International Journal of Technology Engineering Arts Mathematics Science
Vol. 1, Iss. 1, January- June 2021, pp. 24~27

Image based steganography using cryptography

Anuja Phapale [1], Rijil Daniel [2], Pranav Deshmukh[3], Dhanesh Lunkad[4], Yogesh Thadani[5]

[1, 2, 3, 4, 5] Information Technology department, AISSMSIOIT, Maharashtra, India

Corresponding Author: Yogesh Thadani (ythadani36@gmail.com)

Article Information

Article history:

Received April 19, 2021
Revised April 27, 2021
Accepted April 27, 2021

ABSTRACT

In the world of increasing usage of the internet, data security plays an important role in achieving confidentiality, authentication, and integrity for secure communication. Cryptography and Steganography is the method to achieve data security through which information is protected and only the intended person can read the information. In this paper, a technique is proposed where Steganography and Cryptography are used in a combined manner for securing the data. In which the LSB method is used for embedding and extracting the data from the image. A symmetric cryptographic algorithm used to encrypt the data is done by using Armstrong numbers before embedding the data into the image. A key is generated using Armstrong numbers and any specified string and the same key generated is used for encrypting and decrypting the data.

KEYWORDS: Steganography, cryptography, encryption, decryption.

1. INTRODUCTION

Now-a-days, the data is considered as very important asset and securing the data is very much needed. The data must be protected while communication as well as when data is stored in storage disks, so that only intended person able to read and process it. Steganography is one of the techniques used for securing the information. Steganography is the technique of hiding secret data within a non-secret, file or message in order to avoid detection the secret data is then extracted at its destination. In Steganography technique, data is hidden into any object like in Image, Video, Text file, etc. The most popular technique used is Image Steganography [11].

In Image Steganography, there are many algorithms used, the most common algorithm is LSB algorithm. In LSB technique, a LSB bit of each RGB colour band container is manipulated by inserting a bit of data to be hidden. The image created is called stego-image which is used as object for securely communicating. There many other techniques available for the image steganography, like **Discrete Wavelet Transform (DWT)** and **Integer Wavelet Transform (IWT)** [8]. The stego-image created cannot be easily detectable by the humans so it one of very secure manner for communication.

Cryptography is another technique in which it is a study of techniques for making communication secure over internet. Cryptography is very much necessary over medium like internet for secure communication.

In Cryptography, the main primary functions to be achieved are Confidentiality, Authentication, Integrity, Non-repudiation, Key-exchange. In cryptography, the data is encrypted at sender side using key and decrypted at receiver side. The data encrypted is not readable by human. In cryptography many algorithms are present, this algorithmic basically divided into three types: Symmetric encryption, Asymmetric encryption and Hash function.

Symmetric key encryption is also known as secret key encryption where same key is used for encrypting and decrypting the data. This is the most basic encryption method and the problem with this method is distribution of the key. Ex: AES and DES algorithm are the examples of symmetric key encryption algorithm.

Asymmetric key encryption is also known as public key encryption where different key is used for encrypting and decrypting the data. This technique is widely used method due to many advantages. The popular algorithms are RSA algorithm.

Hash functions are encryption algorithm that is used to ensure the integrity of the message by hashing the message means encrypting the data which cannot be decrypted by any means. The popular algorithms are SHA, MD5.

2.RELATED STUDIES

Several sources were used, to study about related methodologies and theory for proposed system. Most related and important points regarding proposed method are mentioned below. LSB method is one of the most popular methods in Steganography. Some of the methods proposes algorithm that hides the bit format of the secret data (data to be hidden). In least significant bits of the cover image to form the stego material [1], [8].

When it comes to using steganography and cryptography in a combined manner, several methods are introduced. Most common way is encrypting secret data, and then hiding it in a cover material. In some methods data to be secured is compressed first and then encrypted [7]. Steganography Methods can be reversible and irreversible. Several techniques does not get original cover data back, i.e. in image processing original cover image is lost after extraction of data. While in some techniques, original cover data is also obtained [6], [15]. Several techniques have drawbacks like image distortion. These techniques focus on embedding part more than extracting part of algorithm.

