International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 11 (2015) pp. 28495-28503

http://www.ripublication.com

Block Based Error Correction Code Watermarking With Video Steganography Using Interpolation And LSB Substitution

Gurbakash Phonsa
phonsa@gmail.com
Priya Sidhu
Priyasidhu9@gmail.com
Lovely Professional University

Abstract

Steganography is the act of concealing mystery messages (hidden content) inside everyday content (cover content) to deliver a stego content. The receiver of a stego content can utilize his insight into the specific strategy for steganography utilized to recover the hidden content from the stego content. Watermarking is a strategy for implanting concealed information that joins copyright assurance data to advanced data which gives an evidence of responsibility for computerized information. A digital watermark is a computerized signal or example embedded into a digital document, for example, text graphics or multimedia and carries information unique to the copyright manner. Interpolation strategies are utilized to enhance limit and picture quality and recover a cover image. Picture interpolation systems, for example, the closest neighbor, bilinear, bspine, cubic, Lagrange and Gaussian have been utilized for re-testing. Simple least-significant-bit (LSB) substitution is a system used to install mystery information in least significant bits of pixels in a host picture. Block based error correcting codingis convolutional code to enhance the strength of the implanted watermark.

Keywords: Steganography, Watermarking, Block-based Error Correcting Codes, Interpolation, Least Significant Bits.

Introduction

Watermarking and steganography are techniques in which the advanced picture is changed in a manner that one can see the foundation picture or the content without any sort of defilement in the picture. Watermarking is utilized to check the identity and validness of the owner of a digital picture. It is defined as a process in which the data which checks the manager is inserted into the computerized image or signal.

These signals could be either videos or pictures or audios. Case in point, acclaimed artists watermark their portraits and pictures. In the event that some individual tries to duplicate the picture, the watermark is duplicated alongside the picture. Watermarking is of two sorts; perceptible watermarking and imperceptible watermarking. As the name recommends, perceptible watermarking alludes to the data unmistakable on the picture or video. Perceptible watermarks are commonly logos or text [9][10]. For example, in a Television show, the telecaster's logo is noticeable at the right half of the screen. Imperceptible watermarking alludes to including data in a video or picture or sound as computerized information. It is not noticeable or discernible, however it can be identified by distinctive means. It can be recovered effectively. [12] It is utilized for copyright insurance, source following and annotation of photos.

Steganography is changing the picture in a manner that just the sender and the proposed beneficiary has the capacity catch the message sent through it. It is imperceptible, and hence the discovery is not simple. It is a finer method for sending mystery messages than encoded messages or cryptography as it doesn't pull in consideration regarding itself. [1] There are numerous routes in which steganography is carried out. The messages show up as articles, pictures, records, or now and then undetectable ink is utilized to compose between the lines. Steganography is attained by disguising the data in machine records. Once in a while stegano-graphic codes are inside the vehicle layer like a picture document, archive record, media documents, and so on. Because of the extensive size of the media documents, they are viewed as perfect for steganography. Steganography is utilized as a part of present day printers or by insights administrations.

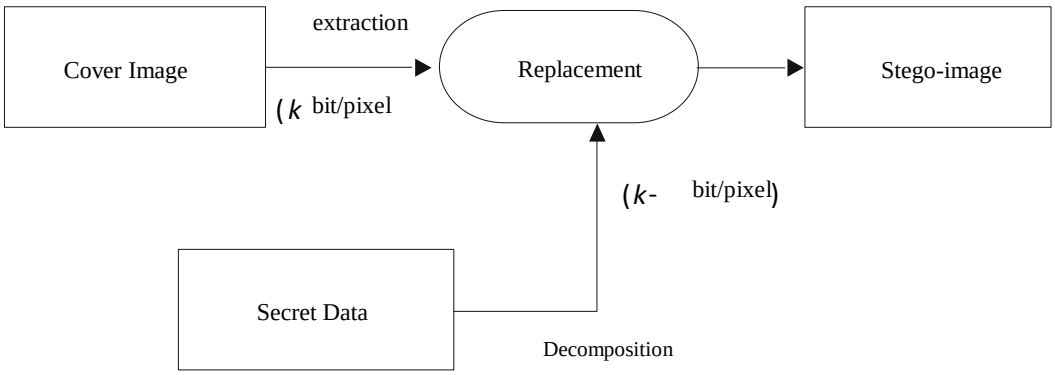

Figure 1: The embedding process [2] LSB substitution[1]

A. LSB Substitution & Interpolation*:*

LSB substitution techniques use the least bits of pixels in a cover image not to present twisting to the human eyes. Image interpolation methods are utilized to recreate a scaled Picture. It is an exchange off between the inserting limit and the picture quality.

