ISSN (Online) : 0974-5645
ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 8(1), 79–86, January 2015
DOI: 10.17485/ijst/2015/v8i1/53100

A Steganography Approach over Video Images to Improve Security

Mritha Ramalingam and Nor Ashidi Mat Isa*

Imaging and Intelligent System Research Team (ISRT), School of Electrical and Electronic Engineering,
Engineering Campus, Universiti Sains Malaysia, Nibong Tebal 14300, Penang, Malaysia;
mritha2011@gmail.com, ashidi@eng.usm.my

Abstract

Nowadays the growth of information technologies makes it convenient for people to transmit mass data like confidential biomedical records, banking or financial data through Internet. However, it also provides vast opportunities for hackers to filch valuable information. Therefore, security becomes an important issue. Steganography is a recently developed technique in the data security field and has received significant attention from both industry and academia. Digital data hiding methods can hide message in multimedia files for secret communications. This paper presents a secure data hiding technique for video images using random key encoding function. Secret data are embedded into the random Red Green Blue (RGB) pixel values of the cover-video images using an encryption key. The cover-video images are pre-processed to prevent overflow/underflow. Experimental results indicate that the extracted data are without any errors. The performance of the proposed scheme is proved in terms of security and (Peak signal noise ratio) PSNR values.

Keywords: Data Hiding, Random Key, Security, Video Steganography

1. Introduction

Steganography is the art of hiding data in digital multimedia files in order to have secure communication[1]. The purpose of steganography method is to hide the very existence of secret data by embedding data into different cover medium like text, images, audio and video[2, 3]. The goal of steganography is to avoid drawing suspicion to the transmission of a secret message. There have been many issues concerning the secrecy of confidential data such as the most important, medical records. These issues are answered by providing a secured technique called as steganography[3].

Steganography is a technique for hiding data in sensitive applications such as military, hospital, banking and legal fields. The digital image is one of the most popular digital medium for carrying covert messages. In general, video files are preferred due to their wide presence and the tolerance of human visual systems (HVS)[4]. Steganography on video files answer the needs for larger spaces in hiding or embedding data. Videos are generally just collections of images and sound. Each steganography communication system consists of an embedding algorithm and an extraction algorithm. To accommodate a secret message, the original carrier, also called the cover-medium, is slightly modified by the embedding algorithm. As a result, the stego-medium is obtained.

A steganography can be categorized into pure or secret key steganography. A pure steganography is a steganography system which does not require the prior exchange of a secret key. Embedding process (E) can be described as a mapping E: C x M → S, where C is the set of possible cover-medium and M is the secret message; S is the Stego-medium. The extraction process consists of a mapping D: S → M, C; extracting the secret message out of the stego-medium.

*Author for correspondence

A secret key steganography is a steganography system which requires the prior exchange of some secret key[5]. Figure 1 shows the key based simple steganographic system. Embedding process (E_K) can be described as a mapping E_K: C x M x K → where C is the set of possible cover-medium and M is the secret message; S is the Stego-medium, K is the secret key used to embed the secret message. The extraction process consists of a mapping D_K→C, M; extracting the secret message out of the stego-medium.

The rest of the paper is organized as follows. Section 2 presents the literature study. Section 3 presents the proposed steganography method. Section 4 discusses the results and performance of the proposed method. Section 5 concludes the work.

2. Literature Review

Steganography differs from cryptography in the sense that cryptography focuses on keeping the message secret while steganography focuses on keeping the existence of the message secret. The strength of the steganography can be amplified by combining it with encryption[6]. Based on the multimedia used, the steganography can be classified into text, image, audio and video[7, 8]. Text steganography hides the secret bits by formatting the text or by encrypting the data[9] using stego-key. Text steganography using digital files is not used very often since text files have a very small amount of redundant data[10, 11].

Image is composed of 8 bits per pixel i.e.256 colours[12]. The colours are generated from three primary colours namely red, green and blue (RGB). Various image steganography approaches have been designed in spatial and transform domains. Most commonly used spatial domain steganography approach is the LSB (Least Significant Bit) substitution technique. LSB method is the easiest and simplest method of hiding data in images[13]. The image based steganography tried to improve the capacity where in more than 50% of the original image size has been used to hide the secure messages[14]. A LSB substitution method was proposed to provide higher embedding capacity without sacrificing the imperceptibility[15]. In transform domain based steganographic techniques, the data hiding is performed using either polynomial structures, Fourier transforms, discrete cosine transforms, discrete wavelet transforms or integer wavelet transforms[16]. The audio steganography technique exploits the properties of the human auditory system to hide information unnoticeably[17].

