IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 17-20
www.iosrjournals.org

A Novel Color Image Based Data Security Technique Using SPKPCLS (Split Plaintext Key Pair Algorithm and Conditional LSB Substitution)

[1]Asst. Prof. Praseeda K Gopinadhan, [2]Asst. Prof. Renjith P R
[1]CSE, SNGCE, Kadayiruppu
kgprasi@gmail.com
[2]Master of Computer Application, Rajagiri College of Social Sciences, kalamassery
renjithkurup@gmail.com

Abstract: *The two important aspects of security that deal with transmitting data over a medium are steganography and cryptography. Cryptography defined as the science and study of secret writing, concerns the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers and other methods, so that only intended people can see the real message [1]. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video [2]. A method that integrates cryptography and steganography is highly robust. This paper proposes the design and implementation SPKPCLS – an algorithm that is a combination of cryptography and steganography to secure data and to hide the same in color images. . The algorithm encrypts the plaintext file using Split Plaintext Key Pair (SPKP) algorithm [3] and stores the ciphertext in a color image using conditional LSB substitution (CLS) algorithm.*

Keywords : *Cryptography, Steganography*

I. Introduction

The ideology of cryptography was introduced earlier, where confidential messages were sent as cipher text. SPKP is a a novel symmetric cryptographic algorithm that splits the plaintext as well as the key in equal numbers and applies the split key on the corresponding split plaintext. Here the number of splits is determined by a pseudo random number (PRN) generator algorithm. The input to the crypto algorithm is a file (the plaintext) and its password (the key). The ciphertext generated by this algorithm is stored in selected pixels of a color image by using (CLS) algorithm.

The combination of cryptography and steganography will make it tough for the eavesdropper to identify the ciphertext from the image and to decode it to retrieve the plain text.

II. Cryptography

Cryptography is still growing and research is still alive for new cryptography algorithms. There are several cryptographic algorithms that can be as simple as shift cipher or as complex as DES etc. As per Kerckhoffs's Desiderata of Cryptography, the security of the system should depend only on the secrecy of the keys and not on the secrecy of the encryption or decryption algorithm [4]. The main goals of cryptography are confidentiality, integrity, authentication and non-repudiation. In general, cryptography can be broadly divided into two – symmetric, where the same key is used for encryption and decryption and asymmetric, where a pair of keys is used for encryption and decryption. Fig. 1 shows symmetric and Fig. 2 shows asymmetric cryptography.

Figure 1: Symmetric Cryptography

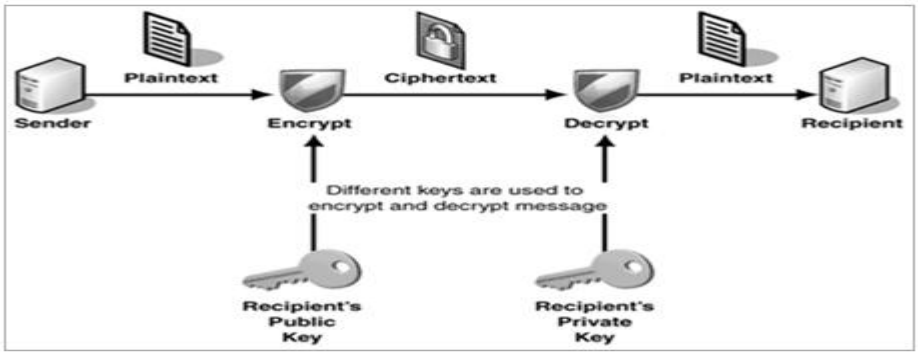

Figure 2: Asymmetric Cryptography

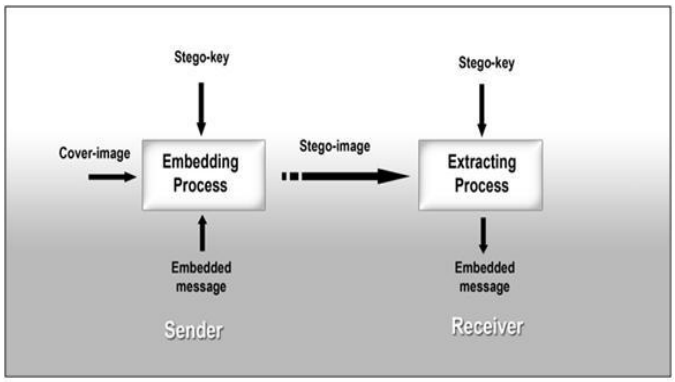

Figure 3: Steganogrpahy

III. Steganography

Steganography includes the hiding of information within computer files such as text, image or video. Three different aspects in information-hiding systems contend with each other: capacity, security, and robustness. Modern steganography attempts to be detectable only if secret information (a secret key) is known, which is similar to Kerckhoffs' Principle in cryptography [4]. Fig. 3 shows the steps involved in steganography

IV. Algorithms Used

A. Cryprographic algorithm - SPKP[3]

The plaintext for the algorithm is a file that contains some text information and the key is the password of the file. The algorithm computes a pseudo random number (PRN) from the password to generate the key. The number of letters and ASCII value of key determines key and hence the number of splits of key and plaintext. The key and plaintext are split equally. Let the plaintext P be split into *p1,p2, p3…pn* & let the key K be split into *k1,k2,k3…kn*. The pairs *(p1,k1), (p2,k2), (p3,k3)…(pn,kn)* undergoes encryption. For a pair *(pi,ki)* called as split plaintext key pair, *pi* is encrypted by the key *ki*.

