Crypto-Stego Technique for Secure Data Transmission

Homer Benny Bandela1*, M.Ganesh Babu2 and Donavalli Venkata Vidya Deepthi3

1 Assistant Professor, Department of CSE, Sir C R Reddy College of Engineering, Eluru, India.
2 Assistant Professor, Department of CSE, Sir C R Reddy College of Engineering, Eluru, India.
3 Assistant Professor, Department of CSE, Sir C R Reddy College of Engineering, Eluru, India.

E-Mail: homer.benny@gmail.com

Abstract: As days are passing, technology is taking its force towards its smartness. But there are some devices which are to be modified for better security results. Cryptography is a technique used for sending secret messages and Steganography is a process related to image. In this paper, we consider Cryptography and Steganography for secure transmission of secret message. The technique used in this paper is to place an image within another image. Encrypted data or Secret data is placed on an image based on pixels and that image is placed as background for other image. When the receiver receives that image he/she thinks it as a normal image but it contains a hidden message and decrypted for original image.

Index Terms: Cryptography, Message, Security, Steganography

1. Introduction

1.1 Computer Networks
Fast growing field in Computer Science and Engineering is Networks. If we are accessing more information from different websites it is because of Computer Networks. Computer Networks are playing a key role in our daily life like Email, Chatting, Whatsapp, Instagram etc. Computer Network technology is now spread to mobiles also. Now a million dollar question is whether we are safe or unsafe in using this type of technology. Figure 1 gives a view of safe or unsafe ambiguity network. Suppose we want to shop online by using computer or mobile, then compulsory last point is payment. When we provide credit card or debit card information it may get notified by the hacker. He/she may misuse the card details for his/her personal work or any other work.

![Figure 1: Safe or Unsafe Network](image-url)
A PC sort out is a social event of PC systems and other preparing gear contraptions that are related together through correspondence channels to energize correspondence and resource sharing among a wide extent of customers through wired or remote media. The best case for PC sort out is the Internet or World Wide Web (WWW). The organized PC gadgets that start, course and end the information are called Network hubs. A portion of the notable hubs are Desktop PCs, Landline telephones, organizing equipment and so forth. When one gadget can trade information with the other, regardless of whether they have an immediate association with one another then we can say that the two gadgets are organized together with one another. The transmission media is utilized to convey the signs and the correspondence conventions are utilized to sort out the system topology, organize size and system traffic which separates the PC systems. A PC arrange encourages relational correspondence where the clients are permitted to impart by means of different methods like phone, video calls, video conferencing, email, texting and visit rooms.

2. Overview
Cryptography is solidly related to the control of cryptanalysis and cryptology which fuses systems, for instance, solidifying words with pictures, microdots, and diverse ways to deal with hide the information away or travel. In any case, in the present PC driven world, cryptography is much of the time associated with scrambling plain or ordinary substance into a figure message (a strategy called encryption), by then back afresh (known as unscrambling).
Cryptography is a procedure which changes over data into a course of action that is stirred up for an unapproved customer, empowering it to be transmitted without unapproved substances disentangling it yet again into a clear association, along these lines dealing the data. There are two sorts of frameworks in cryptography. One is symmetric and another is Asymmetric. In Symmetric or private-key cryptography both the sender and authority share a run of the mill puzzle key while Asymmetric or open key cryptography uses two keys, one for encryption and the other for decoding.

3. Existing system
In cryptography, the type of communication is private which uses encryption. The following are the basic principles used in cryptography.

3.1 The Basic terms/Principles
1) Encryption & Decryption
   Encryption means to convert the original data into some unreadable or encrypted form so that the data will be secure which helps in privacy preservation while sending the data from sender to receiver. On the receiver side, the data can be decrypted or converted to readable form (brought back to its original form). Decryption is nothing but the encrypted data gets converted back to the original data. In cryptography data encryption and decryption is done using a key. Same key or different keys can be used for both encryption and decryption of data.
2) Authentication
   It is a critical standard of cryptography which guarantees that the message was begun from the originator that was asserted in the message. This can be made conceivable if the sender plays out some activity on message that the recipient knows just the message originator can do.
3) Integrity
   Loss of integrity of messages is the common problem in communication which means that Cryptography should ensure that the messages that are being received by the receiver should not get altered/changed/modified anywhere on the communication path with the use of cryptographic hash.
4) No Repudiation
   This is the situation where there is a chance that the sender may deny that he/she has not sent the message to the receiver of the message. Cryptography keeps this sort of circumstance with the utilization of computerized marks.
3.2 Fundamental sorts of Cryptography
There are three fundamental sorts of Cryptography techniques which are as follows:

1. Secret Key Cryptography
2. Public Key Cryptography
3. Hash Functions

1. Secret Key Cryptography
It utilizes only a solitary key as appeared in Figure 2. To scramble a message the sender applies a key while the collector applies a similar key that is utilized by the sender to unscramble the message. This is a symmetric key sort encryption as just single key is utilized. The drawback with this system is the dissemination of key between the sender and the recipient.

