VIT®
UNIVERSITY
(Estd. u/s 3 of UGC Act 1956)
VELLORE ■ CHENNAI
www.vit.ac.in

SCHOOL OF INFORMATION TECHNOLOGY & ENGINEERING

Review -2

Project Report
On
IMAGE CRYPTOGRAPHY USING RSA ALGORITHM

Submitted For Course : Network Information & Security (ITE4001)

Submitted By:

AKASH KUMAR(17BIT0055)

SLOT – F2+TF2

Under Guidance Of:

Prof. SHANTHARAJAH S P

ABSTRACT

Steganography is the art of hiding information within other information in such a way that it is hard or even impossible to identify the existence of any hidden information. There are many different carriers for steganography. Of which, most popular ones are digital images. Due to recent developments in steganalysis, providing security to personal contents, messages, or digital images using steganography has become difficult. By using steganalysis, one can easily reveal existence of hidden information in carrier files. This project introduces a novel steganographic approach for covert communications between two private parties. The approach introduced in this project makes use of both steganographic as well as cryptographic techniques. The process involves converting a Secret image into a text document, then encrypting the generated text into a cipher text using a key (Password) based encryption algorithm, and finally embedding the cipher text on to a cover image. This embedding process is carried out using a threshold based scheme that inserts secret message bits into the cover image only in selected pixels. The security to maintain secrecy of message is achieved by making it infeasible for a third person to detect and retrieve the hidden message. So to overcome the problem of data stealing and ensuring the privacy of the user we are going to secure the message using rsa algorithm and using the steganography techniques and hiding the message into the image so that the message is hidden from the privy eyes and protects the user message.

This is a major distinction between this method and the other methods of covert exchange of information because, for example, in cryptography, the individuals notice the information by seeing the coded information but they will not be able to comprehend the information. However, in steganography, the existence of the information in the sources will not be noticed at all. Although steganography is separate and different from cryptography, but they are related in the way that they both are used to protect valuable information. When communication occurs through images, the images can either be confidential or not. But when we want to transmit an image that has to be known only to the sender and the receiver it becomes complicated. Because, during the transmission there may be loss of data which is been sent or a person could hack these image and misuse it. In such scenarios, security of the data is essential. For this we use the technique for the original image so that it is encrypted at the sender site and can be decrypted only at the receiver site. When encrypting the complete information of associate uncompressed image by a stream cipher, the extra information may be embedded into the image by modifying tiny low proportion of encrypted information. With associate encrypted image containing extra information, one could first decode it victimization the cryptography key, and therefore the decrypted version is analogous to the initial image per the data-hiding key, with the help of spatial correlation in natural image, the embedded information may be with success extracted and therefore the original image may be absolutely recovered.

INTRODUCTION

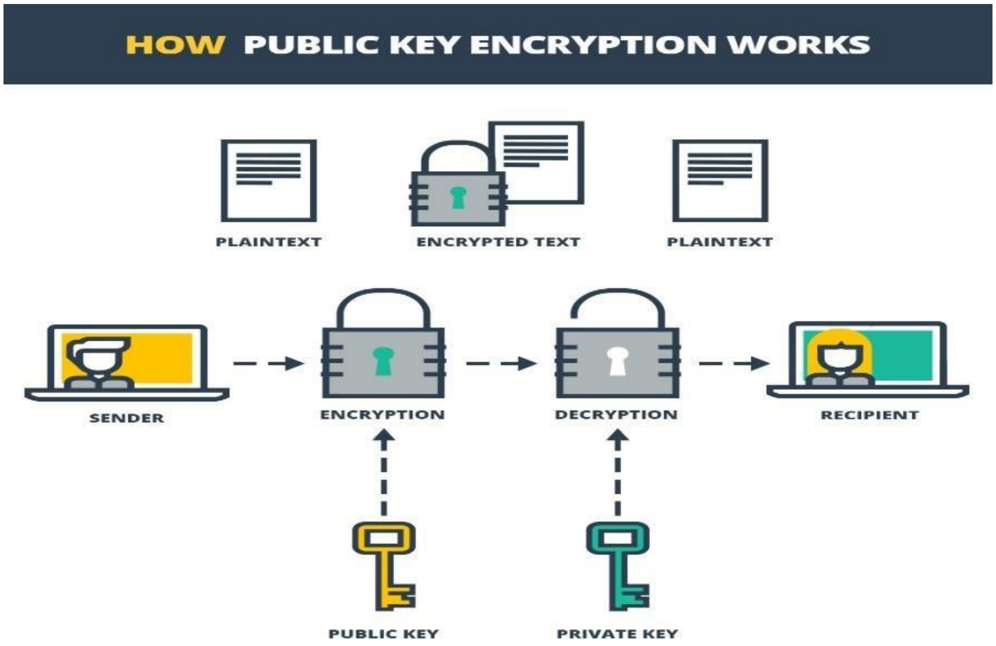
Lately, exponential growth of technology in every aspect of life is observed. Improvement of technology provides facilities to both users and hackers/intruders too. Advancement in technology that encourages hackers/intruders activities result in lack of security to user's confidential data. The most common and popular techniques for data hiding that have been in use since long time are cryptography and steganography.

Cryptography: There are many possible definitions for cryptography. One of which is, "The computerized encoding and decoding of information" to define cryptography. This is a process of converting a message from a human readable or understandable form (plaintext) to nonunderstandable format (cipher text) to enable secure sending and back to original format at other receiving end. The cipher text in cryptography always reveals static information of plaintext. Many methodologies were introduced that follow their own strategy, but all the methodologies use some patterns. The underlying idea in pattern based approach is to decode the encoded message, that is, using a pattern of one's own choice or a standard pattern, a sender encodes the message and thus generates a cipher text. The receiver uses the same pattern and decodes the cipher text to generate message (plaintext). Over a period, cryptographic approaches evolved over phases. It is suggested that a key should be used in the process of encoding and decoding a message. Based on this concept of keys, cryptography is further classified into two types, symmetric-key cryptography and publickey cryptography. In case of symmetric key cryptography, same key has to be used by both sender and the receiver while encoding and decoding respectively. In contrast, in the case of public key cryptography, the keys used by the sender and the receiver are different.

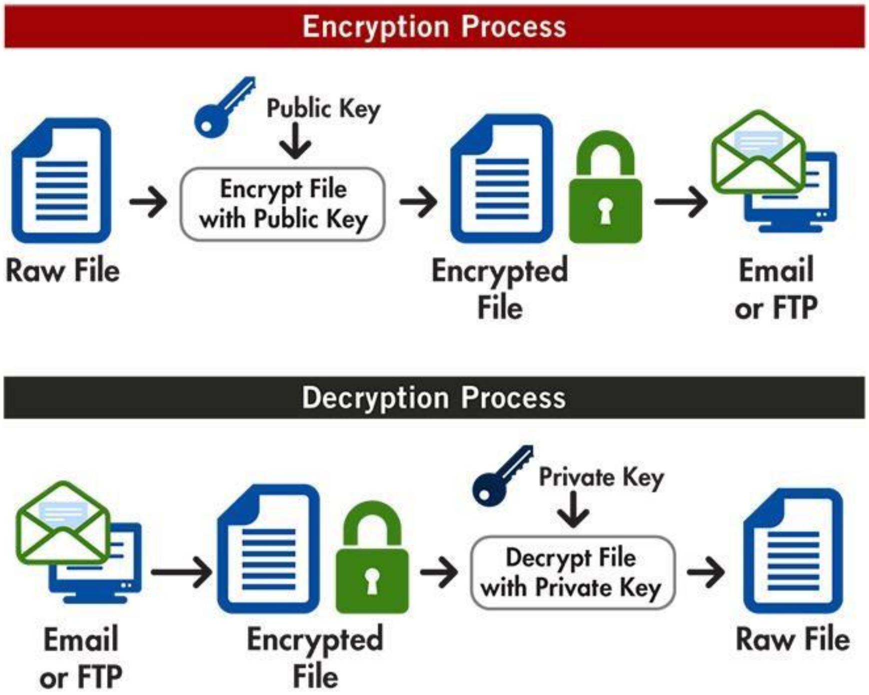
Steganography:

