ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

An Efficient Safe and Secured Video Steganography Using Shadow Derivation

Rohit G Bal[1], Dr P Ezhilarasu[2]

P.G Student, Dept of CSE, HICET, Coimbatore, India[1]
Professor, Dept of CSE, HICET, Coimbatore, India [2]

ABSTRACT: Steganography is the art of hiding the fact that communication is taking place, by concealing information in other information. This paper focus on Secret sharing technique is used to hide information. Secret sharing is a technique for splitting a message into several parts so that all parts are sufficient to recover the message. The current study presents the design and implementation of a steganographic procedure that can automatically analyze a video and hide images efficiently and effectively inside it for application in a digital records environment. Video Fragmentation is used to extract frames (convert video into images) from video for carrier. The secret color image pixels will be converted to m-ary notational system. The (t-1) digits of secret color image pixels are generated using reversible polynomial function. Reversible polynomial function and the participant's numerical key are used to generate secret shares. The secret image and the cover image is embedded together to construct a stego image. All stego images are embedded to construct video. The reversible image sharing process is used to reconstruct the secret image and cover video. The secret is obtained by the Lagrange's formula generated from the sufficient secret shares. Quantization process is applied to enhance the nature of the cover video.

KEYWORDS: Data Hiding, File Security, Data Sharing, Steganography, Secret Key, Image Embedding, Visual Secret Sharing, Image Processing, Frame Extraction, Consumer Videos, Video Analysis, Image Steganography

I. INTRODUCTION

Steganography is the practice of concealing messages or information within other non-secret text or data. Hiding of information or message is achieved through hiding information in other information, thus hiding the existence of the transmitted information. The word steganography is derived from the Greek words "*stegos*" means "cover or protected" and "*graphei*" means "writing" [1] defining it as "concealed writing or covered writing". Cryptography and steganography are different, but both targets at security. Steganography differs from cryptography in the sense that where cryptography concentrates on keeping the contents of a message secret, steganography concentrates on keeping the existence of a message secret [2]. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. A basic steganographic system is shown in Fig.1

In Steganography, the multimedia files such as image, video, audio, etc is used to attach the secret data. The unique feature of the steganography considering cryptography is that unauthorized individuals are not aware of the hidden data in the stego-media [5]. Initial steganography techniques have been first applied to images; however, the video streams have attracted a lot attention recently since they can assure a large amount of capacity increase for hidden/secret data [6]. The hidden data can be embedded either into image or into audio part of the video streams. The objective of this work is to develop a Compressed Video Steganographic Scheme that can embed secret messages into videos which provide provable security with high computing speed, and without producing noticeable changes. A video can be viewed as a sequence of still images. Data embedding in videos and images are similar to each other. However, there are several differences between steganography in images and videos; the first main difference is the size of the carrier media. Videos contain more sample number of transform domain coefficients or the number of pixels. A video can embedded more data because it has higher capacity than a still image [7]. Also, there are some features such as perceptual redundancy in videos is due to their temporal features cannot be found in images.

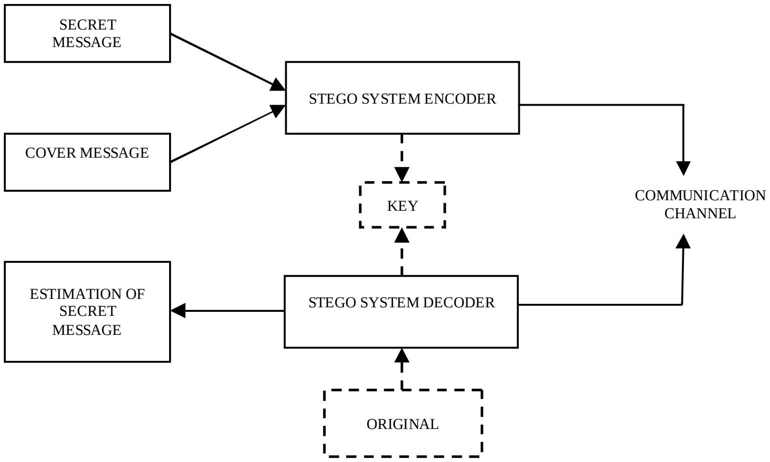

Fig.1 A Basic Steganographic Architecture

The rest of the paper is organized as follows: Section 2 discusses problem statement. Section 3 lays out proposed work. Section 4 presents describes the security analysis of our framework. Section 5 concludes the paper and outlines future enhancements.

