iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VI **Month of publication:** June 2018

DOI: http://doi.org/10.22214/ijraset.2018.6060

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

Reversible Data Hiding in Colour Images using AES Data Encryption System

M. Prem Anand[1], Y. Karthikeyan[2]
[1]*Assistant Professor* [2]*M.E Student*
[1,2] *Department of Electronics & Communication Engineering, Easwari Engineering College, India*

Abstract: ***This paper proposes the enhancement of security system for secret data communication through encrypted data embedding in Colour images. A given input image is converted to any one plane process. After plane separation, the encrypted data hider will conceal the secret data into the image pixels. The data hiding technique uses the LSB replacement algorithm for concealing the secret message bits into the input image. In the data extraction module, the secret data will be extracted by using relevant key for choosing the image pixels to extract the data. By using the decryption key, the data will be extracted from Input image to get the information about the data. Finally the performance of this proposal in Color Image and encryption data hiding will be analyzed based on image and Encrypted data.***
Key words: Lab VIEW, Data Extraction, Encryption, Decryption

I. INTRODUCTION

The identification of objects in an image and this process would probably start with image processing techniques such as noise removal, followed by (low-level) feature extraction to locate lines, regions and possibly areas with certain textures.
The clever bit is to interpret collections of these shapes as single objects, e.g. cars on a road, boxes on a conveyor belt or cancerous cells on a microscope slide. One reason this is an AI problem is that an object can appear very different when viewed from different angles or under different lighting. Another problem is deciding what features belong to what object and which are background or shadows etc. The human visual system performs these tasks mostly unconsciously but a computer requires skilful programming and lots of processing power to approach human performance.
Manipulation of data in the form of an image through several possible techniques. An image is usually interpreted as a two-dimensional array of brightness values, and is most familiarly represented by such patterns as those of a photographic print, slide, television screen, or movie screen. An image can be processed optically or digitally with a computer.

II. METHODOLOGY

This paper targets the internal dynamics of video compression, specifically the motion estimation stage. We have chosen this stage because its contents are processed internally during the video encoding decoding which makes it hard to be detected by image stego-analysis methods and is lossless coded, thus it is not prone to quantization distortions. In the literature, most work applied on data hiding in motion vectors relies on changing the motion vectors based on their attributes such as their magnitude, phase angle, etc.
The data bits of the message are hidden in some of the motion vectors whose magnitude is above a predefined threshold, and are called candidate motion vectors (CMVs). A single bit is hidden in the least significant bit of the larger component of each CMV, the data is encoded as a region where the motion estimation is only allowed to generate motion vectors in that specified region. Using the variable macro block sizes [16X16, 16X8, 8X8, 8X16] of H.264, the authors in used every 2 bits from the message bit stream to select one of the four sizes for the motion estimation process.

A .Data Hiding

Data hiding and watermarking in digital images and raw video have An image is a two-dimensional picture, which has a similar appearance to some subject usually a physical object or a person.
Image is a two-dimensional, such as a photograph, screen display, and as well as a three-dimensional, such as a statue. They may be captured by optical devices—such as cameras, mirrors, lenses, telescopes, microscopes, etc. and natural objects and phenomena, such as the human eye or water surfaces.

The word image is also used in the broader sense of any two-dimensional figure such as a map, a graph, a pie chart, or an abstract painting. In this wider sense, images can also be rendered manually, such as by drawing, painting, carving, rendered automatically by printing or computer graphics technology, or developed by a combination of methods, especially in a pseudo-photograph.

III. EXISTING METHOD

A. Cryptography

Cryptography prior to the modern age was effectively synonymous with *encryption*, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover
Theoriginal information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography is heavily based on mathematical theory and computer practise with assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are secure and solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same
key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.

IV. PROPOSED METHOD

A. Stegnography

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity, and hidden messages may be invisible. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

B .Watermarking

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in carrier. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is used for tracing copyrights. Watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

C, Cryptography VS Steganography

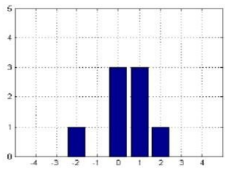
The protection of this multi-media data can be done with encryption or data hiding algorithms. To decrease the transmission time, the data compression is necessary. Since few years, a new problem is trying to combine in a single step, compression, encryption and data hiding. So far, few solutions have been proposed to combine image encryption and compression for example.

Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images. In this paper we propose an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

IV. RESULTS

It was found that the proposed method gives high payload in the cover image with very little error. This is of course on the expense of reducing PSNR and increasing the MSE. The high capacity is getting for the various applications using wavelet transform, Key-1 and Key-2 provides high security. The Optimum Pixel adjustment process was used for reduction of error between the input image and embedded image



