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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Reversible Information Hiding in Videos

V.Priya[1]

PG Scholar, Dept. of CSE, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India[1]

ABSTRACT: Confidentiality is a set of rules that prevents the disclosure of any confidential information to unauthorized individuals or systems. Confidentiality of any information can be achieved by data hiding which is a process to hide data into a cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. Reversible Data Hiding in encrypted images is an emerging trend and it maintains the excellent property that the original cover can be recovered, after data was extracted. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. In the proposed technique, a novel method by reserving room before encryption with a traditional Reversible Data Hiding algorithm is used which enables the data hider to reversibly embed data in the encrypted image. By this technique, the proposed method can achieve better confidentiality and image recovery.

I. INTRODUCTION

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files Steganography's ultimate objectives, which are undetectability, robustness and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography.

Reversible data hiding in images is a technique that hides data in digital images for secret communication. It is a technique to hide additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Traditionally, data hiding is used for secret communication. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to reveal the presence of the embedment. Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before data hiding is actually performed, such as military images or confidential medical images. In this case, the content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image.

II. ABOUT THE PROJECT

With regard to providing confidentiality for images, encryption is an effective and popular means as it converts the original and meaningful content to incomprehensible one. In this project, the content owner first reserves enough space on original image and then convert the image into its encrypted version with the encryption key. Now, the data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. Obviously, standard RDH algorithms of better operators for reserving room before encryption and provide a better performance than the existing methods. Not only does the proposed method separate data extraction from image decryption but also achieves excellent performance in two different prospects:

- Real reversibility is realized, that is, data extraction and image recovery are free of any error.
- For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding ratesis greatly enlarged.

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

III. APPLICATION OF THE DOMAIN

Steganography is employed in various useful applications, e.g., copyright control of materials, enhancing robustness of image search engines and smart IDs (identity cards) where individuals' details are embedded in their photographs. Other applications are video–audio synchronization, companies' safe circulation of secret data, TV broadcasting, TCP/IP packets, and also checksum embedding.

In Medical Imaging Systems where a separation is considered necessary for confidentiality between patients' image data or DNA sequences and their captions, e.g., physician, patient's name, address and other particulars. A link however, must be maintained between the two. Thus, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems.

Steganography would provide an ultimate guarantee of authentication that no other security tool may ensure. Most of new applications in steganography like a watermark, to protect the copyright on information. Photo collections sold on CDs have hidden information which detects unauthorized usage. The same technique used for DVDs is even more effective, since the industry build DVD recorders to detect and disallow copying of protected DVDs.

IV. PROBLEM DEFINITION

The Data hiding deals with the ability of embedding data into a digital cover with a minimum degradation, i.e. the embedded data is invisible or audible to a human observer. Data hiding consists of two sets of data, namely cover medium and embedding data, which is called message. The digital medium or the message can be text, audio, picture or video depending on the size of the message and the capacity of the cover. Early video hiding approaches were proposing still image reversible data hiding technique is extended to video by hiding the message in each frame independently.

V. EXISTING SYSTEM

In this Existing System, the method used in compressing the LSBs is to vacate room for additional data by identifying syndromes of a parity-check matrix, and the side information used at the receiver side is also the spatial correlation of decrypted images. All the three methods try to vacate room from the encrypted images directly. However, since the entropy of encrypted images has been maximized, these techniques can only achieve small payloads generate marked image with poor quality for large payload and all of them are subject to some error rates on data extraction and/or image restoration.

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission. In some application scenarios, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content.

Among different kinds of digital watermarking schemes, reversible watermarking has become a research hotspot recently. Compared with traditional watermarking, it can restore the original cover media through the watermark extracting process; thus, reversible watermarking is very useful, especially in applications dictating high Fidelity of multimedia content, such as military aerial intelligence gathering, medical records, and management of multimedia information..

