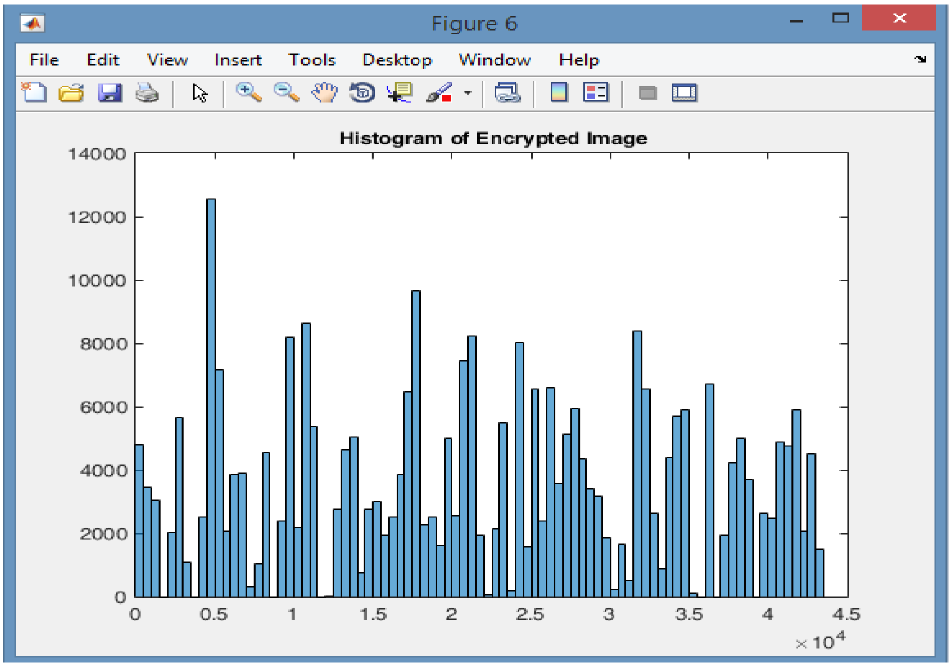

Fig 9 : Encrypted Image Histogram

Again, take another example, in which hide the car model design into the panda image. In Fig 10 and Fig 11 shown the cover image of panda and secret image of car design respectively, now hide the secret image of car design into the cover image of panda using LSB technique and get the embedded image that is same as the cover image of tiger, shown in Fig 12. Now apply the RSA encryption algorithm on it and get the encrypted image that is totally differ then the original image which is shown in Fig 13. To analysis the security levels of the shown the histogram of cover image and encrypted image is shown in the Fig 14 and Fig 15 respectively.

