# Triple Security of Data using Encryption Keys and Image Steganography

Lovpreet Kaur
Thapar University
Patiala
Punjab-147004, India

Harpreet Kaur
Thapar University
Patiala
Punjab-147004, India

Tejbir Kaur
Thapar University
Patiala
Punjab-147004, India

## ABSTRACT
Nowadays secure and safe transmission of data is a very important aspect for all internet users. In the data securing process the use of encryption algorithms almost make it very difficult for an eavesdropper to get access to any user's data. It helps to ensure the privacy of a company/user from others. Keeping in view the importance of steganography and cryptography for secure data transmission this work incorporates the use of multiple keys, LSB substitution method and bit plane technique for further security of image containing data. Simulation results show the feasibility of the proposed method. The data has been successfully embedded using triple security.

## Keywords
Encryption; Cryptography; Steganography; Bit plane method

## 1. INTRODUCTION
Modern world is the wireless world. In the wireless communication we need more security than wired communication. Nowadays wireless communication is used everywhere like schools, colleges, institutes, business, medical areas etc. Also users need security for banking, online transactions and other government sectors. Everyone wants to send his/her data securely from one place to other. For the security of data, we can use three methods single password, multiple passwords, and cryptography. Single passwords are very small. They are usually made with combination of alphabets and numbers. Due to small in length they are easier to get hacked by a hacker. Multiple passwords use two or three passwords for security and are also not optimized method in security point of view. Third method is cryptography; in this the data or plain text is converted into the cipher text. This process is known as encryption. The opposite process that is to get back the original data from cipher text is followed at the other end, known as the decryption process. As we know that network attacks are increasing day by day. To cope up with these attacks, many techniques and approaches have been developed so that data over a network remains safe, confidential and durable. Data security techniques include multiple passwords, cryptography, and biometrics. The conventional methods of encryption can only maintain the data security. Also, encryption process attracts the hacker's attention as it makes the data unreadable but using steganography (advance data hiding scheme) the data is embedded using a cover image, therefore, any unauthorized person would not come to know that there may be some hidden data. Secrecy of data will be maintained without any suspicion and thus, using image steganography data can be effectively hide without any noticeable knowledge to the hacker. Then for the purpose of double security that image which contains data is again stegnographed and hidden into a cover image and become totally safe to transfer by any means.

## 2. RELATED WORK
To upgrade cryptographic secrecy, secrecy metric of degrees of opportunity in an aggressor's learning of the cryptogram, which is like forgery, was introduced. The system provides cryptographic security enhancement [1]-[2]. The issue of end-to-end security was upgraded by turning to consider disorder infused in ciphertext. The primary objective was to create a corrupted wiretap direct in the application layer over which Wyner-sort secrecy encoding was summoned to convey extra secure data [3]-[4]. An efficient symmetric key cryptography algorithm for information security was designed. This block encryption algorithm was much faster and offers the enhanced security features compared to other symmetric key algorithms. Confidentiality and authentications are two main security goals in secure electronic mail (e-mail). A certificate-less-effective key management (CL-EKM) protocol for secure communication in dynamic WSNs characterized by node mobility. A new approach for generating keys from the available data was introduced [5]-[6] Various image encryption and decryption methods were proposed and lossless compression, less processing time and good quality image were obtained [7]-[10]. The technique called steganography is used for hiding the data in a smarter way which makes it difficult for an unauthorized person to detect whether any secret or hidden data is present in the cover media or not [11-12]. For more security, steganography is used in many researches to hide the data or any information in the QR codes. [13]- [19] used steganographic technique for the data hiding purpose. Arooj Nissar account of the various approaches that had been proposed for steganalysis in 2007. Abbas Cheddad concluded with some recommendations and advocated for the object-oriented embedding mechanism. Zhou Zhi worked on a halftone visual cryptography. The obtained visual quality results were better than any other available VC methods. Wang Yong discovered applications in which many researches were attracted to JPEG and its detection becomes also important. There were some blind steganalysis methods, but they were either time consuming or unreliable.

## 3. PROPOSED SCHEME
The proposed algorithm is based on the cryptography and steganography. Encryption is done by generating keys from secret data and steganography is performed by hiding the data in to a cover image. The process of steganography is performed twice. Initially, to hide the encrypted data or

ciphertext into a cover image and then to hide the stego image into another cover image. The flowchart of the proposed scheme for embedding of secret data is shown in figure 1. The secret data can be extracted back by using extracting algorithm which is the reverse process of the embedding algorithm, the algorithm for extraction of data has been given in figure 1(b).

## 3.1 Embedding algorithm (TSA)

Firstly, take two randomly generated data sets and an operation like XOR, AND or OR is performed on these data sets. This will generate a key from the two data sets. After that the data is converted into the cipher text with the help of generated key. This is called the single key generation and the encryption process. The next step is to perform the other operation on the generated key to get another key, this is known as the re-encryption process. This is performed for enhanced security. This process is also called as multiple keys generation. The cipher text obtained after using multiple keys is further protected with the help of image steganography. The next step is to do embedding of the encrypted data in the cover image (image which is used for embedding).

