ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 6, June 2016

Secured Data Hiding in Video Streams

Harshila Gawali , Rucha Samant

Abstract— **Reversible data hiding is a technique by using which we can embed essential data into images, audio, video and so on. This system applies a method of hiding data in an image and video by reserving room before encryption. The proposed scheme increases the amount of data that can be hidden in the image or video which also guarantees the lossless recovery of image or video after extraction is completed. All the previous methods of reversible data hiding were developed such that they were vacating room for data hiding after encrypting the image, which introduces some error rates when data extraction and image recovery process is done. This system proposes a new method for reversible data hiding in which reserving room before encryption (RRBE) is used in images and videos using visual cryptography, so that image or video extraction will be free of any error. It is also known as new watermarking technique which is used to authenticate an image and video by embedding some data in it.**

Index Terms— **RRBE, RRAE, RDH, RSA, encryption, partitioning, self reversible embedding.**

I. INTRODUCTION

Now-a-days security is considered as most important critical factor in any communication systems. Issues in such security systems are integrity, privacy, authentication and no repudiation, such issues must be handled carefully. The security goals are: availability, confidentiality and integrity that can be threatened by security attacks. So to protect the original information from such attacks the data hiding techniques are implemented. To maintain the security and authentication, Reversible Data Hiding i.e RDH techniques are related to steganography and cryptography function [3]. Encryption and data hiding are two techniques of data protection. Data hiding techniques embeds original data which we don't want to disclose into cover media by introducing slight acceptable modifications, while encryption techniques converts plaintext data into unreadable form i.e. cipher text. It is beneficial to embed the data into a digital media to send and receive the secret messages. One can modify the original content of the media using images, so that the embedded data is hidden[1]. Encryption provides confidentiality for images and video as well as it is effective technique which converts the original and secret data to incomprehensible one. If we are able to apply RDH to encrypted image then some good applications can be generated through it.

Harshila Gawali, *Dept of Computer Engg, GES's COE Nasik,India.*
Prof. Rucha Samant, *Dept of Computer Engg, GES's COE Nasik Nasik,India.*

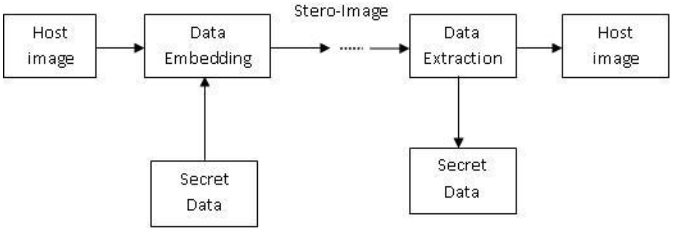


Figure 1: Block diagram of RDH

For example: Suppose that a medical image database stored in some data center, then some notations can be embedded into the encrypted version of a medical image through a RDH technique by a server residing in the data center. Then the server can manage the image or verify its integrity by using the notations, there is no need to have knowledge of the original content. This will protect the patient's privacy. At the same time, a doctor can decrypt as well as restore the image for further diagnosing by using the cryptographic key.

Reversible data hiding in images or videos is a technique, by which the original content can be recovered without loss after the embedded data is extracted. This technique can be widely used in various fields such as medical, military and law forensics, where distortion of the original cover is not allowed. Reversible data hiding technique is used to embed additional data into cover media such as image or video. Recently many new RDH techniques are developed which gives a general framework for RDH. It works by first extracting the features of the original cover media and then compressing them without loss, extra space can be saved by embedding auxiliary data. All previous methods of RDH embed data by reversibly extracting room from the encrypted images, which may lead to some errors while data is being extracted and/or image is being restored. Here a novel method with a traditional RDH algorithm by reserving room before encryption is proposed, and thus it is possible to reversibly embed data in the encrypted image and videos. Goal of the proposed technique is to achieve secured technique for transmitting highly confidential information over the insecure channels of internet. Data hiding into cover media such as video is one of the challenging task compared to data hiding in images, but as videos are more secure way for embedding secure information than images, in proposed method it is possible to hide the data in videos by using public key cryptography. In this system, a novel method is proposed by reserving room before encryption of images/frames with a traditional RDH algorithm.

