IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A NOVEL IMAGE STEGANOGRAPHIC APPROACH FOR HIDING ENCRYPTED TEXT(RSA CRYPTOSYSTEM) USING HSI COLOR MODEL

K.V.C.M Abhijit Rongali[1],Dr.S.Jhansi Rani[2],S.S.Nandini[3]
M.Tech[1],Associate Professor[2],Research Scholar[3]
Department of Computer Science and Systems Engineering,
Andhra University College of Engineering, Visakhapatnam, India.

Abstract:
Today's world, people utilize the processes of encryption and steganography to hide the data and transfer it in a secured manner, preventing third parties from stealing the sensitive information.Encryption algorithm is the process of embedding text into pictures so that the Human Visual System (HVS) cannot detect it and that only the sender and recipient are aware of its presence. We implement image steganography using Hue-Saturation-Intensity (HSI) based on Least Significant Bit (LSB). The suggested technique converts the image from RGB to HSI color space, embeds secret data inside the Intensity Plane (I-Plane), and then converts the image back to RGB color model. Leveraging public and private keys to encrypt and decrypt data is known as cryptography. With the help of the RSA public key cryptography technique, the secret data is encrypted.

Keywords*:*Cryptography, Steganography, RSA Encryption –Decryption.

I. Introduction:

The widespread usage of the Internet and the abundance of public and private data has prompted a huge number of users to employ data-protection techniques incorporating cryptography and steganography. Steganography is short for "covered writing." Secret data is hidden in such a way that an outside observer cannot discover the existence of the secret message. The received stego-file is processed at the receiver's end to extract the concealed message. Thus, stenographic techniques help to reduce the risk of unauthorised data access by ensuring that the hidden information in the cover file is not detectable by such unauthorised users.
Steganography is grouped into three types based on the stego-medium used to embed data: text steganography, audio steganography, and video steganography.Researchers focused on audio steganography in our study, which entails using an audio signal as a cover to conceal secret information. Steganography in audio takes advantage of a flaw in the human hearing system (HAS). The technique for embedding the secret message is a prevalent method of audio steganography that is vulnerable to detection by various steganalysis tools. Similarly, many cryptanalytic techniques [15] can be used to retrieve plaintext from ciphertext. As a result, rather than adopting either strategy individually, the combination of these two techniques can provide a higher level of security.The proposed methodology improves the existing LSB technique for audio steganography and adds RSA encryption techniques to provide multilevel protection for enhanced data security.

