IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 4, PP 60-63

Visual Cryptography For Color Images

Akshay Gawade[1], Mitesh Rambade[2], Kuntan Sutar[3] Sudarshan Chavan [4], Prof. Priyanka Sharma[5]

[1]*Information Technology, Atharva College of Engineering, India*
[2]*Information Technology, Atharva College of Engineering, India*
[3]*Information Technology, Atharva College of Engineering, India*
[4]*Information Technology, Atharva College of Engineering, India*
[5]*Information Technology, Atharva College of Engineering, India*

Abstract: *Visual Cryptography (VC) is a secret sharing scheme, which implements the technique of secretly sharing the visual information like pictures, text etc. Existing VC technologies are not able to maintain the contrast quality of original image after the processing. So to preserve the contrast quality of original image and provide a higher security, this project presents a novel solution in which image is broken down into number of shares. These shares are send to receiver through different transmitting medium in encrypted format. In this method, the one with all the shares is able to achieve secret information; otherwise it is not possible to reveal any information.*

Keywords *– Steganography,visual cryptography, Encryption, Decryption*.

I Introduction

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 the data communication experts. With the rapid advancement of network topology, multimedia information is transmitted over the Internet conveniently. While using secret images, security issues should be taken into consideration. To deal with security problems of secret images, we should develop some secure appropriate method by which we can secure our data on internet.

II Proposed System

The proposed system uses cryptographic techniques, both in terms of shorthand and visual. Steganography uses the LSB algorithm to provide security and the second security block used is visual cryptography. Therefore, the combination of steganography and visual cryptographic algorithm improves the double security of the system.The application creates an image of Stego in which personal data is embedded and protected by a highly secure password. The main intention of the project is to develop a steganography application that guarantees good safety. The proposed approach provides more security and can protect the message from stego attacks. The resolution of the image does not change.The proposed method has inherent application of steganography as information hiding where only intended recipient knows about the hidden secret message. Additionally, it performs visual cryptography and unauthorized person requires all shares even to reveal cover message. Even though intruder gets all shares, apparently, cover message appears as sole hidden secret. Further, only intended recipient gets secret, as only authorized person has key and knowledge of secret message whereas cover message misguides unauthorized user. Hence, the proposed scheme is useful in military, business to send proper secret message to authorized user where it misguides espionage.

