# Image and Text Steganography Based on RSA and Chaos Cryptography Algorithm with Hash-LSB Technique

[1]Manjunath N, [2]S.G.Hiremath

[1] 4th sem, M.Tech (Digital Electronics), EWIT, Bangalore [2] HOD, Dept. of ECE, EWIT, Bangalore
Email: n1989manju@gmail.com

**ABSTRACT: Now a day's security is one of the major problem facing all over the world. To protect your secret information from the strangers it is necessary to convert the information into unrecognizable form. To protect information from unauthorized access various methods for information hiding like steganography, cryptography, hash-Lsb techniques have been developed. In this paper the proposed work is to present a Hash-LSB based embedding of the encrypted text and image. RSA and Chaos algorithms have been applied to encrypt the image and text to intensify the protection or security in the communication area for data sending. RSA encryption is performed for providing more security to data. The main goal of the hash-lsb technique is to embed secret information in a particular text, image or file and extract using a Stegano password or key. Second level is to encrypt and decrypt steganography image using Chaos algorithm, this action is used to manage another cycle of security process implementation.**

**Key words: Steganography, cryptography, hash-lsb technique, RSA and Chaos encryption and decryption algorithms.**

## I. INTRODUCTION:

In the present days, sending the sceret information from sender to the receiver via internet is not secure (e-commerce transactions, spying of the secret information in military domain), so to overcome this problem there are so many techniques in that there are three techniques which are highly secure to send the secret information, they are steganography, cryptography and hash-lsb techniques.

Steganography is a technique in which the sceret information is hidden within an image, text or video files and transmitted from sender to receiver.

This can be done that is hiding the message by embedding the secret message within another digital medium such as text, image, audio and video file. After embedding the secret information it is referred to as stego-medium. A steganographic key is used to control the hiding process so as to restrict detection or recovery of the embedded dat. There are four kinds of steganography.

1 .Fourier Transform Method

2. Statistical Method

3. Hash-LSB Method

4. Domain Method

The most important use of steganographic techniques lay in the field of digital watermarking.

Cryptography is a method used to encrypt and decrypt the Stegano image using RSA and Chaos algorithms and it's another security process implementation. According to key management cryptography technique is divided into two types.

⊡ **Single Key Cryptography: The encryption and decryption keys used for the process are similar.** It is also known as private key cryptography

⊡ **Two Key Cryptography: The encryption and decryption keys used for the process are different.** It is also termed as public key cryptography.

## II. LITERATURE SURVEY:

In this section, detailed literature review is done that aims to review the critical points of current works. Here the information collected about researches and an innovation carried out on the related technologies has been done. This section will highlight the recent trends and innovations in the concerned technology.

In 2003, Sinha proposed a technique known as digital signature method that enables a recipient of a message to corroborate the sender of a message and verify that the message is not damaged [1].

Another technique by Shujun Li in 2004 [2] pointed that all permutation only image cyphers were uncertain against chosen plaintext attacks. In result, they suggested that secret permutations have to be combined with other encryption methods to develop highly secured images.

In 2005[3], a new image encryption scheme was developed by a Zhi-Hong guan in which changing the grey values and positions shuffling of image pixels are combined to make bewildered the relationship between the cypher image and the plain image.

M.Grace Vennice, Prof.T.V.Rao, M. Swapna and Prof.J.Sasi kiran proposed a new method for text steganography by creating a hybrid method in utilizing whitespaces between words and paragraphs in right justification of text and proposed four following parts.

1. Registration

2. Encrypt text information

3. Mapping through that XML scheme

4. Decrypt that information to another language of environment [4].

A arbitrary combinational image encryption accession with bit, pixel and block permutations techniques was proposed by Mitra A in 2006[5], where the main goal of this approach is that an image can be perceived as an adjustment of bits, pixels and blocks. The information present in the image is due to correlations among the blocks, pixels and bits in a given way. This message can be reduced by decreasing the interaction among the bits, pixels and blocks using various permutations techniques.

In 2012, Long Baoa [6], suggested a chaotic technique that shows an excellent chaotic characteristic. To illustrate its application in image processing, a new image encryption method using the proposed chaotic system is also introduced.

