International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Secure Image Transmission using Cipher Block Chaining Mode & Visual Steganography

Manoj Dhande[1], Arjun Mudaliyar[2], Vineeta Pandey[3], Pranali Dalvi[4]

[1]Professor, Department of Computer Engineering, Shah & Anchor Kutchhi Engineering College, Mumbai, India[1]

[2, 3, 4]Students, Department of Computer Engineering, Shah & Anchor Kutchhi Engineering College, Mumbai, India[2]

Abstract: ***With the fast progression of technology in today's information age, data security has become a major concern in terms of data storage and data transmission. Information in any form is not safe in the hands of unauthorized people. Privacy and security of data is of utmost concern nowadays and hence techniques like Cryptography and Steganography are used to overcome these threats. As Cryptography is the technique of encryption of secure data in order to enhance its security and On the other hand, Steganography embeds secret image into a cover media and hides its existence, both these techniques help provide security of data. Neither of them alone is secure enough for sharing information over an unsecure communication channel. In this paper we propose an advanced system of securing data that combines the features of cryptography, steganography along with multimedia data hiding. To enhance the security, we propose the combined concept of visual cryptographic steganography where the secret image will be divided into slices and these slices will be encrypted using Cipher Block Chaining forming a cipher image and then this cipher image will be divided into shares which in turn will be embedded into cover images thus forming stego images. The resultant stego image is then decrypted to recover the original.***

Keywords: Cryptography, Visual steganography, Image encryption, AES, Block cipher encryption

1. Introduction

Due to the rapid advancement in information technology, large number of data is being transmitted every minute over the network. Hence confidentiality and integrity of the data being transmitted need to be preserved. While transmitting information, security related issues should be taken into consideration because hackers may utilize weak links over transmission to hack the information. This gave rise to the use of different cryptographic and steganography schemes in order to encrypt the secret data which helps in retaining its integrity. This paper presents an approach of all the combined concepts as follows:

a) Cryptography

The research which is developed using mathematical methods like security of data, proper user authentication, confidentiality, with respect to information security is called as cryptography. But visual cryptography is a new technique of information security that uses simple algorithm unlike the other traditional cryptography which incorporates complex, computationally intensive algorithms. Visual information of pictures, text etc. is dealt with in order to encrypt in progressive and unexpanded VC algorithm. We have only a few pieces of shares and get an outline of the secret image. This is done by increasing the number of the shares being stacked. These images usually contain private or confidential information so that they should be protected from leakages during transmissions. Recently, many methods have been developed for securing image transmission, for which two mostly used techniques are encryption of image and hiding of data.

b) Cipher Block Chaining Mode:

The CBC mode is about adding XOR each plain block to the cipher block that was previously produced. The result is then encrypted using the cipher algorithm in the usual way. Each subsequent cipher block depends on the previous one. The first plain block is added XOR to a random initialization vector. The vector has the same size as a plain block. Encryption in CBC mode can only be performed by using one thread. Despite this disadvantage, this is a very popular way of using block ciphers, and it is used in many various applications. During decrypting of a cipher block, one should add XOR the output data received from the decryption algorithm to the previous cipher block. Because the receiver knows all the cipher blocks just after obtaining the encrypted message, he can decrypt the message using many threads simultaneously. The encrypted image is a noise image so that no one can obtain the secret image from it unless user has the correct key. However, the encrypted image is not meaningful, which cannot provide additional information before decryption & may arouse an attacker's attention during transmission due to its randomness in form.

c) Steganography

Steganography is the art of hiding the existence of the secret message (data) before sending it to the receiver. Modern ways include hiding secret information in newspaper articles and magazines etc. Multimedia steganography is one of the most recent and secure forms of steganography. It started in 1985 with the advent of the personal computer that applied to classical steganography problems. Visual steganography is the most widely practiced form of steganography and is usually done using image files. It started with concealing messages within the lowest bits of noisy images or sound files. Images in various formats like jpeg have wide color spectrum and hence do not reflect much distortion on embedding data into them. We shall perform steganography on image files and we shall hide the encrypted message into image files in an encrypted format thus achieving a multiple cryptographic system. The most commonly used technique for image steganography is bit insertion where the LSB of a pixel can be modified. Currently there are several techniques of embedding messages using LSB method in steganography.

LSB replacement embeds a message into the cover image by replacing the LSBs of the cover image with message bits to produce stego image. One method increases even pixel values either by one or leaves them unmodified, while odd values are left unchanged or decreased by one.

2. Existing Method

There are various schemes proposed which are related to secure image transmission. In these schemes, the secret image is encrypted in order to retain its confidentiality and integrity. Various cryptography schemes are used to encrypt the secret image which won't allow any unauthorised person to access it. Moreover to enhance the security level, there are various steganography techniques which embeds the secret image into a cover image which also retains the integrity of the secret image.

