ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

Enhanced Image Security via Cryptography and Sound Steganography

Sukina K[1], Reshna T[2]

M.Tech Student, Computer Science, Malabar Institute of Technology, Anjarakandy, Kannur, India [1]

Assistant Professor, Computer Science, Malabar Institute of Technology, Anjarakandy, Kannur, India[2]

Abstract: Images are one of the important type of multimedia which are largely used in the area of computer vision, graphics, medical systems, databases etc. Image transmission is required when the source and destination are situated at a distance. The transmission of image through the network faces a lot of attacks and security problems. Hence a secure image transmission technique is necessary today. Mosaic image is a steganography technique for secure image transmission. But encryption and audio conversion can add the security aspect of the image to be sent. Hence the encrypted mosaic image as an audio will be sent through the network for the secure image transmission. The combined use of cryptography and sound steganography provides an enhancement for image security.

Keywords: Encryption, Mosaic Image, Advanced Encryption Standard.

I. INTRODUCTION

Image is one of the most commonly used multimedia data, so which have got the same consideration as the text data. When the communicating parties far apart, we need to send the image through the network securely. The attackers and intruders are increasing today. Hence a new secure image transmission technique is necessary. The combined use of steganography and cryptography can give more protection for the data. In addition to that, a type conversion also performed for providing more security. There are different applications which require secure image transmission. Enhanced mosaic image transmission is a new concept which combines both sound steganography and cryptography

II. PROPOSED SYSTEM

The proposed system consists of three phases.
a) Mosaic image construction
b) Image encryption
c) Sound Steganography

A. MOSAIC IMAGE CONSTRUCTION

This phase transforms a secret image into a meaningful mosaic image with the same size and looking like a preselected target image by the user. The transformation process consist of

- Fitting tile images
- Colour transformation
- Image rotation
- Embedding information
- Extraction of information
- Secret image retrieval

Fitting Tile Images

The secret image selected first. Then it is divided into tile blocks. The target image can be selected according to the user's interest. Then it is also divided into target blocks. The size of each tile and target block should be equal. Then we need to find the standard deviation vales and mean values for each block. After that, we can fit the blocks with greater similarity

Colour Transformation

The color characteristics of the secret image should be converted into the color characteristics of target image but using the mean and standard deviation values. We are considering the RGB color space here. Because of that, there will be three component value for each pixel in the image.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

Image Rotation

It consist of rotating blocks to fit better with smaller RMSE value. RMSE stands for root mean square error. After a target block B is chosen to fit a tile image T and after the color characteristic of T is transformed, we conduct a further improvement on the color similarity between the resulting tile image T' and the target block B by rotating T' into one of the four direction zero, ninety, one hundred and eighty and two hundred and seventy degrees, which yields a rotated version of T' with the minimum RMSE value with respect to B among the four directions for final use to fit T into B.

Embedding Information

For the secret image retrieval from the receiver side, we need to embed some information into the mosaic image. The information to be embedded are index, mean values, standard deviations and rotation angle. For the embedding purpose, we can use LSB embedding .i e, the information are embedded into the least significant bits of the pixels in the random blocks.

Extraction of Information

The information which are embedded in the mosaic image to be retrieved for the secret image retrieval. The embedding technique can be reversed for the extraction purpose. A lossless extraction leads to the efficient recovery of secret image which was sent.

Secret Image Retrieval

After extraction of recovery information, the secret image can be retrieved using the reverse processes of mosaic image construction. The mosaic image provides a better security for the image data when it sent through the network.

