International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

EFFICIENT DATA HIDING WITH LZW COMPRESSION AND ECC ENCRYPTION FOR SECURE SECRET SHARING

Mr.S.Dilipkumar[1], P.Akilan[2], D.Karthivasan[3],R.Saravanan[4]

[1] Assistant Professor *& Arasu Engineering College, Kumbakonam, Tamilnadu,* INDIA
[2,3,4] *UG scholar & Arasu Engineering college, Kumbakonam, Tamilnadu,* INDIA

Abstract - *Information/data hiding is a mechanism which ensures that the presence of the secret data remains undetected. Two types of data hiding techniques are most popular, they are cryptography and steganography. Where cryptography is science of writing secret code and steganography is art and science of hiding the secret code. In cryptography data is converted to unreadable form, so that unauthorized users cannot access the secret data. Steganography process hides message into cover file and forms a stego file. In image steganography there is a need of method which will increase the security, reduce the distortion in the stego file and recovers the data without any loss. In the era of multimedia and internet there is need of reducing time for transmission. The proposed approach is combination of compression, data hiding technique and encryption. To make the transmission and storage of digital data faster, Lempel-Ziv-Welch (LZW) compression technique is used. LZW is a type of lossless compression technique. In the proposed approach Elliptic curve cryptography (ECC) technique is used for data encryption and steganography uses Modified Pixel Value Differencing (MPVD) with LSB method to hide the encrypted data. If the receiver has encryption key, then only he can obtain the secret message. These proposed techniques will provide higher security and the system yields high quality image, less memory utilization, more complexity and higher embedded capacity.*

Key Words: **steganography, compression, data hiding technique, Elliptic curve cryptography, Lempel-Ziv-Welch, Modified Pixel Value Differencing.**

1.INTRODUCTION

Steganography is the practice of hiding secret messages (hidden text) within every day, seemingly innocuous objects (cover text) to produce a stegno text. The recipient of a stegno text can use his knowledge of the particular method of steganography employed to recover the hidden text from the stegno text. The goal of steganography is to allow parties to converse covertly in such a way that an attacker cannot tell whether or not there is hidden meaning to their conversation. This sets steganography apart from cryptography which, although providing for private communication, can arouse suspicion based solely on the fact that it is being used.

1.1 WORKING PROCESS

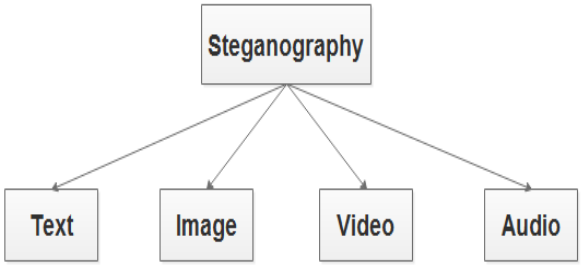
Steganography replaces unneeded or unused bits in regular computer files (Graphics, sound, text) with bits of different and invisible information. Hidden information can be any other regular computer file or encrypted data. Steganography differs from cryptography in a way that it masks the existence of the message where cryptography works to mask the content of the message.

Steganography sometimes used in conjunction with encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden information is not seen.

1.2 TYPES OF STEGANOGRAPHY

There are different ways to hide the message in another, well known are Least Significant bytes and Injection. When a file or an image is created there are few bytes in the file or image which are not necessary or least important.

These type of bytes can be replaced with a message without damaging or replacing the original message, by which the secrete message is hidden in the file or image. Another way is a message can be directly injected into a file or image. But in this way the size of the file would be increasing accordingly depending on the secrete message.



2. PROPOSED SYSTEM

The proposed approach is combination of compression, data hiding technique and encryption. To make the transmission and storage of digital data faster, LZW compression technique is used. LZW is a type of lossless compression technique. In the proposed approach Elliptic curve cryptography (ECC) technique is used for data encryption and also Comprehensive steganographic method by combining the lossless compression, state of the art encryption, modified pixel value differencing (MPVD) and LSB substitution. If the receiver has encryption key, then only he can obtain the secret message. These proposed techniques will provide higher security and the system yields high quality image, less memory utilization, more complexity and higher embedded capacity.

SYSTEM DESIGN

Data hiding is the process of hiding secret message into cover file. In steganography, before the hiding process, the sender must select an appropriate message carrier, an effective message to be hidden as well as a secret key used as a password. Secret message is present in the form of text and cover file is selected in form of image. A robust steganographic algorithm must be selected that should be able to encrypt the message more effectively. The sender then may send the hidden message to the receiver by using any of the modern communication techniques. Uploaded text message was hidden within the image to create stegno image. Generate key for securely sharing the information to receiver.

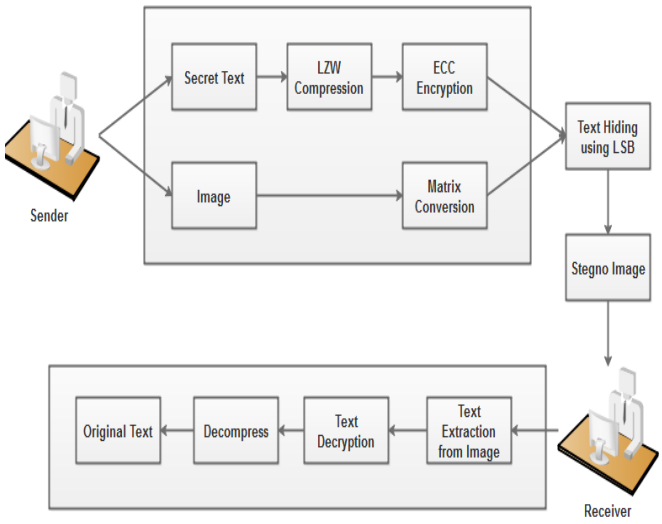


Fig -1: System Architecture

LZW Compression

Secret message is collecting from sender and apply compression on secret text to reduce the size of the compressed text. LZW compression is the process of compressing the secret text before hiding in image. LZW compression is the compression of a file into a smaller file using a table-based lookup algorithm. LZW compression algorithm takes each input sequence of bits of a given length for that particular bit pattern, consisting of the pattern itself and a shorter code.