In 2012, Ahmad Abusukhon [7], proposed a technique that in cryptographic application, the data sent to the distant host at the sender is encrypted first using an encryption key and tat encrypted data are sent to receiver side. This way the hacker will not be having the encryption key where the original data is required and thus the attacker can’t to do anything with the conference.

Harshitha K M, Dr. P. A. Vijaya [8], suggested an idea to intensify the system security by combining the two techniques steganography and cryptography. In this method the messages is first encrypted and then embed in cover file with the help of steganographic system For encryption the secret information is randomly rearranged using the secret key. The random rearrangement is carried out by using mat lab functions rand and randperm. They used LSB algorithm for both embedding and extraction process.

Shailender Gupta, Ankur Goyal and Bharta Bhushan [9] used two techniques Rivert, Shamir, Adleman (RSA) and Diffie Hellman algorithms to encrypt the data then LSB is used to hide encrypted message and as a result their technique demonstrated that the encryption use will not affect the complexity of time in steganalysis if Diffie algorithm is used rather than RSA algorithm. To provide higher security the hidden information is encrypted first buy using RSA or Diffie Hellman algorithm and encrypted ASCII value is converted in binary form. At the same time the image pixels is also converted into binary form. Now the image is used as a cover to implant the information that is encrypted and this process is done by LSB encoder which replaces the least significant bit of pixel values with the encrypted information bits. Upon inflicted of stego image the receiver firstly converts the pixels into their corresponding binary values. The LSB decoder the detaches the encrypted data from image pixel values. The encrypted data is decrypted by decryption algorithms.

By Anal Paul [10] in 2012, described the technique that some chaos based algorithms are working fine and withstand many type of crypto analysis attacks, but more time consuming is required for encryption and decryption process. But some chaos based algorithms are very rapid but their strength to oppose attack is questionable. So these have inspired us to design a crypto system where less amount of time is taken for encryption and decryption and it should withstand all type of crypto assay attacks and hence developed an advanced image encryption technique by using block based arbitrarization and chaos system. In the block based metamorphosis regression, the query image is divided into a number of blocks. Then these blocks are remodeled before operating through a chaos based encryption process and at the side of the receiver after decryption, these blocks are retransformed into their original form or position. This process generates optimal result during encryption and decryption with less error within the threshold and due to sensitive chaos system it becomes more secure and dependability over the network.

By Manoj Kumar Ramaiya in 2013[11], proposed that image steganography is a method for concealing information into a cover image. The most common steganographic technique in spatial domain is the LSB method due to its facility and concealing capacity. Steganographic methods that exist, target on the embedding approach with less concern to pre processing, such secrete image encryption. The stereotyped process is independent of preprocessing step in image based steganography for preferable security, as they do not offer flexibility, strength and high level of security. This proposed technique represents an image steganography based on the data encryption standard using 64 bit of plaintext and 56 bits of secrete key. The preprocessing provides higher security as extraction of image is impossible without the awareness of S-box rules and secrete key of the function.

In 2013, Praloy Shankar De [12] endeavor has been made to concentrate on a cryptography algorithm that was made by using old techniques. DEDD symmetric key cryptosystem is the new method to symmetric key algorithm. By this technique they can doubly encrypt and doubly decrypt the information or message. It means the source machine will generate the cypher text from the plain text double. The receiver or destination machine will also have to decrypt the cyphers for two times and then the contact between them will be concluded. For generating the key, they will take the length of the message in first encryption and in second encryption they will apply shifting method.

In 2013, Neha Chauhan [13] described a region, adaptive watermarking algorithm which will be used for the unique application to identify watermark attacks. The advantages of the suggested watermarking discovery techniques are PSNR and RGB intensity value. For interfere discover using linear classifier by providing these critical features. The watermark is embedded on different regions of the host image by merging DWT and SVD method. Scaling, rotation and translation belongs to geometric attacks are applied at the same time. The asperity of these attacks can be adapted by altering their corresponding parameter values.