B. IMAGE ENCRYPTION

Encryption is a cryptography technique which can be used for providing security for the data. Data may be in different forms. The multimedia data can also be encrypted. The image data can be encrypted before the transmission through the network for secure transmission. AES is the advanced encryption standard used for the image encryption using 128 bit key size. Hence it uses 10 rounds for encryption and decryption. AES is an efficient standard by NIST. The encrypted image by AES can be decrypted only with the same key used for encryption. Since it is a symmetric encryption technique. AES consist of mainly four steps. They are add round key, substitute bytes, shift rows and mix columns. The encryption named cryptography technique actually provides a double protection for the image. AES also uses keys of 192 and 256 bits for heavy duty encryption purposes. AES is largely considered impervious to all attacks, with the exception of brute-force, which attempts to decipher messages using all possible combinations in the 128,192 or 256 bit cipher. It is developed by two Belgian cryptographers Joan Daemen and Vincent Rijimen.

C. SOUND STGANOGRAPHY

After the encryption of mosaic image, it is converted into an audio for providing more security. Actually we need to send an image through the network. For that we transmitting an audio, then the attacker or intruder can't identify the image inside the audio. Hence the proposed system has more relevance in today's insecure world. The steganography actually provides a triple level protection for the image to be sent through the network.

D. SYSTEM ARCHITECTURE

The proposed system consists of architectures for both sender and receiver. The sender can select any secret image as well as target image. Then the mosaic image is constructed using the target image. After that, the mosaic image is encrypted using AES encryption standard. Then the image data is converted into an audio for providing more security.

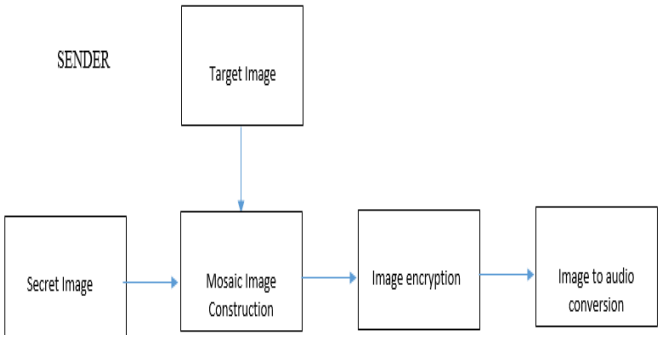

Fig. 1. Proposed architecture for sender

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

For the receiver side, first we will get an audio. So it should be converted into an image. After that, it is decrypted using the same AES standard. So we will get the mosaic image. From that, we need to retrieve the secret image by doing the reverse operations used for constructing the mosaic image.

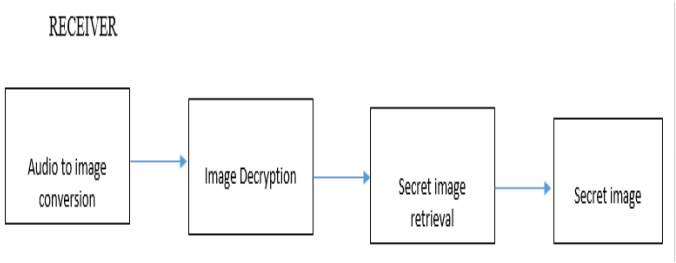

Fig. 1. Proposed architecture for receiver

III.PERFOMANCE ANALYSIS

A number of experiments have been conducted to test the proposed method using many secret and target images with different block sizes.

A. SSIM

It stands for structural similarity. It is a subjective quality measure used to find the structural similarity between two images. In this case, measured the ssim value between the sent secret image and received secret image.it always provides a value of greater than 0.90. Hence it is a better value. Because if the two images are identical, then the value will be one. Hence the recovered secret image is nearly lossless.

Secret Image	Target Image	SSIM
Lena	Pepper	0.9814
Pepper	Lena	0.9758
Barbara	Pepper	0.9844
Pepper	Barbara	0.9773
Birthday_img	Barbara	0.9864
Lena	Barbara	0.9876
Barbara	Lena	0.9856
Cameraman	Lena	0.9721
Lena	Cameraman	0.9684
Cameraman	Pepper	0.9750
Pepper	Cameraman	0.9603
Birthday_img	Lena	0.9859
Lena	Birthday_img	0.9325

Table 1. SSIM between sent and received secret image

B. PSNR

It stands for peak signal to noise ratio. The existing system consist of only mosaic image construction for secure image transmission. But when the transmitted image is attacked, they will get some clues about the secret image embedded into it. But the proposed method will not give the information about the secret image as much the existing system. Hence the PSNR value form proposed method will be lower than that of existing system. PSNR is taken for secret image and transmitted image. The lower value of the PSNR gives more security for secret image to be sent.