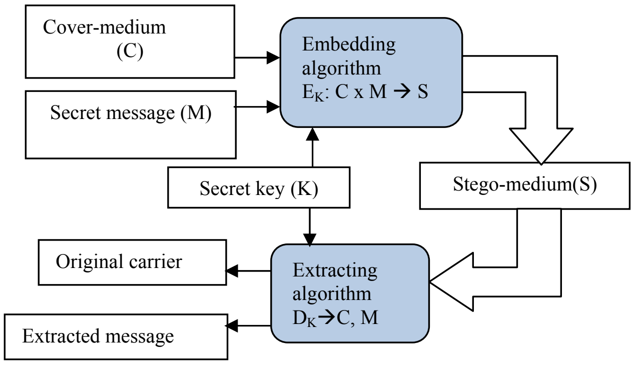

Figure 1. A key based basic steganographic system.

A steganographic approach using random pixel data hiding is proposed in[18]. The authors used the RGB values of the cover-image and LSB insertion method to hide the secret message bits in the red plane of the cover-image. The pixels are selected by using a random number generator. The use of video files as a carrier medium for steganography is more eligible as compared to other techniques. A video steganography method is proposed in [19] where data hiding is done on AVI File using Swapping and permutation encoding. The method works in a manner of hiding the data first in an image file and it will then be attached to a cover media which is the video file in AVI format. The extraction process is as simple as reversing the embedding process. However, the quality of the images needs further investigation.

Although the above discussed method proved to be have better embedding capacity[20], the security of the system need to be improved. Thus it is necessary to develop a steganography technique that can enhance the security based on the growing demands of current multimedia technology. As a result, a new steganography technique to improve the security using encryption technique is discussed in this paper.

3. The Proposed Method

The proposed steganography approach to improve the security is discussed in this section. Figure 2 shows the flow of the proposed steganographic technique. The data encoding and decoding processes are shown in the figure. The proposed algorithm is designed to embed text and image data into the video images. The embedding and extraction algorithm are discussed in detail.

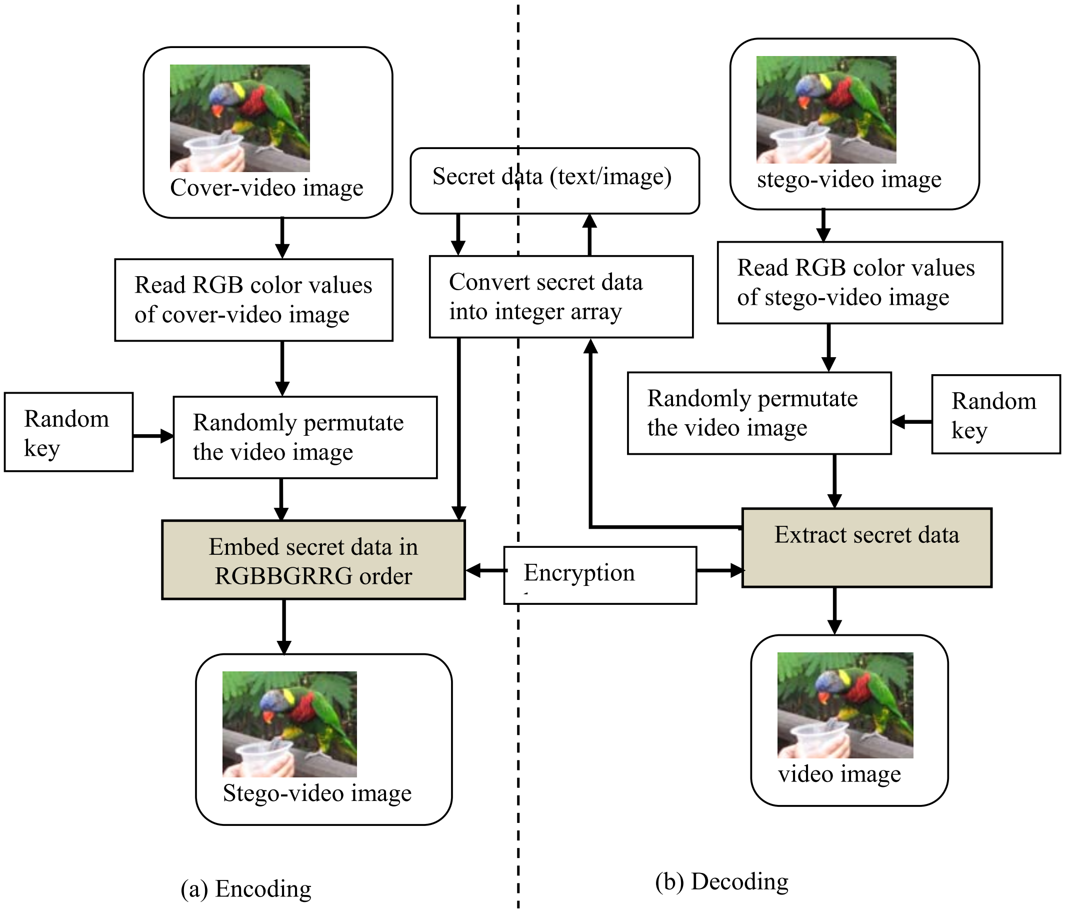
Cover-video image
Secret data (text/image)
stego-video image
Read RGB color values of cover-video image
Convert secret data into integer array
Read RGB color values of stego-video image
Random key
Randomly permutate the video image
Randomly permutate the video image
Random key
Embed secret data in RGBBGRRG order
Encryption
Extract secret data
Stego-video image
video image
(a) Encoding
(b) Decoding