Data Encryption

Encryption is the process of converting plain text into cipher text. Here compressed text is taken as input for encryption process. ECC encryption is used to convert the compressed text into encrypted format. Then secret keys are generated and distributed to the receiver. Compressed text is taken as input for encryption using ECC. It creates encryption keys based on using points on a curve to define the public and private keys. It provides higher level of security with lesser key size compared to other Cryptographic techniques. Encrypted output is converted into binary form. It ensures higher security level. [11]

Data Hiding using LSB

In the process of embedding, the cover image is divided into non-overlapping pixel blocks of 3x3 or 2x2 pixel blocks. Block levels are based cardinality of the cover image. If secret bit is 1 and LSB of stego pixel is 0 or vice-versa, then 1 is added or subtracted to the stego pixel. In this method, the LSB of each pixel is replaced (over-written) by a value zero for the non-edged pixel, or one for an edged pixel. This can be done by using the logical operators. The LSB contains the indication for the existence of edged pixel. Changes to the LSB of a pixel affect its value by only one. Since pixel values range from 0 to 255, there will be a very little change in pixel intensity. The extraction of the LSB can be implemented by checking the odd and even pixel values.

Data Extraction

Data extraction is the process of extracting the original data. Receiver gets the secret message with cover image. Specific key is generated and shared to the receiver during the process of message sending. Key sharing is the process of sharing secret keys to the receiver. Then the receiver can extract the text and decrypt the text using decryption key. Then add decompression to get original text.

3. CONCLUSIONS

This paper proposed a new steganographic algorithm for hiding text files in images. Here provide an overview of steganography and introduce some techniques of steganography which help to embed the data. These techniques are more useful for detecting the stego images as well as the image media relating to security of images

and embed the data for complex image area and can easily estimate the high embedding rate by using the quantitative steganalytic technique. Here we have also used an underlying compression algorithm with maximum compression ratio of 8 bits/ pixel. Developed a system in java based on the proposed algorithm. Here we have tested few images with different sizes of text files to be hidden and concluded that the resulting stego images do not have any noticeable changes. Also we found that for .bmp images this algorithm works very efficiently. Hence this new steganographic approach is robust and very efficient for hiding text files in images.

REFERENCES

[1] Zhou, Jiantao, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au, and Yuan Yan Tang. "Secure reversible image data hiding over encrypted domain via key modulation." IEEE transactions on circuits and systems for video technology 26, no. 3 (2016): 441-452.

[2] Zhang, Xinpeng, Jing Long, Zichi Wang, and Hang Cheng. "Lossless and reversible data hiding in encrypted images with public-key cryptography." IEEE Transactions on Circuits and Systems for Video Technology 26, no. 9 (2016): 1622-1631.

[3] Dragoi, Ioan Catalin, Henri-George Coanda, and Dinu Coltuc. "Improved reversible data hiding in encrypted images based on reserving room after encryption and pixel prediction." In 2017 25th European Signal Processing Conference (EUSIPCO), pp. 2186-2190. IEEE, 2017.

[4] Yi, Shuang, and Yicong Zhou. "Binary-block embedding for reversible data hiding in encrypted images." Signal Processing133 (2017): 40-51.

[5] Cao, Xiaochun, Ling Du, Xingxing Wei, Dan Meng, and Xiaojie Guo. "High capacity reversible data hiding in encrypted images by patch-level sparse representation." IEEE transactions on cybernetics 46, no. 5 (2016): 1132-1143.

[6] Chuman, Tatsuya, Kenta Kurihara, and Hitoshi Kiya. "On the security of block scrambling-based etc systems against extended jigsaw puzzle solver attacks." IEICE TRANSACTIONS on Information and Systems 101, no. 1 (2018): 37-44.

[7] Kurihara, Kenta, Masanori Kikuchi, Shoko Imaizumi, Sayaka Shiota, and Hitoshi Kiya. "An encryption-then-compression system for jpeg/motion jpeg standard." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 98, no. 11 (2015): 2238-2245.

[8] Chuman, Tatsuya, Kenta Iida, and Hitoshi Kiya. "Image manipulation on social media for encryption-then-compression systems." In 2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), pp. 858-863. IEEE, 2017.

[9] Kobayashi, Hiroyuki, and Hitoshi Kiya. "Bitstream-Based JPEG Image Encryption with File-Size Preserving." In 2018 IEEE 7th Global Conference on Consumer Electronics (GCCE), pp. 384-387. IEEE, 2018.

[10] Qian, Zhenxing, Hang Zhou, Xinpeng Zhang, and Weiming Zhang. "Separable reversible data hiding in encrypted JPEG bitstreams." IEEE Transactions on Dependable and Secure Computing (2016).

[11] Unethical Network Attack Detection and Prevention using Fuzzy based Decision System in Mobile Ad-hoc Networks. R.Thanuja,J Electr Eng Technol.2018; 13(5): 2086-2098. http://doi.org/10.5370/JEET.2018.13.5.2086