INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

REVERSIBLE INFORMATION HIDING IN VIDEOS

V.Priya[1] ,Sudharson.D[2]

[1] *PG SCHOLAR, Sri Krishna College of engineering and Technology, Coimbatore, priyavivek91@gmail.com*
[2] *PG SCHOLAR, Sri Krishna College of engineering and Technology, Coimbatore, sudharsondorai@gmail.com*

Address: 36/17, Metha Lay Out, Peelamedu,Coimbatore-641004,Tamilnadu, India
Phone: 0422-2571162
Mobile: +91 9600402395
Email ID: priyavivek91@gmail.com

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.

Keywords: Video, information hiding, reversible, confidential, encryption

1. 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 as in [8]. 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.

The rest of this paper is organized as follows. In Section 2, we discuss about the existing system of the project. In Section 3, the proposed system and architecture of the system is discussed. In Section 4, the expected results of the project are discussed. In Section 5, provides the conclusion and future work of the project.

1.1 Objective

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 converts the image into its encrypted version with the encryption key. Now, the

1.1 Objective

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 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. Obviously, standard RDH algorithms of better operators for reserving room before encryption and provides a better performance than the existing methods.

2. EXISTING SYSTEM:

Yang and Tsai proposed in [1] that , the embedding capacity can be largely increased by raising the heights of peak points in the histogram. The interleaving predictions is a technique where pixels in odd columns will be predicted by pixels in even columns, then pixels in even columns are predicted by pixels in odd columns, or vice versa. In the embedding process, predictive error values of odd columns are used to generate a histogram to embed secret data. Then predictive error values of even columns are used. In the extracting and reversing process, predictive error values of even columns are processed. Then predictive error values of odd columns are processed.

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.

The datas can be imbedded using interpolation errors proposed by Wien Hong as in [5] The reference pixels are adaptively selected in the cover image and pixels other than the reference pixels are interpolated. Interpolation errors are obtained by subtracting the interpolated pixels from the original image. Pixels with larger interpolation errors will be excluded in the embedding process and only those interpolation errors smaller than a pre-defined threshold are employed to conceal data. Data bits are then concealed by modifying the interpolation errors. Because reference pixel values are not changed in the embedding process, the same set of interpolated pixels can be obtained in the decoding process and thus, the embedded data bits can be extracted and the original image can be restored.

In [4], encryption as well as decryption is used. Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm, which usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys.

Thodi proposed a technique of Reversible Data hiding using Expansion embedding techniques[2]. Many of the early approaches to reversible watermarking can be categorized as modulo-arithmetic-based additive spread-spectrum techniques. The use of modulo arithmetic in additive spread-spectrum techniques, which are used in traditional watermarking systems, was to ensure reversibility. Although some of these techniques are robust, the modulo-arithmetic-based reversible data-hiding algorithms are inadequate because of the many wrapped around pixel intensities which not only cause salt-and-pepper artefacts but also hinder watermark retrieval. Another category of high-capacity reversible data-embedding algorithms may be classified as expansion-embedding approaches. A common feature of these approaches is the use of some decorrelating operator to create features with small magnitudes. The data embedding is done by expanding these features in order to create vacancies into which the data bits are embedded.

The resulting high-pass components are the differences of the adjacent pixel values; therefore, this technique is called difference-expansion (DE) embedding. The DE technique is able to embed significantly larger amounts of data than the other earlier approaches. The distortion introduced is also significantly less for comparable payload sizes.

3. 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 Fig. 1 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 Phase Alternative Line (PAL) or National Television System Committee (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.