![Figure 2: Secret Key Cryptography](image)

2. Public Key Cryptography
This kind of cryptography system incorporates two keys in which a safe data transfer can happen between the sender and the collector as appeared in Figure 3. In this system, each social event has a secret key and a shared key. The secret key is kept secret while the shared key is uncovered to every one of those whom you need to speak with.

![Figure 3: Public Key Cryptography](image)

3. Hash Functions
This methodology does exclude with any of the keys. Or on the other hand possibly it uses a fixed length hash regard that is prepared dependent on the plain text as showed up in Figure 4. Hash limits are used to check the decency of the message to ensure that the message has not been balanced, exchanged off or impacted by anything.

![Figure 4: Hash Function](image)

3.3 Hybrid Technique
Steganography is the process of hiding a secret message within a carrier file and extracting it at its destination. Anyone else who views the carrier file will fail to know that it contains some encrypted or hidden data.
4. Literature study

4.1 A Review and Comparative Analysis of Various Encryption Algorithms:
This paper experiences with respect to the sheltered data which is an incredibly troublesome issue that fuses various regions including PCs and correspondence. It gives information related to ambushes on advanced security that plays with the data protection of the customers. Cryptography is one such way to deal with guarantee that mystery, openness, trustworthiness, affirmation, and recognizing confirmation of customer data can be kept up by giving insurance and security to the customer data. Encryption is the path toward changing over the plain substance to figure message by applying some numerical changes or formulae which are called as counts. Distinctive encryption calculations are: DES, AES, RSA, Triple DES, RC5, IDEA and so forth. Among them DES, AES, RC5 and IDEA are symmetric key cryptographic counts. The key burden of this paper is that we can without quite a bit of a stretch break the above said computations.

4.2 Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Counter measures:
This paper details about the Internet and network applications that are growing very fast, so the need to protect such applications are increased by using cryptographic methods. The two cryptographic methods are symmetric and asymmetric. The RSA algorithm belongs to the category of asymmetric key cryptography and the DES algorithm ideally belongs to the category of symmetric key cryptography. This paper does not comprise about the security of user data.

4.3 File Encryption and Decryption Using AES Algorithm in Android Phone:
This paper details about the smart gadgets including smart phones and tablets. Comparing with the conventional computer, smart phone can be easily carried out and provides much more computer functionality, such as communication, processing, data storage as well as many computer related services such as web browsing, video call, video/audio player, wireless network, GPS etc. Various encryption algorithms like 3DES, DES, RSA, Blowfish and others are available to secure the data but these algorithms don’t give total security to the user data. Conventional Encryption cannot provide total security as the hackers can easily break the security in their own methods. As technology is changing the ideas of software professionals should also be changed. These algorithms can be updated and used in better ways.

5. Proposed System

5.1 Hybrid Technique
Cryptography notation with Steganography process is known as hybrid technique. Steganography is the process of hiding a secret message within a carrier file and extracting it at its destination.

![Steganography Technique](image)
This technique starts from encryption onwards. Encrypted message is added to image and the result thus formed is made to union with other image. When the receiver receives this image it will be in normal form. After separation of the image, it is decrypted to message. Steganography carrier file can be .bmp, .jpeg, .gif, .wav, .mp3 and amongst other. Hiding is possible under covering pictures.
Steganography characteristics are embedded with capacity, security and robustness.

![The Magic Triangle](image)

Figure 6: The Magic Triangle

1) **Capacity**
The notion of capacity in hiding the information/data indicates the total number of bits that are hidden and successfully recovered by the stego system.

2) **Security**
The embedded algorithm is secure, if the embedded data/information is not subject to removal after being discovered by the attacker and it depends on the total data/information about the embedded algorithm and the secret key.

3) **Robustness**
Ability of the embedded data to remain intact if the stego system undergoes transformation such as addition of random noise, linear and non-linear filtering, scaling, rotation and loose compression.

5.2 **Algorithm**
Plain text is given as $P = \text{Plain Text}$, Encryption with key is $E(T) = E(P, \text{Key})$, Image with Pixels $P_i$ and each pixel contains three colors RGB and change only bit position 1, $I(P_i) = P_iR(b_1') + P_iG(b_1') + P_iB(b_1')$, Likewise we can go for 4 bit position in three color pixels.

$I_1(P_i) = (P_iR(b_n') + P_iG(b_n') + P_iB(b_n') \text{ (Replace } E(T))$)

Image $(I_1)$ contains hidden information related to the encrypted text. Image $(I_1)$ is made as background of other image $(I_2)$.