Mr. Manoj Dhande et al proposed a scheme [1] combining visual steganography and cryptography to transmit a secret image. In this system, the secret image is going through two levels of security. In first level, secret image is encrypted by using a symmetric key based visual cryptography resulting into new cipher image. In second level, cipher image is embedded divided into cover image for secure transmission. In this, the secret image is divided into 16 slices (i.e. 4 rows and 4 columns). After this, the AES Encryption is performed on these slices. The key used for AES encryption for the slices is 128 bits. A cover image is selected and this same image is used to embed all the sixteen slices of the secret image. For AES Decryption, the same encryption process occurs simply in reverse order. The encryption parameters are the input cipher text, the key and the output plaintext should be same as encryption input.

The main drawback with this method was the high amount of bandwidth it required for image transmission. For an image of 16 slices, 16 stego-images will be created and transmitted thereby increasing the bandwidth need 16 times.

To overcome this drawback, we propose a new method that makes effective use of bandwidth and also maintains security at the same time.

3. Proposed Method

As seen above, there is a lot of scope for improvement in the existing method. The security can be further enhanced. The proposed method makes use of the concepts of Image processing. AES encryption, Block cipher cryptography, Visual Steganography. By combining the aforementioned techniques, a more robust way of securing and transmitting images can be implemented.

In this system, AES (Advanced Encryption Standard) algorithm is being used to encrypt the image, Encryption is done by implementing a block cipher method, Visual Steganography is used to hide the image into other cover image. Image is divided into shares before performing steganography add more security to the secret image while transmission through open and unsafe network such as the Internet.

A) Encryption

The secret image is first imported by the sender. Now, the sender inputs a secret key. This key is used to encrypt the image using AES-128 algorithm with the help of CBC (Cipher Block Chaining) method. The encryption is done block by block meaning each block is encrypted separately for the entire image from the very first block through the last block.

The method of encryption is as follows: The first block is encrypted with a key and an initialization vector using the AES-128 algorithm thereby generating a cipher block. Now using this cipher block and the key provided, the next block is encrypted and the subsequent cipher block is generated. This procedure is followed for all the blocks until the last block is encrypted. The output is a block encrypted image (Cipher Image) and this is the first level of encryption and security.

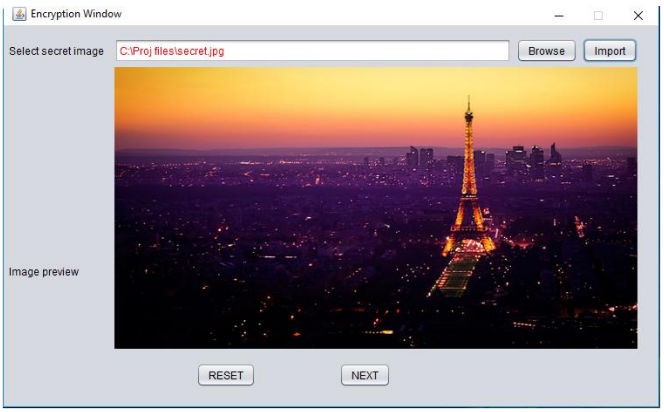

Figure 1: GUI showing the secret image

After this, the output will be given for steganography using the LSB method for image steganography. The image will be divided into 2 shares, and these shares are embedded into other images known as cover images. One share would be embedded into one cover image. Similarly 2 shares would be hidden into 2 cover images. Once the embedded cover images are produced they can be sent to another user over the Internet without worrying about the security of the image. The above can be achieved by sending out the stego-images to the destination via different routes.

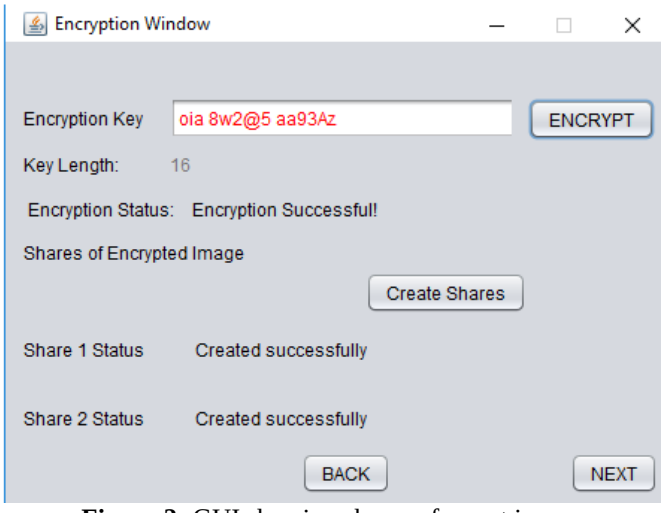

Figure 2: GUI showing shares of secret image

So each stego-image will be following a different path to the intended destination. In this way, even if a hacker gets access to a particular stego-image by exploiting a weak link on the network, he/she won't be able to retrieve the original image. Even in the worst case if the hacker gets access to all the stego-images, still he/she would not be aware of the actual data (shares) hidden in these images as stego-images are just meaningful cover images that wouldn't attract suspicion. Moreover, even if the shares are recovered still the hacker would not be able to retrieve the secret image as the recovered image is still in the encrypted form.