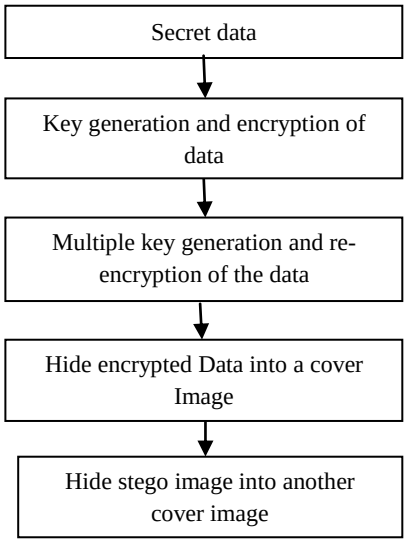



**Fig 1: Triple Security algorithm**

be embedded).Thus a coloured PNG image of pixel size 256×256 is taken as a cover image. It is then converted into gray colour image of same size. For embedding process used LSB substitution method is being used. LSB substitution method will replace the LSB's of the pixel of the cover image by the secret data. Here three LSB's of each pixel of cover image are being replaced by three bits of encrypted data set. The image obtained after embedding the secret data is known as the stego image. This image is now safe to be transmitted into the channel and no one will be able to know that there is some hidden data in the image. Supplementary protection is provided to this obtained stego image by hiding the whole stego image into some another cover image of the same pixel size. This is why the algorithm is named as triple security algorithm. This algorithm thus provides enhanced level of security to any confidential information.

## 3.2 Extracting algorithm

The secret data can be extracted back by using the reverse steps as given in the extracting algorithm which is shown in figure 2.

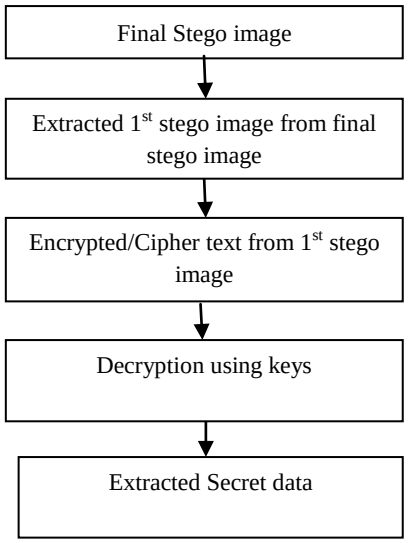


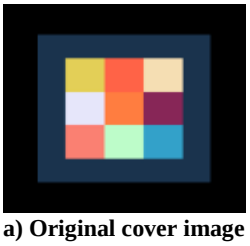

**Fig 2: Extracting algorithm**

## 4. RESULTS

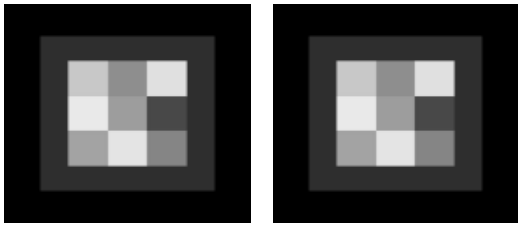
The simulation results of the proposed algorithm have been shown in this section. AND operation has been performed on two randomly created data sets and a key has been generated. Next step is to encrypt the data with OR operation that convert the data into cipher text. After that the key is inverted using 1's complement that will generate the second key. Thus, this new key has been used to re-encrypt the data. Now the second step is to hide the encrypted text in to a cover image. Figure 3(a) shows a colored cover image of PNG format of pixel size 256×256. The gray scale representation of the image is shown in figure 3(b). This image has been used for hiding the encrypted data. Here three LSB's of each pixel are used to hide the encrypted data. Since the pixel size is 256×256 so data which is being hidden (known as payload) can be given as:

Payload=256×256×3=199608 bits

After embedding the data, the final stego image is obtained which is shown in figure 3(c).



**a) Original cover image**



**b) Gray scale image** **c) Stego image(1st)**

**Fig 3: a) Cover Image (256×256), b) Gray scale Image and c)Stego image**

The quality of the stego image is determined by considering image quality parameters such as, PSNR and

MSE and is shown in table 1. High PSNR value and low MSE value show good or acceptable image quality. The value of PSNR is measured in decibel (dB). If PSNR value is more than 30 dB, then image distortion is generally considered as imperceptible.

For an M× N gray scale image, the PSNR value is calculated as the following:

$PSNR=10log_{10}(\frac{255}{MSE})$

The value of MSE is given as:

$$\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(x(i,j)-x'(i,j)\right)\text{ ^ }2$$

Where $x(i, j)$ and $x'(i, j)$ are the pixel values of the cover and the stego image, respectively.

