International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-3 Issue-11 September-2013

New Median Based Adaptive and Robust Digital Image Secured System

Shivani Maheshwari[1], Pushpendra Singh Tomar[2], Manish Shrivastava[3]

Abstract

In the current digital era, Digital multimedia security has become a new research area involving applied statistics, cryptography, information hiding, & computer vision as some of the techniques. The demand for a framework that expedient the way of investigating the spatial redundancy existing in the digital multimedia that facilitate in the development of novel adaptive and robust digital multimedia security systems has increased enormously. In this paper, a new digital image secured system based on the combination of image statistics derived from median analysis and difference between the original and a stego image is shown. The key features of the proposed system and techniques can be summarized as: Universal, Adaptive, Lossless, Immune of digital image is predicted and shown.

Keywords

Image steganography, Data embedding, Statistical Restoration, Digital image security.

1. Introduction

In the current digital era, the rapid escalations in digital multimedia and network have paved ways for people roughly to attain, consume and share multimedia data. Digital data security has become a critical and imperative issue among the researchers with image & video scrambling a hot topic. The need for intellectual property right protection has become a new research area involving statistics, cryptography, information hiding, and computer vision as some of the techniques. Since, the information that could benefit or educate a group (or individual) can also be used against such groups (or individual). Other major applications of image scrambling techniques gyrate around pay-per-view TV, secured data transmission, confidential conferencing as well as various medical, banking and defences applications [1]. Data hiding is art of hiding sensitive data within the digital media without perceptible and statistical changes to the media. In general, the overview of data hiding encompasses within the areas of watermarking and steganography, along with applications has been presented. Digital steganography and watermarking are currently active research areas that deal with encompassing methods of patent protection, image validation, and protected interactions. Steganography (in Greek literally means 'Covered Writing') is widely employed for sharing a secret information/ message between two authorized users without revealing its presence to any of the third party viewers [12]. Technically, it is an art of secret communication. The real image and the embedded image are called the cover image and the stego image, respectively, in image steganography [2]. With the development of fast, powerful graphical computers, image embedding has become a hot topic in recent years. An image in a computer is an collection of numbers that embody light intensities of pixels. These pixels create the image's raster data. Digital images are combination of either 24-bit or 8-bit per pixel. Thus, 8-bit color images can be used to embed information. Here, each pixel is represented as a solitary byte; the range of each pixel is between 0 to 255.

A color image consist of red, green, blue components as main ingredients, which range from 0-255 in time domain [2]. The image can be represented in 8-bit planes i.e from 2^7 as **MSB** (most significant bit) and 2^0 as **LSB**(least significant bit).
Least Significant Bit(LSB) is the lowest bit in a series of numbers in binary; the LSB is located at the far right of a string. For instance, in the binary number: 1100110**1**, the least significant bit is the far right **1**.

This paper works on LSB's of image. Image can be embedded using LSB in two ways-

a. Sequential Access i.e. Raster scan
b. Random Embedding.

Shivani Maheshwari, Information Technology, L.N.C.T, Bhopal, India.
Pushpendra Singh Tomar, Information Technology, L.N.C.T,Bhopal.
Manish Shrivastava, Information Technology, L.N.C.T, Bhopal, India.

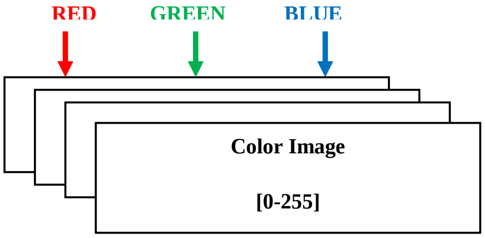

Figure 1: Components of Color Image

There are number of algorithms exists to embedd a color image. Image consist of several features like, mean, variance, normalized variance etc.. on which it can get experienced. First order statistic is used for pixel distribution through histograms ,which is not in scope of this paper.

2. Literature Survey

In current digital era, an organization or country's advanced digital security systems could easily determine their worldwide progress. Digital communication channels have expanded into a realm of mass digital media. Digital carriers include auditory, piece of mail and video mail, diskette breathing space, disk partitions and figure. With all the possible channels in existence today, digital steganography may be classified as an entity of its own with wide range of latent applications.

In this chapter, we discuss various existing steganographic systems for color and grayscale images while analysing their drawbacks and advantages. Further, we also propose that an approach which takes the image characteristics while hiding the secured information could offer improved robustness and embedding efficiency while maintaining its immunity as presented in figure 2. This motivated us in developing an algorithm that change it approach based on the embeddable blocks pixels that are available for hiding. This paper focuses on embedding efficiency and embedding capacity. Immunity to attacks is being not concentrated as per this paper is concern[11].

The digital images are used as cover images to embed information in a concealed manner within the bits of the image. A simplest steganography method involves the manipulation of the least significant bit (LSB) plane of the data.