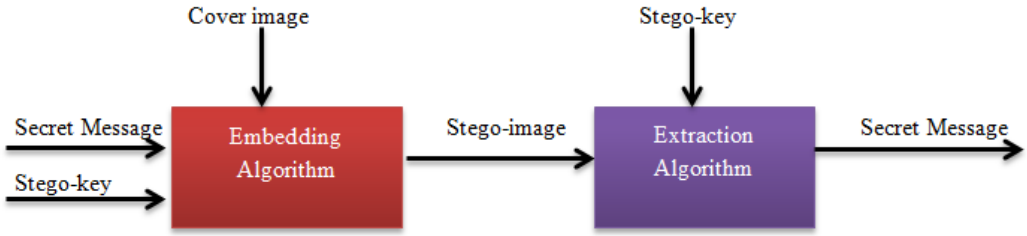


Figure1. A model of the steganographic process with cryptography

II. LITERATURE REVIEW

Researchers have proposed various techniques to hide information in an image.
The technique of hiding secret information or data in an image is called image steganography. Generally, pixel intensities are the methods used in hiding data in image steganography. According to [7], images are the most popular and widely use cover objects used in steganography. The degree of redundancy in images has made it the most sought for, in terms of steganography. Two categories of classification namely spatial – domain and transform domain based have been proposed in image steganography [6]. [8] Explained that spatial domain embeds the message directly into the pixels intensity whereas the transform domain also called the frequency domain transform the image before the message is embedded.Various file formats exist in image steganography. TIFF, JPEG, PNG, GIF and BMP can all be implementing in image steganography [9]. However, each of the file formats poses its own unique advantages and disadvantages. Because pixel intensities are used in image steganography, there is sometimes variation in the intensity of the original image and the stego image or the embedded image. The variation in intensity is so trivial or subtle in that it is not detectable or perceptible to the human eye [8].Most steganographic systems designed for confidential communication has suffered some weaknesses. [14] opined that steganographic attacks comprise of detecting, extracting and destroying the hidden data within the covert media. Visual attacks and statistical attacks [15] are the two widely known attacks against steganography. Statistical attacks use steganalysis [14]. [16] Developed a steganalysis application that was successful in detecting a message embedded in an image. Statistical video steganalysis developed [17] was also successful in detecting a data hidden in a video whose algorithm was based on LSB. Because of the fear of terrorists using steganography to communicate over the internet, [18]came out with a steganalysis called the active warden approach that was capable of detecting embedded messages in images and videos. [19] Showed that the human eye is capable of detecting hidden messages due to distortion. From the attacks above, it is obvious that steganography itself is not an end to the security concern associated with data transfer or communication. In order to mitigate the attacks against steganography and to further strengthen data communication security, cryptography was introduced.

III. RELATED CONCEPTS

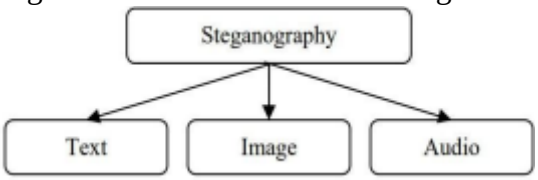
STEGANOGRAPHY:

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information.

Types of Steganography:

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.

Figure 1 shows the four main categories of file formats that can be used for steganography.



Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every nth letter of every word of a text message. It is only since the beginning of the internet and all the different digital file formats that is has decreased in importance. Text steganography using digital files is not used very often since text files have a very small amount of redundant data.

IMAGE STEGANOGRAPHY

Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The use of steganography in newsgroups has been researched by German steganographic expert Niels Provos, who created a scanning cluster which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited.

To hide a message inside an image without changing its visible properties, the cover source can be altered in ”noisy” areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the

usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files.

Least Significant Bits

A simple approach for embedding information in cover image is using Least Significant Bits (LSB). The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small. To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel.

On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size. The result changes that are made to the least significant bits aretoo small to be recognized by the human visual system (HVS), so the message is effectively hidden.

Masking and filtering

Masking and filtering techniques, usually restricted to 24 bits or grayscale images, take a different approach to hiding a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved for example by modifying the luminance of parts of the image. While masking does change the visible properties of an image,it can be done in such a way that the human eye will not notice the anomalies. Since maskinguses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image

processing. The information is not hidden at the ”noise” level but is inside the visible part of the image,which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used.

AUDIO STEGANOGRAPHY

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography.

LSB Coding

Sampling technique followed by Quantization converts analog audio signal to digital binary sequence. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message.

Phase Coding

Human Auditory System (HAS) can’t recognize the phase change in audio signal as easy it can recognize noise in the signal. The phase coding method exploits this fact. This technique encodes the secret message bits as phase shifts in the phase spectrum of a digital signal,achieving an inaudible encoding in terms of signal-to- noise ratio.

Spread Spectrum

There are two approaches are used in this technique: the direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). Direct-sequence spread spectrum (DSSS) is a modulation technique used in telecommunication. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that is being modulated. Direct-sequence spread-

spectrum transmissions multiply the data being transmitted by a "noise" signal.
This noise signal is a pseudorandom sequence of 1 and −1 values, at a frequency much higher than that of the original signal, thereby spreading the energy of the original signal into a much wider band.