In some combined methods of Steganography and cryptography, processing time is more. While some methods have less quality of security.

3.PROPOSED METHOD

As discussed earlier, main aim is to hide the secret data into the vessel image and to make such provisions that its detection is not easily possible.

So in order to achieve this, proposed system introduces method using an encryption technique which is actually based on Armstrong numbers to encrypt the secret data and then to embed the data so if by any means someone will be able to crack the embedding pattern then also recovery of secret data becomes difficult. This provision makes the system more secure and reliable.

Module 1: Embedding along with encryption

Part 1.1: Encryption

STEPS: This process is based on XOR key generation using Armstrong numbers.

1. 4 Armstrong numbers are taken.
2. Then in the next step input value is taken and by combining that input with the Armstrong number, a XOR key is generated.
3. Then 3 matrices each one for r,g,b respectively, are considered.
4. The size of the matrix is 16*16 as the total number of the colors (encrypted data) that can be formed are in range 0 to 255.
5. Then level 1 encryption is performed by xoring a byte (to encrypt) with the byte of the XOR key in a circular manner.
6. Then a special key is generated by the XOR key which further helps in Encryption (level 2 encryption) of the data using a mathematical formula in the corresponding r,g,b matrices.

Part 1.2: Embedding the encrypted data

STEPS:

1. The first step in any image processing technique is that when some changes in the image are supposed to be made, it should be loaded into the main memory.
2. Then the pixel bands (Red, Green and blue bands) for that particular loaded image are extracted.
3. The secret data that is the data which is encrypted above is taken.
4. Then the single byte of data from the data is retrieved.
5. Then the data is split according to the Embedding method.
6. Previously the bands which were extracted are now inserted with the split data above.
7. Accordingly all the bytes are filled into the particular pixel bands of the image.
8. This process is basically carried on the sender side and the image which is being built during the process (stego image) is passed onto the receiver side and then at the receiver side the Extraction process continues.

Module 2: Extraction along with decryption

Part 1.1: Extraction

STEPS:

1) First the stego image is loaded into the main memory.
2) Then the pixels are retrieved from the image.
3) The bands(r,g,b) are extracted from the pixels.
4) By using the sequence in the Embedding technique, bits are extracted and again combined together.
5) In this way the secret data is extracted.

Part 1.2: Decrypting the secret data

STEPS:

1) A byte to be decrypted is retrieved
2) Using this byte, the row and column with the help of the value generated by the mathematical formula for decryption (level 2 decryption) are retrieved.
3) Then the value of the row and column are combined and that is the encrypted data itself.
4) Then level 1 decryption is performed by xoring the above encrypted data with XOR key in a circular manner.
5) Finally the secret data is obtained.

4.RESULTS

The proposed technique was performed for various file formats such as image, text, video etc. after applying technique on each format, PSNR and MSE was calculated. MSE (mean square error) represents deviation between original image and stego image as given in Eq. 1.

$$MSE = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}\left(I_{xy} - I'_{xy}\right)^2 \quad (1)$$

While PSNR (Peak Signal-to-Noise Ratio) tells us about noise in the image. Higher the PSNR as given in Eq. 2, higher is the quality of an image.

$$PSNR = 20 \times log_{10}\left(\frac{255}{MSE^2}\right) \quad (2)$$

According to results obtained, proposed method shows good quality in image processing.

5.FUTURE DIRECTIONS

LSB methods must be updated as more powerful steganalysis techniques are being created by experts. Work can be done regarding size of stego image for specific formats.

Existing Steganography and cryptography methods will be modified accordingly. But nowadays digital data is getting formed on a large manner. So, in the near future, crucial use of Steganography and cryptography techniques will be in digital data area.

Various machine learning techniques are being introduced as well. Large and useful training sets can be major advantage for such techniques. Among various Steganography and cryptography methods, appropriate method should be selected to get better result.