Disadvantages of Existing System

- Low Error Rates

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

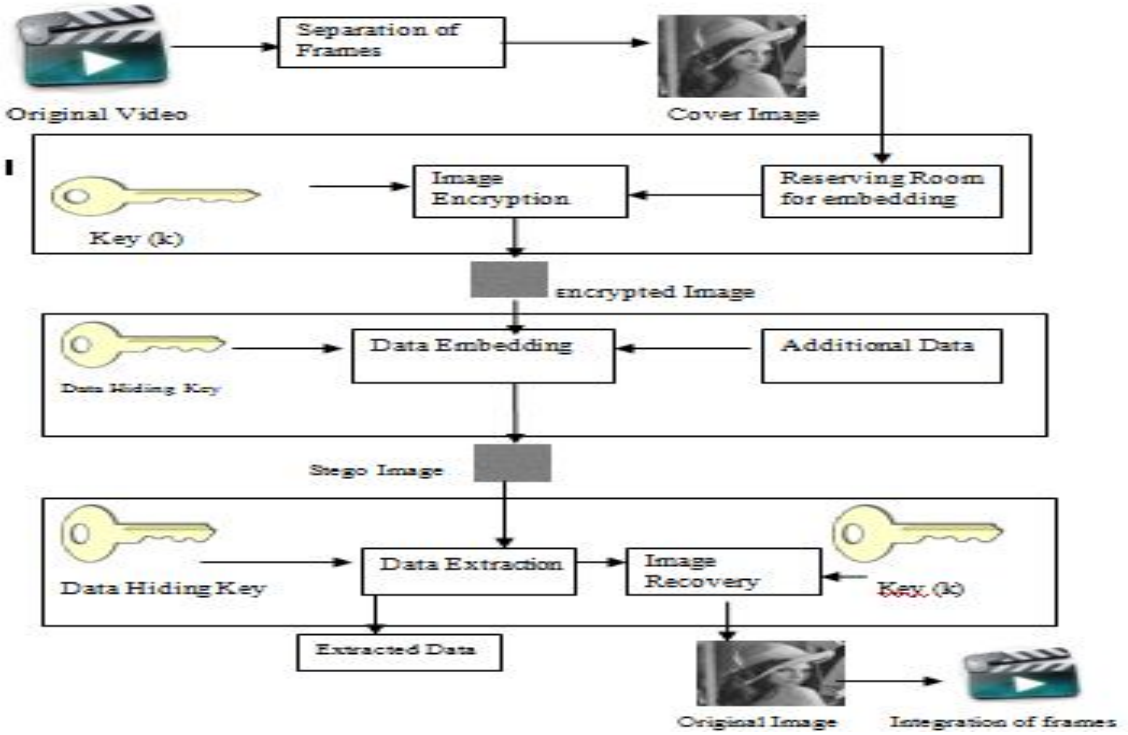
- Image Restoration Problems

VI. PROPOSED SYSTEM

In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel framework, "reserving room before encryption" (RRBE) the content owner first reserves enough space on original image and then converts the image into its encrypted version with the encryption key.

Now, the data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. The data extraction and image recovery are identical to that of Framework Vacating Room After Encryption (VRAE). Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. This is because in this new framework, we follow the customary idea that first losslessly compresses the redundant image content.

The figure describes the architecture of the project. The original video is separated into a set of frames i.e., images depending upon the standards available either as PAL or NTSC. Then the images are encrypted using encryption key. In the encrypted image, enough space is reserved for embedding the additional data. The additional data is embedded using data hiding key. Using Reversible Data Hiding(RDH), additional data is transferred and cover image also can be retrieved without any distortion. Finally, the separated frames are integrated to form the original video.



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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The content owner first reserves enough space on original image and then convert the image into its encrypted version with the encryption key. Now, the data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. The data extraction and image recovery are identical to that of Framework VRAE. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. This is because in this new framework, we follow the customary idea that first losslessly compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.

VII.PROCESSING STEPS

Video Preprocessing (Videos to Frame separation)

In this step the input video will be preprocessed by separation of frames. The frames are separated which can be then used as a cover image for the data hiding process. The selected image which is been selected from the set of frames can act as the cover image. This image is then partitioned into smooth and complex regions for data embedding. Image Partitioning is the process of partitioning the images into group of pixels that are homogenous with respect to some criterion. Different groups must not intersect each other, and adjacent groups must be heterogeneous. Segmentation algorithms are area oriented instead of pixel-oriented.

Encryption Process

In this step, the cover image is encrypted. Encryption is the process of encoding messages in such a way that third parties cannot read it, but only authorized parties can. This encryption process allows secured transmission of cover image. The cover image is encrypted and then data embedding process is done. This is because third parties can identify the data embedment and so first of all cover image is encrypted.

Here symmetric key encryption is used. In this encryption scheme, the encryption and decryption keys are the same. Sender and receiver must share the secret key before communication. The advantage of using this type of encryption is that, it is extremely secure as only the sender and receiver are aware about the key.

Embedding Process

In this step, the additional data which can be text, image etc., is embedded into the cover image which is been partitioned and encrypted. Data hiding is performed by RDH algorithm using the data hiding key. With the help of data hiding key, stego image is generated. Again the embedded data can be recovered only with the help of data hiding key and so the data can be securely maintained in the stego image.

Data Extraction Process

In this step, additional data is extracted from the stego image using the data hiding key. Once the additional data is extracted, cover image is needed to be recovered back. The cover image is decrypted using the same encryption key used during encryption of the image. After the original image being recovered, the frames are integrated back to form the original video.

VIII. CONCLUSION

In this project, Reversible Data Hiding technique is used which enables lossless recovery of the cover image. Using this technique, data hider can reserve space for data embedding prior to cover image encryption. In the existing system, additional data is embedded by vacating space in the cover image after encryption. According to the study on existing methods in previous papers of literature survey image quality is distorted and errors are detected in high rate for data extraction. But in this proposed technique secrecy and confidentiality is maintained for both the cover image and the

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

additional data. Using this technique, cover image can be retrieved with very much lesser errors and data extraction can also produce a recovered plain text in better manner.

REFERENCES

[1] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
[2] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.
[3] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3,pp. 721–730, Mar. 2007.
[4] WienHong, Tung Shou Chen., "Reversible Data Embedding for High quality Images using Interpolation and Reference Pixel Distribution Mechanism," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Apr. 2010.
[5] C.H.Yang, M.H.Tsai., "Improving Histogram based Reversible Data Hiding by Interleaving Predictions ," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Dec. 2009.
[6] Vimal, Mahendrakumar, "Reversible data hiding in images using DCT," IEEE Signal Process. Lett., vol. 3, no. 3, pp. 255–258, Jun. 2013.
[7] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
[8] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.
[9] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.