Figure 2. The proposed steganography system.

3.1 Randomized Algorithm

The random algorithm has become a solution for the less secure methods like sequential encoding and simple LSB in video images. In this random algorithm, the sender and the receiver of the cover-video secretly share a stego-key that is employed as the seed for a pseudo-random number generator. This creates a sequence which is used as the index to have access to the RGB pixel values of the cover-video image. The message bit is embedded in the pixel of the cover image as the index given by the pseudo-random number generator using an encryption key. The two main features of the pseudo-random permutation methods are the use of password to have access to the message, and the well-spread message bits over the cover-video image.

This function determines the message type, prepares header information to be used in the decoding stage, and randomly encodes the message within the pixel values of the cover image. This function first determines the message type and length and encodes this as header information (first 24 randomly encoded values). Then the function uses the random permutation function to randomly select pixel locations to encode the message within. To do this the function determines the dimensions of the cover-image, multiplies the dimensions together to provide the number of pixels available and randomly permutate a list that includes values from 1 to the total pixel values available in a predictable and repeatable way by using the same random seed key value. The function then uses the random permutation list to encode the message values in the cover image. This function is faster than the sequential encoding because the pixel locations are precomputed rather than encoded using counters as well as more secure because the message is encoded across the entire image instead of the left portion of the image.

3.2 Encoding Algorithm

In this encoding process, a random key is used to permutate the cover-video image and then hide the secret data bits are hidden into the random pixels of the cover-video image. The transmitting and receiving end share the encryption key and random-key. The random-key is usually used to seed a pseudo-random number generator to select pixel locations in an image for embedding the secret message.

Inputs: Cover-video image, encryption key, random seed key, secret message

Output: Stego-video image

1. Read the text or image file that is to be hidden in cover-video image
2. Convert the input message into equivalent 8 bit integer array.
3. Read the RGB colour components of the cover-video image
4. Initialize the random key and randomly permute the pixels of cover-video image.
5. Initialize the encryption key and XOR with the secret message bits to be hidden.
6. Embed the secret message bits to those random pixels in the order, RGBBGRRG.
7. Write the above pixel values to result in stego-video image.