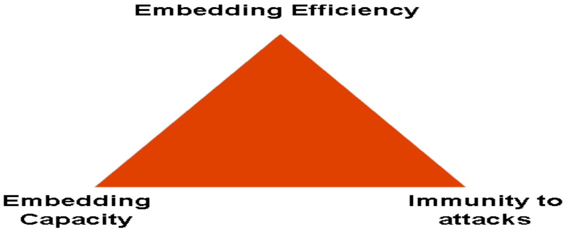

Figure 2: Various issues on steganographic algorithm

Diverse range of techniques, such as direct replacement of the cover's LSB with the information bits or an arithmetic combination between the two are used in several watermarking and steganography applications.

In 1994, Van Schyndel et al. [3] introduced two methods. The first is based on the direct bit-plane manipulation using M-sequence on the LSB of the image data. The use of LSB addition for embedding the secured data is made under second scheme. The decoding process makes the use of the unique and optimal auto-correlation function of M-sequence. The main drawback of these techniques is retaining the dynamic range of original image in order to retrieve the embedded information. The retrieve information could be distorted from the original secured information as the decoding process consists of the optimal auto-correlation function of M-sequence. The two dimension extension of M-sequence array for water mark for embedding more information, but the errors in the reconstructed secured information are reduced and still need the original information in order to retrieve the secured information embedded [4].

In 1996, R.B Wolfgang and E.J.Delp[5] presents a watermarking algorithm where longer M-sequences are employed. The binary M-sequence {0 1} is converted into {1 -1} for coding the watermark and by using longer M-sequence we could localize the changes to fixed locations within the image. This technique also needs the dynamic range of the original cover image in order to retrieve the embedded information.

In 1996, Smith and Comisky[6] introduced quite a few spread spectrum based data-hiding methods which utilize the message data "b" to modulate a carrier signal " ϕ ", which is then combined with the cover image in sections of non-overlapping blocks. The message is extracted via cross correlation between the stego image and the regenerated carrier; hence, cover image escrow is not necessary. A threshold operation is then performed on the resulting cross correlation to determine the binary value of the embedded data bits. Some of the hidden data may be lost if the phase of the modulated carrier is recovered in error. In addition, the amount of data that could be hidden using this method is low.

In 1996, an approach proposed [7] in time domain, called *patchwork* that embeds depending on the statistics of the original image acted as base for several steganographic systems developed. In this technique, pair of picture regions are selected using a pseudorandom series initially. Once a pair is elected, the pixel intensities within one region are increased by a constant value while the pixels of the second region are correspondingly decreased by the same value. The modification is typically small and undetectable, but is not restricted to the LSB. A texture mapping method that copies areas of random textures from one area of the image to another is also described.

These methods provide the basis for hiding data in the digital media while preserving the statistics. Unfortunately, they need original cover media intact to reconstruct the hidden data losslessly. In current digital world, methods that could retrieve the embedded information without prior knowledge of the cover image are gaining more importance. This motivated us to investigate new class of steganographic systems.

3. Methodology

The early approaches for detecting data embedding used to pay little or no attention to first order statistics, namely the histogram, based on the transform domain coefficients which were used for hiding. In this paper, we use a framework to counter such approaches that is based on the statistical restoration framework was proposed which ensures that the histogram, the feature used for steganalysis, remains unchanged after hiding. The main idea behind statistical restoration is as follows - if the feature to be used for steganalysis were explicitly known beforehand, a portion of the coefficients available for hiding can be used for data embedding while the remaining coefficients can be suitably modified to ensure that the statistical feature used for steganalysis remains unchanged.

The foundation of most adaptive embedding algorithms is the application of some manner of consideration to the specific cover media being used for embedding purposes. Image details are considered by the algorithm and good locations for embedding are selected based on local information gathered in the vicinity of a given cover pixel [8]. Many approaches have been proposed using such local measures as, standard deviation, median-based variance, variance, t-order statistics, as well as the number of unique pixel values within a given distance [9-10].

Image Mean

The image mean can be defined as the average pixel value of an image in consideration. In terms of grey scale image, the image mean is equal to the average brightness or intensity of a digital image. Mathematically,image mean ‘α’ can be presented as follows

$$\alpha = \frac{1}{n * m} \sum_{x=1}^{n} \sum_{y=1}^{m} im(x, y)$$

Where, image mean is denoted by ‘α’ and digital image is denoted by ‘*im*’ in consideration of size ‘*m***n*’. Further, this statistical measure defines where two regions within certain constraints could be merged or not.