Secret image	Target image	PSNR from existing system	PSNR from proposed system
Lena	Barbara	11.3488	8.6622
Barbara	Lena	11.1540	8.3898
Cameraman	Lena	9.3625	6.7799
Lena	Cameraman	9.1107	8.7173
Cameraman	Pepper	10.0618	6.7708
pepper	Cameraman	9.2571	8.1538

Table 2. PSNR comparison

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

C. KEY SENSITIVITY ANALYSIS

The AES encryption technique uses 128 bit symmetric key. If any bit of the key value is changed, then we will not get the exact secret image. Hence the key sensitivity of AES provides more protection for the secret image to be sent.

D. HISTOGRAM

We can compare the histogram of both mosaic image and the encrypted image. The histogram of the encrypted image is fairly uniform and significantly different from the histogram of original image and hence does not provide any clue to employ statistical attacks on the histogram.

E. CORRELATION COEFFICIENT

Correlation is the measure of dependency. Smaller values of correlation coefficient between secret image and transmitted image indicates success of encryption process.

$$correlation\ coefficient = cov(x,y)/\sigma x \sigma y$$

The following figure depicts the set of test images:-

Fig. 3. Test images

Sender Side

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

vi. Image from Audio vii. Decrypted Image viii. Retrieved Secret image

Receiver Side

Fig. 4 Experimental result yielded by the proposed method

IV. CONCLUSION

A new secure image transmission method has been proposed, which combines the mosaic image transmission with both cryptography and sound steganography. Cryptography is the study of hiding information. While steganography deals with composing hidden messages. So that only the sender and receiver know that the message even exists. That is, in steganography, only sender and the receiver know the existence of the message where as in cryptography, the existence of the encrypted message is visible to the world.

Due to this, steganography removes the unwanted attention coming to the hidden message. Cryptographic methods tries to protect the content of a message, while steganography uses methods that would hide both the message as well as the content. By combining steganography and cryptography, enhanced the image security of mosaic image transmission sent through the network. The original secret images can be recovered nearly lossless. Good experimental results have shown the feasibility of the proposed method.

ACKNOWLEDGMENT

The authors thank the reviewers for their valuable comments and suggestions that helped us to make the paper in its present form.

REFERENCES

[1] Shikha Singh Abhishek Patanwar, Comparative study of reversible watermarking techniques
[2] Jawad Ahmad and Fawad Ahmed, Efficiency analysis and security evaluation of image encryption schemes.
[3] Dr. Vikas Saxena Jolly Shah, Performance study on image encryption Schemes
[4] Mohammad Sajid Qamruddin Khizrai and ST Bodkhe, Image encryption using di_erent techniques for high security transmission over a network.
[5] I-Jen Lai and Wen-Hsiang Tsai, Secret-fragment-visible mosaic image–a new computer art and its application to information hiding, Information. Forensics and Security, IEEE Transactions on 6 (2011), no. 3, 936–945.
[6] P. Kalpana P. Radhadevi, Secure image encryption using aes
[7] Rucha R Raut and Komal B Bijwe, A survey report on visual cryptography and secret fragment visible mosaic images.
[8] Bhavana K Reena J, Multimedia security techniques.
[9] Rajasthan Reshu Choudhary, Arun JB, Secure image transmission and evaluation of image encryption
[10] Brahim Soukpnar smet ozturk, Analysis and comparison of image encryption algorithms
[11] N. MorimotoA. Lu W. Bender, D. Gruhl, Techniques for data hiding
[12] M. K. Jeya Kumar V. J. Rehna, Member, A strong encryption method of sound steganography by encoding an image to audio