3.3 Decoding Algorithm

Inputs: Stego-video image, encryption key, random key

Output: Secret message

1. Read stego-video image
2. Recover header and random permutation values
3. Read the RGB colour components of each pixel.
4. Initialize random-key that gives the position of the randomly embedded message bits in RGB pixels.
5. Extract each of pixels that are actually containing hidden message bits.
6. The extracted values are permuted with encryption key and gives the secret message
7. Write the extracted message

4. Experimental Results and Discussion

4.1 Experimental Data Setup and Evaluation Criteria

The proposed algorithm is tested in MATLAB with RGB components of the cover-video images. In the proposed scheme, both text and image data are used as secret data for data hiding. The performance of the proposed method is analysed both qualitatively and quantitatively. The performance of the proposed steganography method is compared with method in [18].

The proposed method is evaluated based on the Peak-Signal Noise Ratio (PSNR) values and the distortion values using histograms of the cover-video images and stego-video images. PSNR is most commonly used parameter to measure the quality of images. Typical values of the PSNR for 16 bit data are between 60 and 80 dB[21]. PSNR is defined via the mean squared error (MSE). For two m×n images, cover video image, C and stego-video image, S, the MSE is defined by using Eq. (1) and PSNR is defined using Eq. (2).

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[\mathrm{C(i,j)} - \mathrm{S(i,j)}]^2 \tag{1}$$

PSNR is defined as

$$PSNR = 10\log_{10}\left(\frac{MAX_C^2}{MSE}\right) \tag{2}$$

Here, MAX_C is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented with B bits per sample, MAX_C is 2^B–1. For colour images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three.

Table 1 shows the details of the sample cover-video images used for the demonstration of the proposed method and different secret messages used for data embedding. Figure 3 shows the .bmp images used as cover-images and stego-images in the proposed method.

4.2 Qualitative Results and Analysis

Figure 4 shows an example of the application of proposed method on cover-video image, par.bmp. Figure 4 shows the results of embedding text and image into the cover-video image. In Figure 4a shows the original cover-video image, par.bmp.

4.2.1 Embedding Secret Message (Text)

The performance of the proposed method is visualized using the resulting stego-images obtained by embedding secret data of different size. The secret message of different length are converted into integer values and embedded

Table 1. Sample cover-video images and secret message

S.No	Cover-video (.bmp)	Size	Resolution	Secret message	Size (in bytes)
1	par	2.55 MB	1081 × 825	text1.txt	1548
2	clovers	80 KB	68 × 68	text2.txt	2002
3	tulips	91 KB	176 × 176	text3.txt	1300
4	flower	69 KB	163 × 152	aa.bmp	16800
5				caty.bmp	29000

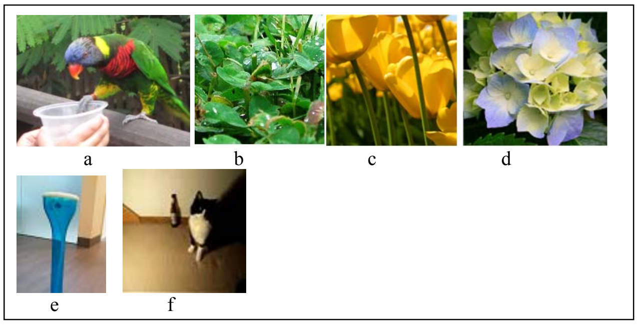

Figure 3. Cover-video images (a) par.bmp (b) clovers.bmp (c) tulips.bmp (d) flower.bmp; Secret images: (e) aa.bmp (d) caty.bmp.

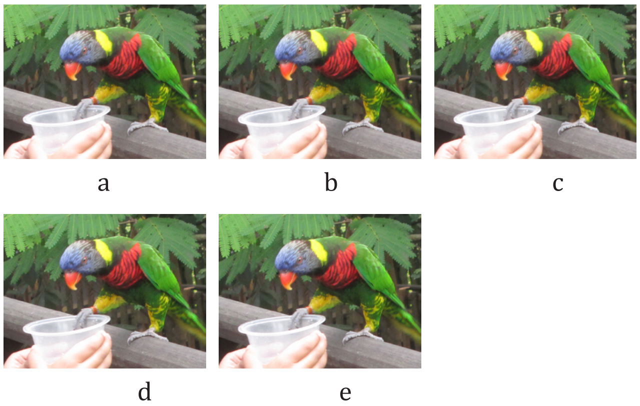

Figure 4. Example of proposed steganography method (a) Original cover-video image (b) Stego-video-text1 (c) Stego-video-text2 (d) Stego-video-aaimg1 (e) Stego-video-catyimg2.