In 2013, Mohammad Ashiqur Rahman [14] proposed a better approach in which the risk estimation influences the process for implementing and substantiates throughput and better shield for the query data. Due to an increase in the internet growth and associated information professionals; security attacks face challenges in determining risk of their networks. The appraisal of difficulties may vary with the system requirements. Hence, a risk assay's technique is appropriate. Moreover, patterning a network with accurate security tactics is a difficult problem. The appraisal of difficulties aids in achieving necessary security tactics. Security apparatus like firewalls are used to allow or abandon traffic. However, the contact between the network speculation and the security tactics is not easy to authorize. A small change in the network features or in the security tactics, can modify the speculation considerably. It is difficult to manually follow a standardized process for configuring the network towards security thickening. Hence, an automatic generation of proper security controls, example, host placements and firewall rules in the network features, is essential to keep the low security risk. They first commence a declarative model for the conditional risk assays. They consider transitive reach ability, that is.; reach ability considering one or more intervening hosts, in order to compute exposure of liabilities. Next, we characterize our risk assay model and the security necessity as an impulsion satisfaction problem using the SMT. A solution to the problem incorporate necessary firewall tactics and host placements. They also examine the scalability of the proposed risk assay method as well as synthesis model.

By Seetaiah Kilaru [15], in 2103 proposed that security is the main responsibility in any field. With the persistent attacks, it will be very difficult for the users to protect the digital images which are transmitting over the network. Singular Value Decomposition provides a solution up to the greater extent. By using wavelets the watermark which is invisible embed into the original watermark. The main target is based on the wireless communication models; hence it is essential to consider some factors into deliberation, they are image size and bandwidth requirements. By taking the parameters into account, compression and transmission process should be carried out. The suggested algorithm uses the Singular Value Decomposition method along with compression. The suggested algorithm is booming against all common attacks which exist in the field of image processing. Tests have been done and results bare satisfactory in terms of gradual and security.

Hiding information or secret message inside images is a suitable technique nowadays. An image with sceret information inside can easily spread over the WWW, who created a scanning array which detects the presence of hidden information inside images that were assigned on the net. However, after checking the images, no hidden information's were found, so the realistic use of steganography still seems to be limited. To conceal information inside an image without changing its visible parameters, the cover source can be amended in noisy areas with many color alterations, so less concentration will be drawn to the changes. The most used techniques to make these variations involve the usage of the Hash-LSB, filtering, masking and transformations on the cover image. These methods can be used with varying degrees of success on different types of image files [16].

## III. PROPOSED WORK:

In this proposed work an image steganography IS implemented using a Hash-LSB encoding and decoding. RSA file or message encryption and decryption and Chaos encryption and decryption algorithm.

The key terminology as given:

**Clear text (Plain Text)**

The intelligible message which will be converted into an unintelligible (encrypted) message

**Cipher text**

A message in encrypted form

**Encryption**

The process of converting a readable message into a non readable message

**Decryption**

The process o f converting a non readable message into readable message

**Key**

A framework used in the encryption and decryption process

**Cryptosystem**

A system to encrypt and decrypt information

**Symmetric Cryptosystem**

The encryption and decryption keys used for the process are similar

**Asymmetric Cryptosystem**

The encryption and decryption keys used for the process are different

**First encryption**

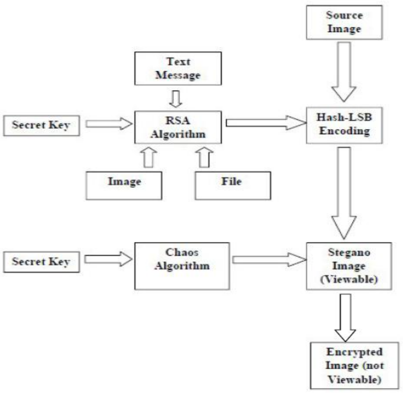
RSA algorithm encrypts only the sceret information or secret data, then merges to cover image using H-LSB techniques. Now a viewable stego image is created that is viewable to our human eyes. Three basic steps are required for the RSA process completion and they are; key generation, encryption and decryption.

**Second encryption**

Chaos algorithm encrypts the overall stegno images.

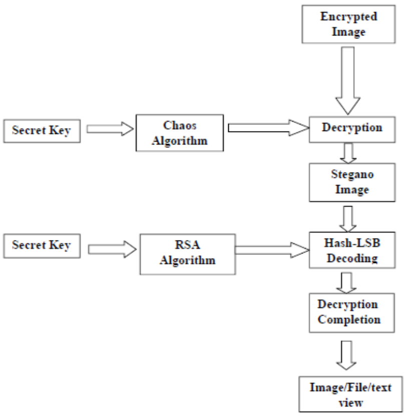
In this level the stegno image created is not viewable and this stegno image is send to the receiver. This implementation process create highly and confident information protection.In this algorithm the random sequence of keys will be generated for encryption and decryption.