II. RELATED WORK

Mainly the data hiding techniques are classified into two techniques:

- ***Reversible data hiding technique:***

In this technique the message data as well as the original cover media can be recovered / extracted with no loss.

- ***Irreversible data hiding technique:***

In this technique the message data can be extracted with no loss but the original cover may be lost. So we can conclude that the reversible data hiding techniques can be used more efficiently.

Method of reversible data hiding techniques are reserving room before encryption and vacating room after encryption as given below:

A. Vacating Room after the Encryption:

In this method it first encrypts the original image using the cipher with the encryption key. Next to this, it is given to the data hider to hide some auxiliary data in it by vacating the room(space) required for data hiding key. At receiver the an authorized third party can be extract the embedded data with the help of data hiding key and also recover the original image by using encryption key. This method compresses the encrypted LSBs of image to vacate the room for additional data.

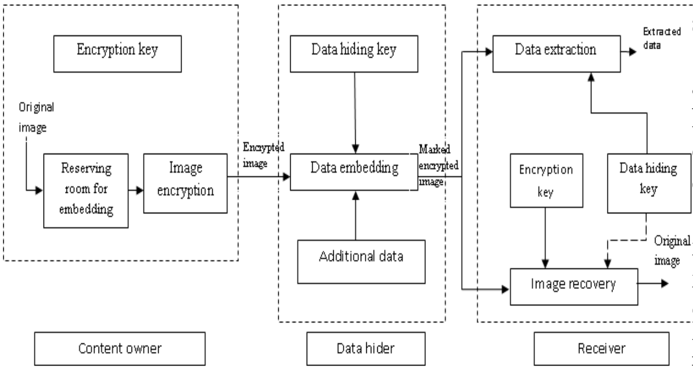


Figure 2: Vacating Room after the Encryption

B. Reserving room before the encryption:

Vacating room from the encrypted images losslessly is sometimes difficult and not efficient, so if we reverse order of encryption and vacate room, i.e., reserving room before encrypting the image, the RDH tasks in encrypted images would be more natural and much easier which gives the novel framework, reserving room before encryption (RRBE). [2]

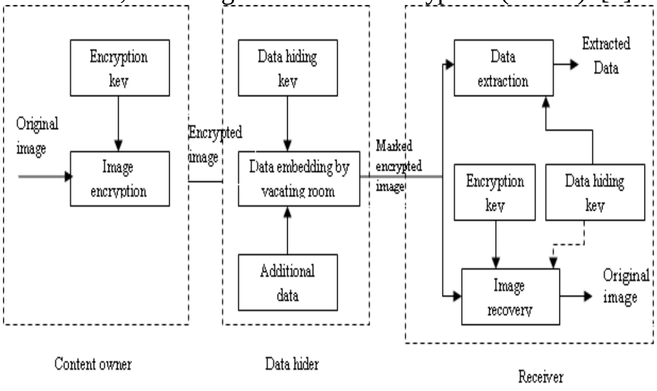


Figure 3: Vacating before the Encryption

There are some standard RDH algorithms available which are ideal for reserving room before encryption and can be easily applied to framework of RRBE to achieve better results compared with techniques from Framework VRAE. [11]

III. LITERATURE SURVEY

A substantial amount of research on reversible data hiding has been done over the past few years. Some important techniques are discussed here. Various techniques have been proposed and research has been done in the field of reversible data hiding. Also many advanced methods have been developed for reversible data hiding and visual cryptography. Some research work in the area of reversible data hiding is listed below:

Jui Tian [4] has proposed a difference expansion technique which works by finding extra storage space by exploring the redundancy in the image content/data. Here the secret data embedding capacity limit and the visual quality of embedded images of the DE method gives low computational complexity.