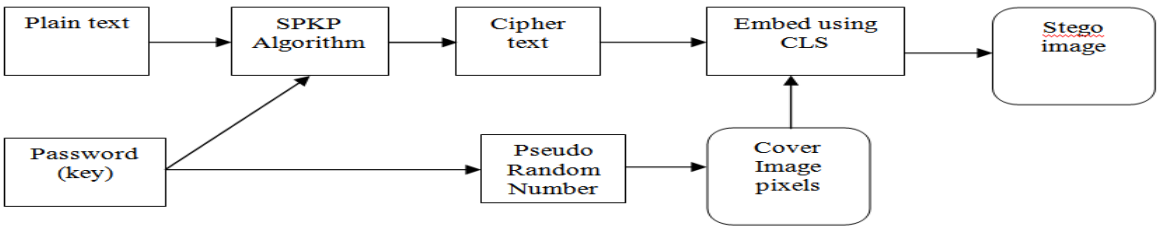

Figure 4: SPKPCLS Block Diagram

The algorithm uses shift cipher is used to create the cipher text. The shift cipher is applied on each split plaintext key pair to get the corresponding cipher text.

B. Steganogarphy algorithm - CLS algorithm

An image is a collection of pixels. Each pixel has a value associated with it. The basic concept of LSB substitution [5] is to embed the confidential data at the rightmost bit i.e. LSB of that value of each pixel.

Conditional LSB algorithm is an adaptation of traditional LSB algorithm. Color image is a collection of pixels with RGB components. Each component has 8 bit value. CLS takes a color image as cover image and embeds confidential data in LSB of R, G and B components of each pixel depending on a condition.

C. SPKPCLS algorithm

As seen earlier, the SPKP algorithm generates a PRN from the password that is used as the key for encryption. This PRN generated from key in the SPKP algorithm is used to choose the embeddable pixels. A pixel is said to be embeddable if the R or G or B component's value is perfectly divisible (modulus operation) by the PRN. The bits of cipher text will be substituted in the LSB of such identified RGB components. This method is superior to LSB substitution in the sense that it makes use of individual components of a pixel such as R,G and B to hide bits of cipher text. This method aids high capacity embedding even in medium resolution images. Fig. 4 shows the block diagram of SPKPCLS algorithm.

The algorithms are implemented in Visual C# in MS.NET platform. The steps of the algorithm is as follows

1. Choose the plaintext
2. Enter the password (key) to generate PRN
3. Use the PRN to encrypt the plaintext using SPKP algorithm
4. Identify the embeddable pixels of cover image using PRN
5. Embed each bit of ciphertext in the chosen R,G,B component of embeddable pixels by using CLS algorithm.
6. Reverse the process for ciphertext extraction from the stego image and then decrypting the plaintext using PRN generated using the password (key).

V. Implentation And Results

SPKPCLS pseudo code

```
for (x = 0; x < myBitmap.Width; x++)
for (y = 0; y < myBitmap.Height; y++)
    pixelColor = myBitmap.GetPixel(x, y);
    bR[lpCnt] = Convert.ToByte(pixelColor.R);
    bG[lpCnt] = Convert.ToByte(pixelColor.G);
    bB[lpCnt] = Convert.ToByte(pixelColor.B);
    if (lpCnt < bitByBit.Length)
    if (bR[bRi] % Globals.RKey == 0)
  bBit = bitByBit[lpCnt] == '1' ? true : false;
    if (bBit)
    bR[bRi] = (byte)(bR[bRi] | 1 << 0);
    else
    bR[bRi] = (byte)(bR[bRi] & ~(1 << 0));
    if (bG[bGi] % Globals.RKey == 0)
  bBit = bitByBit[lpCnt] == '1' ? true : false;
    if (bBit)
    bG[bGi] = (byte)(bG[bGi] | 1 << 0);
    else
    bG[bGi] = (byte)(bG[bGi] & ~(1 << 0));
    if (bB[bBi] % Globals.RKey == 0)
    bBit = bitByBit[lpCnt] == '1' ? true : false;
    if (bBit)
    bB[bBi] = (byte)(bB[bBi] | 1 << 0);
    else
    bR[bBi] = (byte)(bR[bBi] & ~(1 << 0));
myBitmap.SetPixel(x, y, Color.FromArgb(bR[bRi], bG[bGi], bB[bBi]));
```

References

[1] William Stallings, "Cryptography and Network Security" 4th Edition. Pearson Education Inc, Upper Saddle River, New Jersey, 2006.
[2] Wikipedia.org, 'Steganography', 2015. [Online]. Available: https://en.wikipedia.org/wiki/Steganography. [Accessed 26-Oct-2015].
[3] Renjith PR, Anita John, Praseeda K Gopindhan, "SPKP (Split Plaintext Key Pair) Algorithm – A Novel Method for Symmetric Encryption", Special Issue of International Journal of Computer Applications (0975 – 8887) on Advanced Computing and Communication Technologies for HPC Applications - ACCTHPCA, June 2012.
[4] Wikipedia.org, 'Kerckhoffs's principle or Kerckhoffs's Desiderata of Cryptography'. 2015 [Online]. Available: http://en.wikipedia.org/wiki/Kerckhoffs's_principle.[Accessed 11-Jun-2011]
[5] T. Morkel , J.H.P. Eloff, M.S. Olivier , "An overview of image steganography by. Information and Computer Security Architecture", (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.