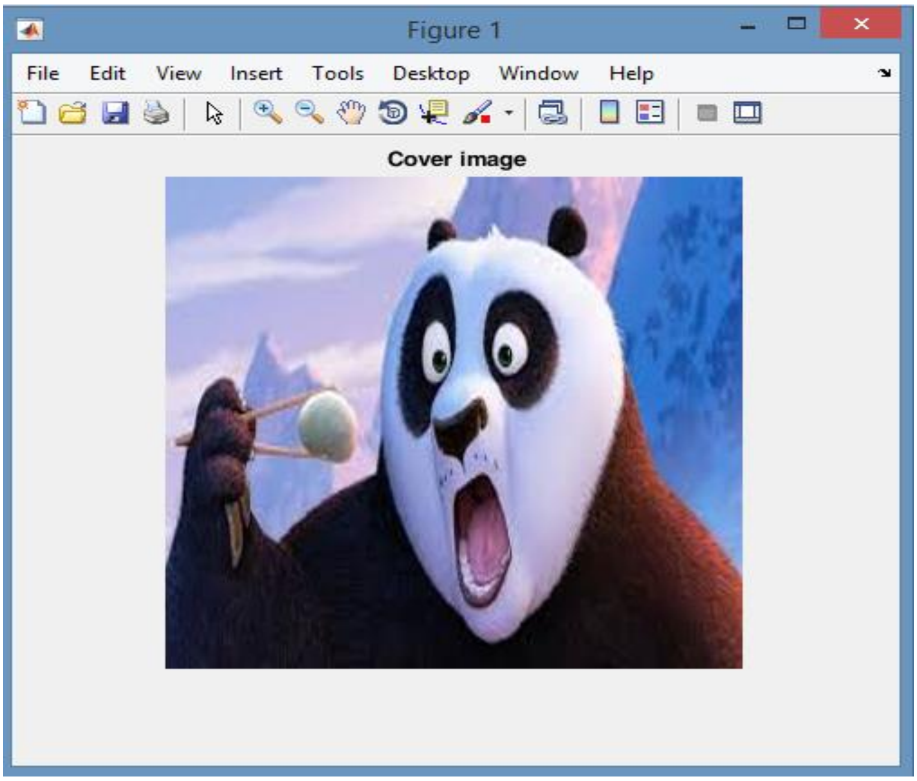

Fig 10 :Cover Image Tiger

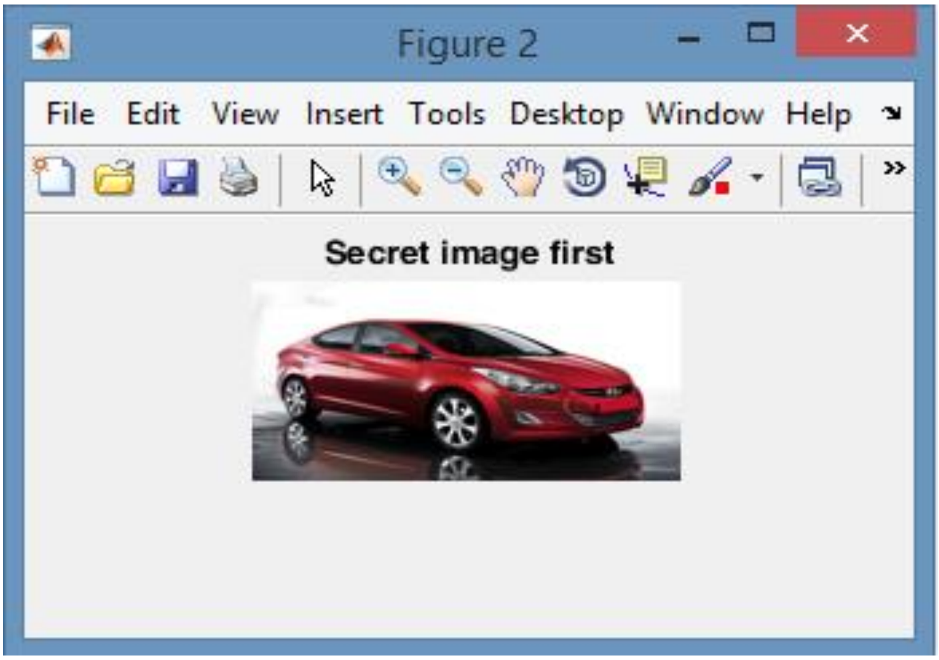

Fig 11 :Secret Image rear coin

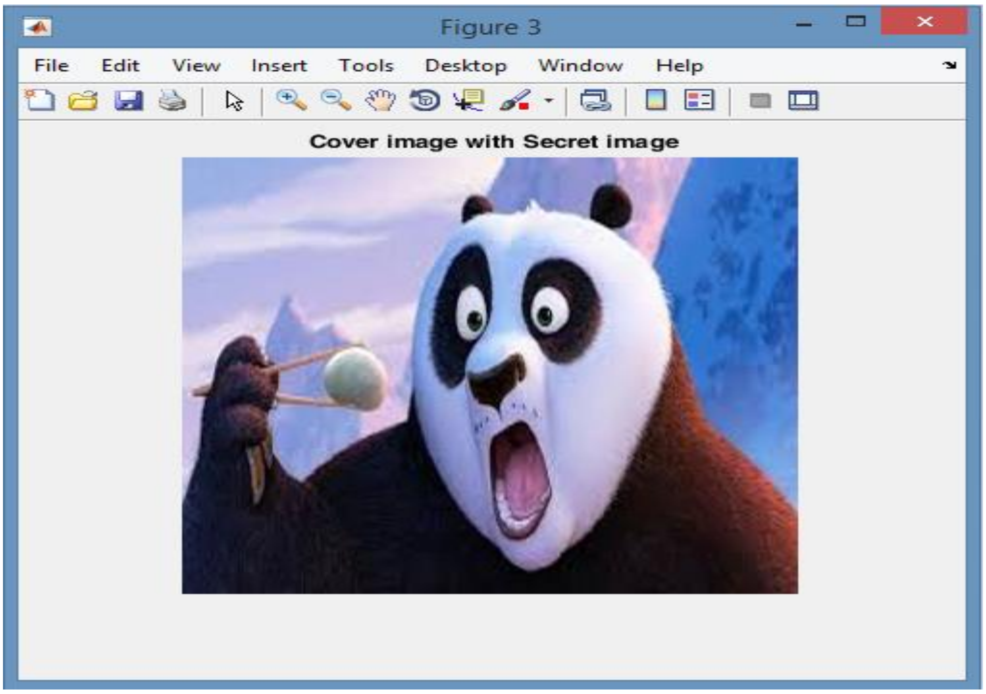

Fig 12 : Embedded Image

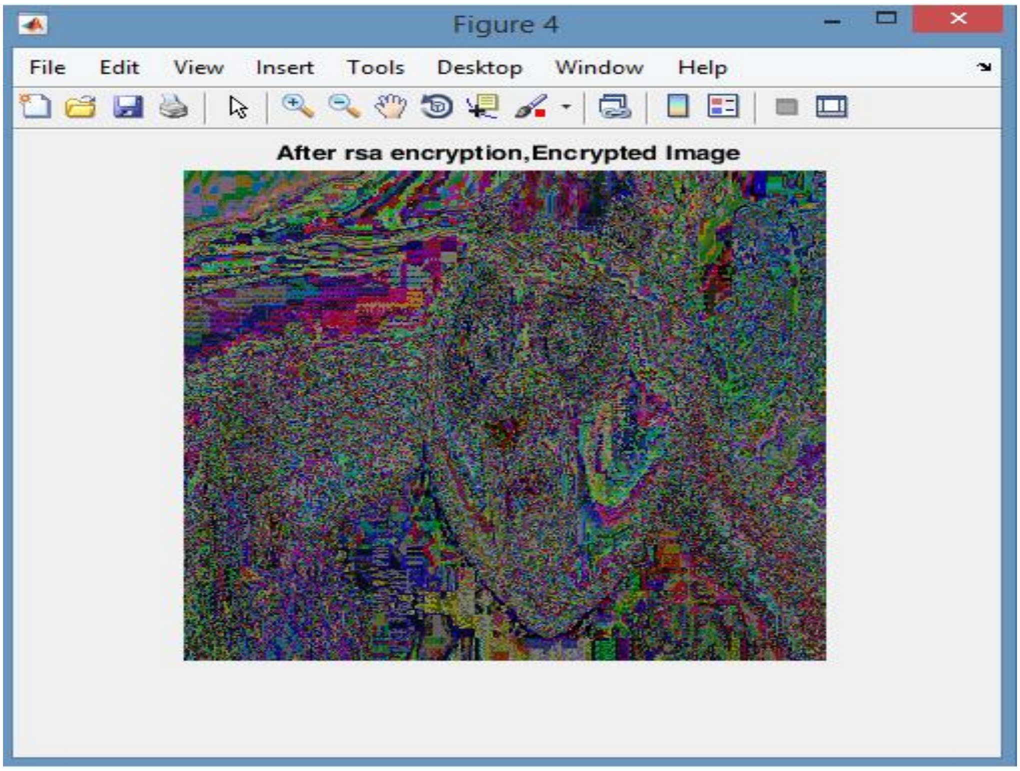

Fig 13: Embedded Image

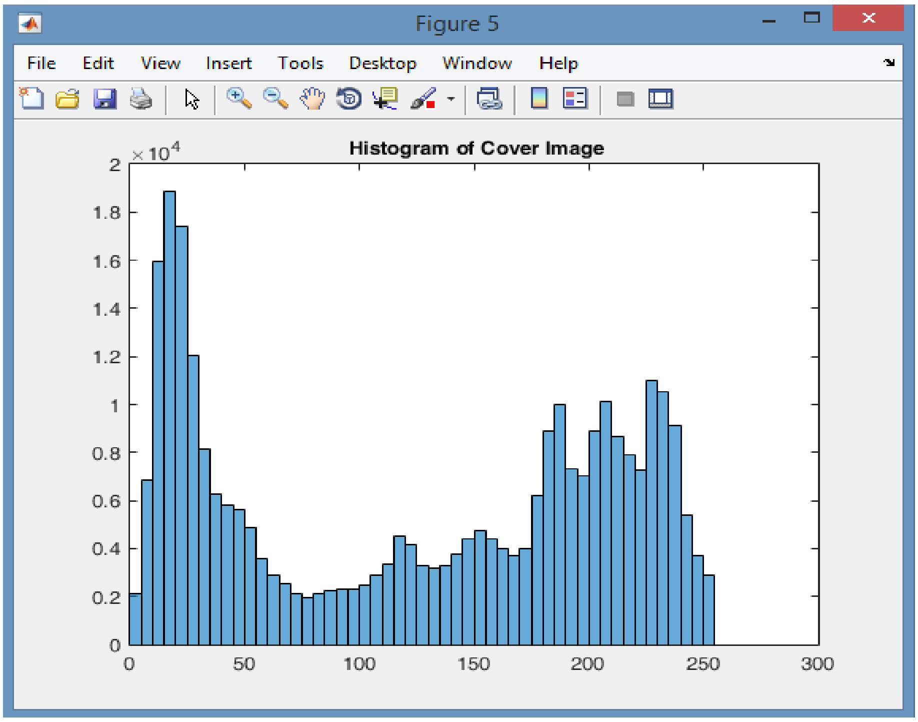

Fig 14 :Histogram of Cover Image

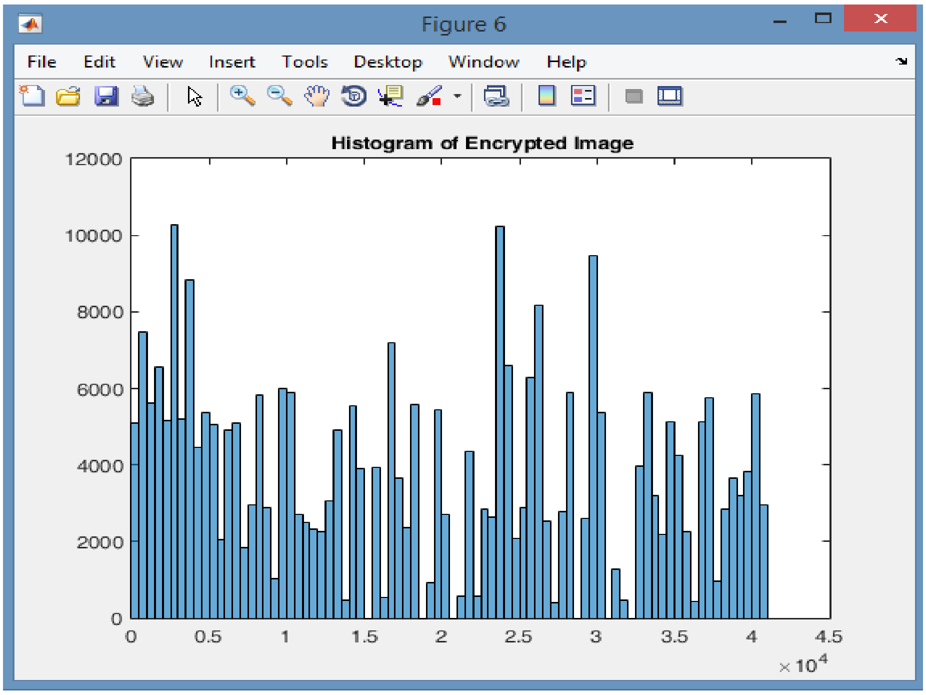

Fig 15 :Histogram of Embedded Image

5. CONCLUSION

In the today world the security of the data is very important to transmit it through any communication channel. The Stenography and cryptography are the most popular technique to enhance the data or image security. In proposed work done, apply the dual level of security, stenography and cryptography together. First hide the secrete image into the cover image and after hiding the image get the steno or embedded image that is seen same as the cover image but it also consists of