EchoHiding

In this method the secret message is embedded into cover audio signal as an echo. Three parameters of the echo of the cover signal namely amplitude, decay rate and offset from original signal are varied to represent encoded secret binary message.Individuals are set below the Human Auditory System (HAS) threshold, so that echo cannot be easily resolved.
Because video files are made up of images and sounds, most of the techniques for hiding data in images and audio are also applicable to video media. during embed ding the secret message to the cover media to produce 'stego-video'.
After that the stego-video is communicated over public channel to the receiver. At the receiving end, receiver uses the secret key along with the extracting algorithm to extract the secret message from the stego-object.

Cryptography

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.
Human being from ages had two inherent needs
(a) To communicate and share information
(b) To communicate selectively.
These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand. The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.
The word 'cryptography' was coined by combining two Greek words, '*Krypto*' meaning hidden and '*Graphene*' meaning writing.

IV. WORKING METHODOLOGY

RSA Algorithm:

The algorithm was given by three MIT's Rivest, Shamir & Adleman and published in year 1977. RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and then the product of these values is used to create a public and a private key, which is further used in encryption and decryption. The RSA algorithm could be used in combination with Hash-LSB in a way that original text is embedded in the cover image in the form of cipher text. By using the RSA algorithm users are raising the level of security. In the instance of steganalysis, only cypher text could be recovered, which is encrypted and unreadable, and hence secure.

RSA Algorithm can be illustrated as follows:

Steps 1: **Key Generation**

1. Select p,q (p and q both prime)
2. Calculate n
   $n=pxq$
   calculate
   $\Phi(n)=(p-1)(q-1)$
3. Select integer e
   $\gcd(\Phi(n),d)=1;1<d<\Phi(n)$
4. Calculate d
   $d= e^{-1} \bmod \Phi(n)$
5. Public key
   $KU=\{e,n\}$
6. Private key
   $KR=\{d,n\}$

Step 2: Encryption

The sender uses M (plaintext) with public key *e* to create the ciphertext, C (Ciphertext)

1. Plain Text:

   $M < n$

2. Cipher text

   $C = M^e \bmod (n)$

Step 3: Decryption

The receiver uses C (ciphertext) with secret key *d* to get back M (plaintext).

1. Cipher text : C
2. Plain Text : $M = C^d \pmod{n}$

RSA Analysis:

The security of RSA depends on the strengths of two separate functions. The RSA cryptosystem is most popular public-key cryptosystem strength of which is based on the practical difficulty of factoring the very large numbers.

- **Encryption Function** − It is considered as a one-way function of converting plaintext into ciphertext and it can be reversed only with the knowledge of private key d.
- **Key Generation** − The difficulty of determining a private key from an RSA public key is equivalent to factoring the modulus n. An attacker thus cannot use knowledge of an RSA public key to determine an RSA private key unless he can factor n. It is also a one way function, going from p & q values to modulus n is easy but reverse is not possible.

HSI COLOR MODEL

1. RBG and CMY are suitable for hardware implementations
2. Unfortunately, algorithms are inadequate for describing colours for human understanding.
3. One does not refer to the color of a car by giving the % of each of the primaries.
4. HIS(Hue,intensity& Saturation): Decouple the Gray-scale information.
   - HUE: It describes the pure color, pure yellow,orange,green or red.
   - Saturation measures the degree to which a pure color is diluted by white light.
   - Brightness is a subjective descriptor to be measured.