into cover-video images. Figure 4b shows the stego-video image with embedded text, text1.txt. Here the size of the resulting stego image remains unchanged after embedding the text message of size 1548 bytes. Figure 4c shows the stego-video image with hidden text, text2.txt. The secret message, text2.txt of size 2002 bytes is hidden into the carrier. The stego-video image maintains the same size and quality which is similar to that of cover-video image. The message is hidden using proposed random key and encryption key process. The embedded data is extracted using the same keys use by the encoder. This proves the strength of the proposed method in terms of quality and security.

4.2.2 Embedding Secrete Message (Image)

The proposed system hides the secret image into the cover-image. Figure 4d depicts the stego-video image with embedded image, aa.bmp (size:16.8 KB, dimension: 66×86). From this, we observed that the size of the stego-video image is similar to the cover-video image after hiding the image of size 16.8 KB. Then, we hide the secret image (size: 29KB, dimension: 99×99) into the cover-video image. We observed that the resulting stego-video image is similar in size of the original image and the HVS is quiet unable to identify the occurrence of distortions in the resulting stego-image. The observed results of all the test images are shown in Figure 7.

The distortions obtained as a result of data embedding are hardly noticeable between the original cover-images and resulting stego-images. This can be visualized in Figure 5. In Figure 5, the cover-images and stego-images are shown respectively. From the figure, it is clearly proved that the difference between the cover-image and the resulting stego-images are hardly observable by HVS.

4.3 Quantitative Results and Analysis

The quantitative performance of the proposed method is supported by qualitative results as well. Qualitatively, the performance of the proposed method is evaluated using the histogram results and PSNR values. The histogram results of the proposed steganography method in RGB domain of a test cover-video image and the resulting stego-video images with different hidden secret messages are shown in Figure 6. Figure 6(a) shows the cover-video image; (b) shows the histogram results of the cover-video image; (c) is the stego-video image with embedded text1.txt;

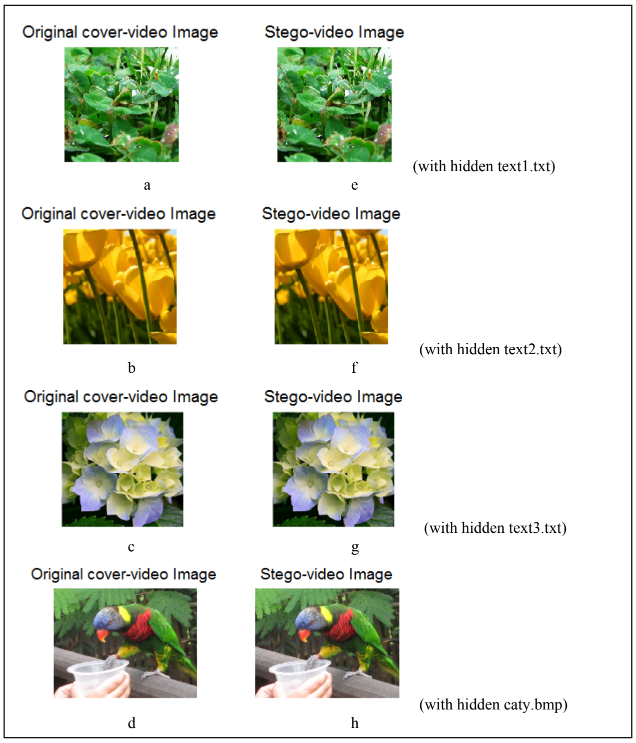

Figure 5. Original cover-images: (a) clover (b) tulips (c) flower (d) par; Stego-images: (e) stego-clover (f) stego-tulips (g) stego-flower (h) stego-par.

