Steganography and Steganalysis through XMP

Brijal Patel
U and P U Patel Department of Computer Engineering,
Chandubhai S. Patel Institute of Technology,
Charotar University of Science and Technology,
CHARUSAT, Changa, Gujrat, India

Ritesh Patel
U and P U Patel Department of Computer Engineering,
Chandubhai S. Patel Institute of Technology,
Charotar University of Science and Technology,
CHARUSAT, Changa, Gujrat, India

ABSTRACT

Steganography and cryptography are two different techniques for hide the secret data. If provide the dual data security so using the combination of both techniques such that steganography and cryptography. The cover image is encrypted through the Advanced Encryption Standard (AES) encryption with CBC mode. Encrypted data (secret data) can be hide using the Extensible Metadata Method (XMP) is performed on to the cover image. The cryptography algorithm Encrypt data with the help of a key which can be use for the authenticate purpose. Only an authenticate user can be decrypt the secret data because of the key must be same if not then data will not be decrypted. The combination of the both these algorithm will provide huge amount of security, robustness, integrity and capacity of embedding the data.

Keywords

Steganography, Cryptography, AES Encryption Standard, Extensible Metadata Platform

1. INTRODUCTION

Since the growth of usage of the internet in the world security is becoming a most important concern for internet users. So make internet a safe environment for all users. A lot of techniques and algorithms be developed but the intruder be sharply toward hack the data. Just before maintain privacy of information has been changed into a significant issue as well as the stegnography propose an authentic solution for such a problem. Steganography is the techniques for embedding the secrecy data into the cover medium such that only the authenticated receiver will knows its existences. Steganography has a medium like image, audio and video to hide some data inside it. Stegnography need a medium similar to image, audio and video toward hide several data within it. Cryptography is the process of protecting the information and secure communication technique. It is the techniques of encryption and decryption using such kind of cryptographic algorithms. The cryptographic AES mechanisms will be using for encryption and decryption of the secret information and also using CBC mode. The secret message will be encrypted using the key and then this secret message will be decrypted using the same key. The encrypted secret data will hide into the cover image based on the XMP.

"Steganalysisis the study of detecting messages hidden using steganography. This is analogous to cryptanalysis applied to cryptography." The aim of steganlysis be toward recognize assumed information streams, establish whether or not they contain hidden message determined keen on them, and if probable improve the hidden information. Some challenges of this are imagine information torrent, such as a indication or a file, might or cannot have hidden data encoded keen on them, the secret data, but some,mayareencrypted previous to inserted keen on the indicator or file,a number of the imagine indicate or file might contain noise or impertinent knowledge encoded keen on them.

XMP (Extensible metadata Platform):

"XMP (Extensible Metadata Platform) is a universal metadata format which can be developed by Adobe Systems and standardized by the International Organization for Standardization (ISO). " For several of application, XMP gives a standard format to the processing, creation and interchange of metadata. To embedding XMP information into image, video and document file formats, such as JPEG and PDF it provides the guidelines, without breaking their readability by applications that do not support XMP.

Inside the XMP, information can be contained of a collection of properties. The property is continuously related to selected thing stated as the source; that is the properties are about the resource. The resource would be involved:

- A file includes easy documents like JPEG (Joint Photographic expert Group) pictures, this or a lot of complicated files like whole PDF documents.
- A significant portion of a file, as determined by the file structure and also the applications that method it. For instance a picture foreign into a PDF file may be a significant entity that might have associated information. However, a spread of pages isn't significant, as a result of there's no specific PDF structure that corresponds to that. In general XMP isn't designed to be used with terribly fine-grained subcomponents, like words or characters.

Stereoscopic is mostly used for create a 3D image and the images is the integration of the left image and right image one for left eye and one for right eye (i.e., stereo pair) respectively. The left image and right image both resolutions must be same. To recognize the common gap range between right and left images a basic Stereo Matching algorithm can apply which is develop the secure Virtual Reality viewable stereoscopic image. Virtual Reality (VR) is the one of the most important application that uses the stereoscopic image. The popular example is Google Cardboard.

Stegnography is used by many applications such as medical, military, online banking, online transaction, financial and commercial purpose. It is also be the used by the terrorist for convert communication which is possible for expose our national security.