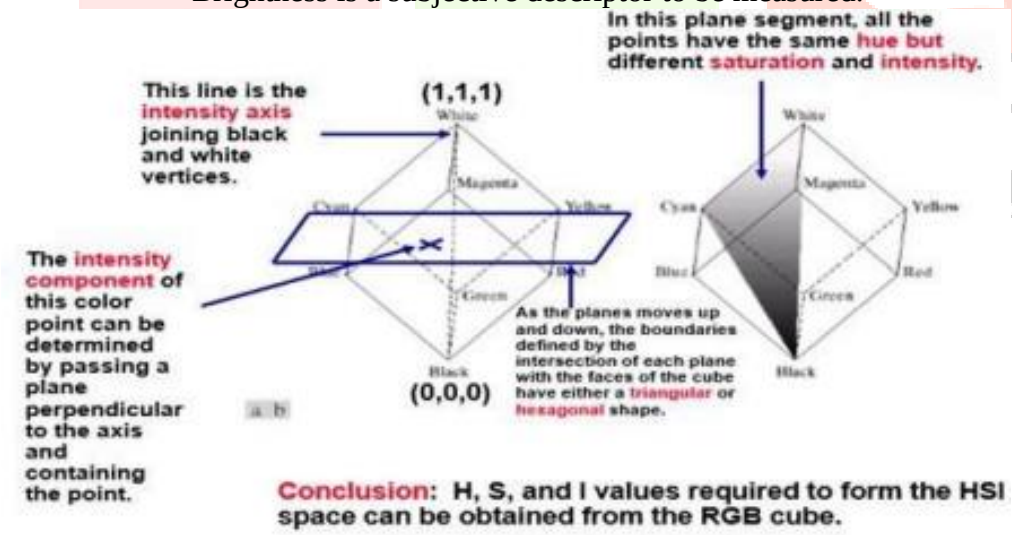


Figure2: Conceptual relation between RGB and HSI color models

5. All points contained in the plane segment define by the intensity & boundary of the cube have the same hue

HUE AND SATURATION IN THE HSI MODEL

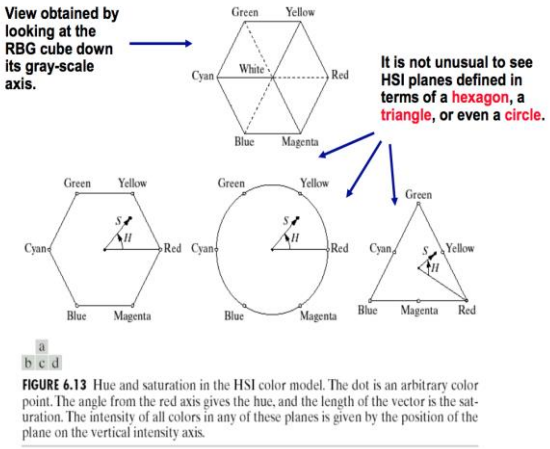
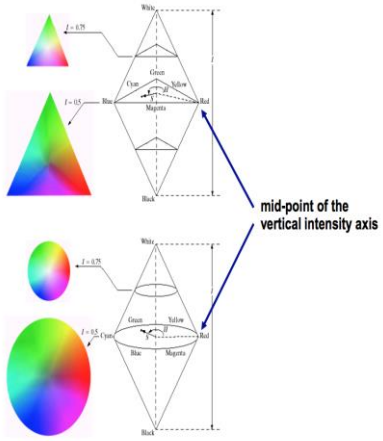


FIGURE 6.13 Hue and saturation in the HSI color model. The dot is an arbitrary color point. The angle from the red axis gives the hue, and the length of the vector is the saturation. The intensity of all colors in any of these planes is given by the position of the plane on the vertical intensity axis.

TRIANGULAR AND CIRCULAR COLOR PLANES IN THE HSI MODEL



Converting from RGB to HSI:

H stands for Hue, S for Saturation and I for Intensity.

Steps

1. Read an RGB image
2. Represent the RGB image in the range of [0,1].
3. Find the HSI components,here the angle is measured with respect to the red axis

$$\theta = \cos^{-1}\left\{\frac{\frac{1}{2}[(R-G)+(R-B)]}{[(R-G)^2+(R-B)(G-B)]^{1/2}}\right\}$$

4. Hue can be normalized to the range [0, 1] by dividing by 360°c

$$H(\text{Hue}) = \begin{cases} \theta & \text{If } B <= G \\ 360-\theta & \text{If } B > G \end{cases}$$

