International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

Secret Data Hiding Approach with Compression and Enhancement

K,Anitha
PG scholar
GudlavalleruEngineering College

P.Ravisankar
Assistant professor
GudlavalleruEngineering College

Abstract:In this project data hiding in video sequence based on the RSA Algorithm for law forensic, medical, military and satellite images is proposed. The side information is embedded along with the message bits into the host image so that the original image is completely recoverable. Then the secret message is be encrypted by RSA algorithm is the most excellent encrypted method since if the attacker obtains the video and decodes the video, the attacker can simply get the cipher text not the inventive secret message. So the RSA algorithm gives more confidentiality and privacy Data hiding plays an important role in protecting sensitive data, it is proposed to compute performance metrics like Peak Signal to Noise Ratio (PSNR), Mean Square Error(MSE), so as to come out with the invertible or lossless data hiding the contrast of a host image to improve its visual quality.

Key words: RSA algorithm,law forensic, medical, military, satellite image,secret message,sensitive data

1. Introduction

As multimedia becomes an important form of information exchange, a large number of digital products are created and transmitted via the Internet. One of the characteristics of digital products is that they are very easy to create, to store, to duplicate, to transmit, and to modify. These results in a serious problem because unauthorized use, copy, or modify of the products will also become very easy. How to protect the products in various aspects presents a problem that challenges the Academicand the business. Several technologies have been proposed for intellectual property right (IPR) protection [1]. One is encryption. However, conventional encryption and copy protection mechanisms do not fully solve this issue in some applications. Recently, data hiding is proposed as a hopeful method for authentication, fingerprint, security, data mining, and copyright protection [2]. Image data hiding represents a class of processes used to embed the data of secret image into another image which is defined as cover images [10]. The hidden data usually can be a string of binary bits (e.g., digital signature), a logo image, identification (ID) number, or any information that is useful [11]. In these approaches, the embedding process should be reversible [5].Usually, steganography is used as a tool for covert communication by embedding the secret data into the cover files such as images, audio and video. In this paper, we only discuss image steganography. For security, steganography should have the ability to resist steganalysis whose purpose is to detect whether a image is modified by steganography. State of the art steganalysis is to extract feature from the image according to the correlation of adjacent pixels and then to train classifier with machine learning [8][9]. To improve security, most recent steganographic methods try to embed data by modifying the complex regions of images that have weak correlation and are difficult to be modeled .

When using image steganography, such as those in [7][10], for covert storage, we can get high detectability. However, different from covert communication, the image here is used as a special kind of storage medium that needs to be erasable as traditional storage medium (e.g. disk). In other words, after the stored data being deleted, the storage medium can be restored to its original state. To make the image “erasable”, the data hiding method must be reversible and thus the image can be used repeatedly. From this point, reversible data hiding (RDH), which is another branch of data hiding, is suitable for covert storage. By RDH, the cover image can be losslessly restored after the message being extracted.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