2. RELATED WORK

In [1] To provide the security of data normally people use either stegnography or cryptography but in this included the both technique stegnography and cryptography for provide the data security better. For this system the steganographic techniques use the spatial domain techniques which are the LSB method (Least significant bit). The LSB technique is use for hide the secret message into the cover image The researcher embedded the one least significant bit or extra as of secret data into the cover image in the LSB. The most significant bit and the intermediate significant bit methods are using some researchers because of enhancement of the security. LSB method is uses the image format like .bmp, .jpg. Discrete Wavelength transform method is suitable for the digital image. DWT is mainly suitable for compression and embedding, for compression it replacing the DCT (Discrete Cosine transform) and DFT (Discrete Fourier transform). Apply the cryptography method for higher security of the secret data. The Vigenere Cipher can encrypt and decrypt the secret message. Sender sends the message to the receiver that time the message can be encrypted using the vigenere cipher and then the encrypted message hide into the cover image with the use of the LSB method. In the receiver side the secret message can be decrypted using the vigenere cipher and receiver gets the original data. This paper proposed the techniques which can protected the various type of image format in future such that .bmp, .jpeg. Transform domain techniques such that DFT and DCT are suitable for extended the image of the different format.

In [2] The most accepted algorithms for steganography are investigated intended for the mechanism. So as to estimate the schedule of assorted method for image steganography, there are necessary to outline necessary to outline some suitable analysis criteria supported the standard of the aim. Furthermore, putting in exact analysis guide line helps in resulting in development of newer algorithms and conjointly to expand the performance of the present algorithms. There are 3 common needs specifically stages of security, aptitude and corporal property could also be used as estimate criteria for the image steganography and algorithms. A side from these we have a tendency to conjointly take into absorption parameters like domain of embedding, image arrangement and time impediment. Wherever a number of the power of future study within the domain of digital media steganography is precisely connect the security and therefore the ability, wherever the event of Algorithms supported objective in images and just beginning the steganographic algorithms. Safety and skill trade-off is a very imperative conclusion in steganography. A mathematical representation correlates the two fundamental

necessities for a steganographic system is a quarter of activated interest for reasons like optimizing concert of embedding algorithms in future, improvement of algorithms offer which each high security and skill beside higher steganalysis and may offer mathematical source for optimizing active algorithms for achievement. DWT remodel to select out the upper frequency sub band from a image in RGB format and once show for skin tone pixels in them employing a skin tone display method and insert into them. Once the approach has some restrictions like selective embedding into human skin tone space offer security though limits capability, overwriting of bits principle alteration within the useful mathematics honour of the photographs and may therefore be detected by Steganalysis. There could also be definite modification that may be implied upon the needed technique similar to choosing color planes with reasonably low donation to skin tone like from blue and innocent from the RGB color plane, and their think about the human skin-tone is a smaller quantity and therefore produces fewer deformation. Because it is shown in, shorter overwriting of bits imply lesser within the algebraically properties of the image, so it is important to accept out algorithms that engraft knowledge with small bit replacements. Developing the steganographic algorithms the possible improvements are cumulative embedding efficiency, decreasing embedding prevention and choosing alternate colour spaces.

In [3] Steganography and Cryptography are two method of diverse knowledge activity. The functioning of is Steganography puts a covering onto the messages with another range of digital media and other is Cryptography on the reverse hand perform the cryptography of the message. The combination of these method, wherever the data is 1st hidden into some selection of image exploitation least significant bit (LSB) activity technique so cryptography exploitation Advanced Encryption Standard (AES) technique. AES could be a block cipher technique with a data block length of 128 bits. AES accept for three completely changed key length sizes like 128 bits, 192 bits, 256 bits. AES is relying ahead the key length fully different numbers of operating round are needed for any AES algorithmic program. The 128 bit knowledge is dividing into sixteen Bytes. These bytes are summarize to a 4×4 array is termed because the position and every one process of AES are performed going on this state. Once the key length is a lesser amount than the necessary range of bits used for a certain AES algorithmic program after that it should be complete by zero cushioning method of desired length. However, if the necessary key length is more than the data bits as in AES-192, AES-256 before the key addition algorithmic program is engaged to expand the key length. The performance of steganography and Cryptography commonly were able with text and images, however this method are often advance entire to audio, and video similarly like this increase up the security within the audio and video process.

3. LIMITATION OF CURRENT WORK

The limitation of the current work is the steganography done for only .jpeg image.