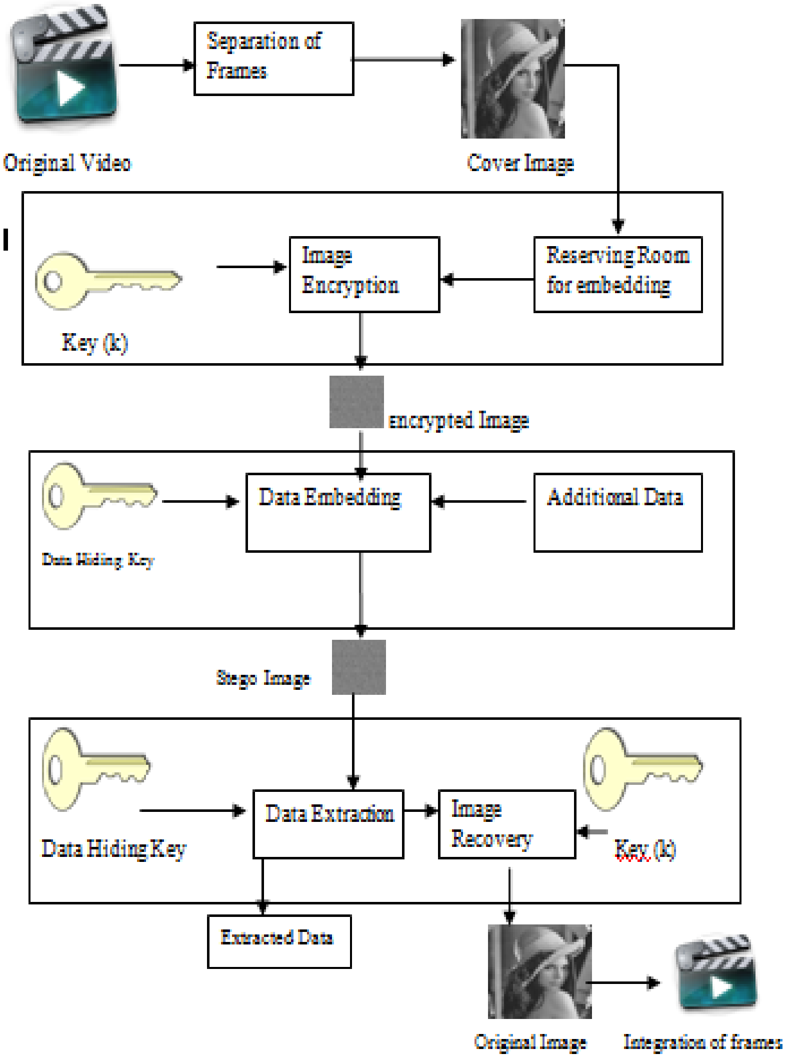

Fig. 1 System Architecture

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 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.

The steps involved in this are as follows:

Video Preprocessing (Videos to Frame separation)

In this step the input video will be pre-processed 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.

4. EXPECTED RESULTS

The standard images have been taken for the analysis of the project. The expected results of the project will both the original image and the embedded image will be identical to each other. The PSNR values of both the images have high embedding rates and provide larger payloads.

5. 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 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. Future work of this project would be Reversible Data Hiding using color images. The PSNR values of the image extracted will be significantly improved. The results of integration of the AVI video files will reflect the same as the original video with minimum distortion.

REFERENCES

1. 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.
2. 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.
3. 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.
4. Vimal, Mahendrakumar, "Reversible data hiding in images using DCT," *IEEE Signal Process. Lett.*, vol. 3, no. 3, pp. 255–258, Jun. 2013.
5. 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.
6. 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.
7. 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. 2011W
8. X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

A Brief Author Biography

V.Priya *– Completed B.Tech(INFORMATION TECHNOLOGY) in Sri Ramakrishna Engineering College from Anna University Chennai. Now pursuing M.E (SOFTWARE ENGINEERING) in Sri Krishna College of Engineering and Technology under Anna University, Chennai. My research interests include Information Security and Data Mining*

Sudharson.D*-Graduated as Computer Science Engineer from Coimbatore Institute of Engineering and Technology from from Anna University Chennai. Now pursuing M.E (SOFTWARE ENGINEERING) in Sri Krishna College of Engineering and Technology under Anna University, Chennai. I am passionate about Image processing and Database Technology*