It can be defined as "The art and science of communicating in a way which hides the existence of the communication". A steganographic model facilitates hiding or embedding of sender's secret message in a file (carrier) that does not give out a clue about the existence of secret message in it when viewed. For this, any media format or file format like .bmp, .doc, .gif, .jpeg, .mp3, .ppt, .txt and .wav is taken as a carrier that can act as cover for the sender's message, that is, a message here is hidden in a carrier and that carrier is transmitted. The underlying operation of this methodology is both logical and technical. In general, a steganography algorithm takes a secret message and a carrier as input and gives a carrier message as output (in which the message is embedded). In the process of steganography, the carrier which hides the message in it will be sent to the receiver. The carrier gives the receiver no information about the message but reveals it only after using the tool or algorithm that is used by the sender. Both cryptography and steganography have found usage in many applications. For example, transmission of attack plans by military teams to hide information about their strategies. Many other applications of data hiding techniques other than its original objective, have gained importance, which include authentication and identification, watermarking and transmitting passwords etc.

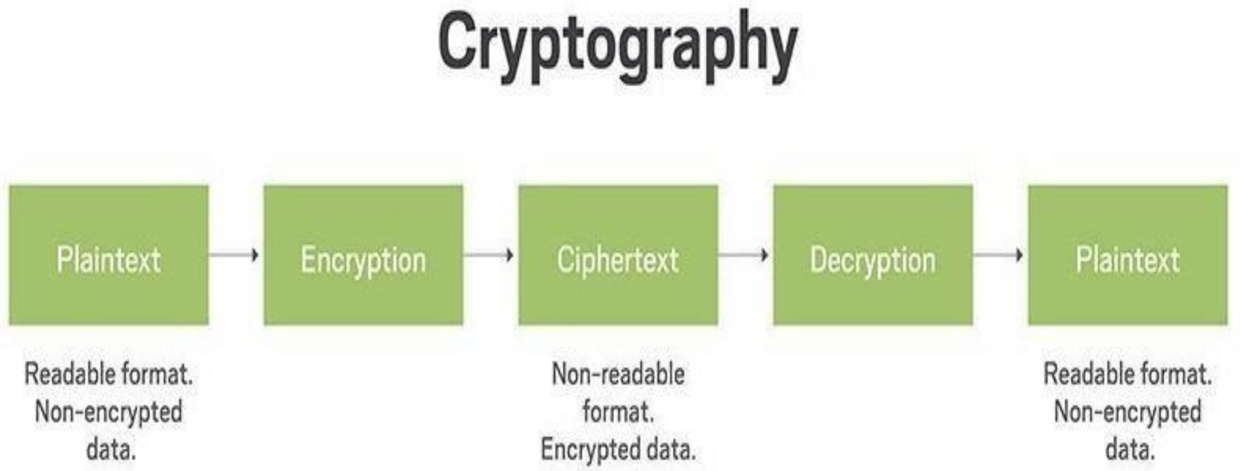
Basic Process With Their Diagram:



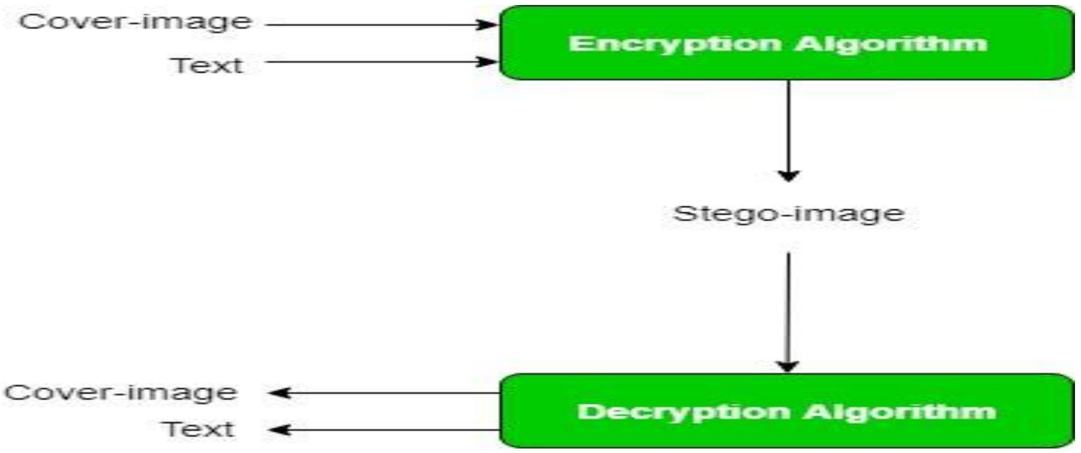
(a). basic encryption



(b). basic encryption & decryption


Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.