II. Related work

I In the year 1979 Blakley and Shamir [8] had developed (t, n) threshold scheme, where a sender hides and splits the secret into n number of shadows. The sender then gives a share of the shadows to the approved participants. The secret data can be revealed if any t out of n authorized participants with their corresponding shadows is present. Shamir [9] developed the Visual secret sharing from the (t, n) – threshold concept. Random images called shadows are generated from secret image. During transmission the shadow is send out instead of shadows Chen et al [11] and Wang [10] describes the problems like pixel expansion, contrast, and meaninglessness which are more attracted by the attackers. Embedded image called stego image which is meaningful is used to hide the shadow from attackers. Wu, Y.S., Thien, C.C., Lin [14] and Lin and Tsai [13] recommended t-1 polynomial to generate shadows in secret sharing technique. To hide secret cover image and secret image are incorporated. The reconstruction of image has distortions because of truncation of gray value pixels (greater than 250). These kinds of small distortions are not tolerable in medical images and other sensitive images Chang Et Al. [12], Thien and Lin [15] and Zhao Et Al [16] overcome these problems by using two pixels to describe the grey values that are greater than 250. This result in expansion of secret image therefore alters the quality of the stego image. To increase the volume of the embedded secret stream, in early 2009, instead of embedding one secret pixel into the (t -1) degree polynomial F(x) (t-3) secret digits into polynomial F(x).

There has been a rapid growth of interest in this subject over the last ten years and for two main causes. Firstly, the publishing and broadcasting industries have become highly involved in techniques for concealing encrypted copyright marks and serial numbers in multimedia products such as digital films, audio recordings, e-books, etc; an appreciation of new market chances generated by digital distribution is linked with a fear that digital works could be too easy to copy. Secondly, directions by various governments to keep under control of the handiness of encryption services have inspired people to study methods by which private messages can be attached in apparently not harmful cover messages. The effort with which this can be done may be an argument against forcing restrictions [4].

In Steganography there are several problems which occur during different stages which are discussed below. The size of data that user wanted to hide inside the carrier is the main problem in the steganography. The main draw back when the carrier is image is the capacity of secret data/information. Next problem that faced there is quality of data, if the quality is increased, there will be suspicious changes which will be become visible to human eye. Here challenge is to create an algorithm for hiding high rate of data without altering the quality of data. Other thing we are discussing here is the hiding in video; usually video is accessible in compressed form. The steganographic algorithm is not appropriate compressed format (i.e. video format) so complete or partial decompression is required. This needless burden should be prevented or lessen. If compressed domain steganography is necessity, then compressed domain must be used to integrate the secret data. Steganographic technique is handy when secret is not easily discoverable. If existence of secret message is discovered with probability greater than random guess or assumption, that steganographic technique is not valid or inaccurate. Like cryptography, steganography also affected by attack method usually called as steganalysis. Ample research work on this topic is performed on images. One approach is based only upon the first order statistics and is relevant on idempotent embedding technique. Other major approach is based on the concept of blind steganalysis, which is developed by blind classifiers. At first the classifiers should be trained to learn the differences between cover and stego image's characteristics.

As a summery, the main problems in the Steganography are as follows:

- Size of hidden data
- Quality of image
- Algorithms applied
- Level of data protecting
- Level of suspecting

III.PROPOSED ALGORITHM

The proposed steganographic system consists of 2 main parts:-

1. Encryption System
2. Decryption System

1. ENCRYPTION SYSTEM

Encryption system is used to embedded the data / message into carrier i.e. video. It consists of following modules:-

1.1 Frame Extraction

Frame extraction is process of extracting frame from video. Stego video is converted into frames. From the frames one frame is selected for encryption.

1.2 Channel (RGB) Representation

Colour images are used as secret and as cover image. Colour images are of the form of 3 channels i.e. red, green and blue. Each channel has pixel value between 0-255. Both colour and secret image are represented in RGB format

1.3 Shadow Derivation

Encryption is done with help of shadow generation. With help of modulo operation and a prime number m secret pixels are converted to m-ary notational system. Let p be the pixel value of secret image and c1, c2 … ct-1 d are coefficients of invertible polynomial function F(x). c1, c2 … ct-1 are the output of m-ary notational system. d is calculated with help of prime number m and pixel value (p) of every pixel of each channel with formula d= p mod m. All channels (Red, Green, and Blue) are framed with invertible polynomial function. The inputs of invertible polynomial F(x) = c1+c2x1+c3x2…+ct-1xt-2+dxt-1 mod m are t-1 digits of red channel of secret color image and d of red channel of cover colour image. Similarly F(x) will be generated for green and blue channels. With the help of the participant's numerical key the output of invertible polynomial function will be encrypted. With their appropriate numerical key value each participant generates their shadows.