LSB substitution conceals the mystery information in a few bits of every pixel of the cover picture. The hidden information are to be installed into the k-rightmost

LSB's of the cover picture. We can first recover the rightmost k-bit LSB from every pixel of the spread picture and adjust the mystery information to a k-bit by disintegrating every pixel. At last, the installing methodology is finished by supplanting the k-bit rightmost LSBs, and the stego-picture is acquired by supplanting k-bit with cover picture and mystery message. Image interpolation methods, for example, the closest neighbor, bilinear, B-spline, cubic, bicubic, Langrange and Gaussian have been utilized for re-examining. The closest neighbor technique can discover the closest comparing pixels of the cover image for each one square and set them to another pixel esteem for the terminus picture utilizing neighboring pixels. The bilinear interpolation strategy decides the new esteem from the weighted normal of the four closest pixels. These routines are utilized to change the extent of pictures to gauge obscure estimations of pixels [1].Recently, the Interpolation by Neighboring Pixels (INP) strategy was proposed to expand the payload in information hiding [2] [10].The idea of INP is that pixels at close neighboring areas have a tendency to have comparative power values. It implies that we can enhance the picture quality with less contortion.

B. Block Based Error Correction Codes:

Robustness is a most essential property of watermark. it implies that the watermark is still exhibited in the image and can be distinguished after contortion. Conceivably, the measure of image distortion important to debase the desired image quality ought to destruct and uproot the watermark in the conventional watermarking without ECC. So it is needed to improve the vigor of the installed watermark by presenting the ECC, which can control the mistake and enhance the dependability of information transmission in computerized correspondence. With ECC affixing some repetition bits in the first implanted watermark, along these lines a piece of the concentrated watermark can be adjusted [3] [5].The block based error correction code performs in two ways. It consist of a Transmitter and a receiver. The transmitter is a Forward error correction (FEC) encoder that maps every k-bit obstruct into an n-bit square code word. After that code word is transmitted and the signal is simple for remote transmission. The recipient demodulates incoming signal. The block is passed through a FEC decoder. [4]

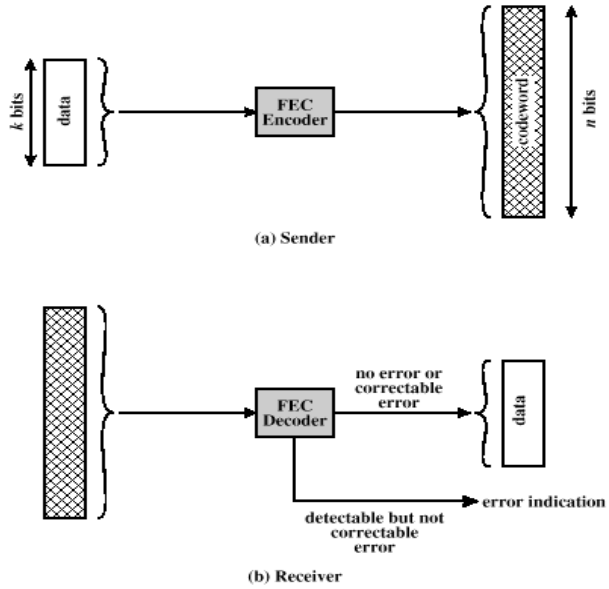

Figure 2: The Block Based ECC process [4]

This work can be further enhanced by using the soft computing techniques to ease the computation. These techniques helps enlarge to get the optimized results. [6]

Proposed Work

A. Embedding Process:

An Image is utilized as watermark for applying watermarking on stego pictures.

Step 1. Uploading an input video and extract frames from video.

Step 2. Applying addition on cover frames utilizing closest neighbor procedure.

Step 3. Text messages will be covered up into added cover frames utilizing LSB procedure.

1. Select a spread picture of size M*N as a data.
2. RGB part just of a picture is embedded with the message to be concealed.
3. Use a pixel decision channel to get the best ranges to cover information in the spread picture to get an unrivaled rate. Most significant bits (MSB) are left and the channel is joined with Least Significant Bit (LSB) of every pixel to cover information.
4. Bit Replacement system is used for shrouding the message.

Step 4. After inserting the hidden message in spread edges next step is to secure the stego picture utilizing imperceptible watermarking. Picture is utilized as imperceptible watermark. DWT method is utilized for undetectable watermarking.

1. First of all we stack the color video and afterward change over video into casings and edges into pictures.

2. Decompose each one picture into three color parts (RGB) and apply DWT to every part of video edge. [5]
3. Then apply watermark into LH and HL groups i.e. mid recurrence groups of each one level so change over every pixel esteem into twofold.
4. We begin to implant the watermark from Hl5 (fifth level mid recurrence band) and after that succession into LH5, Hl4, LH4, Hl3, LH3, Hl2, LH2, Hl1 and LH1.
5. Last put away the watermarked video outline information into exhibit for watermark extraction before applying reverse DWT.