4. EVALUATING ALGORITHM

4.1 Algorithm:

For embedding method

Input: Cover image, Secret message, secret key

Output: “Stego image”

Step 1: Select cover image which can hide a inside data

Step 2: Extract the pixels of the cover image

Step 3: Choose secret message and encrypt it using AES with CBC mode

Step 4: Provide the secret key for encryption of secret message

Step 5: Embedded the encrypted message into cover image

For Extraction method

Input: Stego image, Secret key

Output: Secret message file

Step 1: Browse Stego image file

Step 2: Decrypt the stego image using the same key

Step 3: Retrieve the secret message file

Extensible Metadata Platform

Adobe's Extensible Metadata Platform (XMP) is a file labelling technology that lets you embed metadata into files themselves during the content creation process. XMP metadata travels with the file, and can be embedded in many common file formats including PDF, TIFF, and JPEG. Metadata properties are grouped in schemas. Each schema is identified by a unique namespace URI and holds an arbitrary number of properties.

Cardboard camera stores elements of a VR photo as metadata in a JPEG file. The container image acts as the left eye image, while the right eye and an (optional) audio file are stored as base64-encoded binary blobs in the image's metadata. This allows the photo to be backwards-compatible with ordinary image viewers, which recognize the container (left eye) image and display it as a 2D panoramic photo. Metadata is stored using Adobe's XMP standard, and is further described in their specification. The metadata tag GPano stored in the standard format of the XMP which can be used to explain the imaging form of photo.

Using XMP image is hiding into another image through the image header. Some XMP metadata tags are describe below.

- can_put_xmp(xmp_obj) If a given XMPMeta object has written in to the file this tags will determines it.
- get_xmp()Get XMP header from file.
- put_xmp(xmp_obj)The XMPMeta object will be write in to the file.
- close_file(close_flags=0)After use file will be closed. Until this tags have been called XMP will not written to file.

5. RESULT AND DISCUSSION

Fig.1 is main GUI window which appears on home screen it contains the encryption and decryption of the image and stegnography on image.

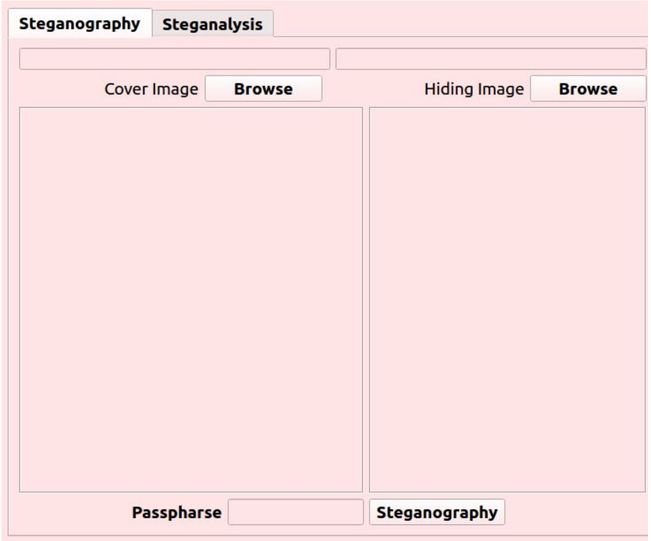
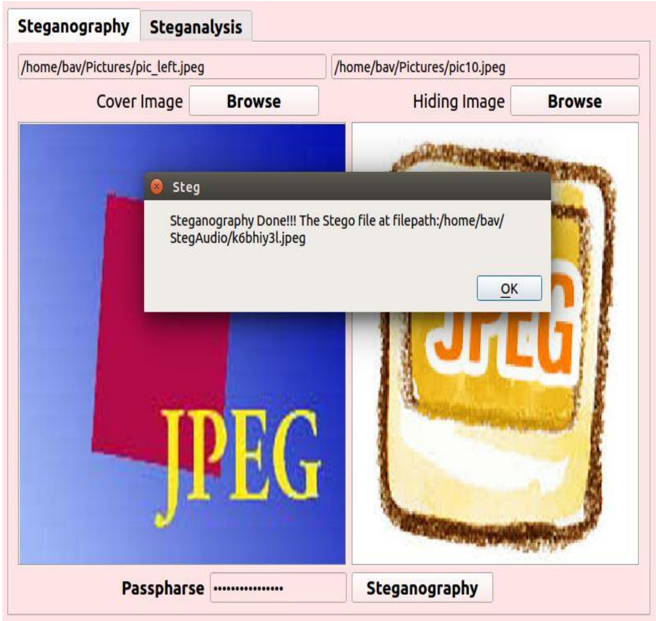


Fig.1: Opening GUI

Fig.2 is the steganography of the encrypted image. The secret image is encrypted with the secret key. Encrypted image is encoding with base64. The encoded data have embedding into the image. With the use of the Extensible Metadata Platform (XMP) encrypted image will hide into the cover image.