(c). basic cryptography process for encryption & decryption

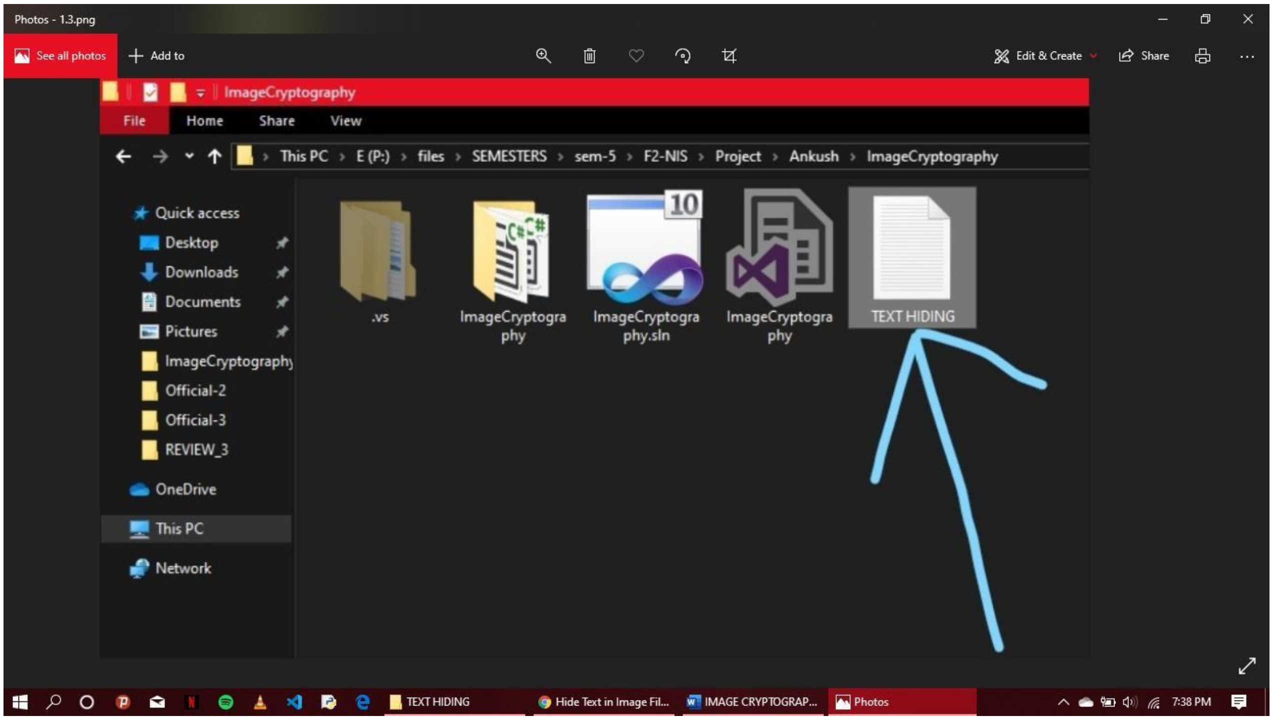


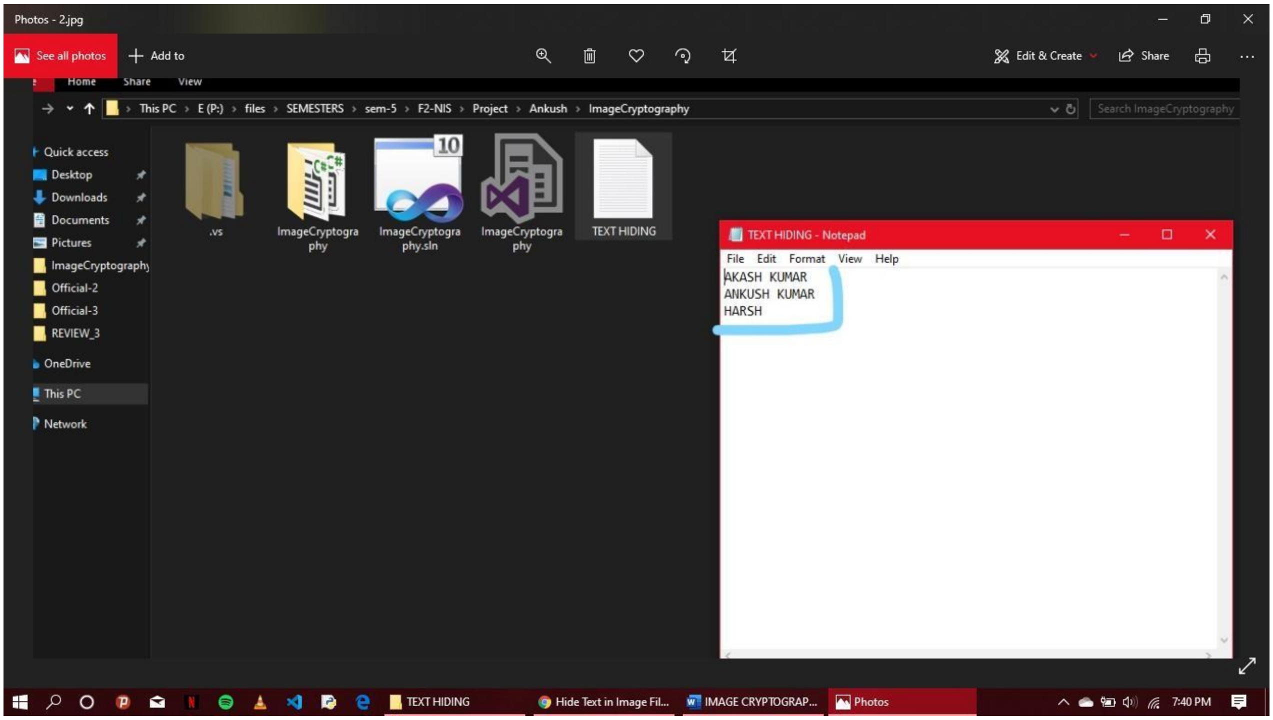
(d) . basic steganography process

Working Flow With The Help Of Diagram:

1). Select a Proper PNG / JPG Image

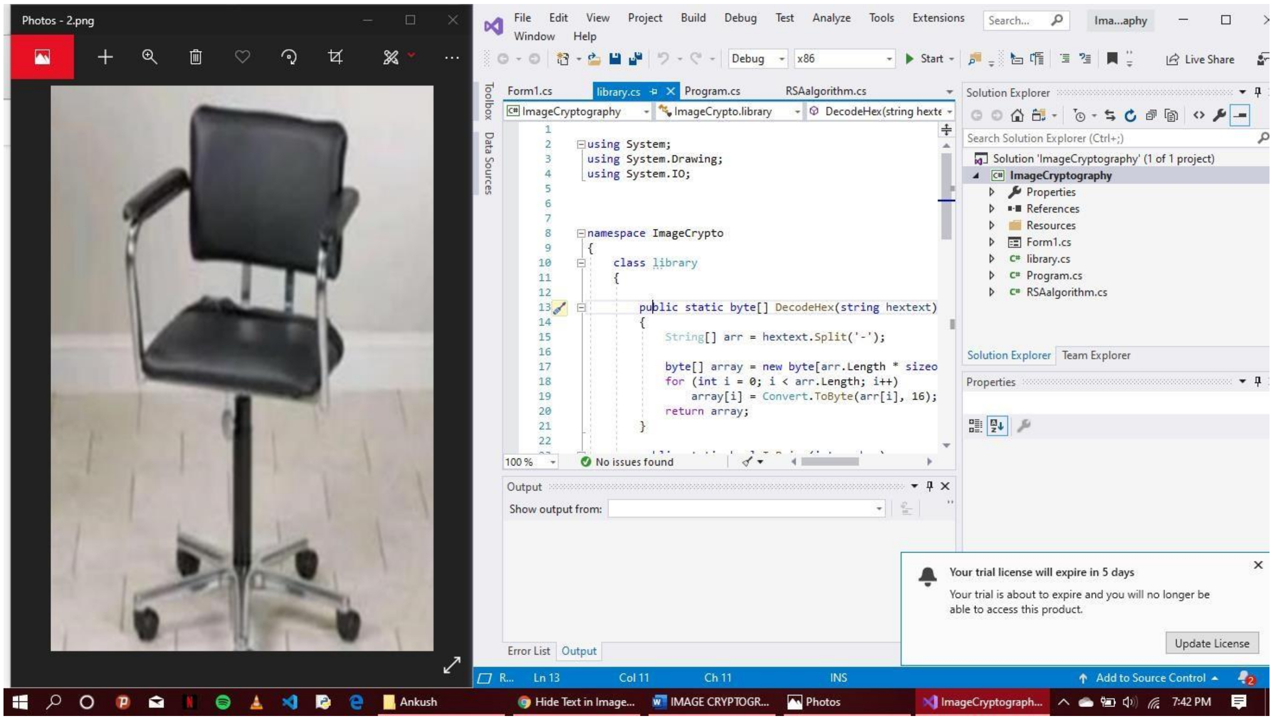
2). Select Your Text File





```
AKASH KUMAR
ANKUSH KUMAR
HARSH
```

3). Encrypt the Data Onto the Image



```
using System;
using System.Drawing;
using System.IO;



namespace ImageCrypto
{
    class library
    {

        public static byte[] DecodeHex(string hextext)
        {
            String[] arr = hextext.Split('-');

            byte[] array = new byte[arr.Length * sizeo
            for (int i = 0; i < arr.Length; i++)
                array[i] = Convert.ToByte(arr[i], 16);
            return array;
        }

```

Your trial license will expire in 5 days

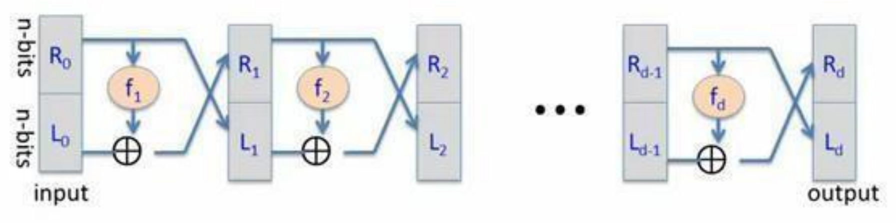
Your trial is about to expire and you will no longer be able to access this product.

Traditional Approaches:

In this section, we discuss several encoding techniques that are often used in day-to-day functions to ensure data security. Currently, there are many methods which could hide data. All the methods may be applied at any time irrespective of the content available. Each of these methods when used to encode and decode, data has its own constraints that need to be considered. There are certain requirements that must be satisfied. These requirements can be: the format of the input file, the size of the input file and the encryption key. In the following sections, both cryptographic and steganographic methods that provide data confidentiality are described.