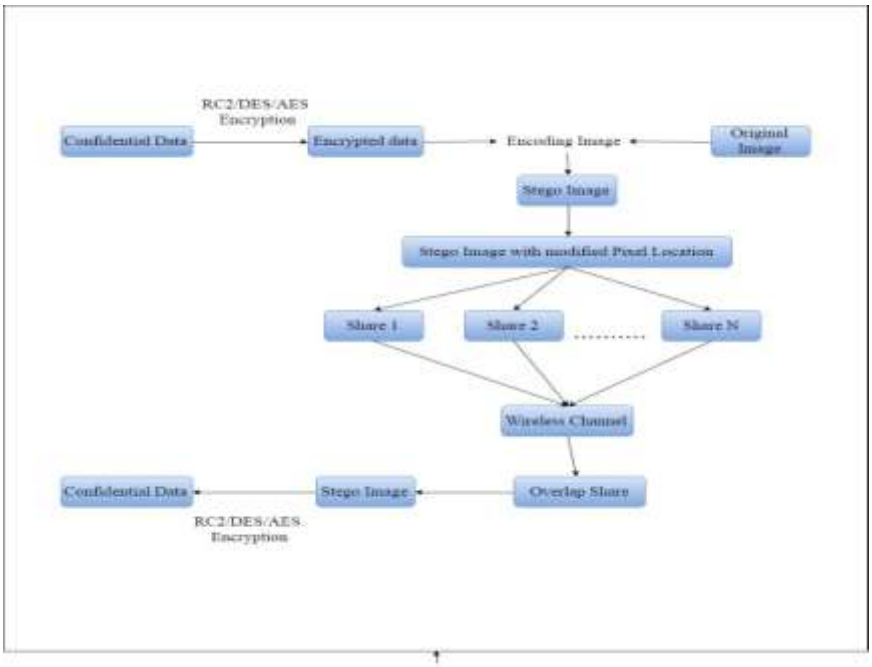

Figure 1.1: System Block Diagram

III. Review Of Literature

1.1 An Efficient Tagged Visual Cryptography for Colour Images

R.M.Shiny, P.Jayalakshmi, A.Rajakrishnammal, T.Sivaprabha Abirami.R [5] proposed a tagged visual cryptography for colour images, where the secret image is split into two base shares based on the traditional visual cryptography scheme. The generated base shares are stamped with the tag pattern using the probabilistic visual cryptography scheme to obtain the tagged shares. One of the main advantage of using tag patterns is providing the participants with augmented information to identify the relevant shares among the numerous shares. During reconstruction the tag patterns are obtained by folding up the individual tagged shares.Superimposing the shares results in the secret colour image which retains its original size thus ensuring no pixel expansion.

3.2 Colour Extended Visual Cryptography Using Error Diffusion

In Koo Kang, Gonzalo R. Arce and Heung-Kyu Lee [4] developed an encryption method to construct colour EVC scheme with VIP synchronization and error diffusion for visual quality improvement. Some methods for colour visual cryptography are not satisfactory in terms of producing either meaningless shares or meaningful shares with low visual quality, leading to suspicion of encryption. This schemes introduces the concept of visual information pixel (VIP) synchronization and error diffusion to attain a colour visual cryptography encryption method that produces meaningful colour shares with high visual quality.

3.3 Multi-pixel Visual Cryptography for colour images with Meaningful Shares

In Kiran Kumari et al [3] they used Multi-pixel Visual Cryptography for colour images to generate two meaningful shares. Some filters are proposed for better visual quality of recovered image and a simple watermarking algorithm is proposed to generate meaningful shares.

3.4 Contrast-Enhanced Visual Cryptography Schemes Based on Additional Pixel Patterns

To overcome this limitation Thomas Monoth and Babu Anto P [2] proposed their own model. This model achieves better contrast and reduces the noise in the reconstructed secret image without any computational complexity. In this method, additional pixel patterns are used to improve the contrast of the reconstructed secret image. By using additional pixel patterns for the white pixels, the contrast of the reconstructed secret image can be improved than in the case of existing visual cryptography schemes. But, in this model security for shared images got reduced.

IV. Methodology

1. Steganography

LSB Algorithm

The replacement of LSB (less significant bit) is the process of adjusting the pixels of less significant bits of the carrier image. It's a simple approach to embedding a message in the image. The insertion of the least

significant bit varies according to the number of bits in an image. For an 8-bit image, the least significant bit, which is the eighth bit of each image byte, is changed to the secret message bit. For 24-bit images, the colours of each component are changed to RGB (red, green, and blue). There are many approaches available to hide data within an image: one of the least significant bit sending approaches is "Optimal pixel regulation procedure".

2. Encryption and Decryption Algorithm

The different symmetric encryption algorithms are as follows

2.1. Data encryption standard (DES) Algorithm :

Data Encryption Standard" (DES) is also known as Data Encryption Algorithm (DEA). DEA takes 64 bits of plaintext and 56 bits of key to produce 64 bits cipher text block. The DES algorithm always functions on blocks of equal size and uses the permutations and substitutions in algorithm. The data encryption algorithm uses a 56-bit key, so the defender can't analyze the key. Thus, the Cryptanalysis problem is avoided by using this algorithm. But the inconvenience of the algorithm is the brute force attack. This can be avoided by using the Triple DES algorithm.

2.2 Triple DES Algorithm :

Triple DES is an extension to the DES algorithm. Triple DES uses the same approach for encryption as DES. 3DES takes three 64 bit keys which has a total length of 192 bits. We can guarantee more than one key that has two or three keys for encryption and decryption, so that security is more robust. It is 3 times stronger than the normal DES algorithm, so this algorithm can avoid brute force attack. The main disadvantage of using the 3DES algorithm is that the number of calculations is high, reducing the speed to a greater extent. And the second disadvantage is that both DES and 3DES use the same block size 64 to avoid security problems.

2.3 AES Algorithm :

Advanced Encryption Standard algorithms are used to avoid these limitations. Advanced Encryption Standards (AES) takes a block of size 128 bits as input and produces the output block of the same size. AES supports different key sizes like 128, 192 and 256-bit keys. Each encryption key size will change the number of bits and also the complexity of cipher text. The major limitation of AES is error propagation. The encryption operation and key generation both engage in the number of non-linear operations, so, for lengthy operations it is not suitable.

