Obscuration of Chat using Steganography and AES on GIF image format

Himanshu Pise*, Vidhi Kala, Saurabh Somkuwar, Nidhi Dev, Prof. Prajwali Korde
Department of Information Technology
International Institute of Information Technology, Hinjawadi-Pune 411057
(Savitribai Phule Pune University)

Abstract: - **The objective of this project is to obscure/hide and encrypt textual chat data into a well-known image format Graphics Interchange Format commonly known as GIF using the concept of steganography. Steganography can be achieved by applying the LSB or Least Significant Bit Algorithm. The textual data that is used for communication in social media messenger services can be encrypted by symmetric encryption algorithm which is known as Advanced encryption standard. GIF's are currently used massively in social media messaging services and the work could be included in most of the social media instant messaging chat APIs which are built and based upon the idea of security fundamentals.**

Keywords— Steganography, Encryption, LSB Algorithm, AES Algorithm, Symmetric Encryption, GIF, BMP, Cryptography

I. INTRODUCTION

The internet has become an integral part of today's generation of individuals, from communicating through instant messages and emails to banking. It has touched every aspect of life. With the growing use of the internet protecting important information has become a necessity. Instant messaging has been a boon in today's society where everyone is connected via numerous internet apps. GIF or graphic interchange format has widened its popularity since the introduction to stickers and emoticons commonly called as emoji(s). Numerous APIs that have been built to index the database of GIFs have now collaborated with popular instant messaging apps. Widely used and popular of them are GIPHY and TENOR, GIF database indexes.

Steganography is the practice of concealing/hiding/obscuring a file, message, image, or video within another file, message, image, or video. The idea of hiding textual chat data in GIFs may well be used to transfer messages online to the intended recipient and also secure it with popular encryption standards of symmetric encryption.

II. PROPOSED TECHNIQUE

Since the project requires the insight of what it is about Fig-1 depicts the working of project and how GIF will work thereon.

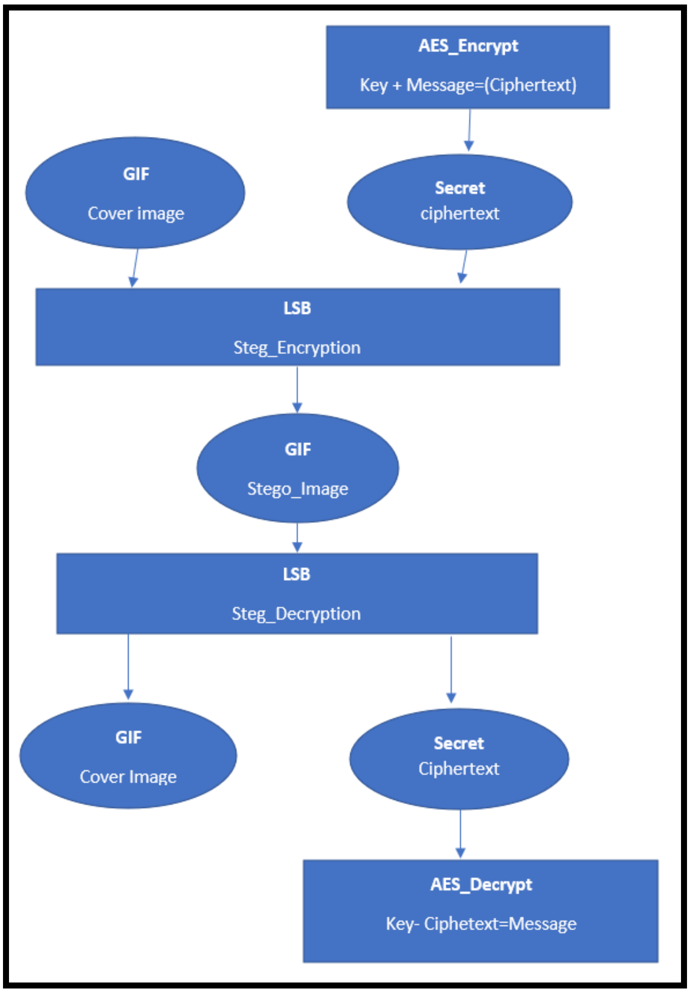


Fig-1: Working of project

A. *Converting GIFs into multiple BMPs*

The format supports up to eight bits per pixel for each image, allowing one image to reference its palette of up to 256 different colours chosen from the 24-bit RGB colour space. It also supports animations and allows a separate palette of up to 256 colours for every frame. These palette limitations make GIF less suitable for reproducing colour photographs and other images with colour gradients, but it's well-suited for fewer complicated images like graphics or logos with solid areas of colour. Unlike video, the GIF file format doesn't support audio. They often appear grainy when used on high-quality images since they support up to 256 colours only. The GIFs need to be converted into BMP or Bitmap image format since the GIFs are a collection of BMPs. The LSB algorithm works well with BMPs.