1.4 Quantization Process

The encryption process will decrease the quality of the cover image. In order to preserve the cover image pixel quantization process {Q = (p/m)*m} is done which will help to retain the quality of image during reconstruction. Quantization is done with help of two operation i.e. division and multiplication. Divide the cover image pixel by prime number m and take floor value and multiply the prime number with floor value to generate quantized image pixel.

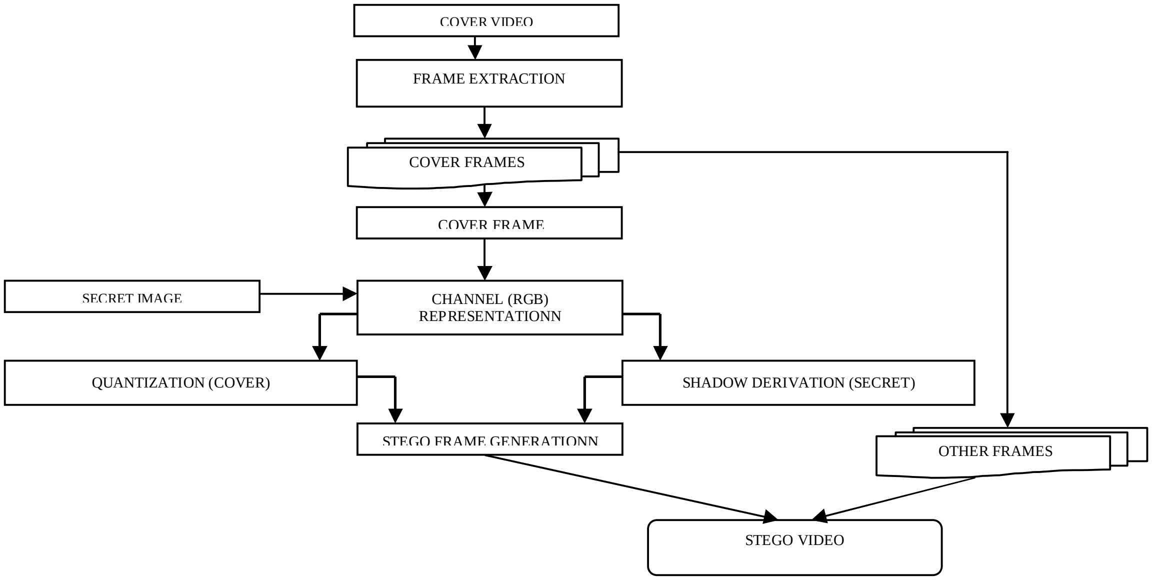

Fig.2 Block Diagram (Encryption System)

1.5 Stego Image Generation

The cover image is used the hide the generated shadow images. The stego image is output from embedding cover image pixel with secret image pixels. The quantized value of cover image is used for cover image for creating stego image.

1.6 Stego Video Generation

Combining the stego frame with other frames and converting sequence of frames to video.

2. DECRYPTION SYSTEM

Decryption system is used to separate the data / message from carrier i.e. video. It consists of following modules:-

2.1 Frame Extraction

Refer section 1.1

2.2 Shadow Reconstruction

Shadows can be reconstructed from the stego images. n shadows are reconstructed from n stego images with help of prime number m and formula y = sp mod m, where y be pixel value of shadow and sp be the secret pixel value. Each authorized participant will have a stego image and a key. Key is used for decrypting the image