Wen-Chung Kuo, Po-Yu Lai, Lih-Chyau Wuu [5] introduced a newer methodology of histogram shift based adaptive reversible data hiding. The aim was to enhance the data hiding capacity and embedding point adaptively a new proposed scheme was based on histogram and slope methodologies. This method provides high embedding capacity and also maintains the high and better quality of stego-image.

Weiming Zhang, Kede Ma, Xianfeng Zhao, Nenghai Yu and Fenghua Li [6 have introduced a new method for data hiding reversibly in an image by reserving room before encrypting the image. Vacating room in losslessly from the encrypted images is difficult and sometimes inefficient.

In the field of reversible data hiding Abraham .G, Jose. R in [7] has proposed a novel scheme to reversibly hide data into encrypted grayscale image in a separate manner. Content owner firstly encrypts the image by permutation of pixels using the encryption key. After which the data hider hides the data into the image which is already in the encrypted version by histogram modification based technique by using data hiding key. Naor [8] proposed method of Visual cryptography. In a kout of n scheme of VC, a secret binary image is encoded into n no of shares of random binary pattern. These n shares are Xored with n transparent factors, and then distributed amongst n end users. k or more users can visually reveal the secret image by superimposing any k transparencies together.

In Koo Kang, Gonzalo R. Arce , Heung-Kyu Lee [9] introduced the new color visual cryptography encryption methodology that produces no of meaningful color shares by visual information pixel synchronization and error diffusion half toning.

In Wei Qiao, Hongdong Yin, Huaqing Liang [10] proposed a new secret visual cryptography scheme for color images. First of all a colored image is partitioned into three monochromatic images in tone cyan, magenta and yellow. These images are transmitted into binary form by using the halftone technique. And finally, the traditional binary to hide to get the sharing images.

IV. PROPOSED SYSTEM

The proposed method makes use of color visual cryptography. As shown in Figure 4 and Figure 5 system first encrypts data to be embedded by using RSA algorithm then it embeds data into cover media (image/video) by first creating space for data by checking RGB co-ordinates and then performs encryption on cover media along with encrypted message. The data recovery and image extraction are reverse of encryption process.

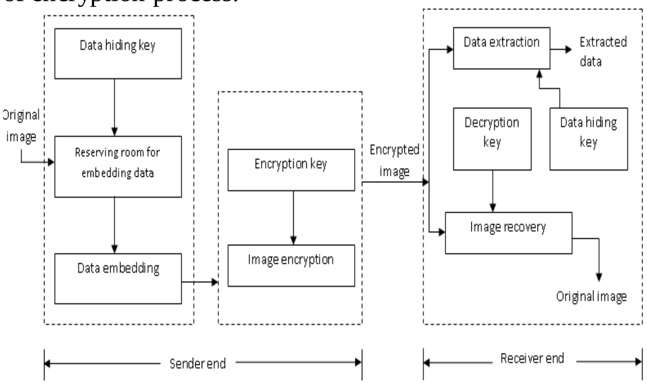


Figure 4: System Architecture for hiding data in image

If cover media contains video then first frames are extracted from the video which are treated as image and rest of the process remains same. The first step that is partitioning the image is done using the color visual cryptography algorithm. Here the input image is partitioned into shares. The first step can be divided as: Cover image Partitioning and Self

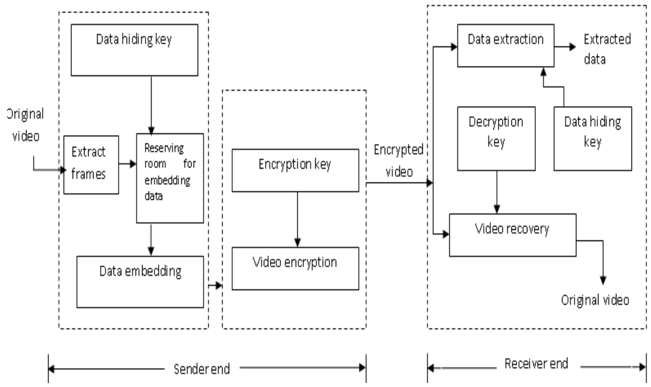


Figure 5: System Architecture for hiding data in video

Reversible Embedding which is then followed by cover image encryption. Image partitioning step algorithm divides the original cover media or image/video into two shares using the color visual cryptography, then the two shares generated are embedded together and rooms/space are reserved for the purpose of hiding data and finally encrypt the new rearranged cover to generate its encrypted version.