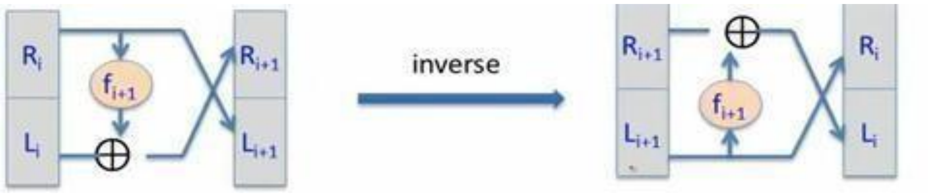
Data encryption standard (DES)

DES is an encryption standard where encryption is done in individual blocks called block cipher. The block size used here is 64 bits. The core idea behind this standard is Fiestel network. This standard involves 16 identical stages in its process. Each block of 64 bits is divided into two blocks; left and right of 32-bits. The right part is given as input to a Fiestel function. An XOR operation is applied between the output of Fiestel function and the left part and the resultant is considered as the right part of the second stage. For the left part in the second stage, the right part from the previous stage is simply copied .The same procedure is contained for 16 iterations to get a final output of the 64-bit block. This is how each block of 64-bits is encrypted with DES.



Encryption circuit block diagram

Decryption on the other hand, is just a reverse process to encryption which can also be called as inversion where an XOR operation is applied between the right part and the output of the Fiestel function. The resultant is considered as the left part to the next stage. And the left part is just copied as the right part of the next stage. This process is carried out through all the 16 stages.



Inverse circuit of encryption circuit

Traditional Approaches

Fiestel Function:

This function takes 32-bits of a block as input and submits to an expansion function. The task of the expansion function is to expand the input; therefore this expansion function takes 32-bit information as input and gives 48-bit output. The Fiestel function takes another input (key) which is of 48-bits length between the key value and 48-bit output from expansion function, an XOR operation is performed. From the resultant 48-bits, every 6 bits were given as input to an S-Box and a total of 8 S-boxes were used.

Least Significant Bit Substitution (LSB)

LSB substitution is a popular technique to embed data on to digital images. We know that an image will be stored in the form of bytes. In this kind of encoding, by using the LSB of each byte, 1-bit information can be stored in the image as secret message . Accordingly 1bit per byte can be stored in 8-bit images while 3-bits can be stored in 24-bit images for every 24-bits. Depending upon the color palette of a cover image, a secret message can be stored in two LSB’s which cannot be identified by human visual system (HVS) . But the main drawback of this encoding method is that images after encoding can be intercepted easily i.e, information can be changed or image format can be changed.

Jsteg

This was the first publicly available steganographic system for JPEG images. This encoding technique is similar to that of the LSB technique. This technique uses the concept of discrete cosine transformation (DCT). The JPEG image format uses a discrete DCT to transform successive 8 × 8 pixel blocks of the image into 64 DCT coefficients each.

Here, encoding is done by sequentially replacing the LSB of DCT coefficients with message’s data. Andreas Westfeld and Andreas Pfitzmann noticed that steganographic systems that change least-significant bits sequentially cause distortions detectable by steganalysis. The disadvantage with this system is, embedding step changes the LSB of colors in an image, that is, embedding uniformly distributed message bits reduces the frequency difference between adjacent colors.

SURVEYS

SURVEY-1 : A new encryption algorithm for image cryptosystems:

There are two types of data first one is text data and image data. The major difference is size of image data is large compare to text data. The plain data rarely permit loss when a compression technique is used. In this paper they used efficient cryptosystem for images the method used in this is “VECTOR QUANTIZATION “ which provide high security to the image. The other goal is to reduce the complexity of the encryption and decryption algorithm. Image security has become a important topic in the current world. There are some research issues on image cryptosystem. The first one is encrypt the image data using the same method as for text data. Mainly image are represented in 2D arrays they should convert into 1D arrays before enciphering there are various techniques are used on 1D lists. The sequence of image data can be encrypted by using block cipher. Product cipher can also used in order to encrypt the image data. To prove the feasibility of our image cryptosystem we can analyze the security for the following five attacks cipherimageonly attack,know plain text attack, chosen-image attack, jigsaw puzzle attack, and neighbor attack. Since JPEG require 64-element quantization table for encoding/decoding this will applied to JPEG. Many image can sent with only one encrypted codebook designed for these images.

Disadvantages:

Image are different form of text we use traditional algorithm (I,e is RSA) to encrypt the image directly actually this is not a good idea for two reasons. One is image size is greater than the text. Therefore this cryptosystems need more time to encrypt the image data. The second reason is decrypted message must be equal to original message. Under a cipherimage-only attack the illegal users are assumed to obtain information from network.

SURVEY-2 : A technique for image encryption using digital signature:

In this paper a new technique is used to encrypt an image for secure image transmission. The digital signature of the original image is add to the encoded version of the original image the image is encoded using error control code such has BOSE-CHAUDHURI HOCHQUENGHEM(BCH) code. At the DS is used to verify the authenticity of the image.

An information security method that uses a “digital holographic” technique. Information security is becoming the more and more important in the progress of exchange of data for electronic. The digital signature of an image is produced by using a one-way hash function. There are standard digital image algorithms that convert a message of any length into a fixed length message digest, usually 128 bits long. The standard techniques for creating a hash are MD2, MD4, MD5 and Secure Hash Algorithm (SHA). Hash functions are used because they are unique for a particular image and are very difficult to revert. A public key encryption algorithm (such as RSA) is used in conjunction with the message digest prior to transmission . In this process we are adding the more redundancy if an image containing more redundancy will be more secure. This technique uses the digital signature to encrypt the image and this techniques works well with images of all the sizes. This encryption technique provide three layer of security in the initial stage an error control code is used to determine in the real world based on the size of input images. At the receiver end the digital signature can be used to verify the authenticity of the transmitted image. A digital correlation technique in either the JTC can be used to verify the authenticity of the decrypted image. This clearly solves the problem of image recovery and image degradation.

SURVEY-3 : A new image encryption algorithm based on hyper-chaos:

In this paper a new image encryption is employs an image total shuffling matrix to shuffle the position of the image pixels and also use hyper-chaotic system to confuse the relationship between the plain-image and cipher-image. In this chaos-based algorithm has suggested a new and efficient way to deal with the problem of fast and highly secure image encryption. In a two dimensional chaotic cat map is generalized to 3D for designing a real-time secure symmetric encryption which employs the 3D cat map mainly to confuse the relationship between the cipher-image and the plainimage. Encoding the binary images using one-dimensional chaotic map is not secure. In this algorithm Logistic map and hyper-chaotic system are mainly used for the secret keys and key size is 1070.

SURVEY-4 : A new crypto-watermarking method for safe medical images transfer.

Nower days the usage of digital images has increased rapidly over the internet.There is a need for secure and faster diagnosis rate in the field of medical world.The transmission of images these days has become more routine and there is a need for finding an efficient way for transferring the images over the network.Here in this paper they proposed a new technique for encrypting an image for safer transmission over the internet connection without ant dataloss.It deals with the image encryption and watermarking.

In this paper they have made a method that combines both encryption and watermarking which is useful for transmission of an image.They have maken use of both encryptionrithm,secret key and also with the private keys.In this combination method they have under gone the method of encrypting the image with secret key and encrypt the secret key with public and private key method.The stream cypher method is robust to moderat noise like JPEG compression with high qualityfactor.They have used the watermarking method based on DC inorder to encrypt secret key in the image.They have also chosen working in frequency domain because of JPEG's robustness. They applied this method(encryption) to med-ical images and finally they presented a result of the full combination methods on medical image.

SURVEY-5 : A symmetric image encryption scheme based on 3D chaotic cat maps.

Due to various features of images such as bulk data capacity and high redundancy encryption of images is different from that of texts, which are generally difficult to handle by traditional methods The exceptionally desirable properties of mixing and sensitivity to initial conditions and parameters of chaotic maps, chaos-based encryption has an efficient way for dealing with the problem of fast and highly secure image encryption. In this paper, two-dimensional chaotic cat map is generalized to 3D for designing a real-time secure symmetric encryption format inorder to encrypt the image.