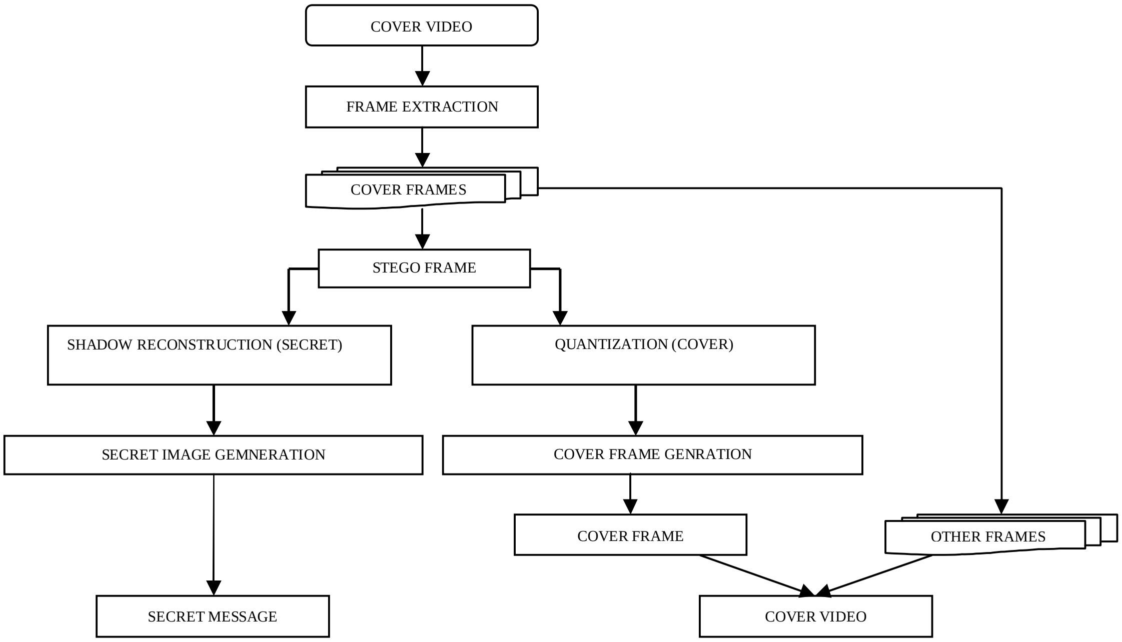

Fig.3 Block Diagram (Decryption System)

2.3 Quantization Process

Refer section 1.1

2.4 Secret Image Reconstruction

Secrets can be reconstructed only with minimum of t shadows, less than t is of no use. The Lagrange’s formula is formed by using participant’s numerical key and shadow value.

2.5 Cover Frame Reconstruction

Quantization operation Q= (sp/m)*m will be used to get back the color cover image without loss. Quantization operation is performed on the stego image, which will generate a quantized value. This quantized value is added with the last digit of Lagrange’s interpolation equation, the result of which reconstructs the cover image pixel.

2.6 Cover Video Reconstruction

In this the cover frame is combined the cover frame with other frames and converting sequence of frames to video.

IV. SIMULATION RESULTS

In this Section, the proposed schemes simulation results and performance of the proposed scheme are explained; AVI format video is taken as carrier. The experimental platform was programmed in Matlab version 7.9. The Peak to Signal Noise Ratio (PSNR) is used to calculate the distortions present in the stego video. The PSNR values is calculated using the equation

$$PSNR = 10 \times 10\log_{10}\left(\frac{255^2}{MSE}\right) dB$$

MSE - Mean Square Error between the original cover color image and the stego color image. For a cover image of size H x W, the MSE is given as below,

$$\mathrm{MSE}_{\mathrm{colour}} = \frac{1}{\mathrm{H\,X\,W}}\sum_{i=1}^{H}\sum_{j=1}^{W}\frac{\mathrm{R+G+B}}{3}$$

Where R, G, B are calculated as

$$\mathrm{R} = \left(\mathrm{R}_{\mathrm{X}_{ij}} - \mathrm{R}_{\mathrm{Y}_{ij}}\right)^2$$

$$\mathrm{G} = \left(\mathrm{G}_{\mathrm{X}_{ij}} - \mathrm{G}_{\mathrm{Y}_{ij}}\right)^2$$

$$\mathrm{B} = \left(\mathrm{B}_{\mathrm{X}_{ij}} - \mathrm{B}_{\mathrm{Y}_{ij}}\right)^2$$

Rxij and Ryij - Pixel values of the Red component in the original cover color image and the stego color image, respectively

Gxij and Gyij - Pixel values of the Green Component in the original cover color image and the stego color image, respectively

Bxij and Byij - Pixel values of the Blue component in the original cover color image and the stego color image, respectively.

A higher PSNR value means that the quality of the stego color image is similar to that of original color cover image. PSNR value less than 35 dB means that some of the important signal characteristics are lost. PSNR value less than 30 dB is an unacceptable quality. Good quality is implied by PSNR value greater than 35 dB.