/home/bav/Pictures/pic_left.jpeg

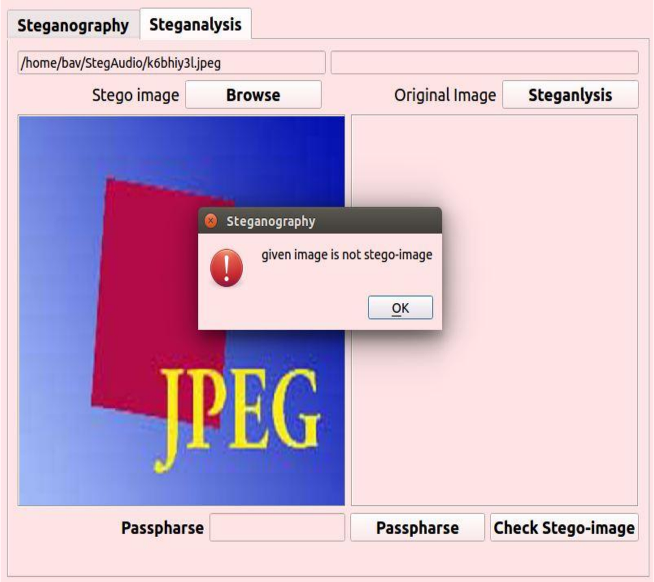
/home/bav/Pictures/pic10.jpeg

Steg

Steganography Done!!! The Stego file at filepath:/home/bav/StegAudio/k6bhiy3l.jpeg

Fig.2 Steganography of the encrypted image

Fig.3 identify the secret image will be existence in cover image or not. This image called Stego-image. This process is known as a steganalysis.

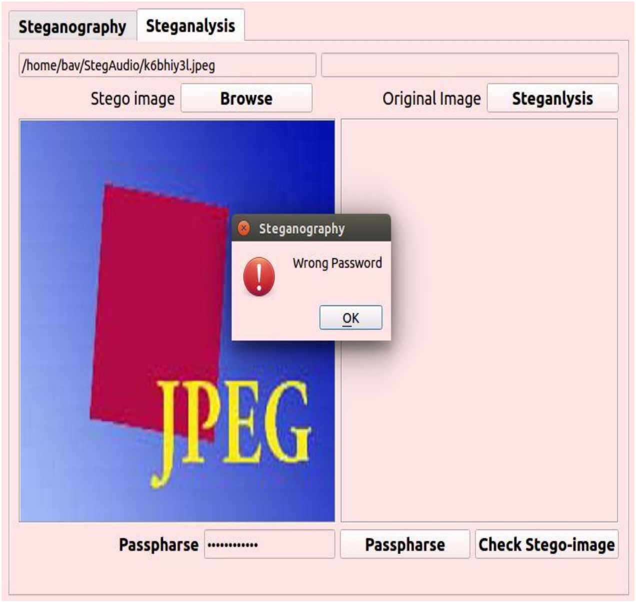

/home/bav/StegAudio/k6bhiy3l.jpeg

Steganography

given image is not stego-image

Fig.3 Image Steganalysis

Fig.4 is for the data authentication. The data authentication is done by the Advanced Encryption Standard (AES) with CBC mode. For encryption and decryption the secret key must be same so only the authenticate user can be decrypt the secret image.



/home/bav/StegAudio/k6bhiy3l.jpeg

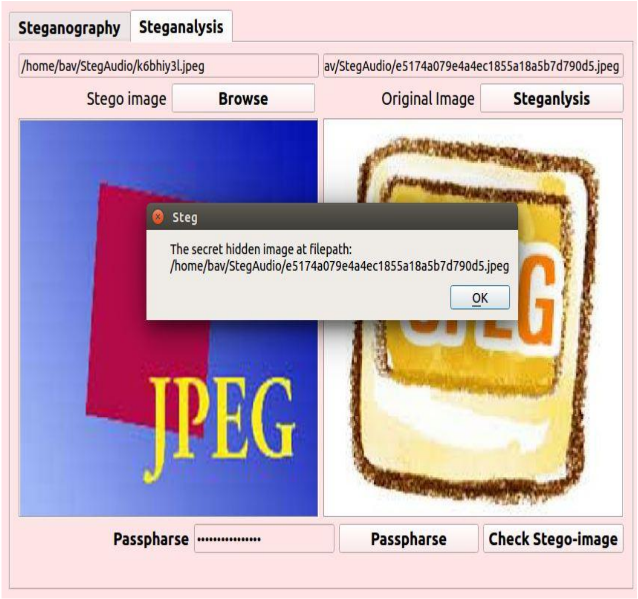
Steganography

Wrong Password

Passpharse ••••••••••

Fig.4 Data Authentication

Fig.5 is the decryption of the image. Decode the image from the encrypted image using base64 decoding. Decrypt the image with the use of the same (for encryption) secret key. With the use of the Extensible Metadata Platform (XMP) decrypted image will extracted into the cover image.