2. LITERTURE SURVEY

For studying the concepts of video steganography, we have surveyed many latest papers. In this section we have described the relevant papers of different authors. We thank these authors for providing the knowledge of video steganography. These papers were very important to us for studying the basic concept Arup Kumar Bhaumik, Minkyu Choi, RosslinJ.Robles, and MaricelO.Balitanas [9], the main requirements of any data hiding system are security, capacity and robustness It is very difficult to archive all these factors together because these are inversely proportional to each other. Authors have focuses on maximizing security and capacity factor of data hiding. The data hiding method uses high resolution digital video as a cover signal. It provides the ability to hide a significant quality of information making it different from typical data hiding mechanisms. They have used the large payloads like video in video and picture in video as a cover image. Ahmed Ch. Shakir [10], the confidential communications over public networks can be done using digital media like text, images, audio and video on the internet. Simply hiding the contents of a message using cryptography was not adequate. Hiding of message should provide an additional layer of security. To provide the more security the author suggested the new procedures in steganography for hiding ciphered Information inside a digital color bitmap image. He has used quadratic method depending on the locations concluded by the binary image, beside of public key cryptography. He had concluded that the conjunction between cryptography and steganography produce immune information. Andreas Westfield and Gritta Wolf [11], in this work author have described a steganographic system which embeds secret messages into a video stream. Normally the compression methods are used in video conferences for securing acceptable quality. But usually, compression methods are lossy because reconstructed image may not be identical with the original. There are some drawback of compression and data embedding method. Signal noise and irrelevance are common examples of data embedding. But compression methods try to remove signal noise and irrelevance. If signal is compressed more, then there are fewer possibilities of data embedding. The author have solved this problem, they have investigated a typical signal path for data embedding. Shailender Gupta et al. [12] have proposed an information hiding scheme for the least significant bit steganography along with cryptographic method. In this proposed scheme, the raw data was encrypted before embedding it into the image.To provide higher security, the secret value is. Meanwhile, the image pixels were also converted to binary form and then the encrypted secret information was embedded into the image by an LSB encoder. LaxmanTawade et al. [13] have proposed an efficient data hiding scheme using secret reference matrices. The data was hidden in 8 bit grayscale image using 256 X 256 matrix which was constructed by using 4 x 4 table with unreported digits from 0~15.The proposed method was to improve the holding capacity of cover image and increase the complexity to crack the Secret Reference Matrix (SRM). They also proposed a new spatial domain data hiding scheme by using a secret reference matrix (SRM) for data embedding and extraction. VikasTyagi et al. [14] have proposed a steganographic method using Least Significant Bit (LSB) along with a cryptographic algorithm. The symmetric cryptographic algorithm was used for encryption of the secret message. This algorithm uses random size of the key. After converting the information into secret code or encrypted form it was patched into the image. For patching the secret data, the least significant bit of the image was used.

3. EXISTING SYSTEM

Embedding and Extracting:

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M‟ s bit. This technique works good for image steganography. To the human eye the stego image will look identical to the carrier image.. For hiding information inside the images, the LSB (Least Significant Byte) method is usually used. This method is simple and easy to retrieve the data and the image quality is better so that it provides good security.

Least Significant Bit (LSB) embedding is a simple strategy to implement steganography. Like all steganographic methods, it embeds the data into the cover so that it cannot be detected by a casual observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane, LSB

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

embedding is performed on the least significant bit(s).

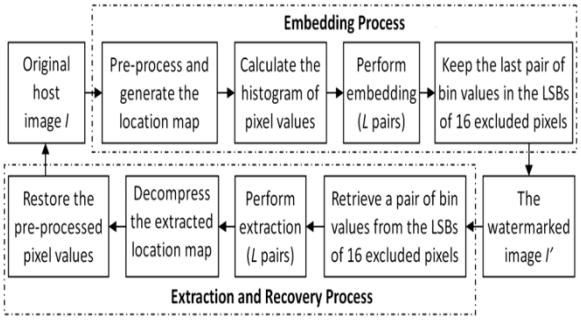

Fig 1. Block diagram of the existing system

This minimizes the variation in colors that the embedding creates. For example, embedding into the least significant bit changes the color value by one. Embedding into the second bit-plane can change the color value by 2. If embedding is performed on the least significant two pixels, the result is that a color in the cover can be any of four colors after embedding. Steganography avoids introducing as much variation as possible, to minimize the likelihood of detection. In a LSB embedding, we always lose some information from the cover image. This is an effect of embedding directly into a pixel. To do this we must discard some of the cover's information and replace it with information from the data to hide. LSB algorithms have a choice about how they embed that data to hide. They can embed losslessly, preserving all information about the data, or the data may be generalized so that it takes up less space.

One of the major disadvantage associated with LSB method is that intruder can change the least significant bit of all the image pixels. In this way hidden message will be destroyed by changing the image quality, a little bit, i.e. in the range of +1 or -1 at each pixel position.

4. PROPOSED SYSTEM

Previous to performing experiment on the video file format and relate a variety of steganographic technique, imperative parameters, such as the numeral, size, timestamps, and location of the video tags, must be known since they are the definite data that will be changed and customized. Data size evaluation every frame of the Video is in use a data source for Data Hiding. Primary the highest size of the hiding data is intended. The size of the image is Then the secret message is be encrypted by with RSA algorithm is the most excellent encrypted method since if the attacker obtains the video and decodes the video, the attacker can simply get the cipher text not the inventive secret message. So the RSA algorithm gives more confidentiality and privacy.