In this paper, the well-known two-dimensional 2D chaotic cat map has been generalized to threedimensional.The generalised 3D chaotic then used for designing a fast and secure symmetric image encryption scheme. This new scheme employs the 3D cat map to shuffle the positions of pixels of an image and uses another chaotic map to confuse the relationship between cipher-image and plain-image, thereby increasing its resistance to various attacks like the statistical and differential attacks. Thorough the experiment tests have been conducted with indetailed numerical analysis, demonstrating the high security and fast speed of the new image encryption scheme. This format is mainly suitable for real-time Internet image encryption and applications for transmission.

SURVEY-6 : An Image Encryption Using a Combination of Permutation Technique Followed by Encryption

Information encryption is broadly used to guarantee security in open systems, for example, the web. Each kind of information has its own particular highlights, subsequently, extraordinary detective hniques ought to be utilized to shield secret picture information from unapproved get to. The greater part of the accessible encryption calculations are utilized for content information, in any case, because of extensive information size and continuous compels, calculations that are useful for literary information may not be appropriate for mixed media information. In the vast majority of the common pictures the estimations of the neighboring pixels are emphatically associated. This implies the estimation of any given pixel can be sensibly anticipated from the estimations of its neighbors. In this paper, we present another change system in view of the mix of picture stage and an outstanding encryption calculation called RijnDael. The first picture was isolated into 4 pixels × 4 pixels pieces, which were revamped into a permuted picture utilizing a change procedure exhibited here, and afterward the produced picture was scrambled utilizing the RijnDael calculation. The outcomes demonstrated that the connection between's picture components was altogether diminished by utilizing the blend procedure and higher entropy was accomplished.

SURVEY-7 : A Study on RSA Algorithm for Cryptography

The idea of the RSA public key cryptosystem was from Diffie and Hellman, who introduced the method of the exponential key exchange. The Diffie-Hellman key exchange is the second most popular public key algorithms, after the RSA. However, the first ever known description of a similar system was made in 1973 by Cifford Cocks, a mathematician working at the GCHQ, a UK intelligence agency. The system was never set up considering relatively expensive computers required to implement it at the time. Because of its top secret classification, it was not until, 1998 that his discovery was revealed. During the fall of 1976, Ronald Rivest, Adi Shamir and Leonard Adleman, all young faculty members at the Masschusettes Institute of Technology began working on a novel type of cryptographic design. Rivest and Shamir were computer scientists at the MIT while Adleman was a number theorist at the Institution. In their project, Ronald and Adi would develop ideas while Leonard would attempt to bring the ideas down, by cracking them. Leonard was time and again successful at cracking them until one night when Ronald developed an algorithm that Leonard could not crack. The Algorithm was named RSA from their names Rivest, Shamir, and Adleman. To this day, the algorithm has never been broken (Ohya & Volovich 2011).

SURVEY-8 : A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique

The basic need of every growing area in today’s world is communication. Everyone wants to keep the inside information of work to be secret and safe. We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a certain level it's not safe. Steganography and Cryptography are two methods which could be used to share information in a concealed manner. Cryptography includes modification of a message in a way which could be in digesting or encrypted form guarded by an encryption key which is known by sender and receiver only and without using encryption key the message couldn’t be accessed. But in cryptography it’s always clear to intermediate person that the message is in encrypted form, whereas in steganography the secret message is made to hide in cover image so that it couldn’t be clearer to any intermediate person that whether there is any message hidden in the information being shared. The cover image containing the secret message is then transferred to the recipient. The recipient is able to extract the message with the help of retrieving process and secret key provided by the sender.

SURVEY-9 : Image and Text Steganography Based on RSA and Chaos Cryptography Algorithm with Hash-LSB Technique

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. Another technique by Shujun Li in 2004 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, a new image encryption scheme was developed by a Zhi-Hong guan in which changing thegrey values and positions shuffling of image pixels are combined to make bewildered the relationship between the cypher image and the plain image.

LITERATURE SURVEY TABLE

S.NO	Research paper Name	Author	Technique Used	Draw Back	Advantages
1	Burnett, S., & Paine, S. (2001). *The RSA security's official guide to cryptography*. McGraw-Hill, Inc	Burnett, S., & Paine, S.	VECTOR QUANTIZATION	Under a cipherimageonly attack the illegal users are assumed to obtain information from network. One is image size is greater than the text	Since JPEG require 64-element quantization table forencoding/decoding this will applied to JPEG
-2	Sinha, A., & Singh, K. (2003). A technique for image encryption using digital signature. *Optics communications*, *218*(4), 229-234.	Sinha, A., & Singh, K.	Digital holographic		This encryption technique provide three layer of securityhis process we are adding the more redundancy if an image containing more redundancy will be more secure.

3	Gao, T., & Chen, Z. (2008). A new image encryption algorithm based on hyperchaos. *Physics Letters A*, *372*(4), 394-400.	Gao, T., & Chen, Z.	use hyper-chaotic system	Encoding the binary images using onedimensional chaotic map is not secure.	3D cat map mainly to confuse the relationship between the cipherimage and the plainimage.
4	Puech, W., & Rodrigues, J. M. (2004, September). A new crypto-watermarking method for medical images safe transfer. In *Signal Processing Conference, 2004 12th European* (pp. 1481-1484). IEEE.	Puech,& Rodrigues,	Cryptowatermarking.	robustness to JPEG compression of the stream cypher method	Encrypt the Secret key with Public and private key method.
5	Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals*, *21*(3), 749-761.	Chen, G., Mao, Y., & Chui, C. K.	3D chaotic cat maps	twodimensional chaotic cat map has to be generalized to a threedimensional chaotic cat	high security and fast speed

6	Younes, M. A. B., & Jantan, A. (2008). An image encryption approach using a combination of permutation technique followed by encryption. *International journal of computer science and network security*, *8*(4), 191197.	Younes, M. A. B., & Jantan, A.	Permutation Technique Followed by Encryption		enhances the security level of the encrypted images by reducing the correlation
7	Saranya et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 57085709 A Study on RSA Algorithm for Cryptography	Saranya Vinothini Vasumathi	RSA	Fake publickey algorithms	Ensuring Data Protection From the Privy Eye
8	A Secure Image Steganography Based on RSA Algorithm and HashLSB Technique Rituparna Halder, Susmit Sengupta, Sudipta Ghosh, Debashish Kundu	Anil Kumar Rohini Sharma	RSA AND HASH LSB TECHNIQUES	all permutation only image cyphers were uncertain against chosen plaintext attacks.	Stronger Than Encryption Before

9	Image and Text Steganography Based on RSA and Chaos Cryptography Algorithm with Hash-LSB Technique 1Manjunath N, 2S.G.Hiremath	Manjunath N, S.G.Hiremath	RSA and Chaos Cryptography Algorithm with Hash-LSB Technique		

PSEUDOCODE :

Here I'm showing the simple bitwise XOR approach.