Image Variance

The image variance can be defined as the spread of the pixel value of an image in consideration. In terms of grey scale image, the image mean is equal to the average brightness or intensity of a digital image. Mathematically, image mean ‘α’ can be presented as follows

$$\beta = \frac{1}{n * m} \sum_{x=1}^{n} \sum_{y=1}^{m} (im(x, y) - \alpha)^2$$

Where, ‘β’ is the image variance, ‘α’ is the image mean and ‘*im*’ is the digital image in consideration of size ‘*m***n*’. Further, this statistical measure defines where a regionis homogenous within certain constraints or contains image pixels over a broader range.

The digital images are used as cover images to embed information in a concealed manner within the bits of the image. A simplest steganographic method involves the manipulation of the least significant bit (LSB) plane of the data.

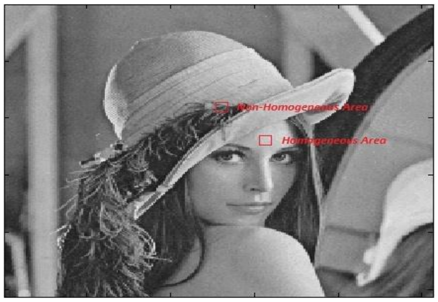

Figure 3: Shows the Homogenous area (image variance = 23.57) and Non-homogeneous area (image variance = 345.18) within the Lena image

4. Proposed Concept

The focus here is on developing an adaptive and robust digital multimedia security system. The proposed system offers highest level of security for applications ranging from copyright protection to secured communication. For implementing the work proposed, make use of Patch-work algorithm for embedding of data and image on the basis of calculating horizontal variance of each 3*3 block of image part. The following objectives are investigated:

a. Develop data hiding systems to hide significant amount of secured data with a limited distortion.

b. Develop and implement a new class of statistical structure for multimedia security systems for minimizing distortion.

c. Develop new concepts to design digital image security system with enhanced capacity.

The encoding process is an extensive process with many decisions and evaluations to be made depending on the desired security and capacity. If computational resources and processing time are crucial considerations as in implementation within a mobile device, a straightforward application may be formulated with less flexibility. Figure 4 is a diagram of the general structure of the encoding process.

Input Image

The cover image may be of any image format using the 8-bit, rule of 2's representation. Index images are to be included but with an additional pre-processing step of converting palette values into the RGB color space. The proposed algorithm may also be applied on 24-bit, three color layer images treating individual layers as an individual 8-bit image.

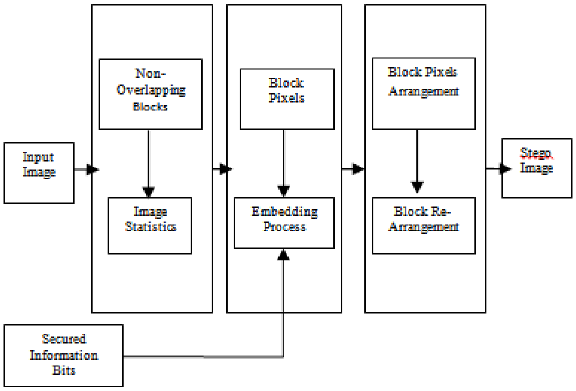

Figure 4: General structure of the encoding process

Secured Information Bits

The secured information that is needed to transmitted over the covert channel. It can be of any format image or text file are employed in this thesis. The data is converted into binary bit stream of "1" and "0" which would be used during the embedding process.

Embedding Procedure

Key is constructed based on selected parameters and the size and format of the secret message. If message is an image, dimensions are included; if the message is a text file, then the number of characters is included; if message is an auditory data, then numeral of sample is integrated; etc. Secret message is converted into binary representation and bits are incorporated into the least significant layers of the cover image. Image is reconverted back into decimal representation.

Post-processing Stage

This stage is a combination of recombining the image blocks and block pixel values. The stego image is recombined into various non-overlapping blocks of size {m, n} after embedding significant amount of information based the block statistics of the image are calculated. Each block is scanned and the presented variation measure is applied gauging the level of noise similarity within the proximal area of a given pixel. Again, horizontal and vertical edges are given less precedence while accentuating any diagonal edge power. Measure is assigned for all pixels and stored in memory.

Stego Image

The decoding process is a straightforward process where all necessary parameters are dictated based on the size of the secret message. Pixel selection variation process is applied and image is decomposed into normalized sequence based bit layers based on the specified sequencecode. Embedded bits are extracted and converted back into decimal representation. Secret message is then reconstructed.