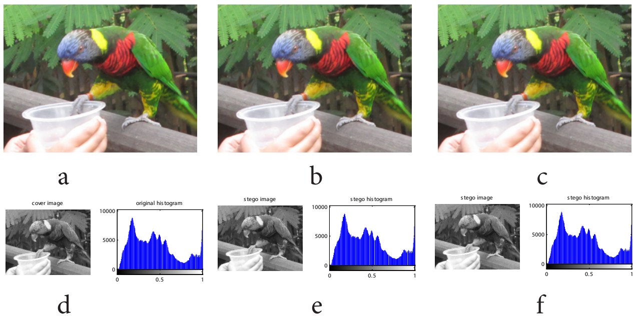

Figure 6 (a)–Original cover-video image, (b) stego-video image with embedded text1.txt (c) stego-video image with embedded caty.bmp; (d) histogram of carrier, (e) histogram result of stego-video image with embedded text1.txt; (f) histogram result of stego-video image with embedded caty.bmp

(d) is the respective histogram of stego-image containing embedded text1.txt; (e) is the stego-image with embedded image, caty.bmp; (f) shows the histogram result of stego-video image containing caty.bmp.

Quantitative result analysis:

S.No	Stego-images (.bmp)	Size (KB)	MSE (%)	
			Proposed method	Method in
1	Steg-clovers	80	0.03	0.09
2	Steg-tulips	91	0.03	0.07
3	Steg-flower	69	0.02	0.10

Encoding of secret message with encryption key and random seed value into the cover-video image is simplified as, secret message + encryption key + random seed key + cover-video image = stego-video image

Using the same encryption key and random seed value, the decoder extracts the hidden data from stego image. i.e Data extraction is simplified as, stego-video image + encryption key + random seed key = extracted data + original cover-video image

The stego-video frames retains the same size, because of the utilization of random seed key and encryption key for data encoding and decoding processes. Figure 7 shows the variation in size of the original cover-images and resulting stego-images. From the figure, it is clearly shown that the size of the original cover-image and the resulting stego-images obtained by hiding secret data using proposed method are same. The use of random seed and encryption key enables the efficient data embedding without varying the size of the cover-images.

Table 2 shows the MSE values measured over stego-video images with different hidden secret messages. The Table shows the MSE on the stego-video images using proposed method and method[18]. Also, Table 2 shows

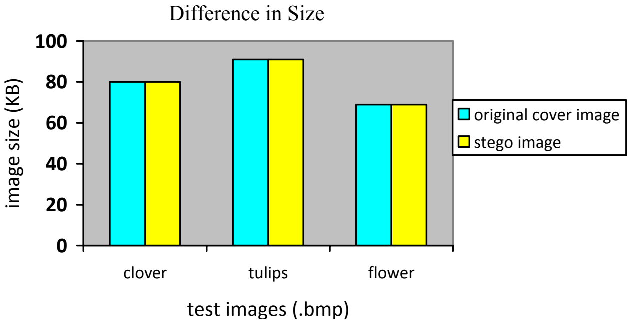

Figure 7. Difference in size: cover-images vs stego-images.

Table 2. Comparison of MSE values

S.No	Cover-image (.bmp)	Stego-image (.bmp)	Data embedded (in bytes)	Data extracted (in bytes)	MSE (%)	
					Proposed method	Method[18]
1	clovers (80 KB)	clovers	1548	1548	0.03	0.09
2	tulips (91 KB)	tulips	2002	2002	0.03	0.07
3	flower (69 KB)	flower	1300	1300	0.02	0.10

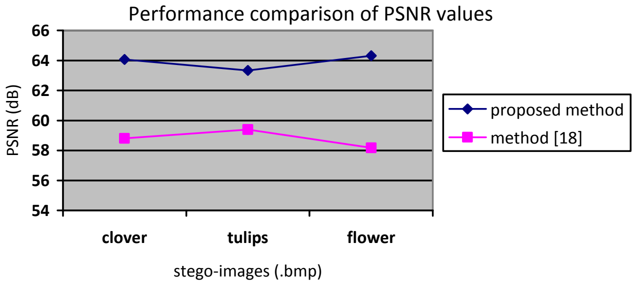

Figure 8. Performance comparison of PSNR values.

that the size of the embedded data and extracted data are similar using the proposed method. From the table, it is observed that the MSE values of proposed method are lesser than the comparing method. This proves the better quality and security of the proposed steganography system.

The lesser values of MSE indicate the better PSNR values. Figure 8 show the comparison of the PSNR values obtained using proposed method and method[18]. Similar cover-images and secret data are used to measure the PSNR values by applying the proposed method and method[18]. From the figure it is clear that the PSNR values of the proposed method are higher than the comparing method. This proves that the quality of the video images is retained intact without any distortions.