secrete image that is hidden in it. After get the steno or embedded image, apply the most popular asymmetric RSA algorithm on it, to encrypt the embedded image. After encryption get the encrypted image that totally differ then the original images. So, no one can get the secrete image data from the encrypted image, it is very difficult to get the secrete image data from the encrypted image through unauthorized person. The histogram also shown that the encrypted image data are totally differ then the cover image or original image data. Hence it is very difficult to creak it.

REFERENCE

1. Gaurav Kumar Soni, Akash Rawat, Smriti Jain and Saurabh Kumar Sharma, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique", Smart Systems and IoT: Innovations in Computing, Smart Innovation, Systems and Technologies 141, PP-483-492, 2020.
2. Farah JihanAufa, Endroyono and AchmadAffandi, "Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm", 4th International Conference on Science and Technology (ICST), Yogyakarta, Indonesia, pp-1-5, 2018.
3. Dalia Mubarak Alsaffar, Atheer Sultan Almutiri, BashaierAlqahtani, Rahaf Mohammed Alamri, Hanan FahhadAlqahtani, Nada Nasser Alqahtani, Ghadeer Mohammed alshammari, and Azza. A. Ali, "Image Encryption Based on AES and RSA Algorithms", IEEE, pp-1-5, March 2020.
4. Calabrese, Thomas. Information security intelligence: Cryptographic principles and applications. Cengage Learning, 2004
5. Gandharba Swain, "Very High Capacity Image Steganography Technique Using Quotient
Value Differencing and LSB Substitution", Springer Arabian Journal for Science and Engineering, pp-1-10, June 2018.
6. Savita Goel, Shilpi Gupta, and Nisha Kaushik, "Image Steganography – Least Significant Bit with Multiple Progressions",3rd International Conference on Front. of Intell. Comput. (FICTA), Vol. 2, Advances in Intelligent Systems and Computing 328, pp-105-112, 2014.
7. Gaurav Kumar Soni, Himanshu Arora and Bhavesh Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm", International Conference on Aritificial Intelligence: Advanced and Application 2019, Algorithm for Intelligent System, pp-83-90, 2020.
8. YaniPartiAstuti, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto and Christy Atika Sari, "Simple and Secure Image Steganography using LSB and Triple XOR Operation on MSB", IEEE International Conference on Information and Communications Technology (ICOIACT), pp-191-195, 2018.
9. SorinaDumitrescu, Xiaolin Wu and Nasir Memon, “On Steganalysis of Random LSB Embedding in Continuous-Tone Images”, Proceedings of International Conference on Image Processing, Vol-3, PP-641-644, 2002
10. Xiaolong Li, Bin Yang, Daofang Cheng, and Tieyong Zeng, "A Generalization of LSB Matching", IEEE Signal Processing Letters, Vol-16, No-2, pp-69-72, February 2009.