5. The Satuaration component is given by $S(\text{Saturation}) = 1 - \frac{3}{(R+G+B)}[\min(R,G,B)]$

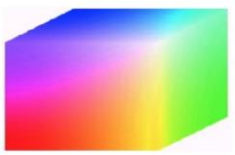
6. Finally, the Intensity component is given by the

$$I(\text{Intensity}) = \frac{1}{3}(R+G+B)$$

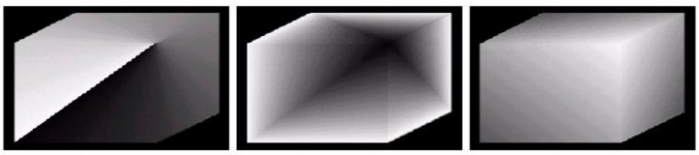
7. For convenience h,s and i values are converted in the ranges of [0,360],[0,100],[0,255], respectively by *H=h* x *180/π ;*

S=s x *100 ;*

and I = i x *255.*



RGB Cube



Converting colors from HSI to RGB:

- **RG Sector ($0^0 \leq H < 120^0$):** When H is in the sector,the RGB component are given by the equations.

$$B = I(1 - S)$$

$$R = I\left[1 + \frac{S\cos H}{\cos(60° - H)}\right]$$

$$G = 3I - (R + B)$$

- **GB Sector ($0^0 \leq H < 240^0$):** If the given value of H is in this sector,first subtract 120^0 from it.

H = H -120^0

Then the RGB components are

$$R = I(1 - S)$$

$$G = I\left[1 + \frac{S\cos H}{\cos(60^o - H)}\right]$$

$$B = 3I - (R + G)$$

- **BR Sector ($240^0 \leq H \leq 360^0$):** Finally, if H is in this range,subtract 240^0 from it.

H = H -240^0

Then the RGB components are

$$G = I(1 - S)$$

$$B = I\left[1 + \frac{S\cos H}{\cos(60^o - H)}\right]$$

$$R = 3I - (G + B)$$

Methodology

Individually, both steganography and cryptography techniques are insufficient for completing information security; therefore, the two techniques are being combined to achieve reliable and strong mechanism [1-9]. The proposed system based on combining these techniques. This can maintains the requirements used for security and robustness in order to transmit important information. The proposed system use cryptography technique based on RSA to encrypt the secret information then hidden it in the covering image using LSB steganography technique.

Sender side :The secret information (message) is encrypted according to RSA to generate encrypted message using public key. Then both encrypted and public key are embedded into cover image. Many procedures for hiding process are used for system evaluation.

Receiver side

1. Both encrypted message and public key are extracted from stego image based on inverse LSB steganography. Then use public key to generate private key according to RSA algorithm.

2.The original secret information is recovered by decrypting the extracted message.

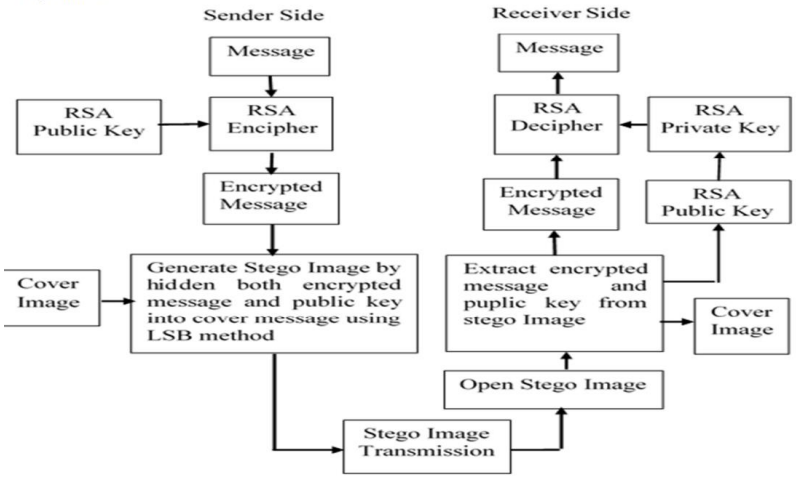


Figure. Proposed system structure.