Encrypter:

```
1. Open the text and image file.

2. loop while( character count <= total characters)

    i.   character=convert to 16 bit integer(character) //by default the pixels and
         characters will be 8-bit in Matlab. This caused me a lot of problems

    ii.  pixel=convert to 16 bit integer(pixel)

    iii. encrypted_pixel= (pixel) bitwise_xor (character)

    iv.  pixel=next pixel

    v.   character=next character.

    vi.  character count= character count + 1

3. end loop

4. rest of encrypted_pixels = pixels of original image
```

Decrypter:

```
1. Open the original image and encrypted image.

2. loop while( pixel count <= total pixel)

    i.   original pixel=convert to 16 bit integer(original pixel)

    ii.  encrypted_pixel=convert to 16 bit integer(encrypted_pixel)

    iii. a= (original pixel) bitwise_xor (encrypted_pixel)

    iv.  if a=0 then break else decrypted_text=a

    v.   original pixel=next original pixel

    vi.  encrypted_pixel=next encrypted_pixel.

3. end loop
```

IMPLEMENTATION SOURCE CODE(1) :

```
using System;  using
```

```
System.Collections.Generic; using
System.Linq; using
System.Text; using
System.IO; using
System.Drawing;

namespace ImageCrypto
{      class
library
    {          public static byte[] DecodeHex(string
hextext)
        {
            String[] arr = hextext.Split('');
byte[] array = new byte[arr.Length];
for (int i = 0; i < arr.Length; i++)
array[i]
= Convert.ToByte(arr[i], 16);             return
array;
        }          public static bool
IsPrime(int number)
        {
            if (number < 2) return false;
if (number % 2 == 0) return (number == 2);
int root = (int)Math.Sqrt((double)number);
for (int i = 3; i <= root; i += 2)
            {
                if (number % i == 0)
return false;              }
            return true;
        }          public static Bitmap
ConvertByteToImage(byte[] bytes)
        {
            return (new Bitmap(Image.FromStream(new
MemoryStream(bytes))));
        }
        public static byte[] ConvertImageToByte(Image
My_Image)         {
            MemoryStream m1 = new
MemoryStream();             new
Bitmap(My_Image).Save(m1,
System.Drawing.Imaging.ImageFormat.Jpeg);
byte[] header = new byte[] { 255, 216 };
header = m1.ToArray();             return
(header);
        }
    }
}
```

R.S.A ALGORITHM SOURCE CODE(2):

```
using System; using
System.Collections.Generic; using
System.Linq; using
System.Text; using
System.Collections; using
System.Drawing;

namespace ImageCrypto
{      class
RSAalgorithm
    {          public static long
square(long a)
        {
            return (a * a);
        }          public static long BigMod(int b,
int p, int m) //b^p%m=?
        {             if (p == 0)
return 1;             else if (p % 2 == 0)
return square(BigMod(b, p / 2, m))
% m;             else                 return ((b % m) *
BigMod(b, p - 1, m)) % m;
        }          public static int n_value(int prime1,
int prime2)
        {
            return( prime1 * prime2);
        }          public static int cal_phi(int prime1,
int prime2)
        {
            return ( (prime1 - 1) * (prime2- 1) );
        }          public static Int32 cal_privateKey(int phi,
int e, int n )
        {
int d = 0 ;             int
RES = 0;

            for (d = 1; ; d++)
            {
                RES = (d * e) % phi;
if (RES ==
1) break;
}
return d;
}
    }
}
```

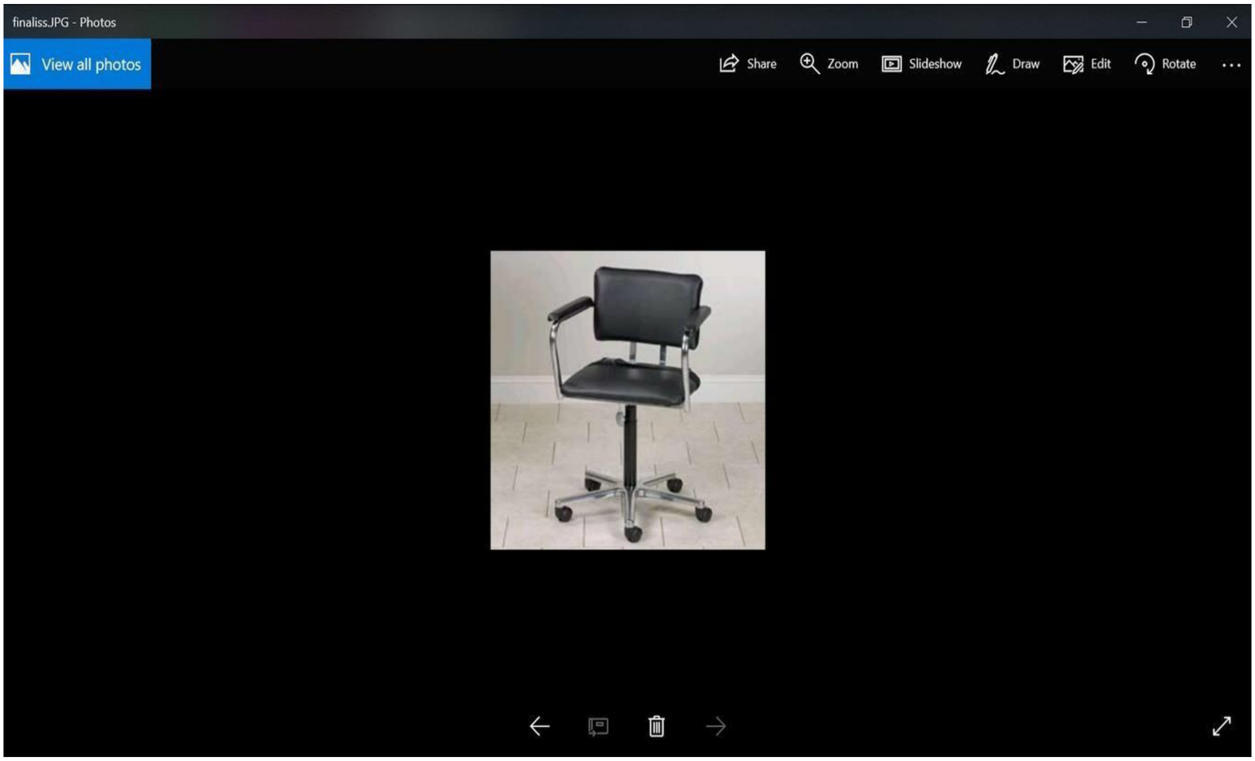
ENCRYPTION:

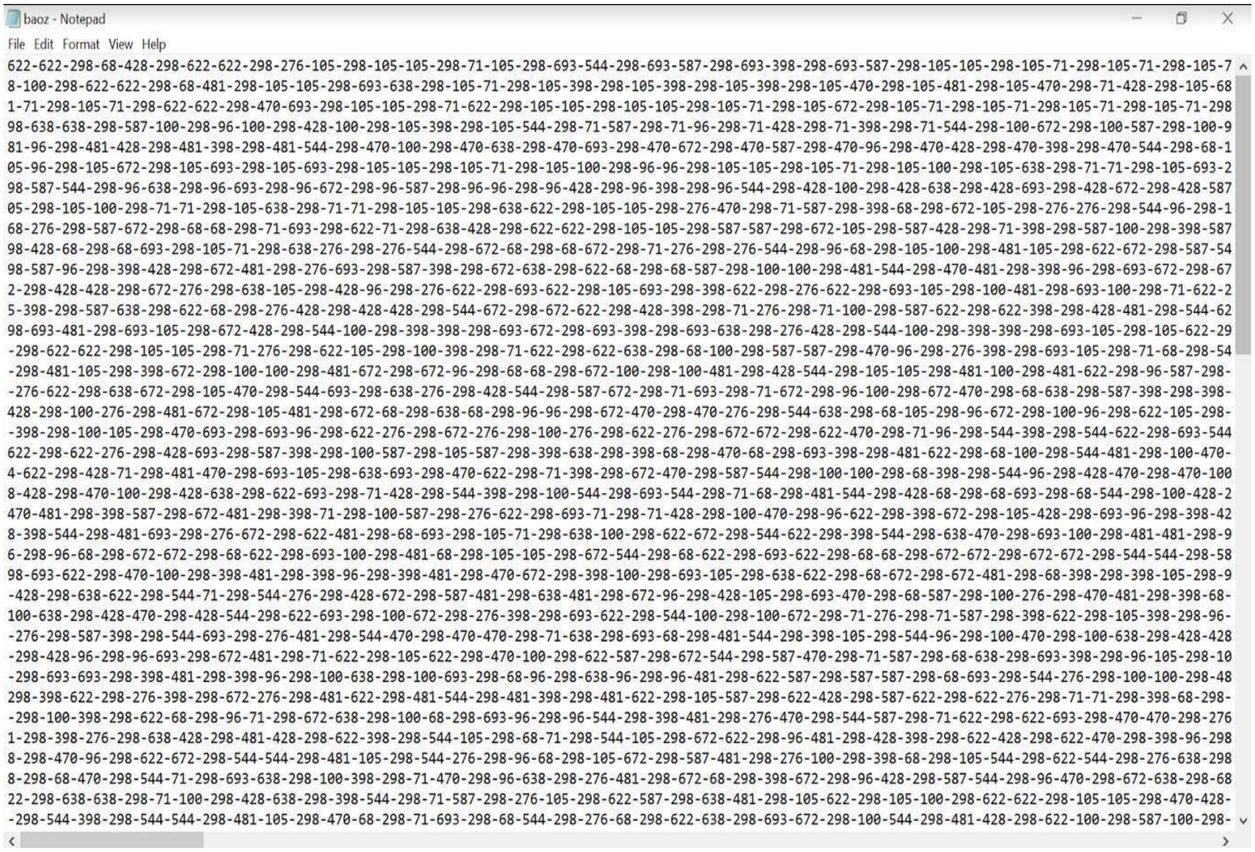
```
public string encrypt(string imageToEncrypt)
{     string hex =
imageToEncrypt;    char[] ar =
hex.ToCharArray();    String c =
"";    progressBar1.Maximum =
ar.Length;    for (int i = 0; i <
ar.Length; i++)
   {

Application.DoEvents();       progressBar1.Value = i;
if (c == "")           c = c +
ImageCrypto.RSAalgorithm.BigMod(ar[i], RSA_E, n);       else
c = c + "-" + ImageCrypto.RSAalgorithm.BigMod(ar[i], RSA_E,
n);     }     return c;
}
```