Table 1, 2 shows comparison of existing and proposed work,

Steganography Method	P.S.N.R (db)
LSB Substitution	32.23
Small Shadow	35.12
Secret Sharing	39.30
Proposed	42.50

Table 1

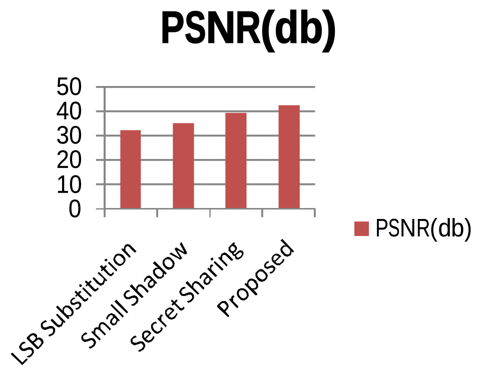

Table 2

Comparison of PSNR values

V. Conclusion and Future Work

This proposed system investigates the problem of occurrence of meaningless and the large distortions in the reconstructed shadows. Existing solutions are either limited to a small amount of data. Hence, this paper proposes several solutions for color image pixels that reveals the secret image without loss and preserves the cover image using quantization. This methodology can be further enhanced for 3D images and can be used for embedding text.

References

1. Moerland, T., *"Steganography and Steganalysis"*, Leiden Institute of Advanced Computing Science www.liacs.nl/home/ tmoerl/privtech.pdf
2. Wang, H & Wang, S, *"Cyber warfare: Steganography vs. Steganalysis"*, Communications of the ACM, 47:10, October 2004
3. Dunbar, B., *"Steganographic techniques and their use in an Open-Systems environment"*, *SANS Institute*, January 2002
4. Wolfgang, R.B. and E.J. Delp, 1996. *"Watermark for digital images"*, Proceeding of the IEEE
5. International Conference on Image Processing, Sep. 16-19, IEEE Computer Society, Washington DC., USA, pp: 219-222. DOI: 10.1109/ICIP.1996.560423
6. Cetin, O., Ozcerit, A.T., Cakiroglu, M., (2006), *"A New Data Embedding Method into Motion Pictures"* The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing, Las Vegas, USA.
7. Hartung. F., Girod. B., (1998), *"Digital watermarking of uncompressed and compressed video"*, Trans. Of Signal Processing – Special Issue on Copyright protection and Access Control for Multimedia Services, 66(3):283-301
8. Sherly, A, P., Amritha, P, P., *"A Compressed Video Steganography using TPVD"*, International Journal of Database Management Systems (IJDMS) Vol.2, No.3, August 2010
9. L.Jani Anbarasi., S.Kannan., *"Secured Secret Color Image Sharing With Steganography"*, ICRTIT-2012, ISBN: 978-1-4673-1601-9/12/$31.00 ©2012 IEEE
10. M. Naor and A. Shamir, "*Visual cryptography*", Advances in Cryptography: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.
11. Wang, R.Z., Su, C.H., 2006. *"Secret image sharing with smaller shadow images Pattern Recognition"*, Lett. 27(6), 55l–555.
12. Chang, C.C., Lin, C.C., Lin, C.H., Chen, Y.H., 2008. *"A novel secret image sharing schemin color images using small shadow images"*, Inform. Sci. l78 (ll), 2433–2447
13. Chang, C.C., Hsieh, Y.P., Lin, C.H., 2008. *"Sharing secrets in stego images with authentication"*, Pattern Recognition 4l (l0), 3l30–3l37.
14. Lin, C.C., Tsai, W.H., 2004. *"Secret image sharing with steganography and authentication"*, J.Syst. Software 73 (3), 405–4l4
15. Wu, Y.S., Thien, C.C., Lin, J.C., 2004. *"Sharing and hiding secret images with size constraint"*, Pattern Recognition 37 (7), l377–l385.
16. Lin, J.C., Thien, C.C., 2002. *"Secret image sharing"*, Computer Graphics 26 (l), 765–770.
17. Chi-Shiang Chan , Pei-Yu Lin, 2010 *"Invertible secret image sharing with steganography"*, Pattern Recognition Letters 31 (2010) 1887–1893

BIOGRAPHY

Rohit G Bal received the B.Tech degree in Computer Science and Engineering from College Of Engineering Thrikaripur, Kerala in 2011. He is currently doing the Post graduation in Computer Science and Engineering in Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu, now working on the research project in Image Processing. His area of interest includes computer network, security in computer and image processing.

Dr.P.Ezhilarasu received the B.E degree in Computer Science and Engineering from Bharathiar University Coimbatore then M.E degree in Computer Science and Engineering from Anna University Chennai. He commended his Ph.D in Faculty of Information and Communication from Anna University Chennai .He is having more than 20 years of experience in Teaching, Research and Industry. He guided so many UG and PG students in his career. He handled more than 25 subjects in his career. His area of interest includes Image Processing, Data mining, soft computing.