**Sender side process**



**Sender side process view**

**Receiver side process**



**Receiver side process view**

In this work for data secure transmission there are three level processes.

1. Secrete message encryption decryption using RSA algorithm.
2. Encrypted and decrypted file embedding and recapturing cover image using Hash-LSB method.
3. Encrypt and decrypt steganography image using chaos algorithm.

## IV. CONCLUSION AND FUTURE SCOPE:

The main aim is to implement a secured image steganography based on RSA and Hash-LSB techniques. An RSA encryption method is used to encode the secret information and then hide into the cover image using discrete cosine transform and H-LSB technique. After encrypt the covered image using chaos algorithm using secret key value. The dual encryption process done using RSA and Chaos algorithm. Then the dual encryption process completion processed cover file transfer recipient. The reverse process will be done recapture the original data according to secret key value for both RSA and Chaos algorithm.

In future work this thesis will be continuing using video file like 3gp, MP4 and cryptography algorithm also possible to implement higher level. Similarly the steganography method can be developed for 3D images.

## REFERENCE

[1] A.Sinha, K.Singh, “A technique for image encryption using digital signature,” Source; Optics Communications, vol.218, no.4, 2003.

[2] Li. Shujun, Li. Chengqing, C. Guanrong, Fellow., IEEE., Dan Zhang., and Nikolaos,G., Bourbakis Fellow., IEEE. "A general Cryptanalysis of permutation-only multimedia encryption algorithms,"2004.

[3] G. Zhi-Hong, H. Fangjun, and G. Wen i.e., “Chaos – based image encryption algorithm, “Department of Electrical and computer Engineering, University of Waterloo, ON N2L 3G1, Canada. Published by: Elsevier, 2005, pp. 153-157.

[4] M.Grace Vennice, Prof.T.V.Rao, M.Swapna, Prof.J.Sasi kiran, ‖ Hiding the Text Information using Steganography‖ , in international Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 1, Jan-Feb 2012.

[5] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science,vol. 1, no. 1, p.127, 2006.

[6] Long Bao, Yicong Zhou,C. L. Philip Chen,” A New Chaotic System for Image Encryption”, 2012 International Conference on System Science and Engineering June 30-July 2, 2012, Dalian, China.

[7] Ahmad Abusukhon and Mohammad Talib, “A Novel Network Security Algorithm Based on Private Key Encryption”, IEEE 2012.

[8] Harshitha K M and Dr. P. A. Vijaya , ―secure data hiding algorithm using encrypted secret message‖ in International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012.

[9] Shailender Gupta, Ankur Goyal , Bharat Bhushan, ― Information Hiding Using Least Significant Bit Steganography and Cryptography‖, in I.J.Modern Education and Computer Science, June 2012.

[10] Anal Paul, Nibaran Das and Agyan Kumar Prusty, "An Advanced Gray Image Encryption Scheme by Using Discrete Logarithm with Logistic and HEH64 Chaotic Functions", IEEE 2012.

[11] Manoj Kumar Ramaiya, Naveen Hemrajani and Anil Kishore Saxena, "Improvisation of Security aspect in Steganography applying DES", IEEE 2013.

[12] Praloy Shankar De, Prasenjit Maiti," DEDD Symmetric-Key Cryptosystem", International Journal of Advanced Computer Research (IJACR), Volume-3 Number-1 Issue-8 March-2013.

[13] Neha Chauhan, Akhilesh A. Waoo, P. S. Patheja," Attack Detection in Watermarked Images with PSNR and RGB Intensity", International Journal of Advanced Computer Research (IJACR), Volume-3 Number-1 Issue-9 March-2013.

[14] Mohammad Ashiqur Rahman and Ehab Al-Shaer, "A Formal Approach for Network Security Management Based on Qualitative Risk Analysis", IEEE 2013.

[15] Seetaiah Kilaru, Yojana Kanukuntla, K B S Chary," An effective algorithm for Image security based on Compression and Decomposition method", International Journal of Advanced Computer Research (ISSN (IJACR) Volume-3 Number-1 Issue-8 March-2013.