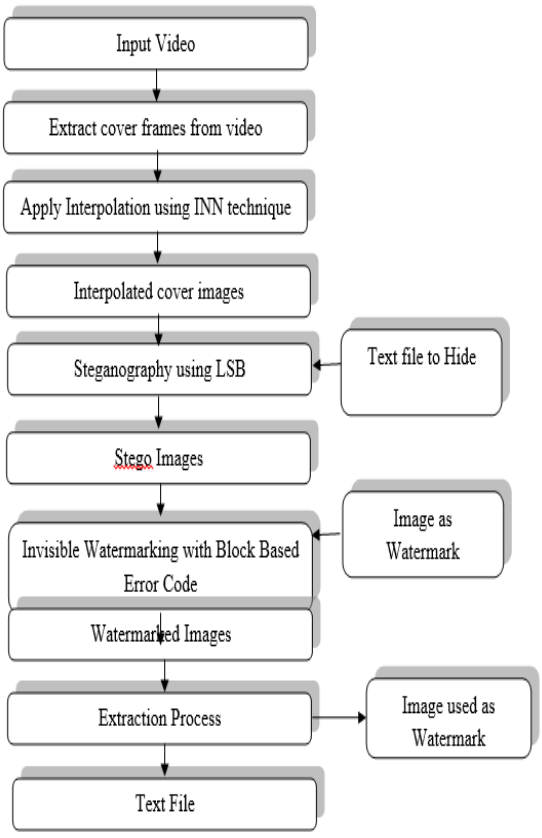

Figure 3: Proposed Model

B. Extraction Algorithm

Amid extraction transform the hidden message is concentrated from the watermarked stego document and we likewise concentrate picture that is utilized as watermark.

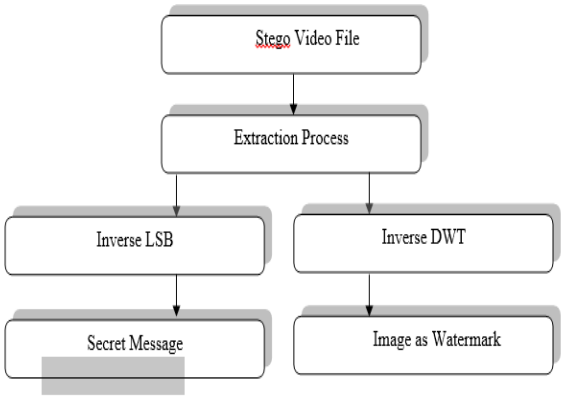

Figure 4: Algorithm of Extraction

Step 1. Extract the picture utilized as watermark utilizing IDWT calculation.

1. Load the watermarked video and after that different it into the casings.
2. Convert every pixel of mid recurrence band into paired and concentrate the hidden picture.
3. Combine three exhibits for three pictures RGB so that the first video will recover. [8]
4. After the de-watermarking process the hidden key will be matched with the first key if key is matched at exactly that point the hidden message will be recovered.

Step 2. Extract hidden instant message utilizing ILSB calculation.

1. Obtain the stego-picture.
2. Secret bits are concentrated the k-rightmost slightest huge bits of pixel.
3. Construct the concentrated hidden bits.
4. Repeat Step 2 through Step 3 until all hidden bits are concentrated.

Results and Discussions

The objective of research is to hide the secret message in video frames while maintain the better quality of frames, we use interpolation technique that provides better embedding capacity while maintain the quality of cover images so that very few distortion, which is unpredictable by human visual system, will affect the image.

A. Performance Analysis:

The following 5 videos are used.

(a) 001 (b) 002 (c) 003 (d) 004 (e) 005

Figure 5: Input Video Files

Proposed technique has been implemented over 5 input videos. From each video 40 frames are extracted for embedding process. Each frame is saved in .png format and resized with dimensions of 200x200. Interpolation is applied on these frames before applying the steganography process for secret message embedding. After applying the interpolation process, secret message is embedded in cover frames using LSB technique. Length of secret message embedded is 430 bytes and at last step for enhancing the security of stego video, invisible watermarking is used.

Performance of proposed work is evaluated using two measures- Mean Square Error (MSE) and Peak Signal to Noise Ration (PSNR) which are shown as the following.