Any image file format can be used as the cover image here a GIF. However, the GIF image was first converted into BMP format before anything can be done on it. After the whole process, the image was converted back to its original format. BMP format is preferred because it

is supported by the C# and libraries in Visual Studio; it applies lossless file compression method and allows

for easy interchange and viewing of image data stored on local or remote computer systems. Also, it seems to maintain a high degree of image quality after the message has been embedded

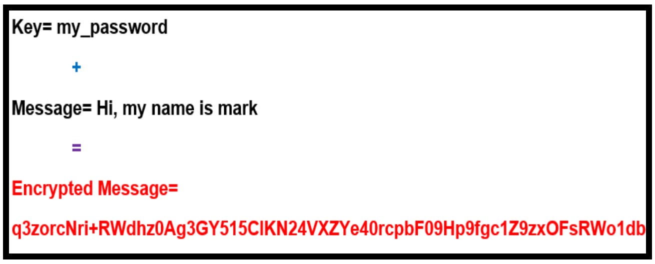
I II III

Fig-2 Bitmaps I, II, III extracted from popular Rotating_Earth.GIF

B. Converting Simple text into encrypted text

The Advanced Encryption Standard or AES, also known by its original name Rijndael, could also be a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the textual message.

This method initializes AES SymmetricAlgorithm and MD5 HashAlgorithm objects. The AES object is used to encrypt the text from the Richtextbox (which first has to be converted to a byte array). The MD5 object is used to create an MD5 hash from the provided password, to be able to use it as a symmetrical key, since the AES algorithm uses a 16-byte encryption key (minimum key size for AES is 128 bit) – this will ensure that we shall get a unique (1:1) 16-byte representation of the user's password.Fig-3 shows the conversion of the simple text into ciphertext.



Key= my_password

+

Message= Hi, my name is mark

=

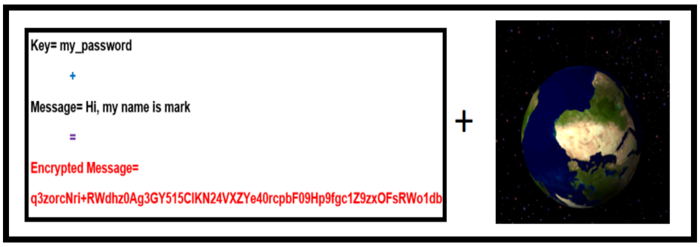
Encrypted Message=

q3zorcNri+RWdhz0Ag3GY515ClKN24VXZYe40rcpbF09Hp9fgc1Z9zxOFsRWo1db

Fig-3 AES hashed ciphertext message

C. Merging the Bitmap Image with encrypted text

The bitmap image can be encrypted with the textual ciphertext. This is implemented by steganography tool which includes the text file or message with the bitmap image.



Key= my_password

+

Message= Hi, my name is mark

=

Encrypted Message=

q3zorcNri+RWdhz0Ag3GY515ClKN24VXZYe40rcpbF09Hp9fgc1Z9zxOFsRWo1db

Fig-4 Image with the ciphertext which will be the stego_image

The tool was implemented using simple LSB methods where the last bit of each pixel in the image is manipulated to add the data in it. We chose the LSB algorithm as it is a common algorithm for most of the steganographic operations.

III. RESULTS AND DISCUSSIONS

Once the image is ready in the format of BMP it can be then turned into GIF format by combining many other BMPs to form a GIF. All the bitmap images can be encoded with the textual data once the message is being sent.

After careful observation, of all the below values

MSE

Mean Squared error or MSE is the average of the squares of errors and calculated by

$$MSE=\sum M,N(I1(m,n)-I2(m,n)]2\ /M*N$$

Here the values of M and N are to image and their rows and columns respectively

PSNR

Peak Signal to Noise Ratio or PSNR between the cover image and the steganographic image is calculated by the given equation. A higher PSNR indicates that the quality of the steganographic image is similar to the cover image.

$$PSNR=\log10(R2\ /MSE)$$

Correlation

Correlation, the best-known method, it not only evaluates the degree of closeness between two functions but also determines the extent to which the cover image and the steganographic image are close to each other even after embedding data.

