Secure Image Transmission using Visual Steganography

Prof. Manoj Dhande
Prof. Dept. of Computer Engg.
Shah & Anchor Kutchhi Engg. College
Mumbai, Maharashtra, India

Pooja Jaiswal, Saloni Barvalia,
Smit Shah, Krishma Shah
Students, Dept. of Computer Engg.
Shah & Anchor Kutchhi Engg. College
Mumbai, Maharashtra, India

***Abstract*—**In today’s information age, information sharing and transfer has increased exponentially. The threat of an intruder accessing secret information has been an ever existing concern for all. Cryptography and Steganography are the most widely used techniques to overcome these threats. Steganography is a branch of security technique which involves the art of hiding the existence of the message between sender and the intended recipient. Here, steganography has been used to hide digital images. Cryptography involves converting the message text into an unreadable cipher. To overcome this predictability, we propose the concept of visual cryptographic steganography where slices of original secret image upon encryption are embedded within a cover image. The resultant stego image is then decrypted to recover the original image.

Keywords*—*Steganography, Cryptography, Shares, Visual cryptography, Encryption, Decryption, AES.

*****

I. INTRODUCTION

The rapid advancement of network technology, large amount of multimedia information is transmitted over the Internet conveniently. Various confidential data and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over transmission to hack the information. To deal with this, secret image sharing schemes have been developed. Visual steganography is one such scheme that will help eliminating hacking and also complex computation in decryption.

Original image having secret information is going through two levels of encryption. 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.

To transmit or store an image in a safer way against unauthorized persons, there are at least three possible major approaches: encryption with keys, hiding the image in other media or objects i.e. steganography, sharing of image among distinct parts which is visual cryptography.

128-bit encryption is clearly sufficient to address all commercial and non-top secret government applications. Once the encryption engine discussion is put to rest, much more energy should be focused on solution-level deployment issues.

Combination of these three major approaches is also possible. Secret sharing of image or encryption of image with the help of key produce images which will give with a minimal loss. So, there may be chances that attacker may come to know about secret data and he can hack it.

II. SYSTEM ARCHITECTURE

A. *Selection of Secret Image*

Secret image has been selected as an input for encoding and decoding process. Here, big image embedding can be achieved. Any format of image can be used for secret image selection.

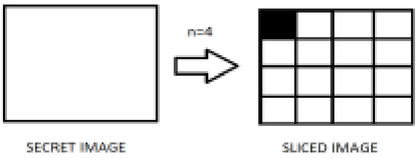


Figure 1. Secret image selection

B. *Secret image splitting*

We consider a matrix of image with rows and columns split into sixteen slices. The image is divided into four rows and columns. [1] With a consideration of 2^n formula with n is 4. Length of the image is calculated and divided by 4. Similarly width is calculated and divided by 4.

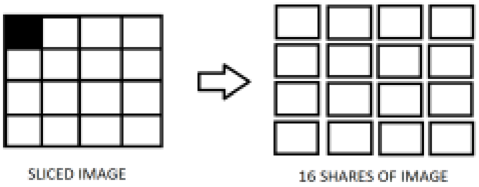


Figure 2. Secret image splitting

C. *AES Encrption*

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. Secret data is encrypted by AES (Advanced Encryption Standard) and embedded within skin region of image that will provide an excellent secure location for data hiding.

However, AES is quite different from DES in a number of ways. AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits.[3] As well as these differences AES differs from DES in that it is not a feistel structure.

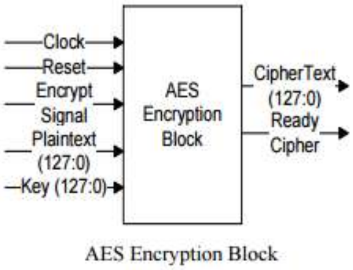


Figure 3. AES encryption

The main loop of AES performs the following functions:
SubBytes() - SubBytes()adds confusion by processing each byte through an S-Box.
ShiftRows() - ShiftRows() provides diffusion by mixing data within rows. Row zero of the State is not shifted, row 1 is shifted 1 byte, row 2 is shifted 2 bytes, and row 3 is shifted 3 bytes.
MixColumns() - MixColumns()also provides diffusion by mixing data within columns. The 4 bytes of each column in the State are treated as a 4-byte number and transformed to another 4-byte number via finite field mathematics.
AddRoundKey() - The actual 'encryption' is performed in the function, when each byte in the State is XORed with the subkey. The subkey is derived from the key according to a key expansion schedule.

The cipher takes a plaintext block size of 128 bits, or 16 bytes. The key length can be 16, 24, or 32 bytes (128, 192, or 256 bits). The algorithm referred here is AES-128 depending on the key length. The input to the encryption and decryption algorithms is a single 128-bit block.

D. *Selection of Cover Image*

A cover image is selected and same image is used to embed all sixteen slices of secret image. It is used for secure transmission as it will hide the secret image.
These cover images on the secret images are sent for decryption process.

E. *AES Decryption*

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. [3]
In decryption the key schedule remains the same; the only operations we need to implement are the Inverse subBytes, shiftRows and mixColumns, while addRoundKey stays the same.