6.CONCLUSION

A system is developed to hide the data into an image by combining two technologies like Steganography and Cryptography and therefore achieving its benefits. Thus, two layers of security are established which makes system more powerful according to security purposes. System can work with various kinds of data or information (Text, image, audio, and video). The main goal of system is to enhance capacity to hide the information and to increase the quality of stego image.

REFERENCES

[1] WeiqiLuo, Member, IEEE, Fangjun Huang, Member, IEEE, and Jiwu Huang, Senior Member, IEEE (2010) "Edge Adaptive Image Steganography Based on LSB"

[2] "Steganalysis based on the entropy distribution of the image and identifying the method used for encoding" IEEE paper (2010)

[3] Xiang Zhang, FeiPeng, IEEE Member, and Min Long (2018) "Robust Coverless Image Steganography based on DCT and LDA"

[4] Nien-ching Huang, Meng-tsan Li, Chung-ming Wang (2009), "Toward optimal embedding capacity for permutation steganography"

[5] C.-H. Yang, C.-Y.Weng, H.-K.Tso, S.-J.Wang, "A data hiding scheme using the varieties of pixel-value differencing in multimedia images", J. Syst. Softw. (2011)

[6] K. UpendraRaju and N. AmuthaPrabha, " review of reversible steganography" FEBRUARY 2018 ISSN 1819-6608 ARPN Journal of Engineering and Applied Sciences.

[7] PratikshaSethi, V.Kapoor, "A Secured System for Information Hiding in Image Steganography using Genetic Algorithm and Cryptography", International Journal of Computer Applications, June 2016

[8] E.Emad, A.Safey, ARefaat, Z.Osama, E.Sayed, E.Mohamed. "A secure image steganography algorithm based on least significant bit and integer wavelet transform", Journal of Systems Engineering and Electronics, 2018

Table 1. Results of Proposed Methodology

Cover image	Secret data	Stego image	Extracted data	MSE	PSNR
				0.870	48.735
	SecretVideo.mp4		SecretVideo.mp4	0.435	51.743
	Secret text data		Secret text data	0.951	48.346

[9] X. Liao, Q. yan Wen, J. Zhang, "A Steganography method for digital images with four-pixel differencing and modified LSB substitution", J.Vis.Commun.Image Represent.22 (2011)1–8.
[10] Dr EktaWalia, Payal Jain and Navdeep. "An analysis of LSB & DCT based Steganography."
[11] Mansi S. Subhedara,∗, Vijay H. Mankar "Current status and key issues in image steganography: A survey", ELSEVIER
[12] VinitAghamTareekPattewar "A Novel Approach Towards Separable Reversible Data Hiding Technique", International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) 2014
[13]J. Xu, A.H. Sung, P. Shi, Q. Liu, "JPEG compression immune steganography using wavelet transform", Proc. of the International Conference on Information Technology: Coding and Computing, ITCC'04, vol. 2.
[14]G. Liu, W. Liu, Y. Dai, S. Lian, "Adaptive steganography based on block complexity and matrix embedding", Multimedia Syst. (2013) 1–12.
[15] s.chakraborty,anandjalal,charulbhatnagar, "Secret image using grayscale payload decomposition and irreversible image steganography", Journal of information security and applications,2013
[16]Wien Hong, Tung-Shou Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism", J. Vis. Commun. Image R. 22 (2011).
[17] s.pavithradeepa, s. kannimuthu, v. keerthika "security using Colours and Armstrong numbers", proceedings of the national conference on innovations in emerging technology, 2011
[18] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, 2010.
[19] S.K. Muttoo, S. Kumar, "A multilayered secure, robust and high capacity image steganographic algorithm", World Comput. Sci. Inform. Technol. J., 1, 239–246.
[20] Bin Li, Student Member, IEEE, Yanmei Fang, and Jiwu Huang, "Steganalysis of Multiple-Base Notational System Steganography", IEEE (2008)