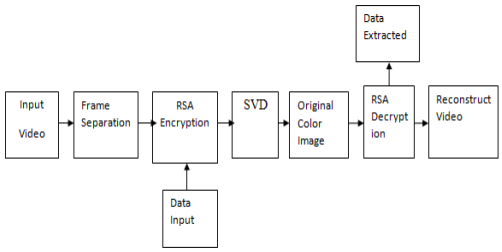

Fig 2.Block diagram of the proposed system

A. *Video Input*

Video signals differ from image signals in several important characteristics. Of course the most important difference is that video signals have a camera frame rate of anywhere from 15 to 60 frames/s, which provides the illusion of smooth motion in the displayed signal. Another difference between images and video is the ability to exploit temporal redundancy as well as spatial redundancy in designing compression methods for video. Such video is taken as input.

B. *Framing of video*

A complete image captured from a video during a known time interval is called as frame. Such numbers of frames are obtained from a video. These frames are used for further processing of data embedding; frames in video are always sequentially placed so at the time of data retrieval there is no need for searching the sequence of the obtained video and its frames.

C . *RSA Algorithm*

RSA is the algorithm used by modern computers to encrypt and decrypt messages. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message the opposite key from the one used to encrypt a message is used to decrypt it.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

RSA Algorithm steps

Step1: Choose p = 3 and q = 11

Step2: Compute n = p * q = 3 * 11 = 33

Step3: Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20

Step4: Choose e such that 1 < e <φ(n) and e and n are co prime. Let e = 7

Step5: Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]

Step6: Public key is (e, n) => (7, 33)

Step7: Private key is (d, n) => (3, 33)

Step8: The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$

Step9: The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

D. *Discrete Wavelet Transform*:

Wavelet Transform decomposes a signal into a set of basic functions, these basis functions are called wavelets. Wavelets are mathematical function that separate data into different frequency component with a resolution matched to its scale. DWT transforms used to improve the visual quality.

An image is decomposed into two different components i.e. high and low frequency.The low frequency usually contains slowly varying gray value information in an image.The high frequency components contain sharp variations in an image like edges and noise.

E *Singular Value Decomposition*

The Singular Value Decomposition is one of the most useful tools of linear algebra with several applications to multimedia which includes Image compression, watermarking and other Signal Processing. Given a real matrix, A (m, n); 1≤m≤M, 1≤n≤N, it can be decomposed into a product of three matrices given by equation1.

$$A = USV^{T} \quad (1)$$

Where U and V are orthogonal matrices, The main property of SVD based watermarking is that the largest of the modified singular values change very little for most types of attacks like transpose, flip, rotation, scaling and translation. The diagonal entries of S are called the singular value of A, the columns of U are called the left singular vectors of A, and the columns of V are called the right singular vectors of A. This decomposition is known as the Singular Value Decomposition (SVD) of A.

F. *Data Recovery*

At this stage, Secret hidden text messagesare extracted from encrypted video streams followed by reconstruction of video frames as shown in Fig.2. Hidden text are extracted using RSA decryption. Finally all extracted message characters are applied RSA module to decrypt the data with symmetric keys. Then the video bit streams are decoded to reconstruct the each encode frame and all the frames concatenated to form recovered original video.