**Table 1: PSNR, MSE and payload values for stego image obtained in 1(c)**

| PSNR(dB) | MSE | PAYLOAD(bits) |
|---|---|---|
| **49.2520** | **0.78** | **199608** |

A low MSE and high PSNR values show an excellent image quality of stego image. The first stego image has been further embedded in to another cover image shown in figure 4.

**Fig 4: Final cover Image**

The image is hidden in the bit 2 of the cover image. The image is now fully secured to transmit over any channel. Obtained stego image is known as final stego image and is shown in figure 5.

**Fig 5: Final Stego Image**

The advantage of steganography technique is its simplicity and safety because stego image is not distinguished by human eye.

## 5. CONCLUSION

In this paper, encryption using multiple keys, LSB substitution scheme and bit plane technique for image steganography has been used for providing better security to secret information. The results show that the stego image is obtained without making a perceptible distortion. Moreover, the results of the used scheme show that the used scheme provides enhanced protection as well as good quality of the stego image is maintained. PSNR and MSE values of the stego images are also calculated. As a future work this data embedding and protection can be done for audio or video files using images of large pixel sizes.

## 5. ACKNOWLEDGMENTS

Our special thanks to mentor, teachers of the department and then friends who devoted their valuable time and help us in all possible ways towards successful completion of this work. We would like to thanks our parents for their years of unyielding love and encouragement. We admire their determination and sacrifice. Lastly, we thank all those who have contributed directly or indirectly to this work.

## 7. REFERENCES

[1] Harrison, k. Willie, Almeida Joao, W. Steven McLaughlin, and Barros Joao 2011. Coding for Cryptographic Security Enhancement Using Stopping Sets, IEEE Transactions on Information Forensics and Security, vol.6, no.3, pp. 575 – 584.

[2] Khiabani, s. Yahya, Shuangqing Wei, Yuan Jian, and Wang Jian 2012. Enhancement of Secrecy of Block Ciphered Systems by Deliberate Noise, IEEE Transactions on Information Forensics and Security, vol.7, no.5, pp. 1604 – 1613.

[3] Verma, S., Choubey, R. and Soni R. 2012. An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security, International Journal of Emerging Technology and Advanced Engineering, vol. 2, no. 7, pp. 18-21.

[4] Li Fagen, Zhong Di, and Takag Tsuyoshi 2016. Efficient Deniably Authenticated Encryption and Its Application to E-Mail, IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2477 – 2486.

[5] Sultana and Bertino Elisa 2015. Effective Key Management in Dynamic Wireless Sensor Networks, IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 371 – 383.

[6] Kakkar Ajay, Singh M. L., Bansal P. K. 2012. Secure Communication by using multiple keys having variable length in a real time environment for multiple stations, Journal of Engineering Science and Technology, vol. 7, no. 4, pp. 505-516.

[7] Vikas Agrawal, Shruti Agrawal, Rajesh Deshmukh, "Analysis and Review of Encryption and Decryption for Secure Communication," International Journal of Scientific Engineering and Research, 2014.

[8] S.S. Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN," Pattern Recognition, 34, 1229-1245, 2001.

[9] Narendra K. Pareek, Vinod Patidar and Krishan K. Sud, "Diffusion–substitution based gray image encryption scheme," Digital Signal Processing, 23, 894-901, 2013.

[10] Yuanyuan Sun, Rudan Xu, Lina Chen and Xiaopeng Hu, "Image compression and encryption scheme using fractal dictionary and Julia set," IET Image Process, 9(3), 173-183, 2015.

[11] Liao X,Wen QY, Zhang J, "A steganographic method

for digital images with four-pixel differencing and modified LSB substitution," Journal of visual communication and image representation, 22 (1), 1-8, 2011.

[12] H. Dadgostar a, F. Afsari, "Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB," Journal of Information Security and Applications, 1-14, 2016.

[13] Li Bin (2008).Steganalysis of Multiple BaseNotational System Steganography, IEEE Signal Processing Letters, 15, 493-496.

[14] Zhang Liang and Wang Haili (2009). A High-Capacity Steganography Scheme for JPEG2000 Baseline System, IEEE transactions on Image Processing,18(8), 1797-1803.

[15] Cheddad Abbas, Condell Joan, Curran Kevin and Mc Kevitt Paul (2010). Digital image steganography: Survey and analysis of current methods, School of Computing and Intelligent System, 909(3), 727-752.

[16] Arooj Nissar, "Classification of steganalysis techniques: A study," Department of Information Technology, pp. 1758-1770.

[17] WangYong (2010). Reliable JPEG steganalysis based on multi-directional correlations, Department of Applied Mathematics, Information Science and Technology Institute, 25(8), 577-587.

[18] Zhou Zhi, Arce Gonzalo R. and Di Crescenzo Giovanni (2006) Halftone Visual Cryptography, IEEE Transaction on Image Processing, 15(8), 2441-2453.

[19] Maninder singh and Dhanwant singh (2015). Energy efficient key management scheme for wireless sensor networks, International Journal of Research in Information Technology, 3 (8), 166-173, 2015.