Most Significant Bit (MSB)

Most Significant Bit (MSB) is a substitution method popularly used for embedding secret message [16]. It is known that in 8 bits the first bit is Most- Significant-Bit (MSB) and the last bit Least-Significant-Bit (LSB) [5]. Images created from pixels, i.e. if any pixel created by using these three colours red, green and blue, are called RGB. Each colour of a pixel is one-byte information that shows the density of that colour. MSB involves the following steps. Convert text into binary equivalent.Get pixel value of each pixel one by one. Replace each bit of cipher text with first bit of each pixel in image.

V. RESULTS

The proposed system was implemented using Python & Matlab. The system first generated public and private key pairs for the receiver after which the public key was published to the general public. The sender inputs the public key of the receiver and also supplies the secret message. After that, new layer of security called steganography was added to further enhance the security of communication process.

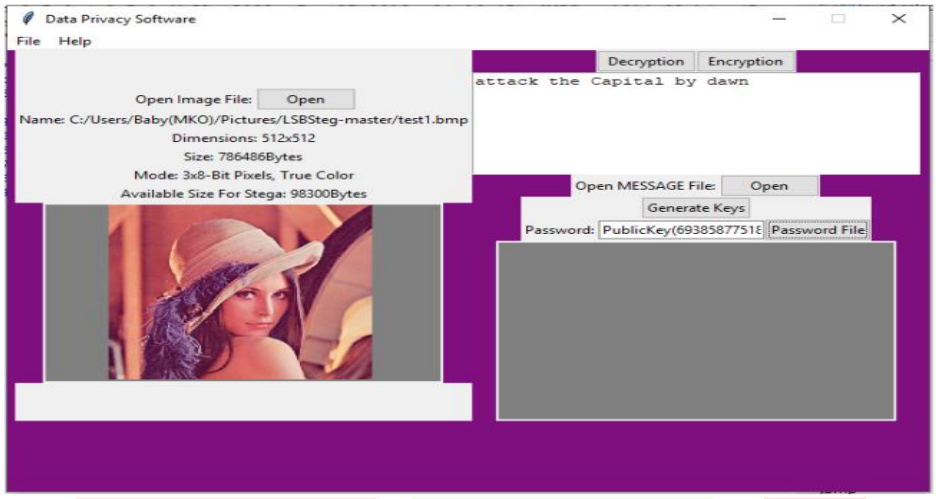


Figure3: The encryption interface from sender

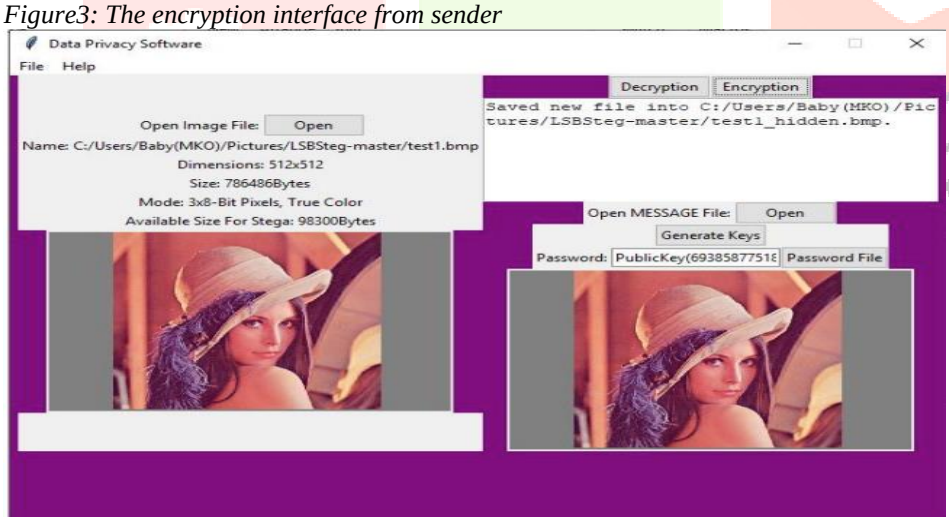


Figure4:Ciphertext Interface after a successful encryption and encoding

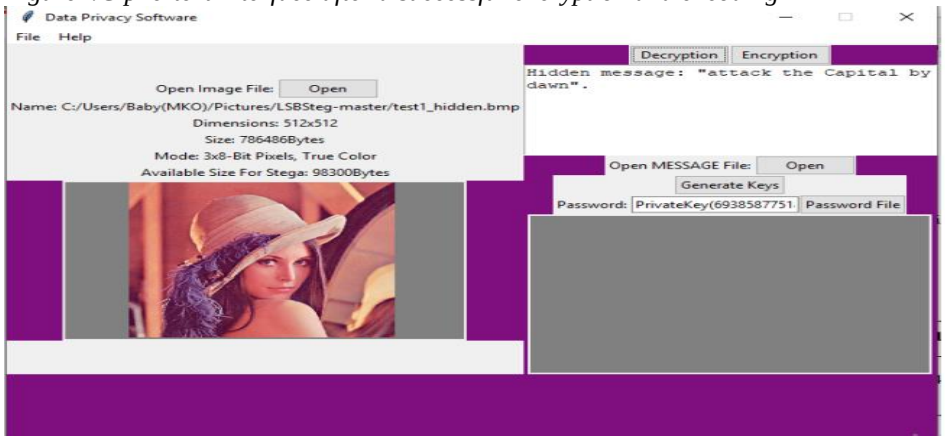


Figure5: Ciphertext Interface after a successful encryption and encoding

VI. CONCLUSION & FUTURE SCOPE

An image steganographic approach for hiding encrypted text (RSA cryptosystem) using HSI color model is designed to satisfy the user goals, that is to hide the data in a very secure way so that except sender and receiver no one can know what is inside the image. Steganography is a process of hiding the text in a image and cryptography is the process of encrypting and decrypting the text using the public key and private key. This project is developed in-order to maintain the confidentiality of the data by using the hybrid model of RSA-Cryptosystem and HSI color model.