- **Mathematical model:**

Let S be a closed system.

S = {I, D, R, N}

where

I =$(i_1, i_2, i_3,…….., i_n)$ - Set of images

R =$(i'_1, i'_{2,}\ i'_{3,……….,}\ i'_n)$ - Images with rooms reserved

D =$(t_1, t_{2,}\ t_3,…….., t_n)$ - Data to be embedded

DR=$(i't_{1,}\ \ i't_2,i't_{3,……….,}i't_{n)}$-Embedded images with room reserved

N =$(e_1,e_2,e_3,………,e_n)$- Encrypted images

- Rules:

1. Let f_i be a rule of I into R such that it returns

$f_i(I) \rightarrow R$

$f_i(i'_n) \rightarrow (i'_n) \in R$

2. Let f_d be a rule of I into DR such that it returns

$f_d(D,R) \rightarrow DR$

$f_d(t_n) \rightarrow (t_i) \in DR$

3. Let f_n be a rule of I into R such that it returns

$f_n(R) \rightarrow N$

$f_d(i'_n) \rightarrow (e_n) \in DR$

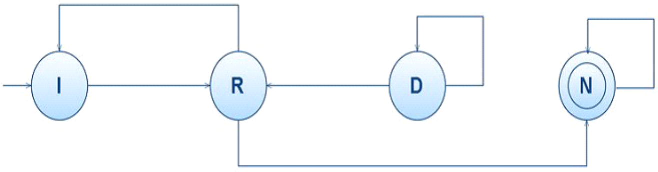


Figure 6: State transition diagram

All relations have one-to-one-mapping.

V. FRAME EXTRACTION

Key frame extraction and Video division are the bases of video investigation and substance/content based video recovery. Key frame extraction [13], is a vital part in video examination and administration, giving a suitable video outline to video recovery, searching and indexing. The utilization of key frames decreases the measure of information required in video indexing and gives the structure to taking care of video substance. Key casing is the edge/frame which can represent the salient content and information of the shot/video. The extracted key frame summarizes the characteristics of the video, and the image characteristics of a video can be traced by all the key frames in time sequence. For video, a typical initial step is to separate the recordings into "shots," each speaking to persistent arrangement of activities or an sequence of actions. A shot speaks to an arrangement of frames that are caught from a one of a kind and nonstop record from a camera.

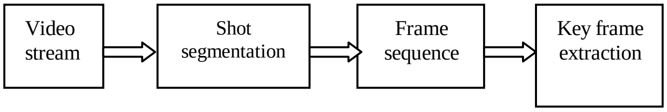


Figure 7: The basic framework of the key frame extraction algorithm from MPEG video stream

At that point key frames are to be separated. Video division is the establishment of key frame extraction, and key frames are the salient content of the video (key elements to depict the video substance).

VI. TEXT ENCRYPTION

For message encryption RSA algorithm is utilized. RSA is public key cryptography algorithm which uses private key for encryption and public key for decryption.

VII. IMAGE ENCRYPTION ALGORITHM

The main steps involved in image encryption methodology are:

A. Partitioning the image:

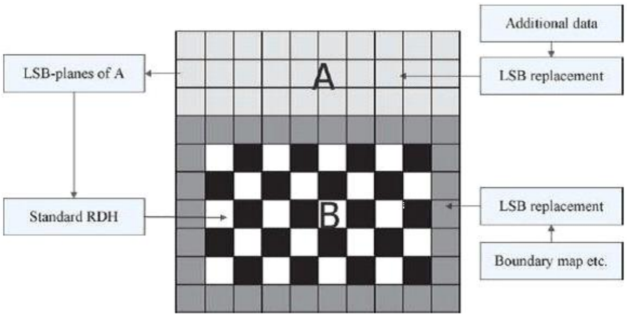


Figure 8: Illustration of image partition and embedding process

Toward the starting, partitioning the image step separates the first picture into two sections A and B then, the LSBs of A are reversibly implanted into B with a standard RDH calculation so that LSBs of A can be utilized for storing the messages; finally, scramble the reworked image to produce its last form.