/home/bav/StegAudio/k6bhiy3l.jpeg

av/StegAudio/e5174a079e4a4ec1855a18a5b7d790d5.jpeg

Steg

The secret hidden image at filepath:
/home/bav/StegAudio/e5174a079e4a4ec1855a18a5b7d790d5.jpeg

Passpharse ••••••••••••••

Fig.5 Decryption of the image

6. CONCLUSION AND FUTURE WORK

To provide security the researcher use either cryptography or stegnography. In the proposed system, Steganographic method uses the Extensible Metadata Platform (XMP) that is the Adobe metadata method which uses the format like .jpeg. In this, we can also contains the cryptography algorithm to provide more security such that Advanced Encryption System (AES) with Cipher Block Change (CBC) mode.

Here the XMP can hide the data into the cover image only for .jpeg media type. Now going forward the image media type is .bmp, .png etc. And also the stegnography method can hide the audio and video file using the Extensible Metadata Platform (XMP).

7. REFERENCES

[1] Prashanti, G., B. V. Jyothirmai, and K. Sai Chandana. "Data confidentiality using steganography and cryptographic techniques." *2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*. IEEE, 2017.

[2] Roy, Ratnakirti, et al. "Evaluating image steganography techniques: Future research challenges." *2013 International Conference on Computing, Management and Telecommunications (ComManTel)*. IEEE, 2013.

[3] Patel, Farah R., and A. N. Cheeran. "Performance Evaluation of Steganography and AES encryption based on different formats of the Image." *Performance Evaluation* 4.5 (2015).

[4] Rote, Geeta D., and A. M. Patil. "Steganography with Cryptography Technique for Data Hiding." *International Journal of Science and Research (IJSR)* (2013).

[5] Chanu, Yambem Jina, Kh Manglem Singh, and Themrichon Tuithung. "Image steganography and steganalysis: A survey." *International Journal of Computer Applications* 52.2 (2012).

[6] Abikoye, O. C., K. S. Adewole, and A. J. Oladipupo. "Efficient data hiding system using cryptography and steganography." (2012).

[7] Varsha, Rajender S. "Data Hiding Using Steganography and Cryptography." *International Journal of Computer Science and Mobile Computing* 4.4 (2015): 802-805.

[8] Wu, Hao-tian, and Jiwu Huang. "Secure JPEG steganography by LSB+ matching and multi-band embedding." *2011 18th IEEE International Conference on Image Processing*. IEEE, 2011.

[9] Behera, Sanjeeb Kumar, and Minati Mishra. "Steganography--A Game of Hide and Seek in Information Communication." *arXiv preprint arXiv:1604.00493* (2016).

[10] Ball, Alex, and Mansur Darlington. "Briefing Paper: The Adobe eXtensible Metadata Platform (XMP)." *UKOLN research organization* (2007).

[11] Kaur, Navneet, and Sunny Behal. "A Survey on various types of Steganography and Analysis of Hiding Techniques." *International journal of engineering trends and technology* 11.8 (2014): 388-392.

[12] Seyyedi, Seyyed Amin, and Rauf Kh Sadykhov. "Digital Image Steganography Concept and Evaluation." *International Journal of Computer Applications* 66.5 (2013).

[13] Gasiorowski-Denis, Elizabeth. "Adobe Extensible Metadata Platform (XMP) becomes an ISO standard." (2016).

[14] Park, Hyung Ju, Kwang Yeol Park, and Dong Hwan Har. "Identification of digital images with the Adobe™ eXtensible Metadata Platform." *Archiving Conference*. Vol. 2008. No. 1. Society for Imaging Science and Technology, 2008.

[15] Ge, Huayong, Mingsheng Huang, and Qian Wang. "Steganography and steganalysis based on digital image." *2011 4th International Congress on Image and Signal Processing*. Vol. 1. IEEE, 2011.