2.4 RC2 Algorithm :

RC2 also known as Rivest Cipher was developed to act as a replacement for Data Encryption Standard (DES) and was created by Ron Rivest in 1987 [6, 7]. RC2 is known as a 64-bit block cipher code and has the key size ranging from 8-bit to 128-bit. Each bit size has an increment of 8-bits from the previous key size. The key sizes ranging from 8-bit to 40-bit in RC2 are considered to be weak as using brute-force encrypted messages can be decrypted in a short amount of time. The term key in the case of RC2 is a combination of two things, a KEY and an IV (Initialization Vector). The KEY has 12 characters which support 96-bits and IV consists of 8 characters which support another 64-bits which combined together makes the entire key [1, 6, 7].

V. Slicing And Stacking Methods

We get the input as original image, patch size, number of shares(n). The original image is divided into n number of shares using slicing method. And at the receiver side get all the meaningless shares and stack together to form original image. The algorithm of slicing the original image and stacking the original image is follow.

3.1. Proposed Algorithm for slicing the original image :

Input: Original image, patch size, number of slides
Output: Meaningless shares of original images

1. Get original image
2. Get patch size and get total slides
3. Generate all statistics like,

1. Cols = width / patch size
2. Rows = height / patch size
3. Total patches = rows * cols
4. Patches per slide = total patches / slides

4. Generate blank slide images and store in slide array
5. Generate XY coordinates of all patches and store in patchXY array

6. Generates patchIDX array for shuffling
7. Shuffle the array
8. For(i=0; i<=total patches; i++)
1. Fetch the coordinate of x,y of current patch
2. Copy all the pixels of current patch to the selected slide
9. Increment slide and go to step 8.
10. Update panel
11. Save slides

3.2 Proposed Algorithm for stacking the slices of image :

Input: All meaningless shares of original images
Output: final images same as original image
1. Open all side images
2. For (i=0; i<total slides; i++)
a. XOR the all the pixel of current slide and stacked slide
3. Update panel
4. Save image

VI. Conclusion

The proposed system discussed the implementation of steganography in a safe manner together with visual cryptography. It can be concluded that when the security of the normal image is applied using steganography and the cryptographic visual technique, it makes the task of the researchers to decipher the coded secret message impractical.The approach proposed in this project uses a new steganographic approach called an ImageSteganography. The application creates an image of Stego in which personal data is embedded and is protected by a password that is highly secure.The main intention of the project is to develop a steganography application that guarantees good safety. The proposed approach provides more security and can protect the message from stego attacks. Image resolution does not change much and is insignificant when we embed the message in the image and the image is protected with the personal password.. So, it is not possible to damage the data by unauthorized personnel.

References

[1]. M. Naor and A. Shamir, "Visual cryptography," in Proc. Adv. Cryptol.:EUROCRYPT, vol. 950. 1995, pp. 1–12.
[2]. "Contrast-Enhanced Visual Cryptography Schemes Based on Additional Pixel Patterns", by Thomas Monoth and Babu Anto P, 978-0-7695-4215-7/10 2010 IEEE.
[3]. "Multi-pixel Visual Cryptography for color images with Meaningful Shares", by Ms. Kiran Kumari et. al. / International Journal of Engineering Science and Technology Vol. 2(6), 2010, 2398-2407.
[4]. "Color Extended Visual Cryptography Using Error Diffusion", by InKoo Kang, Gonzalo R. Arce, and Heung-Kyu Lee, 1057-7149/ 2010 IEEE.
[5]. "An Efficient Tagged Visual Cryptography for Color Images", by R.M.Shiny, P.Jayalakshmi, A.Rajakrishnammal, T.Sivaprabha Abirami.R, 978-1-5090-0612-0/16/$31.00 ©2016 IEEE.
[6]. "A Watermarking-based Visual Cryptography Scheme with Meaningful Shares", by HAN Yan-yan and Xi'an China, 978-0-7695-4584-4/11 2011 IEEE.
[7]. "A Semi-blind Image Watermarking based on Discrete Wavelet Transform and Secret Sharing", by B Surekha and Dr GN Swamy, 978-1-4577-2078-9/12/2011 IEEE.
[8]. "Electronic Medical Report Security Using Visual Secret Sharing Scheme ", by Rajendra Basavegowda and Sheshadri Seenappa, 978-0-7695-4994-1/13, 2013 IEEE