B. Self-Reversible Embedding:

The target of self-reversible installing procedure is to insert the LSB-planes of A into B by utilizing conventional RDH calculations. Note that this step does not depend on a particular RDH algorithm[19]. Pixels in whatever remains of picture B are initially arranged into two arrangements of pixels : white pixels with its records i and j fulfilling (i + j) mod 2 = 0 and dark pixels whose files fulfills (i + j) mod 2 = 1, as appeared in Figure. 7. At that point, every white pixel Bi,j , is evaluated by the introduction of interpolation value which is obtained from the four dark pixels encompassing it as takes after:

$$B'_{i,j=} w_1B_{i-1,j} + w_2B_{i+1,j} + w_3B_{i,j-1} + w_4B_{i,j+1}$$

where the weight w_i , $1 \leq i \leq 4$, is controlled by the same technique as proposed in [10]. The evaluating error is ascertained through $B_{i,j} – B_{i,j}$ and after that some information can be implanted into the estimating error sequence with histogram shift.

C. Image encryption

After modified self-installed picture is gotten, meant by X, it can encode X to develop the scrambled picture, which will be meant by E. With a stream cipher, the encryption form of X is effortlessly acquired. For instance, a dark quality Xi,j going from 0 to 255 can be spoken to with 8 bits, $X_{i,j}(0),X_{i,j}(1),........X_{i,j}(7)$, such that

$$Xi,j(k)$$

The encoded bits $E_{i,j}(k)$can be ascertained utilizing exclusive or operation

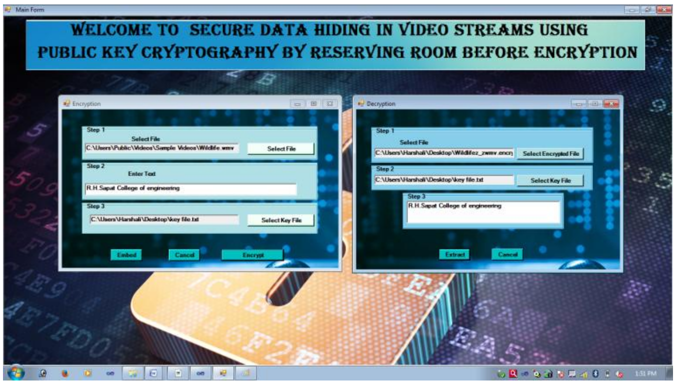
$$E_{i,j}(k)=X_{i,j}(k)\ r_{i,j}(k)$$

where $r_{i,j}(k)$ is produced using so as to utilize a standard stream cipher acquired the encryption key.

VIII. EXPERIMENTAL RESULTS

As and when information is installed into the picture, there is event of bending in a picture. So it is normal that after the information extraction has been done the picture/video quality ought to be kept up like the first picture.

It might likewise be normal that the original substance can be recovered with no misfortune after decoding and recover concealed message at recipient site. This demonstrates that the reversible information concealing technique for scrambled picture is beneficial. Along these lines, to keep up the nature of a picture/video, RDH systems are utilized. The system provides a secure way to transfer data without degrading the quality of cover image, colour visual cryptography technique has also contributed to it, as the cover is losslessly recovered. This enables to achieve real reversibility which is desirable in medical or military applications.