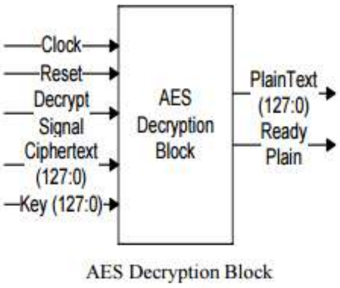


Figure 4. AES decryption

III. IMPLEMENTATION

The implementation is done using Java8 and Netbeans IDE.
Slices of the secret image:

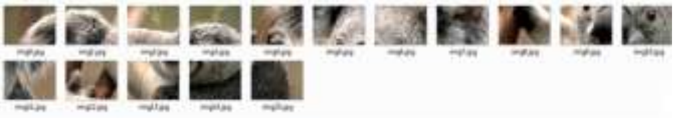
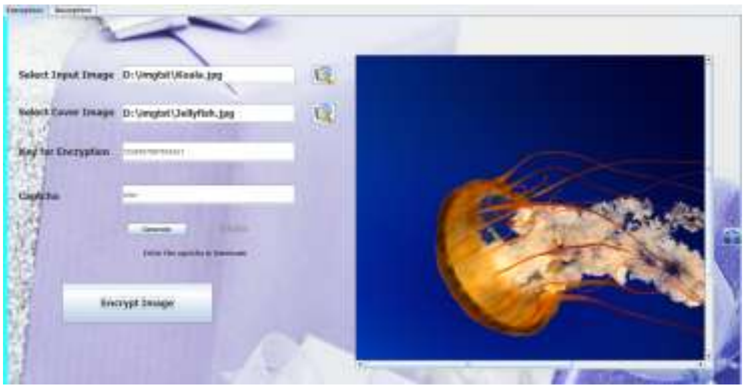


Figure 5. Slices of the secret image



Select Input Image D:\imgbit\Koala.jpg

Select Cover Image D:\imgbit\Jellyfish.jpg

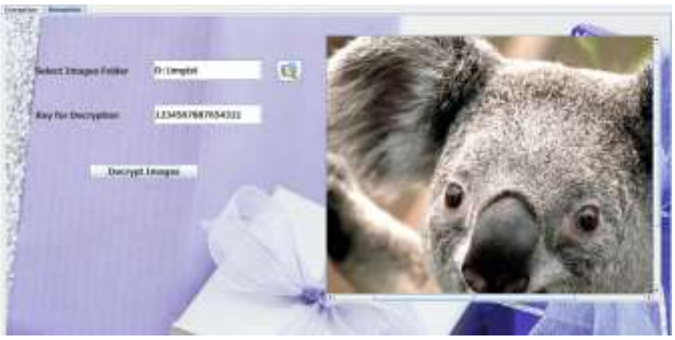
Key for Encryption [illegible]

Captcha

Enter the captcha to Generate

Figure 6. GUI of image encryption

The above GUI shows selection of secret images and the cover image is displayed. A key of 16 bytes is used for encryption process.



Select Images Folder D:\imgbit

Key for Decryption 1234567887654321

Figure 7. GUI of image decryption

The above GUI shows selection of folder which contains all the 16 encrypted slices of the image. Same key is inserted for decryption process. The secret image is displayed.

IV. RESULT ANALYSIS

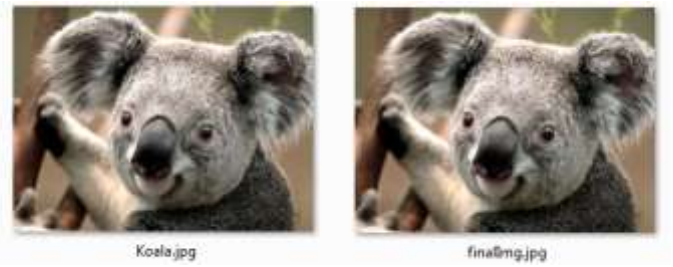
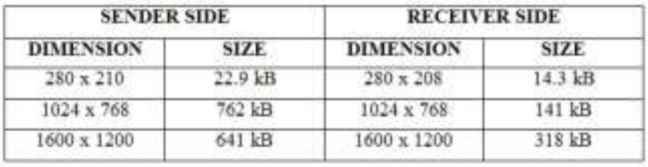


Figure 8. Comparison of original and final image

The first image Koala.jpg is the original secret image used for transmission. The second image finalImg.jpg is the image received after the decryption process.
As we can see, the final decoded image is very much similar to the original image.

Image quality parameters:



SENDER SIDE		RECEIVER SIDE	
DIMENSION	SIZE	DIMENSION	SIZE
280 x 210	22.9 kB	280 x 208	14.3 kB
1024 x 768	762 kB	1024 x 768	141 kB
1600 x 1200	641 kB	1600 x 1200	318 kB

As we can see after decoding, size of the image is reduced but the dimensions still remain similar. We have considered various sizes of image for testing and get the above table.
The size of the image is reduced by half after the decoding process.

V. CONCLUSION

The main aim of the paper was to introduce the working of steganography and cryptography together as both are having various features to protect data over a network. Also, if they are not used in combination, exact result is not achieved.

Therefore, it provides higher levels of security to the information being transmitted. Through result analysis, we see that the cipher image has been transmitted and is very much similar to the original image with minimal quality reduction.

References

[1] “Enhanced Visual Cryptography Scheme for Secret Image Retrieval using Average Filter”2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN) by Vandana G. Pujari, Prof. Shivchandra R. Khot, Prof. Kishor T. Mane.

[2] “Recovering Secret Image in Visual Cryptography”2011 IEEE by John Blesswin, Rema, Jenifer Joselin Karunya University.

[3] “Image Encryption and Decryption using AES”2012 International Journal of Engineering and Advanced Technology (IJEAT) by Manoj. B, Manjula N Harihar.

[4] “A Review on Steganography and Cryptography”2015 ICACEA by Rina Mishra, Praveen Bhanodiya.

[5] “Visual Cryptographic Steganography in Images”2010 Second International conference on Computing, Communication and Networking Technologies by Piyush Marwaha, Paresh Marwaha.