Table 1: PSNR and MSE calculations for input videos using proposed work

S#	Video (200x200)	Image as a Watermark	Mean Square Error	Peak Signal to Noise Ratio
1	001	Baboon(512x512)	18.34	50.29
2	002	Desert (160x120)	21.57	47.69
3	003	Flower2(160x120)	35.19	40.73
4	004	Jellyfish(160x120)	36.43	39.49
5	005	Flower (160x120)	29.9	45.11

B. Comparison between proposed work and existing work:

In table 2 Peak Signal to Noise Ration (PSNR) is calculated for existing work and proposed work. Each input video is divided into frames with dimensions of (200x200) and interpolation technique is applied on each frame. After interpolation on frames secret file is embedded in frames using LSB technique. Digital image Baboon (200x200) is used as watermark on stego frames. Invisible watermarking is used on stego frames for copyright protection after invisible watermarking we will get secured stego video.

Table 2: Results of Proposed Work and Previous Work

S#	Video (200x200)	Image as a Watermark	Peak Signal to Noise Ratio (Existing work)	Peak Signal to Noise Ratio (Proposed work)
1	001	Baboon(512x512)	44.35	50.29
2	002	Baboon(512x512)	42.09	47.57
3	003	Baboon(512x512)	35.83	40.79
4	004	Baboon(512x512)	34.82	39.41
5	005	Baboon(512x512)	39.71	45.09

From the comparison of PSNR value with existing technique, obtained result shows that steganography with invisible watermarking can provide better results with interpolation with very less distortion in visual representation of cover images.

Experimental results shows that secured stego file with proposed work contain less noise and distortion which is non-identifiable for human visual system.

Conclusion & Future Scope

In this work, steganography used with invisible watermarking and interpolation technique is used for scale up the image before applying the steganography for data hiding. Each video is divided into 40 frames with dimensions of 200x200. Nearest neighbor technique for interpolation is one of the most basic forms of interpolation. As the genuine pixels are relatively replicated to their new areas, their position in connection to each other continues as before. With the most basic nearest neighbor interpolation, just copy the exact same pixel values over to the filler pixel closest to the pixel.Steganography procedure is requisitioned concealing the mystery message in picture utilizing LSB substitution. DWT method is utilized as a part of purposed work for the copyright security of information. Discrete wavelet transform divides an image into 4 coefficient images in the single level. PSNR and MSE are evaluated on watermarked stego videos and results shows that we can achieve better embedding capacity with less noise o cover media after applying the steganography using LSB and invisible watermarking.

This work is limited to acquiring watermarking from single video. The future scope can be extended to work on the different videos simultaneously .Also in future more parameters like by enhancing the number of pixels quality can be considered. As we can also extend this work for the infinite number of users. We can further apply new formulas or algorithm for the enhancement of PSNR in watermarking and reducing time for execution. The proposed algorithm can be implemented on different tools. To enhance this work the multi variant concept can be included with some defined level of threshold which can improve the security. [6]

References

[1] K.-H. &. K. Young, "Steganographic method based on interpolation and LSB substitution of digital images", *Springer Science+Media New York, 2014*.

[2] H. Y. Lee CF, "An efficient image interpolation increasing payload in reversible data hiding", *Expert Syst Appl 39:6712–6719, 2012.*

[3] J. c. Yonghong Chen, "Digital Image Watermarking Based on Mixed Error Correcting Code," *Journal of Information and Security, April 2012*.

[4] "www.ics.uci.edu," [Online]. Available: www.ics.uci.edu/~magda/ Courses/netsys270/ch10_2_v1.ppt+&cd=3&hl=en&ct=clnk&gl=in.

[5] S. B. D. A. C. N. A. S, "Robust Video Watermarking based on Discrete Wavelet Transform," *International Journal of Computer Network and Security, Jan-Mar 2012*.

[6] Phonsa, G. Sandhar, R. K.(2014, May). Distinctive feature mining based on varying threshold based image extraction for single and multiple

objects. In Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on (pp. 1537-1541). IEEE.

[7] Y. L. Chang-Tsun Li, " Steganographic Method for Colour Image Using Expandable Progressive Exponential Clustering," *IEEE International Conference on Digital Ecosystems and Technologies, 2007*.

[8] C. T. P. A. B. S, "A Survey on Different Video Watermarking Techniques and Comparative Analysis," *IEEE 10th International Symposium on Consumer Electronics, March 2006.*

[9] G. S. D. E, "Hidden influences on image quality when comparing interpolation methods," *IEEE 15th International Conference on Systems, Signals and Image Processing, June 2008*.

[10] N. S. S. Y. P. M, "A secure video steganography with encryption based on LSB technique," *Computational Intelligence and Computing Research IEEE International Conference on image processing, Dec. 2013*.

[11] "www.differencebetween.net," [Online]. Available: http://www.difference between.net/business/product-services/differences-between-watermarking-and-steganography/.