WELCOME TO SECURE DATA HIDING IN VIDEO STREAMS USING PUBLIC KEY CRYPTOGRAPHY BY RESERVING ROOM BEFORE ENCRYPTION

Encryption:

Step 1 Select File: C:\Users\Public\Videos\Sample Videos\Wildlife.wmv

Step 2 Enter Text: R.H.Sapat College of engineering

Step 3: C:\Users\Harshali\Desktop\key file.txt

Decryption:

Step 1 Select File: C:\Users\Harshali\Desktop\Wildlifez_zwmv.encr

Step 2: C:\Users\Harshali\Desktop\key file.txt

Step 3: R.H.Sapat College of engineering

Figure 9: Snapshot of proposed system

IX. CONCLUSION

With the increased use of internet, proposed system focuses mainly on RDH as the secured way of communicating over insecure channels of internet. Past techniques actualize RDH in encoded pictures by abandoning room after encryption, instead of which proposed framework works by holding room before encryption. Accordingly the information hider can profit by the additional space/room discharged out in past stage to try less. The proposed strategy can exploit all conventional RDH strategies for plain pictures and videos and accomplish better execution without loss of secrecy.

Proposed system also working towards parallelizing the RDH process into videos, such that it can embed multiple lines of information/data into multiple frames extracted from video. It will improve the performance of the system by minimizing the time complexity of embedding process.

ACKNOWLEDGMENT

I take this chance to express gratitude toward Prof. N.V.Alone, Head of the Computer Engineering office, for his support and direction. I likewise need to thank my aide Prof. R.C.Samant for her persistent help and gigantic help. She offered me in an expansive scope of issues from giving me course, some assistance with helping to discover answers for issues, delineating necessities and continually having room schedule-wise to see me. I additionally stretch out true on account of all the staff individuals for their significant help. To wrap things up I am extremely grateful to my colleagues for all their important recommendations and backing.

REFERENCES

[1] *Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography", IEEE Transactions on Circuits and Systems for Video Technology, DOI 10.1109/TCSVT.2015.2433194.*

[2] *K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," IEEE Trans. Information Forensics & Security, 8(3), pp. 553-562, 2013.*

[3] *Shweta Patil Student, Electronics Amrutvahini college of engineering, Sangamner Maharashtra, India," Data Hiding Techniques: A Review" International Journal of Computer Appl0ications (0975 – 8887) Volume 122 – No.17, July 2015.*

[4] *M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.*

[5] *Wen Chung Kuo, Po Yu Lai, Lih Chyau Wuu, " Adaptive Reversible Data Hiding Based on Histogram", 10th International Conference on Intelligent Systems Design and Application, IEEE 2010 (2002) The IEEE website. [Online]. Available: http://www.ieee.org/*

[6] *Kede Ma. Weiming Zhang, Xianfeng Zhao, Nenghai Yu,Fenghua Li, "Reversible Data Hiding in Encryted Images by Reserving Room Before Encrytion", IEEE Trans on Information Forensics and security, Vol. 8, No.3, march 2013*

[7] *Jose, R.; Abraham, G, "A separable reversible data hiding in encrypted image with improved performance", Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy(AICERA/ICMiCR), 2013 Annual International Conference, IEEE 2013.*

[8] *Moni Naor, Adi Shamir," Visual Cryptography",in Proc. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1-12,Springer-Verlag, LNCS*

[9] *InKoo Kang, Gonzalo R. Arce , Heung-Kyu Lee, " Color Extende visual cryptography using error diffusion", ICASSP IEEE 2009*

[10] *Wei Qiao, Hongdong Huaqing Liang, "A kind of Visual Crytography Scheme For color Images based on halftyone technique", International Conference on Measuring Technology and Mechatronics automation ,2009 IEEE*

[11] *V Yu, Song Wei, "Study on Reversible Data Hiding Scheme for Digital Images", 2nd International Asia Conference on Informatics in Control, Automation and Robotics,(CAR) 2012*

[12] *Susan Hohenberger and Brent Waters, "Attribute-Based Encryption with Fast Decryption" May 8, 2013*

[13] *Guozhu Liu, and Junming Zhao "Key Frame Extraction from MPEG Video Stream", Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT '09) Huangshan, P. R. China, 26-28,Dec. 2009, pp. 007-011*