$I_2 = \text{BG (I1)}$.

Image contains another hidden image which is encrypted and called as carrier image. This image $(I_2)$ is sent to receiver. When receiver receives this image he cannot identify that there is another image behind it. Image $I_1$ and $I_2$ are separated and hidden image is extracted for original message.

6. **Implementation**
The shade of every pixel is characterized by 3 bytes. The diverse hues for a pixel can be the same number of as $2^{8*3}$ or 1,67,77,216. The shading change of a pixel isn't noticeable to the human eye, if the LSBs of the shading bytes are changed. The concealed data is conveyed by the LSBs of the shading bytes. Shading data that has a place with every pixel of an image is given underneath in Figure 7.
Pixel uses a total of 24 bits, 8 bits for red, 8 bits for green and 8 bits for blue. We can use images to hide things if we replace the last bit of every color’s byte with a bit from the message. Suppose the Message is: 0100 0001. The image with 3 pixels is shown in Figure 8.

```
Pixel 1 – 11111000 11001001 00000011
Pixel 2 – 11111000 11001001 00000011
Pixel 3 – 11111000 11001001 00000011
```

Now we hide our message 01000001 in the image as follows.

```
Pixel 1 – 11111000 11001000 00000010
Pixel 2 – 11111001 11001000 00000011
Pixel 3 – 11111000 11001000 00000011
```

The color does not change but it contains the hidden message as shown in Figure 9.

```
Figure 8: Three same colors
```

```
Figure 9: Hidden Message
```

We get an image, divide it into pixels and add our secret message to it at LSB bit position 1. We can add up to 4 bit positions. Over 5 bit onwards image can be easily identified that it contains hidden message. Adding bits also depends upon the size of picture files. The range of the RGB is given in below Figures 10, 11, 12.
Figure 10: for RED Color.

Figure 11: for GREEN Color

Figure 12: for BLUE Color
Based on RGB we can hide our secret data in images. We can use up to 4 bits. Over that can be easily identified that there is some hidden data in image as shown in Figure 13.

![Original image and image with over 4 bits](image)

**Figure 13: Original image and image with over 4 bits**

### 6.1 Crypto-Stego:

Cryptography and Steganography is called as Crypto-Stego. Cryptography manages securing the setting of a message. Steganography manages hiding their very presence. In cryptography, the enemy is permitted to distinguish, catch and adjust messages ensured by a crypto framework. The target of stego is to cover the messages inside various harmless messages such that do not empower any enemy to attempt and perceive that there is a second hidden/secret message present in it. Figure 14 and 15 gives an unpleasant detail of sending and accepting end of Crypto-Stego.

![Sending End](image)

**Figure 14: Sending End**

![Receiving End](image)

**Figure 15: Receiving End**

Carrier Medium is given in below Figure 16.
The stego image will be same after hidden message as shown in Figure 17.

After image (I1) with hidden data is made to cover with black background color as shown in Figure 18.
Image I2 is replaced over the image I1 as shown in Figure 19.

Figure 19: Image within Image

Vise-versa image I1 and I2 are separated and I1 contains secret message and message is extracted from image. Likewise we can send binary audio and video messages. This paper shows betterment over other older techniques.

7. Conclusion
The combination of Cryptography and Steganography is used here so as to provide security when one additional image is put over an existing image. It is extremely an intriguing subject that a large portion of us manage in our everyday life that can be utilized for shrouded correspondence. The breaking points of Steganography were investigated as far as hypothesis and practice. Image was enhanced in Steganography system using LSB approach and insert it into or placing an image under another image to provide a means of secure communication which makes various fields to think of this technique.

References
[1] Mihir H Rajyaguru “CRYSTOGRAPHY – Combination of Cryptography and Stegnography with rapidly changing key”
[2] Rajdeep Bharat, Rahul Hans “A Review and Comparative Analysis of various Encryption Algorithms”
[3] Nivedita Bisht, Sapna Singh “A Comparative Study of some Symmetric and Asymmetric key cryptography algorithms”
[4] Prashant Kumar Arya, Dr. Mahendra Singh Aswal, Dr. Vinod Kumar “Comparative Study of Asymmetric Key cryptography Algorithms”
[5] Rejani R, Deepu V Krishnan “Study of Symmetric Key Cryptography Algorithms”
[6] Harsh Mathur, Prof. Zahid Alam “Analysis in Symmetric and Asymmetric Cryptography Algorithm”
[7] Omer K Jasim, Safia Abbas, El-Sayed M Horbaty, Abdel – Badeeh M Salem “Evolution of an Emerging Symmetric Quantum Cryptography Algorithm”
[8] Neha Gary, Partibha Yadav “Comparison of Asymmetric Algorithms in Cryptography”