Future Scope

The Future scope for the proposed method might be the development of an enhanced steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly the steganography technique can be developed for 3D images. Further research could be done on the design and development of similar system for other operating systems. Other asymmetric cryptography could be used to replace RSA. Finally, other image formats could be used to test the compatibility, efficiency and effectiveness of the system.

VII. REFERENCES

1. Basic and Applied Engineering Research. Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 8; pp. 32-35.
2. Savithri G, K.L.Sudha.(July 2014). Android Application for Secret Image Transmission and Reception Using Chaotic Steganography. International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 7,
3. Jeon, W., J. Kim, Y. Lee, and D. Won, 2011. A Practical Analysis of Smartphone Security, In M.J. Smith, G. Salvendy (Eds.): Human Interface, Springer-Verlag Berlin Heidelberg,311-320.
4. Apau, R., Hayfron-Acquah, J.B., and Twum, F. (June 2016). Enhancing Data Security using Video Steganography, RSA and Huffman Code Algorithms with LSB Insertion. International Journal of Computer Applications, 143 (4), 28-36.
5. Shelke, M. F. M., Dongre, M. A. A., & Soni, M. P. D. (2014). Comparison of different techniques for Steganography in images. *International Journal of Application or Innovation in Engineering & Management*, *3*(2).
6. Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image steganography. In *ISSA* (pp. 1-11).
7. Eltyeb E. and Elgabar,A (2013)―Comparison of LSB Steganography in BMP and JPEG Images‖, International Journal of Soft Computing and Engineering (IJSCE) ISSN:2231-2307, Volume-3, Issue-5.
8. Al-Vahed, A., & Sahhavi, H. (2011). An overview of modern cryptography. *World Applied Programming*, *1*(1), 3-8.