Histogram of Prediction Error after embedding

154	155	155
154	154	156
152	154	155

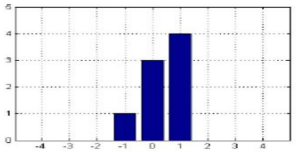
Fig.1 Embedding Result

154	**155**	**155**
154	154	155
153	154	155

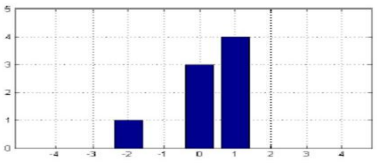
(a) An example of Cover block

0	**1**	**1**
0	154	**1**
-1	0	**1**

(b) Prediction Error block



(c) Histogram of original Prediction Error block



(d) Result of Histogram Shifting

0	**1**	**1**
0	154	2
-2	0	1

(e) Resultant of secret hiding

Fig 2. Intermediate Results

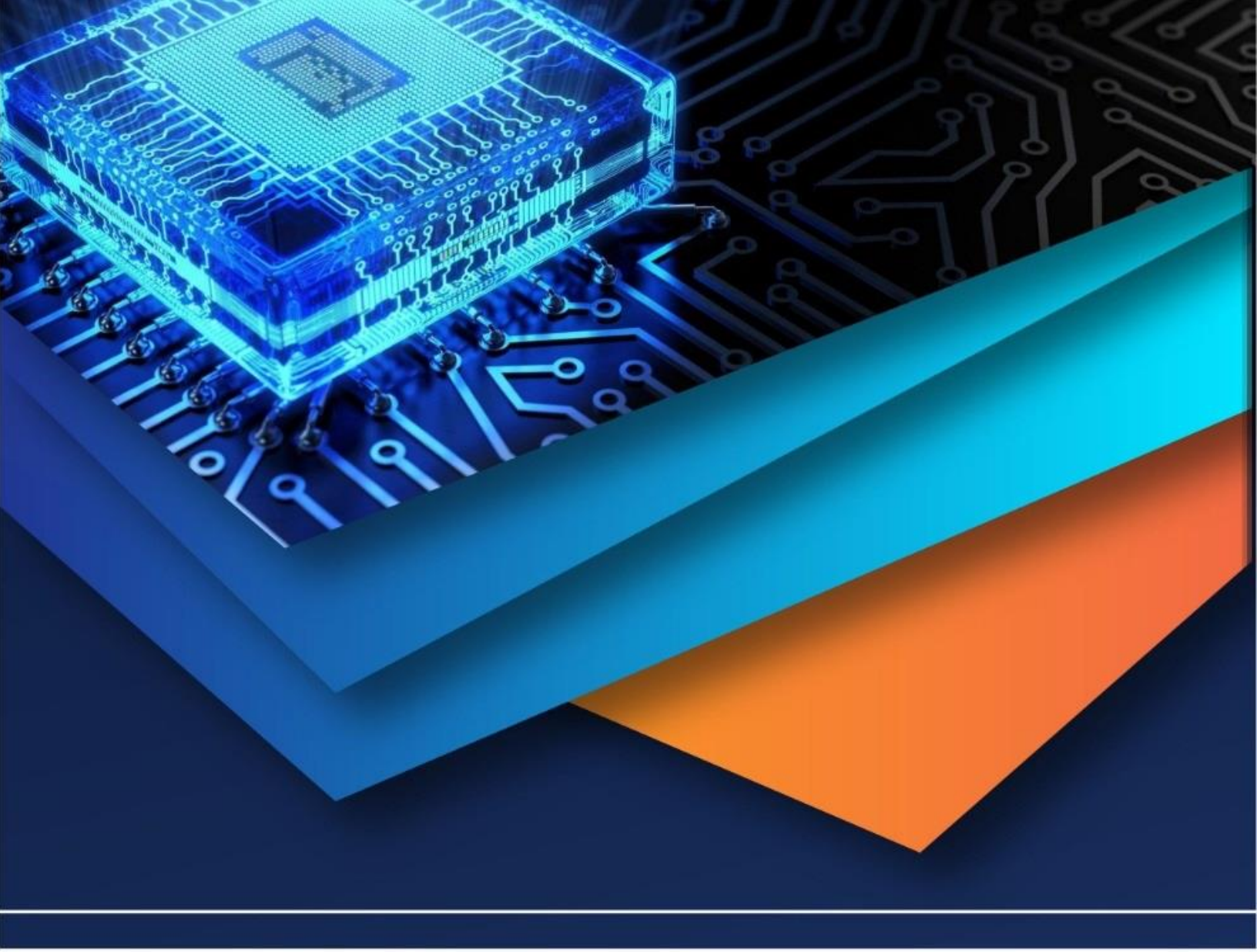
VI.CONCLUSION

Data hiding using steganography has two primary objectives firstly that steganography should provide the maximum possible payload, and the second, embedded data must be imperceptible to the observer. It should be stressed on the fact that steganography is not meant to be robust. It was found that the proposed method gives high payload in the cover image with very little error. This is of course on the expense of reducing PSNR and increasing the MSE. The high capacity is getting for the various applications using wavelet transform, Key-1 and Key-2 provides high security. The Optimum Pixel adjustment process was used for reduction of error between the input image and embedded image. The drawback of the proposed method is the computational overhead. This can be reduced by high speed computers.

REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt," Digital image steganography: Survey and analysis of current methods Signal Processing", 90 (2010),727–752
[2] C.K. Chan, L.M. Chen, "Hiding data in images by simple LSB substitution", Pattern recognition, 37 (2004), 469–474
[3] R.Amirtharajan, Adarsh D,Vignesh V and R. John BoscoBalaguru, "PVD Blend with Pixel Indicator - OPAP Composite for High Fidelity Steganography", International Journal of Computer Applications 7(9),(October 2010),31–37
[4] R.O. EI Safy, H. H. Zayed, A. EI Dessouki,"AnAdaptive Steganographic Technique Based on IntegerWaveletTransform", International conference on Networking and media convergence ICNM-(2009), 111 - 117.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY