Elysium Journal by Engineering Research & Management

P-ISSN: 2347-4408
E-ISSN: 2347-4734

A NOVEL VISUAL CRYPTOGRAPHY APPROACH FOR MEDICAL IMAGE TRANSACTIONS USING VIDEO STEGANOGRAPHY

T.H.Vijayalakshmi[1], Mrs.G.Anitha[2]

PG student, Department of Information Technology, Rajalakshmi Engineering College, Thandalam, Chennai
E-mail id:Viji1211@gmail.com
Assistant Professor, Department of Information Technology, Rajalakshmi Engineering College, Thandalam, Chennai
E-mail id: anitha.g @rajalakshmi.edu.in

Abstract: Visual Cryptography is very essential to transfer important secret information like medical images, military secrets, bank account details and other secret information in a secure manner. This paper provides a secure and an efficient method for Steganography. Steganography can be separated into many types such as Audio, Video, text, Image, etc. The process of concealing some secret data in the cover video is called Video Steganography. In the proposed system, cover video will be splitted into frames. The secret medical image is converted into greyscale image that converts into binary image of (zeros and ones) and splitted into N-shares by using Visual Cryptography. This N-share is embedded into random frames. By this method, the possibility of finding the hidden secret information by an attacker is very less when compared to the normal method of concealing secret information inside the frames.

Keywords: Cryptography, Steganography, Video Steganography; Visual Cryptography;

1. INTRODUCTION

Steganography is the practice of concealing secret information or messages within the other non-secret text or data or information. Steganography is defining as "hide or conceal the secret data". The targets of both Steganography and Cryptography are the same, which is used for security. Today steganography is mostly used on computers with digital data being the carriers and communication networks being the high speed to deliver the secret information. Steganography can be separated into many types that shown in the (fig1.1). The proposed work is based on video steganography. The main advantages of using videos are the huge size of data that can be hidden inside .The fact that it is a moving stream of images and sounds Therefore, the hidden of any image is small but otherwise perceptible distortions might unobserved by humans because of the continuous flow of information. Video steganography uses such as MPEG, H.264, Mp4, AVI or other video formats.

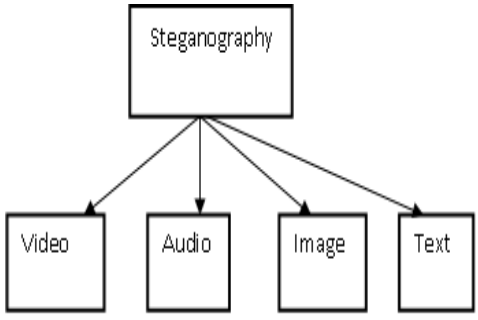

Fig.1.Steganography categories

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables that the user to store secret information and to transmit the secret data across insecure networks (like the Internet) so that it cannot be read by anyone except the original recipient. Cryptography can be defined as the conversion of data into a scrambled code that can be deciphered and sent across a public or private network.

Cryptography can be classified into two main categories used to encrypting the secret data (i) symmetrical (ii) asymmetrical. Both encryption and decryption methods uses same key in Symmetric algorithms. Both encryption and decryption techniques uses the two different keys in Asymmetric algorithms. The keys used for encryption and decryption are private-key, secret-key, and shared-key. Cryptographic algorithm is a mathematical function used in the encryption and decryption process. It works in combination with a key a phrase, number, and word to encrypt the plaintext. Then the plaintext of same text encrypts to into different cipher text with different keys.

2. RELATED WORKS

The biometric data is dithered into two images (known as sheets) that are kept in two separate database servers. It is very problematic to cross-database matching for defining identities when both sheets are simultaneously available at that time by using visual cryptography. [1] A similar process is used to de-identify fingerprint images described by Arun Ross.

Yunjung Lee"Streaming Video Service Model Using Secure Steganographic Method" Secret information is scrambled by session key generated with symmetric key by pseudo-random number; shared by sender and receiver that increase confidentiality. [2]To share the secret key with video spilling server and customer, the server encrypts the secret key with client's public key and sends it to customer.

Parvathi divya, mahesh,"various techniques in video steganography "presents a review on various techniques used for video Steganography. Various techniques are used like DCT, DWT, LSB, and IWT. [3]It has high hidden capacity and not seeing of visual quality.

Shivani khosla, paramjeet kaur"secure data hiding technique using video steganagraphy and watermarking "which provides a strong mainstay for its security. It also limits the perceivable alteration that might occur while processing it. [4]DCT (discrete cosine transformation) has strong toughness and it is used for digital image watermarking, it provides high degree of redundancy.

P-ISSN: 2347-4408
E-ISSN: 2347-4734

Rohit G bal ezhilarasu "an efficient safe and secured video steganography using shadow derivation" It focuses on Secret sharing technique, used to pelt information. Secret distribution is a technique for unbearable a message into several parts so that all parts are sufficient to recover the message. It can routinely analyze a video and hide images efficiently and effectively inside it for application in a digital records environment.[5] Large alteration occurs during reconstruction of the shadow image, so limited small data can be hidden.

Rucha bahirat, Amit kolhe "Overview of secure data transmission using steganography" The two most important aspects of stegnography system are the worth of stego object and the volume of the cover media. [6]It can build up a better steganography approach to raise the PSNR value and to reduction the MSE**.** High or increase PSNR value and strong level of security, Low hidden capacity.

K.V.Ramana"Error Diffusion Based Colour Visual Cryptography for Secure Communication" There are some prevailing colour visual cryptography schemes that might produce either evocative or meaningless shares that produce less visual quality which doubtful any kind of encryption involved in producing such shares. [7] To overcome this problem, recently presented error diffusion and the Visual Information Pixel (VIP) synchronization approaches to achieve colour visual cryptography that can produce significant shares besides making the shares in such a way that they are satisfying to human eyes.

V.Lokeswara Reddy, K.V.Vinodkumar "A Novel Data Embedding Technique for Hiding Text in Video File using Steganography" Video Steganography deals with concealing secret data or information inside video. [8]By using LSB Hiding large amount of data is possible, Hiding only text and not an image.

Shivani Khosla, Paramjeet Kaur focus on hiding text in a cover video file and to improve the hidden information. This can be done by using LSB method. Usually Video contains collection of both images and audio. Concealing huge amount of data in video is probable compare with others. [9] Video Steganography deals with concealing secret data or information within a video.

Mitali Garg, Vikas Wasson "Data Security with Image Clustering Using Steganography" It strives to hide the existence of transferred message in applicable medium i.e. Image, Audio or Video. Various methods with robustness, Payload and Detectability are available and have their particular pros and a cons. [10] Various Steganography technique is employed conditional on requirements of presentation for which they are designed.

Chandra Prakash Shukla, Mr. Ramneet S Chadha"A Survey of Steganography Technique, Attacks and Applications" This emphasis on media with hidden information is called stego media and without hidden data are called cover media. Steganography can use for hide both legal and illegal data. [11] Civilians or people may use it for defensive privacy while terrorists may use it for spreading terroristic data.

The proposed effective is to hides the secret data into a video using the video Steganography. The proposed work is discussed in the Section. Video steganography provides high level of data protection. Hiding data in the image limited to its size alone. But video contains multiple images (ie frames) thus the data can be hidden in anyone of the frame. Multiple files can be hidden at the same time.

3. PROPOSED SYSTEM

The proposed effective method is to hide the secret information into a video using the video Steganography. This method uses some frames (or images) of the video to hide the secret message. The secret data is not hidden in sequential frames. Instead of using sequential frames, the proposed work using random frames for hiding the secret data. This provides additional security to the secret data.

3.1 PROPOSED MODEL

The proposed system consists of 2 main parts:-

1. SENDER
2. RECEIVER

Sender: (Embedding Process)

The sender process should contain the cover video and a secret message as the inputs.

Step1: First take an original video as cover video. Then convert it into number of frames or images.
Step2: select the frames randomly and then select the secret image.
Step3: Before enter into (VCS scheme) the secret image is converting into grayscale image and binary image of (zero's and ones)
Step4: Then apply Visual Cryptography Schemes (VCS) and embed secret information of plans or n-shares.
Step5: These n-shares are embedded into the random frames.
Step6: These embedded frames are converted into Stego-Video.
Step7: At last, have a Stego video. This video is ready for the transmission through the internet.

Receiver: (Extracting Process)

It basically follows the reverse process of the hiding algorithm to obtain the secret message.
Step1: Load the Stego video.
Step2: The stego video is extracted into frames.
Step3: And select the random frames to reconstruct the secret image.
Step3: Apply the inverse process of Visual Cryptography Schemes (VCS) of n-shares.
Step4: Get the secret message and reconstruct the original or cover video.

Elysium Journal
Engineering Research & Management

P-ISSN: 2347-4408
E-ISSN: 2347-4734

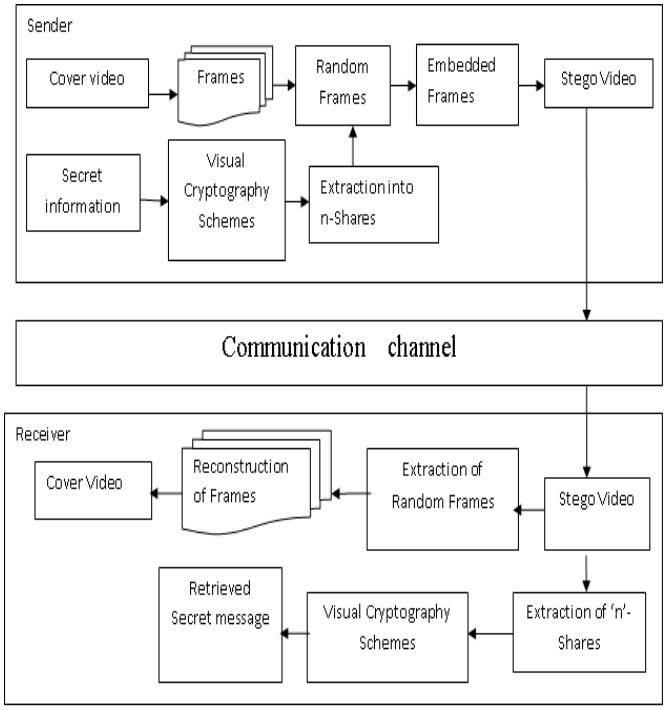

Figure 2. Architecture diagram

3.2 FRAME GENERATION

Firstly the video is split into the audio and video separately. Thereafter the video part will be converting into the N number of frames. Frame rate can be calculated by number of frames per seconds.

TABLE 1: Experimental result of frames generation

Videos in sec	size	q	No of frames
00:00:13	386KB	24.8	325
00:00:15	602KB	24.8	379
00:01:48	3.08MB	24.8	2723

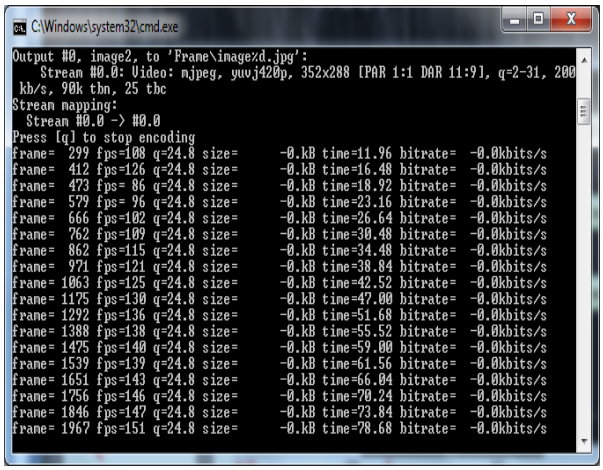

Figure 3. Frames Generation

3.3 VISUAL CRYPTOGRAPHY SCHEME (VCS)

To encrypt the secret data by using visual cryptography scheme, that the secret data is divided into two shares. The two shares of each pixel in the original image that can be replaced with the non-overlapping block. This overlapping block contains two sub pixels. If anyone contains only one share will not able to reconstruct the secret data and only one part of single share does not contain complete secret data. (Fig .4)shows the encrypted scheme for (VCS) visual cryptography scheme which is applied on the every shares of pixel of the secret data. If pixel P is white of the secret content then it is changed with two identical blocks of sub pixels of original secret content. If the pixel P is black of the secret data then it is also changed with two another blocks of sub pixels. To decrypt the secret original content of each share using the (VCS) visual cryptography scheme to reveal the original secret content.

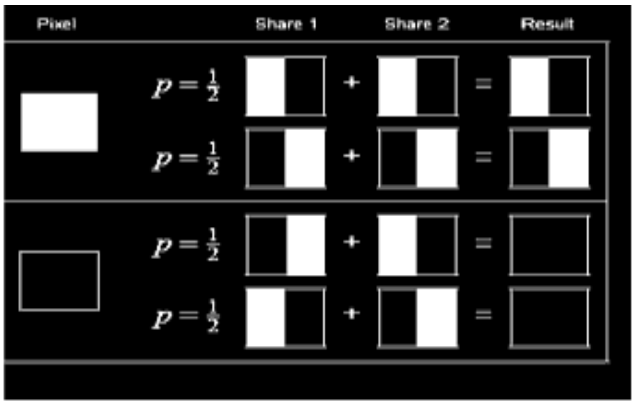

Figure 4.vcs

(i.e. matrix of original image)
The most popular color format is 24bitsRBG format in which 8bits of each color are present.

$$\begin{pmatrix} 10001001 \\ 01010000 \\ 01001110 \end{pmatrix}$$

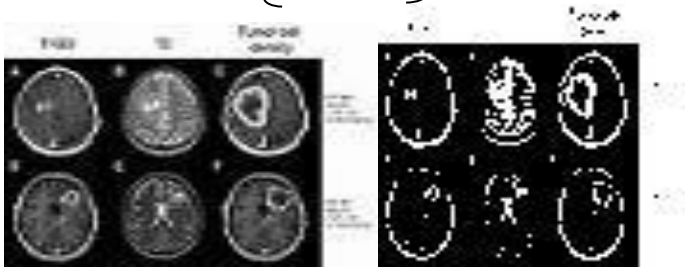

Figure 6.Experimental result of greyscale image and binary image

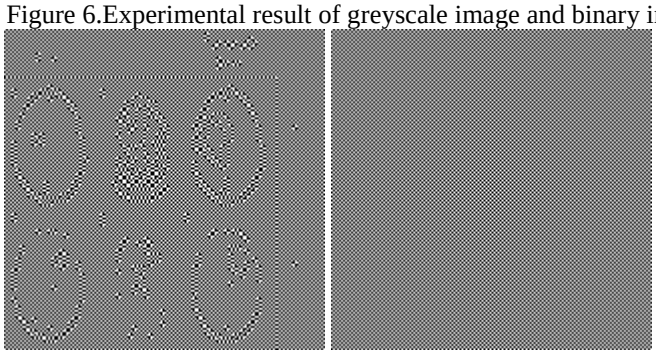

Figure 5.Experimental result of two shares

P-ISSN: 2347-4408
E-ISSN: 2347-4734

4. EXPERIMENT RESULT

Data hiding techniques can be used to embed a secret message into a compressed video bit stream for copyright protection, access control and transaction tracking. Some data hiding techniques to assess the quality of compressed video in the absence of the original reference. The quality is estimated based on computing the degradations of the extracted hidden message. Data hiding is also used for error detection and concealment in applications of video transmission.