DECRYPTION:

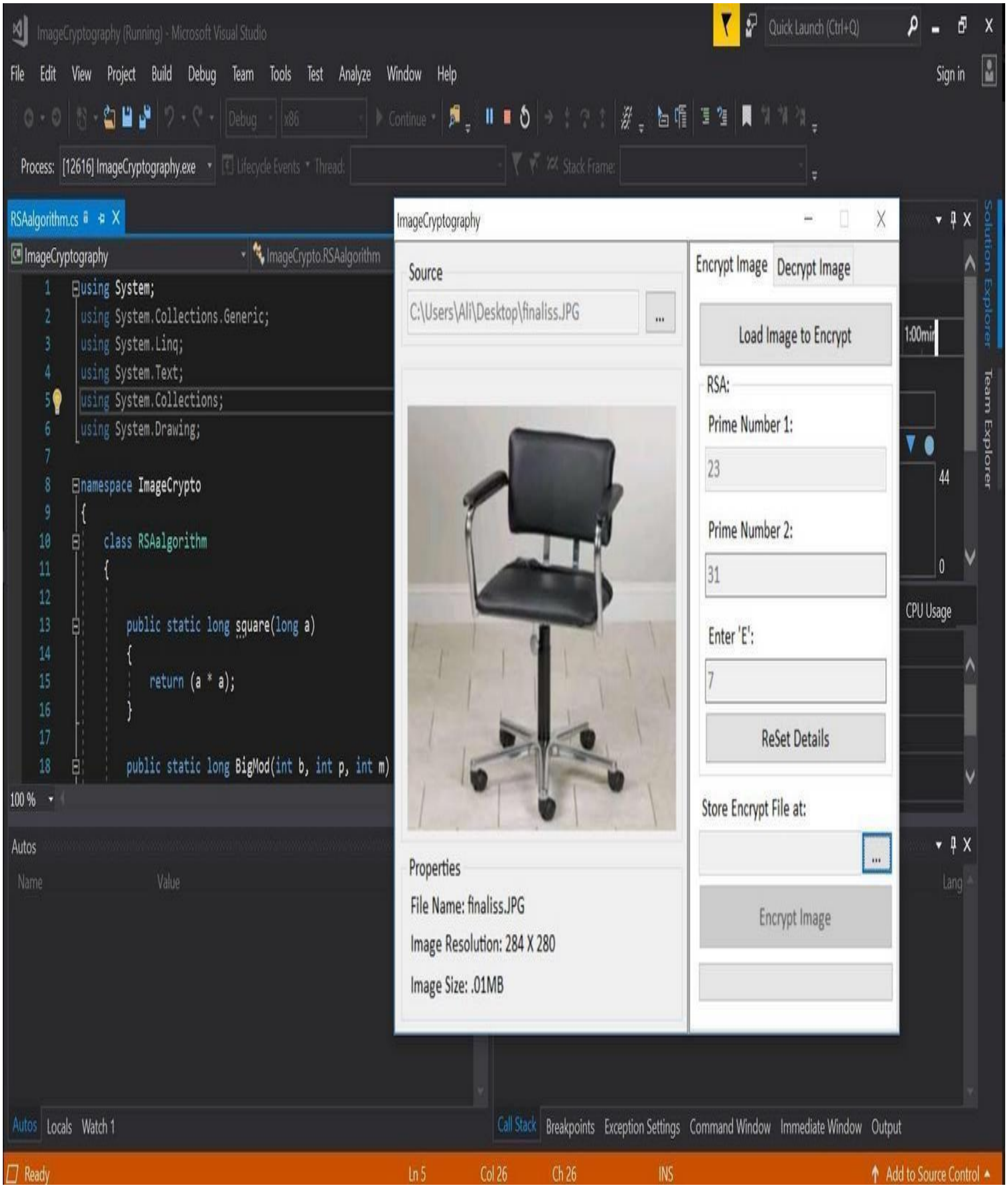
```
public string decrypt(String imageToDecrypt)
{                    char[]   ar   =
imageToDecrypt.ToCharArray();     int
i = 0, j = 0;     string c = "", dc =
"";     progressBar2.Maximum =
ar.Length;     try     {
for (; i < ar.Length; i++)
{

Application.DoEvents();           c
= "";
          progressBar2.Value = i;
for (j = i; ar[j] != '-'; j++)
c = c + ar[j];           i = j;
int xx = Convert.ToInt16(c);
          dc = dc + ((char)ImageCrypto.RSAalgorithm.BigMod(xx, d,
n)).ToString();
       }
}
    catch (Exception ex) { }      return
dc;
}
```