The MSE, PSNR and Correlation values for various image file formats are shown in the Table

Cover Image	**Stego Image**	**MSE**	**PSNR**	**Correlation**
Cover_barbara.bmp	Stego_barbara.bmp	2.18	44.17	0.991
Cover_silhouette.bmp	Cover_silhouette.bmp	3.84	47.4	0.994
Cover_leonardo.gif	Stego_leonardo.gif	3.67	46.1	0.998
Cover_rotatingearth.gif	Stego_roationgearth.gif	3.88	48.3	0.994
Cover_dicetransparency.png	Stego_dicetransparency.png	2.95	43.1	0.998
Cover_logo.png	Stego_logo.png	2.65	46.15	0.997

Table-1: Quality metrics and comparisons between different Image formats

The file formats possessing lowest MSE were recorded in PNG and BMP formats. This shows that PNG can also be specified for steganography and the conversion of GIF to PNG form and vice versa.

CONCLUSION

The technique helps us understand that a message which isn’t encrypted is likely to be tampered or read between the network. The project amplifies the scope that the message is well hidden and also well encrypted inside a GIF image file. Since the encryption is pretty much standard simple attacks won’t allow the text to be read.

Advancing times require advanced methodologies to tackle, convey, send and receive messages online. Increase in cyber threats has impacted popular instant messaging apps vigorously. Including this feature might add an extra layer of stringent security and deny any such intruders.

The scope of the project is not only limited to instant messaging but can also be complied with email and the security-obsessed crowd and/or software tools.

REFERENCES

[1] Roshani Padate, Aamna Patel. : Image Encryption and Decryption using AES Algorithm, International Journal of Electronics & Communication Engineering & Technology, Volume 6 Issue 1 January(2015),pp.(23-29).

[2] Amrita B, Shweta C, Monika S: Hiding Compressed and Encrypted Data by using a Technique of Steganography, International Journal of Engineering Research & Technology, Volume 9 Issue 04 April (2020), pp.333-334.

[3] Solomon O.Akinola, Adebanke A.Olatidoye .: On The Image Quality and Encoding Times Of LSB, MSB and Combined LSB-MSB Steganography Algorithm Using Digital Images, International Journal of Computer Science & Information Technology(IJCSIT), volume 7, Issue 4 August 2015 pp.79-91.

[4] Sultana, S., Khanam, A., Islam, M.R., Nitu, A.M., Uddin, M.P., Afjal, M.I., Rabbi, M.F.: A Modified Filtering Approach of LSB Image Steganography Using Stream Builder along with AES Encryption, HBRP Recent Trends in Information Technology and its Applications, Volume 1 Issue 2, pp. 1-10 (2018).

[5] V.Yamini Priya, K.Priyadharshini, K.Sowndharya .S.Swati, K.Shweta.: Hiding Data in Video Sequences using RC6 Algorithm, International Journal of Computer Science and Mobile Computing, Volume 9, Issue 1 January (2020),pp.144-149.

[6] Sharmin Sultana, Afrida Khanam, Md.Rashedul Islam, Adiba Mahjabin Nitu, Md.Palash Uddin, Masud Ibn Afjal, Md.Fazle Rabbi.: A Modified Filtering Approach of LSB Image Steganography Using Stream Builder along with AES Encryption, HBRP Publication Recent Trends in Information Technology and its Application, Volume 1, Issue 2(2018), pp.1-10

[7] Andika Amirulhaqi, Tito Waluyo Purboyo, Ratna Astuti Nugrahaeni.: Security on GIF Images Using Steganography with LSB Method, Spread Spectrum and the Vignere Cipher, International Journal of Applied Engineering Research ISSN, Volume 12, Issue (2017) pp.13604-13609

[8] Jayanti Bhadra ,A.M Bojamma ,Pradas.C.N ,M.N.Nachappa.:An Insight to Steganography, IJISET - International Journal of Innovative Science, Engineering & Technology, Volume 1, Issue 10, December 2014,pp.29-42

[9] Samruddi Yadav, Prof.Swati Deshpande, Prof.Smita Bansod.: Image Steganography using IWT along with AES Encryption.International Journal of Computer Techniques ,volume 3,Issue 5,sep - Oct 2016,pp 37-43

[10] Nagham Hamid, Abid Yahya, R.Badlishah Ahmad, Osamah M.Al-Qershi.: Image Steganography Techniques: An Overview, International Journal of Computer Science and security(IJCSS), volume 6, Issue 3(2012), pp.168-187