1. The graphical representation of both LSB and VCS schemes which specifies the quality of the secret images after reconstructed.
2. If the two shares splitted equal number of pixels that provides less pixel quality and does not upload multiple files at the time.
3. The VCS schemes splits the shares in different pixel range and it also embed multiple files at a time and does not affect the quality of the stego video.

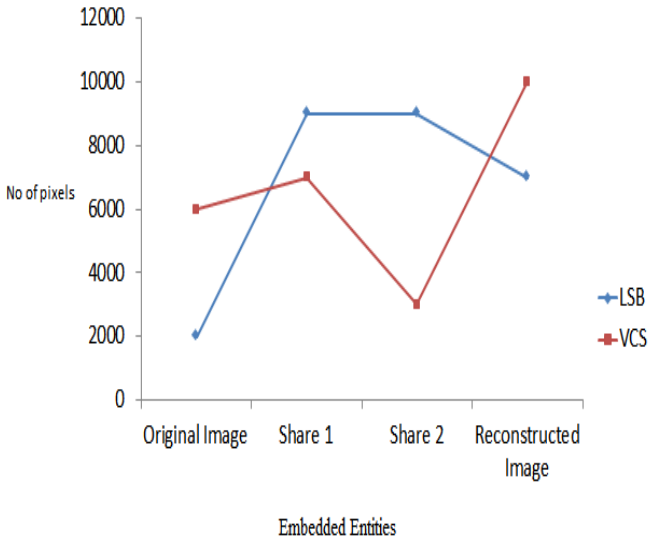

Figure 6.Representation of pixel entities

5. CONCLUSION

Thus, this paper provides a feasible solution for Video Steganography. Since the proposed system uses Visual Cryptography Schemes (VCS), the process of retrieving the secret data from the stego video becomes very simple. This method provides highly secure because the random frames are placed in the video, the attacker is left clueless to know the relevant secret information hidden in the video. Hence highly private data like secret medical images, military secrets and bank account details can be easily embedded inside the ordinary video and can be transmitted over the internet even in unsafe connection.

REFERENCES

[1] Arun Ross, Asem Othman, "Visual Cryptography For Biometric Privacy" IEEE Transactions On Information Forensics And Security, Vol. 6, No. 1, March 2011.

[2] Yunjung Lee"Streaming Video Service Model Using Secure Steganographic Method" International Journal Of Security And Its Applications Vol.7, No.6 (2013), Pp.79-88.

[3] K.Parvathi Divya, K.Mahesh "Various Techniques in Video Steganography" International Journal Of Computer & Organization Trends – Volume 5 – February 2014.

[4] Shivani Khosla,Paramjeet Kaur " Secure Data Hiding Technique Using Video Steganagraphy And Watermarking" 2014.

[5] Rohit G Bal Ezhilarasu" An Efficient Safe And Secured Video Steganography Using Shadow Derivation" 2014.

[6] Rucha Bahirat, Amit Kolhe" Overview Of Secure Data Transmission Using Steganography" International Journal Of Emerging Technology And Advanced Engineering 2014.

[7] K.V.Ramana"Error Diffusion Based Color Visual Cryptography For Secure Communication" International Journal Of Advanced Research In Computer And Communication Engineering Vol. 3, Issue 1, January 2014.

[8] K.V.Vinodkumar , V. Lokeswara Reddy "A Novel Data Embedding Technique For Hiding Text In Video File Using Steganography "International Journal Of Computer Applications (0975 – 8887) Volume 77 – No.17, September 2013 .

[9] Shivani Khosla , Paramjeet Kaur"Secure Data Hiding Technique Using Video Steganography And Watermarking "International Journal Of Computer Applications (0975 – 8887) Volume 95– No.20, June 2014.

[10] Mitali Garg, Vikas Wasson"Data Security With Image Clustering Using Steganography" International Journal Of Emerging Research In Management &Technology2014.

[11] Chandra Prakash Shukla, Mr. Ramneet S Chadha" A Survey Of Steganography Technique, Attacks And Applications" International Journal Of Advanced Research In Computer Science And Software Engineering , Volume 4, Issue 2, February 2014.