G. *RESULT ANALYSIS*

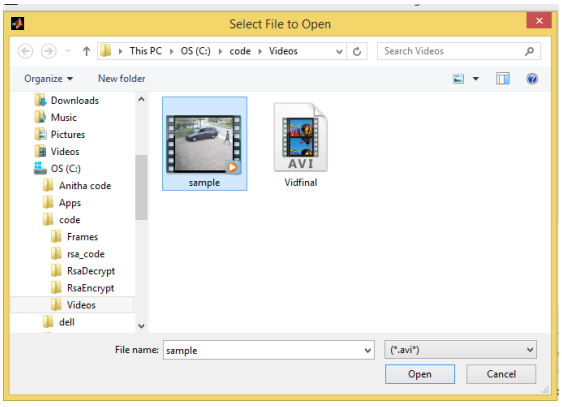

Fig 3 : Input video

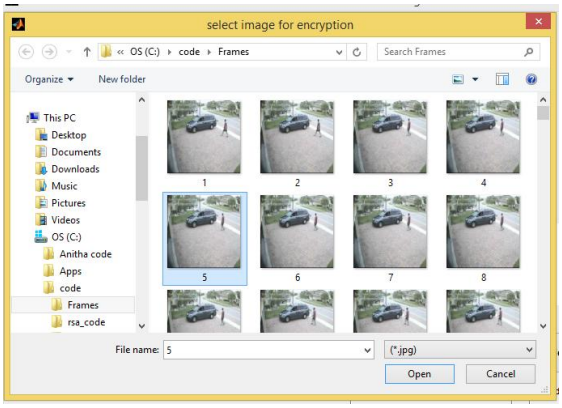

Fig 4: frame conversion

Fig 5:RSA encryption

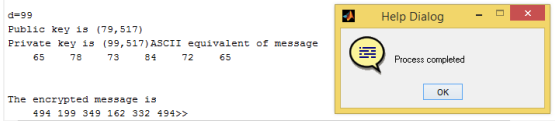

Fig 6: Encryption message

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

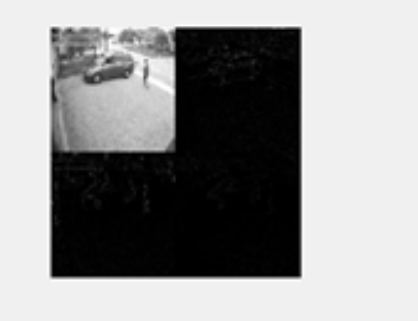

Fig 7: DWT image

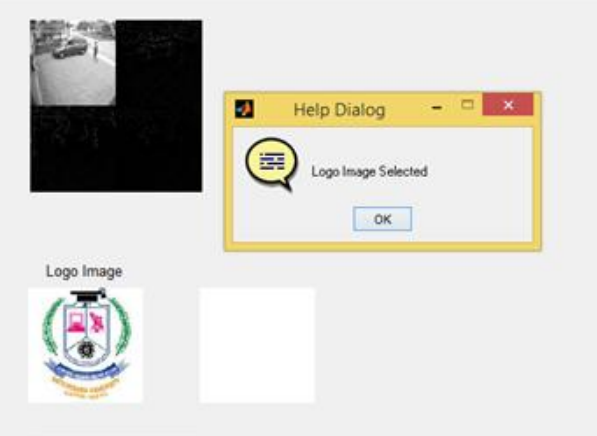

Fig 8: Logo image

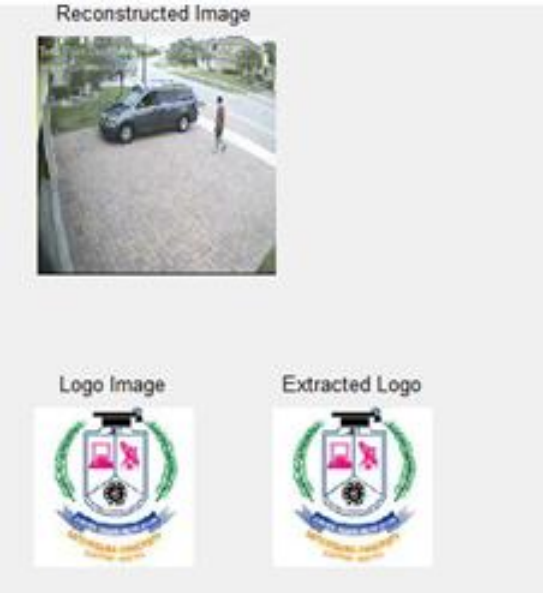

Fig: extraction of logo

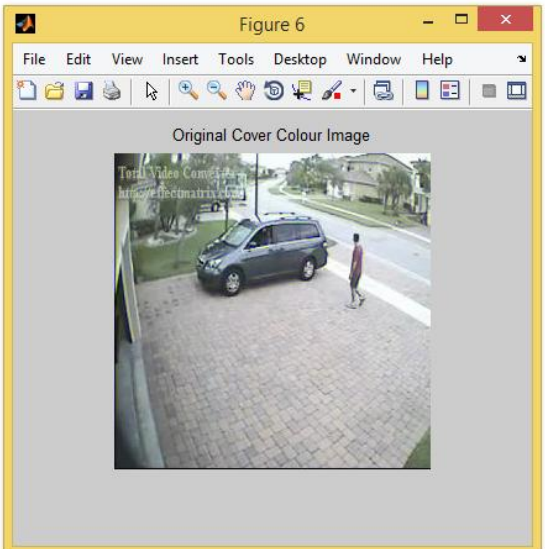

Fig 9: Original cover image

Fig 10: RSA decryption

```
The decrypted mes in ASCII is
    65   78   73   84   72   65
The decrypted message is: ANITHA
```