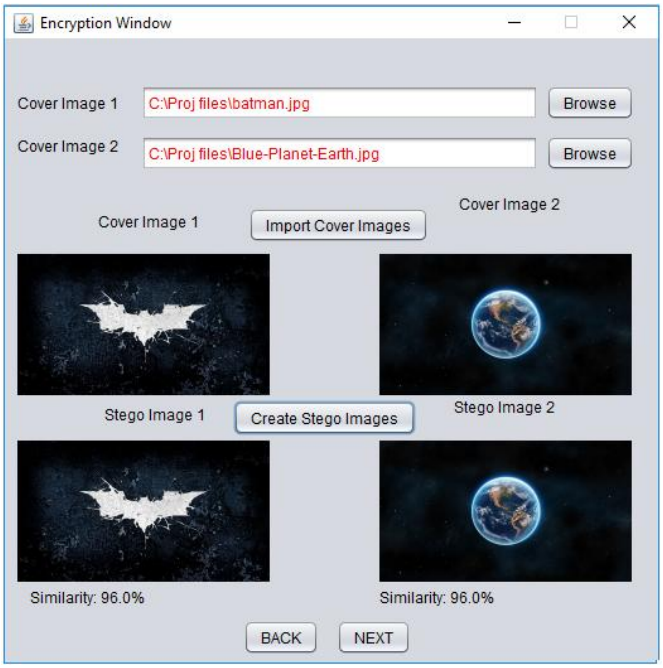

Figure 3: GUI showing the Visual Steganography

B) Decryption

On the receiving end, all the stego-images are received and the user is aware of the key used to encrypt the image as symmetric key cryptography is used. The receiver extracts all the shares from the stego-images and combines them to form a single image. This image is still AES encrypted.

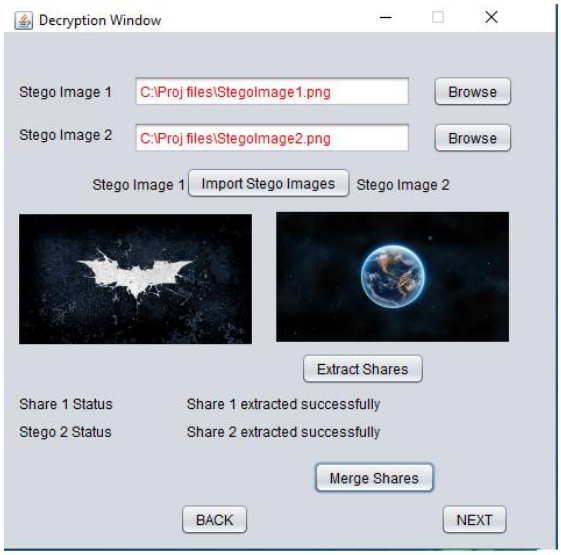

Figure 4: GUI showing the decryption window

Here the reverse process of the above mentioned procedure is used i.e Cipher Block Chaining for decryption.

The first block is decrypted using the decryption key and then the same initialization vector is used to retrieve the first block of the original secret image. The same process follows for the subsequent cipher blocks with the previous cipher block being used instead of the initialization vector and resulting into the corresponding blocks of the secret image. This process is followed until the last block is decrypted thereby finalizing the entire decryption process. The original image is now decrypted and retrieved safely.

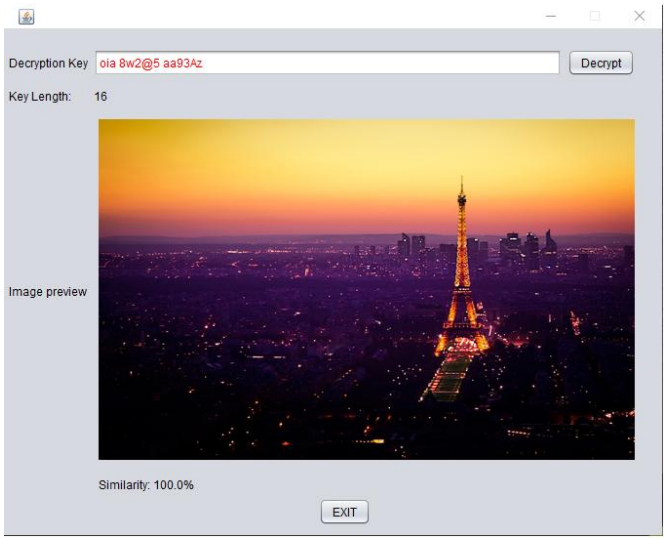

Figure 5: GUI showing the decrypted image

4. Result and Analysis

The image that is recovered after decryption is of the same dimension and size. The quality of the image is not lost at all i.e. the image chosen for encryption and the image retrieved after decryption are digitally same. The method used to compare the images is to compare the corresponding pixels of the images one by one. At the end, the percentage of the number of pixels that is same in both the images is calculated. In our analysis, all the pixels matched giving a cent percent result thereby retrieving the image in its original form with the original size, dimension and quality.