5. Simulation and Analysis

In this section, the simulations results of proposed multimedia security system are presented. Computer simulations were simulated using MATLAB software package. Analysis was done using 100 color images of varying sizes, texture and contour. The experimental results demonstrate that the proposed system can provide excellent perceptual quality of marked image.The potential method include invisible annotation, alteration ,reverse embedding, transformation in time-domain, pixel occurance, edge detection and detection of image embedding ability.In addition, for testing the capacity barriers of the proposed system varying sizes of embedding message are employed. The simulations were carried out in three phases as shown in figure 5:

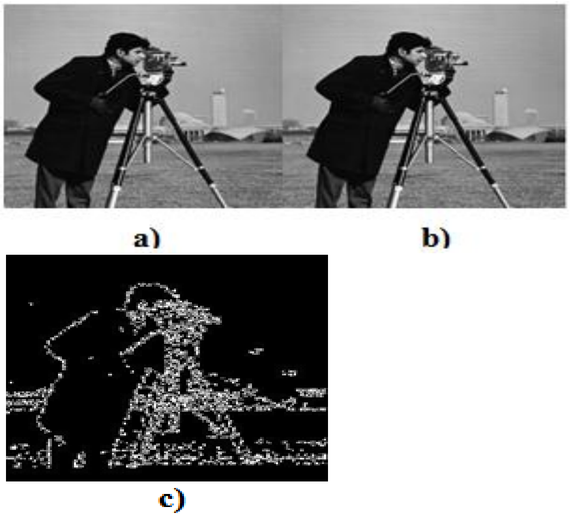

Figure 5 : a) cover "cameraman" gray-scale image b) Data embedding under cover image c)Stego image showing area where data is being embedded

6. Conclusion

In this paper, a new digital image secured system based on the combination of image statistics derived from median analysis is being designed. The key features of the proposed system and techniques can be summarized as:Universal, Adaptive, Lossless, Immune . In order to simultaneously enhance the embedding capacity and reduce any visual and statistical distortion in the cover image,we have divide each image matrix into 3*3 blocks,further calculated median of each individual blocks.On the basis of image statistics on LSB and find out exact bits to be embedded. This elaboration is formulated to further improve upon the benefits of the adaptive selection of the number of bits to embed per pixel needs to be addressed.

References

[1] N. F. Johnson, Z. Duric, S. Jajodia, Information Hiding Techniques Steganography and Watermarking Attacks and Countermeasures (Advances in Information Security), Springer Publishers, ISBN 1461369673, 2012.

[2] M. H. Mohamed,N.M.AL-Aidroos and Mohamed A. Bamatraf. " A Combined Image Steganography Technique Based on Edge Concept & Dynamic LSB",International Journal Of Engineering Research and Technology(IJERT), Vol 1, Issue-8, October-2012, pp.1-7.

[3] Van Schyndel, R.G.; Tirkel, A.Z.; Osborne, C.F.; "A digital watermark" Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference Volume 2, 13-16 Nov. 1994 Page(s):86 - 90 vol.2 .

[4] Tirkel, A.Z.; Osborne, C.F.; Van Schyndel, R.G.; "Image watermarking a spread spectrum application" Spread Spectrum Techniques and Applications Proceedings, 1996., IEEE 4th International Symposium, 22-25 Sept. 1996 Page(s):785 - 789 vol.2.

[5] Wolfgang, R.B.; Delp, E.J.; "A watermark for digital images" Image Processing, 1996 Proceedings, International Conference on Volume 3, 16-19 Sept. 1996 Page(s):219 - 222.

[6] J. R. Smith and B. O. Comisky, "Modulation and information hiding in images," in Information Hiding, First International Workshop, Lecture Notes in Computer Science, R. Anderson, Ed. Berlin, Germany: Springer-Verlag, 1996, vol. 1174, pp. 207–226.

[7] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems. J.*, vol. 35, 1996.

[8] Rafael C. Gonzalez and Richard E. Woods, "Digital Image Processing", Prentice Hall Inc., ISBN 0-201-18075-8, 2002.

[9] Wang, Zhou, Alan C. Bovik, Hamid R. Sheikh, and Eero P. Somoncelli. "Image Quality Assessment: From Error Visibility to Structural Similarity." IEEE Transactions on Image Processing, Vol. 13, NO.4, April 2004.

[10] Mitra, Sanjit K. and Giovanni L. Sicuranza. Nonlinear Image Processing. Academic Press Series in Communications, Networking, and Multimedia. San Diego, 2001.

[11] W. Bender, D. Gruhl, N. Morimoto and A. Lu . "Techniques for Data Hiding" IBM Systems Journal, Vol. 35, 1996, pp. 3&4.

[12] Stefan Katzenbesisser, Fabien A.Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House INC, ISBN 1-58053-035-4, 2000.

Shivani Maheshwari is form Bhopal(M.P),born on 18/05/1987.Is B.E, M.tech. Scholar(IT) in Laxmi Narain College Of Technology, Bhopal(M.P).

Pushpendra Singh Tomar is form Bhopal (M.P), born on 24/10/1984 is B.E, M.tech. (IT), is currently working as a Asst. Prof. at L.N.C.T, Bhopal (M.P). Active member of CSI.