Fig 11 : Decrypted message

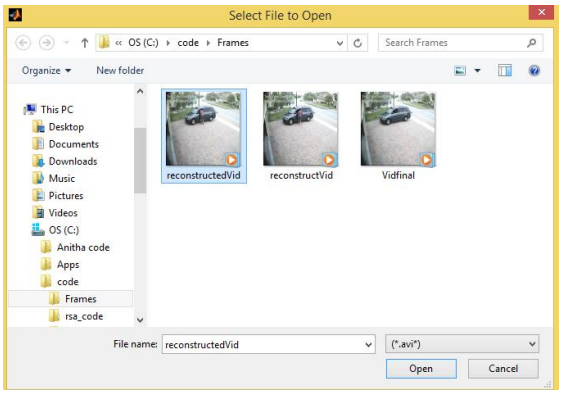

Fig12 : Reconstruct video

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

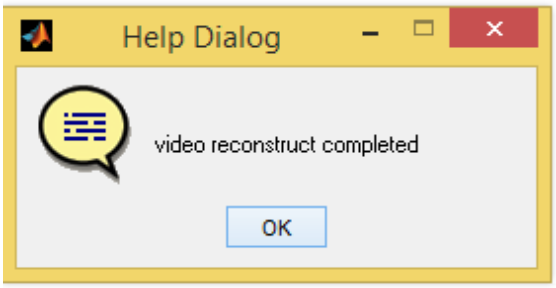

Fig 13: reconstruct completed

The Quality of the reconstructed image is measured in terms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance s_q^2. The MSE between the original image f and the reconstructed image g at decoder is defined as

$$\mathbf{MSE} = \sigma_q^2 = \frac{1}{N} \sum_{j,k} (f[j,k] - g[j,k])^2 \quad (1)$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is given by

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

Existing system PSNR	MSE	Proposed system PSNR
30.38	0.2000	55.12

Table1: MSE and PSNR values

The results showed that the proposed algorithm makes the secret message and video is more secure, and PSNR value is improved by a factor of 55%.

5. CONCLUSION

In this paper a novel method for data hiding in a video sequence. The goal of proposed algorithm is to encrypt the secret message using RSA algorithm and a then hide that encrypted message in the video frames using RSA algorithm.The secret message into cover video without producing any changes of quality of video. In this work, this is a new way of hiding the information in a video with more security. This project very much usable and trustworthy to send data over any unsecure channel.The results showed that the proposed algorithm makes the secret message more secure, improves the embedding capacity and PSNR is very good.

References:

[1]Hao-Tian Wu, Member, IEEE, Jean-Luc Dugelay, Fellow, IEEE, and Yun-Qing Shi, Fellow, IEEE " Reversible Image Data Hiding with Contrast Enhancement" IEEE SIGNAL PROCESSING LETTERS, VOL. 22, NO. 1, JANUARY 2015

[2] M.-Z.Gao, Z.-G.Wu, and L.Wang, "Comprehensive evaluation for HE based contrast enhancement techniques," Adv. Intell. Syst. Applicat.,vol. 2, pp. 331–338, 2013.

[3] H. T.Wu and J. Huang, "Reversible image watermarking on prediction error by efficient histogram modification," Signal Process., vol. 92, no. 12, pp. 3000–3009, Dec. 2012..

[4] Z. Zhao,H.Luo,Z.-M. Lu, and J.-S. Pan, "Reversible data hiding based on multilevel histogram modification and sequential recovery," Int. J. Electron. Commun.(AEÜ), vol. 65, pp. 814–826, 2011.

[5] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Jan. 2011.

[6] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

[7] 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.

[8] D. Coltuc and J.-M. Chassery, "Very fast watermarking by reversible contrast mapping," IEEE Signal Process. Lett., vol. 14, no. 4, pp. 255–258, Apr. 2007.

[9] Z. Ni, Y. Q. Shi, N. Ansari, andW. Su, "Reversible data hiding," IEEETrans Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

[10] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.