The images were also compared online at the site http://www.fileformat.info/tool/hash.htm. This is a site that calculates the hash of the files using number of hashing algorithms. Both the image files were uploaded and their hashes were calculated. Corresponding hash values were compared for both the images. The hash outputs for the images were same for all the algorithms. This proves that the integrity of the image is maintained. Furthermore, an online hex editor was used to compare the hex data of both the files i.e. the images were compared digitally. The website https://www.onlinehexeditor.com/ is used to obtain the hex data of any file. The secret image and the decrypted image, both were uploaded and their hex value was obtained. When compared, they were totally same further proving that the image is completely retained and the exact image is obtained as it was before encryption.

The following tables show the input images and the results with the time required by images of various size and dimensions:

Test image details:

Sr. no.	Image type	Name	Size(KB)	Dimension	Bits per pixel
1	Secret image	tree.jpg	174	800x450	24
	Cover image 1	batman.jpg	390	1920x1080	24
	Cover image 2	earth.jpg	700	1920x1080	24
2	Secret image	secret.jpg	121	620x349	24
	Cover image 1	prism.png	369	1024x576	32
	Cover image 2	island.jpg	0.98	2000x1125	24
3	Secret image	football.jpg	29.3	620x413	24
	Cover image 1	galaxy.jpg	334	1152x720	24
	Cover image 2	puppies.jpg	52.8	736x552	24
4	Secret image	batman.jpg	390	1920x1080	24
	Cover image 1	batman.jpg	390	1920x1080	24
	Cover image 2	batman.jpg	390	1920x1080	24

Time and memory requirements

Sr. no.	Parameter	Encryption	Creating stego images	Extracting shares	Decryption
1	Time (ms)	540	3736	477	120
	Memory(KB)	16614	42181	58833	52210
2	Time (ms)	577	2231	418	104
	Memory(KB)	15523	30874	43214	38234
3	Time (ms)	509	1530	272	82
	Memory(KB)	16068	21890	26582	25851
4	Time (ms)	554	4748	663	114
	Memory(KB)	23135	32850	46367	39494

Percentage similarity between the secret image and the image after decryption is 100%. Hence the original image is retrieved as it is without any loss of quality and detail.

5. Conclusion

The proposed method improves the security and efficiency of the image encryption. This method clearly overcomes the shortcomings of the previous method. Image transmission over the Internet is secured by introducing new levels of encryption. The image is first encrypted and then embedded into other images. This increases the privacy of the image many folds. Even if the attacker gets hold of the stego-image in transit, he/she would not be able to yield our the secret image thereby achieving higher level of security as compared to other traditional image securing methods.

References

[1] Manoj Dhande, Pooja Jaiswal and Saloni Barvalia, "Secure Image Transmission using Visual Steganography" International Journal on Recent and Innovation Trends in Computing and Communication, April 2016.
[2] Kamaldeep Joshi and Rajkumar Yadav "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", 2015 Third International Conference on Image Infonnation Processing IEEE, 2015.
[3] Shiji Johny and Anil Antony, "Secure Image Transmission using Visual Cryptography Scheme without Changing the Color of the Image" IEEE International Conference on Engineering and Technology (ICETECH 15), 2015.
[4] R Gayathri and Dr. V. Nagarajan, "Secure data hiding using Steganographic technique with Visual Cryptography and Watermarking scheme", IEEE ICCSP 2015 conference.
[5] Dipesh Shrestha and Sanjeeb Prasad Panday, "Visual Cryptography using Image Pixel Transparency with Cover Image", 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), 2015.
[6] Vandana G. Pujari, Shivchandra R. Khot and Kishor T. Mane, "Enhanced Visual Cryptography Scheme for Secret Image Retrieval using Average Filter", 2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN), 2014.
[7] Archana B. Dhole and Prof. Nitin J. Janwe, "An Implementation of Algorithms in Visual Cryptography in Images", International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013
[8] Kai-Hui Lee and Pei-Ling Chiu, "An Extended Visual Cryptography Algorithm for General Access Structures", IEEE Transactions of Information Forensics and Security, vol 7, No. 1, February 2012