From the histogram results and PSNR values, it is observed that the quality of the videos is maintained well with less error values. The higher values of PSNR indicate the better quality and improved security of the proposed steganography method than the comparing method.

5. Conclusion

A random key based encoding and decoding in video images is proposed in this paper. The proposed method utilizes the encryption key to enhance the security of the system. The experimental results proved the quality of the video images are maintained well. From the results, it is concluded that the proposed method allows embedding of secret data of different length in the cover-video images without varying the size of the original video images. The hidden secret data is extracted without any errors. This proves the security of the random key encoding. The advantage of random key based steganography in video images is that the better security.

6. References

1. Anderson RJ, Petitcolas FAP. On the limits of steganography. IEEE J Sel Area Comm, Special Issue on Copyright & Privacy Protection. 1998; 16(4):474–81.
2. Rocha A, Goldenstein S. Steganography and Steganalysis in Digital Multimedia: Hype or Hallelujah. RITA. 2008; 15(1):83–110.
3. Cheddad A, Condell J, Curran K, Kevitt PM. Digital image steganography: Survey and analysis of current methods. Signal Process. 2010 Mar; 90(3):727–52.
4. Cetin O, Ozcerit AT. A new steganography algorithm based on color histograms for data embedding into raw video streams. Comput Secur. 2009 Oct; 28(7):670–82.
5. Chandramouli R, Kharrazi M, Memon N. Image steganography and steganalysis: Concepts and Practice. Proceedings of the 2nd International Workshop on Digital Watermarking; 2003 Oct.
6. Samima S, Roy R, Changder S. Secure key based image realization steganography. International Conference on Image Information Processing (ICIIP); 2013.
7. Wang H, Wang S. Cyber warfare: Steganography vs. Steganalysis. Comm ACM. 2004 Oct; 47(10).
8. Chen M, Zhang R, Niu X, Yang Y. Analysis of Current Steganography Tools: Classifications & Features. 2006.
9. Kataria S, Singh K, Kumar V, Nehra MS. ECR (encryption with cover text and reordering) based text steganography. IEEE Second Int Conf on Image Inf Process; 2013. p. 612–6.
10. Agarwal M. Text steganographic approaches: a comparison. Int J Netw Secur Appl. 2013; 5(1):91–106.

11. Shahreza MH, Shahreza M. A new synonym text steganography. IEEE Int Conf on Intelligent Inf Hiding and Multimedia Sig Process; 2008. p. 1524–6.
12. Amirtharajan R, Ramkrishnan K, Krishna MV, Nandhini J, Rayappan JBB. Who decides hiding capacity? I, the pixel intensity. 2012.
13. Al-Frajat AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB. Hiding Data in Video File: An Overview. J Appl Sci Res. 2010; 10:1644–9.
14. Lin CC, Shiu PF. High Capacity Data Hiding scheme for DCT-based images. Journal of Information Hiding and Multimedia Signal Processing. 2010; 1(3):314–23.
15. Swain G. Digital Image Steganography using Nine-Pixel Differencing and Modified LSB Substitution. Indian Journal of Science and Technology. 2014; 7(9):1448–54.
16. Djebbar F, Ayad B, Hamam H, Abed-Meraim K. A view on latest audio steganography techniques. Int Conf on Innovations in Inf Tech; 2011. IEEE. p. 409–14.
17. Wadhwa A. A survey on audio steganography techniques for digital data security. Int J Adv Res Comput Sci Software Eng. 4(4):618–22.
18. Laskar SA, Hemachandran K. Steganography based on Random Pixel Selection for Efficient Data Hiding. International Journal of Computer Engineering and Technology. 2013; 4(2):31–44.
19. Kavitha R, Murugan A. Lossless Steganography on AVI File using Swapping Algorithm, SRM University. Conference on Computational Intelligence and Multimedia Applications; 2007. p. 13–15, 83–8.
20. Leea Y, Cheng L. High capacity steganographic model. IEEE Proc Visual Image Signal Process. 2000; 147(3).
21. Huynh-Thu Q, Ghanbari M. Scope of validity of PSNR in image/video quality assessment. Electron Lett. 2008; 44(13).