OUTPUT:





```
622-622-298-68-428-298-622-622-298-276-105-298-105-105-298-71-105-298-693-544-298-693-587-298-693-398-298-693-587-298-105-105-298-105-71-298-105-71-298-105-7
8-100-298-622-622-298-68-481-298-105-105-298-693-638-298-105-71-298-105-398-298-105-398-298-105-398-298-105-470-298-105-481-298-105-470-298-71-428-298-105-68
1-71-298-105-71-298-622-622-298-470-693-298-105-105-298-71-622-298-105-105-298-105-105-298-105-71-298-105-672-298-105-71-298-105-71-298-105-71-298-105-71-298
98-638-638-298-587-100-298-96-100-298-428-100-298-105-398-298-105-544-298-71-587-298-71-96-298-71-428-298-71-398-298-71-544-298-100-672-298-100-587-298-100-9
81-96-298-481-428-298-481-398-298-481-544-298-470-100-298-470-638-298-470-693-298-470-672-298-470-587-298-470-96-298-470-428-298-470-398-298-470-544-298-68-1
05-96-298-105-672-298-105-693-298-105-693-298-105-105-298-105-71-298-105-100-298-96-96-298-105-105-298-105-71-298-105-100-298-105-638-298-71-71-298-105-693-2
98-587-544-298-96-638-298-96-693-298-96-672-298-96-587-298-96-96-298-96-428-298-96-398-298-96-544-298-428-100-298-428-638-298-428-693-298-428-672-298-428-587
05-298-105-100-298-71-71-298-105-638-298-71-71-298-105-105-298-638-622-298-105-105-298-276-470-298-71-587-298-398-68-298-672-105-298-276-276-298-544-96-298-1
68-276-298-587-672-298-68-68-298-71-693-298-622-71-298-638-428-298-622-622-298-105-105-298-587-587-298-672-105-298-587-428-298-71-398-298-587-100-298-398-587
98-428-68-298-68-693-298-105-71-298-638-276-298-276-544-298-672-68-298-68-672-298-71-276-298-276-544-298-96-68-298-105-100-298-481-105-298-622-672-298-587-54
98-587-96-298-398-428-298-672-481-298-276-693-298-587-398-298-672-638-298-622-68-298-68-587-298-100-100-298-481-544-298-470-481-298-398-96-298-693-672-298-67
2-298-428-428-298-672-276-298-638-105-298-428-96-298-276-622-298-693-622-298-105-693-298-398-622-298-276-622-298-693-105-298-100-481-298-693-100-298-71-622-2
5-398-298-587-638-298-622-68-298-276-428-298-428-428-298-544-672-298-672-622-298-428-398-298-71-276-298-71-100-298-587-622-298-622-398-298-428-481-298-544-62
98-693-481-298-693-105-298-672-428-298-544-100-298-398-398-298-693-672-298-693-398-298-693-638-298-276-428-298-544-100-298-398-398-298-693-105-298-105-622-29
-298-622-622-298-105-105-298-71-276-298-622-105-298-100-398-298-71-622-298-622-638-298-68-100-298-587-587-298-470-96-298-276-398-298-693-105-298-71-68-298-54
-298-481-105-298-398-672-298-100-100-298-481-672-298-672-96-298-68-68-298-672-100-298-100-481-298-428-544-298-105-105-298-481-100-298-481-622-298-96-587-298-
-276-622-298-638-672-298-105-470-298-544-693-298-638-276-298-428-544-298-587-672-298-71-693-298-71-672-298-96-100-298-672-470-298-68-638-298-587-398-298-398-
428-298-100-276-298-481-672-298-105-481-298-672-68-298-638-68-298-96-96-298-672-470-298-470-276-298-544-638-298-68-105-298-96-672-298-100-96-298-622-105-298-
-398-298-100-105-298-470-693-298-693-96-298-622-276-298-672-276-298-100-276-298-622-276-298-672-672-298-622-470-298-71-96-298-544-398-298-544-622-298-693-544
622-298-622-276-298-428-693-298-587-398-298-100-587-298-105-587-298-398-638-298-398-68-298-470-68-298-693-398-298-481-622-298-68-100-298-544-481-298-100-470-
4-622-298-428-71-298-481-470-298-693-105-298-638-693-298-470-622-298-71-398-298-672-470-298-587-544-298-100-100-298-68-398-298-544-96-298-428-470-298-470-100
8-428-298-470-100-298-428-638-298-622-693-298-71-428-298-544-398-298-100-544-298-693-544-298-71-68-298-481-544-298-428-68-298-68-693-298-68-544-298-100-428-2
470-481-298-398-587-298-672-481-298-398-71-298-100-587-298-276-622-298-693-71-298-71-428-298-100-470-298-96-622-298-398-672-298-105-428-298-693-96-298-398-42
8-398-544-298-481-693-298-276-672-298-622-481-298-68-693-298-105-71-298-638-100-298-622-672-298-544-622-298-398-544-298-638-470-298-693-100-298-481-481-298-9
6-298-96-68-298-672-672-298-68-622-298-693-100-298-481-68-298-105-105-298-672-544-298-68-622-298-693-622-298-68-68-298-672-672-298-672-672-298-544-544-298-58
98-693-622-298-470-100-298-398-481-298-398-96-298-398-481-298-470-672-298-398-100-298-693-105-298-638-622-298-68-672-298-672-481-298-68-398-298-398-105-298-9
-428-298-638-622-298-544-71-298-544-276-298-428-672-298-587-481-298-638-481-298-672-96-298-428-105-298-693-470-298-68-587-298-100-276-298-470-481-298-398-68-
100-638-298-428-470-298-428-544-298-622-693-298-100-672-298-276-398-298-693-622-298-544-100-298-100-672-298-71-276-298-71-587-298-398-622-298-105-398-298-96-
-276-298-587-398-298-544-693-298-276-481-298-544-470-298-470-470-298-71-638-298-693-68-298-481-544-298-398-105-298-544-96-298-100-470-298-100-638-298-428-428
-298-428-96-298-96-693-298-672-481-298-71-622-298-105-622-298-470-100-298-622-587-298-672-544-298-587-470-298-71-587-298-68-638-298-693-398-298-96-105-298-10
-298-693-693-298-398-481-298-398-96-298-100-638-298-100-693-298-68-96-298-638-96-298-96-481-298-622-587-298-587-587-298-68-693-298-544-276-298-100-100-298-48
298-398-622-298-276-398-298-672-276-298-481-622-298-481-544-298-481-398-298-481-622-298-105-587-298-622-428-298-587-622-298-622-276-298-71-71-298-398-68-298-
-298-100-398-298-622-68-298-96-71-298-672-638-298-100-68-298-693-96-298-96-544-298-398-481-298-276-470-298-544-587-298-71-622-298-622-693-298-470-470-298-276
1-298-398-276-298-638-428-298-481-428-298-622-398-298-544-105-298-68-71-298-544-105-298-672-622-298-96-481-298-428-398-298-622-428-298-622-470-298-398-96-298
8-298-470-96-298-622-672-298-544-544-298-481-105-298-544-276-298-96-68-298-105-672-298-587-481-298-276-100-298-398-68-298-105-544-298-622-544-298-276-638-298
8-298-68-470-298-544-71-298-693-638-298-100-398-298-71-470-298-96-638-298-276-481-298-672-68-298-398-672-298-96-428-298-587-544-298-96-470-298-672-638-298-68
22-298-638-638-298-71-100-298-428-638-298-398-544-298-71-587-298-276-105-298-622-587-298-638-481-298-105-622-298-105-100-298-622-622-298-105-105-298-470-428-
-298-544-398-298-544-544-298-481-105-298-470-68-298-71-693-298-68-544-298-276-68-298-622-638-298-693-672-298-100-544-298-481-428-298-622-100-298-587-100-298-
```



```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Collections;
using System.Drawing;

namespace ImageCrypto
{
    class RSAalgorithm
    {

        public static long square(long a)
        {
            return (a * a);
        }

        public static long BigMod(int b, int p, int m)
```

Source

C:\Users\Ali\Desktop\finaliss.JPG

Properties

File Name: finaliss.JPG

Image Resolution: 284 X 280

Image Size: .01MB

RSA:

Prime Number 1: 23

Prime Number 2: 31

Enter 'E': 7

References :

1. Burnett, S., & Paine, S. (2001). *The RSA security's official guide to cryptography*. McGraw-Hill, Inc..
2. Sinha, A., & Singh, K. (2003). A technique for image encryption using digital signature. *Optics communications*, *218*(4), 229-234.
3. Gao, T., & Chen, Z. (2008). A new image encryption algorithm based on hyper-chaos. *Physics Letters A*, *372*(4), 394-400.
4. Puech, W., & Rodrigues, J. M. (2004, September). A new crypto-watermarking method for medical images safe transfer. In *Signal Processing Conference, 2004 12th European* (pp. 14811484). IEEE.
5. Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals*, *21*(3), 749-761
6. Younes, M. A. B., & Jantan, A. (2008). An image encryption approach using a combination of permutation technique followed by encryption. *International journal of computer science and network security*, *8*(4), 191-197.
7. Saranya et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) ,

2014, 5708-5709 A Study on RSA Algorithm for Cryptography

8. A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique Rituparna Halder, Susmit Sengupta, Sudipta Ghosh, Debashish Kundu
9. Image and Text Steganography Based on RSA and Chaos Cryptography Algorithm with HashLSB Technique 1Manjunath N, 2S.G.Hiremath