ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

3-D Difference Histogram Modification for Reversible Data Hiding

MEERA K[1], MANU G THOMAS[2]

M. Tech Student Computer Science, Jawaharlal College of Engineering and Technology, Calicut University, India[1]

M.E, Computer Science and Engineering, Annamalai University, Chidambaram, India[2]

Abstract: 3-Dimensional Difference Histogram Modification for reversible data hiding is a technique, in which a reversible data hiding scheme is proposed by using difference-pair-mapping for 3-d images. For each pixel pair, it calculate the differences of neighbouring pixel values and select some difference numbers for difference expansion.. Then, a three-dimensional difference-histogram is generated. Finally, reversible data embedding is implemented according to the improved Difference Pair Mapping and LSB method. In 3-d Difference Histogram Modification for Reversible Data Hiding, a separable reversible data hiding is implemented. The LSB algorithm is improved to RGB-LSB algorithm for 3-d images. The image redundancy can be better exploited and an improved embedding performance is achieved by this approach. A pixel-pair-selection strategy is also adapted to use the pixel-pairs located in smooth image regions to embed data. This can further enhance the embedding performance.

Keywords: Reversible data hiding, Difference Expansion, Histogram Modification, image encryption, RGB- LSB technique.

I. INTRODUCTION

Now a day the data security and integrity are the two challenging areas for research. There are numerous researches progressing on the field like internet security, steganography, and cryptography. Steganography is the art or practice of concealing a message, or file within another message, image or file. The word steganography is of Greek origin and means “covered writing” or “concealed writing”. Steganography is an important sub-discipline of information hiding. It conceals private or secret information within a cover medium. The secret message, also known as the payload, is first embedded by the sender into the cover medium to produce the stego medium. The embedding is usually aided by secret keys in order to increase the security. Then the stego medium is delivered to the recipient party through a public channel. The goal of steganography is to keep the mere presence of the secret message undetectable. Only the sender and the recipient know the secret keys; therefore, third parties are not able to discover the secret message hiding in the stego medium as they are not able to extract the secret message without the legal secret keys. Various types of media can be selected to serve as the cover medium, including text, audio, video, images or three- dimensional models.

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. The word cryptography originated from the Greek word cryptology meaning “hidden secret”. More generally, it is about constructing and analysing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation. Data hiding is referred to as a process to hide data, representing some information into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. Data hiding has recently been proposed as a promising technique for the purpose of information assurance, authentication, fingerprint, security, data mining, and copyright protection, etc. By data hiding, pieces of information represented by some data are hidden in a cover media.

Images used in military, medical science are the media in which it found certain distortions sometimes which is not acceptable. Hence for data hiding it have a technique using which it can extract data correctly and after that original cover content can be perfectly recovered. This technique is also known as reversible data hiding or it is also named as lossless, distortion free, or invertible data hiding technique.

Reversible data hiding (RDH) aims to embed secret message into a cover image by slightly modifying its pixel values, and, unlike conventional data hiding, the embedded message as well as the cover image should be completely recovered from the marked content. RDH is a special type of information hiding and its feasibility is mainly due to the lossless compressibility of natural images. The reversibility in RDH is quite desirable and helpful in some practical applications such as medical image processing, multimedia archive management, image trans-coding and video error-concealment coding, etc.

Many RDH methods have been proposed so far, e.g., the methods based on lossless compression, difference expansion, histogram modification, prediction-error expansion, and integer transform, etc. Among them, the histogram-based ones have attracted much attention. The histogram-based methods modify the histogram in such a way that certain bins are shifted to create vacant space while some other bins are utilized to carry data by filling

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

the vacant space. This type of methods can well control the embedding distortion and provide a sufficient EC. For each pixel pair, it calculates the differences of neighbouring pixel values and selects some difference numbers for difference expansion. The original values of difference numbers, location of expanded difference numbers and the extra storage space are obtained by difference expansion.

Histogram modification is used to enhance the image. There are two methods of histogram modification. They are histogram stretching and histogram equalization. If the image is under exposed its values would only occupy the lower part of the dynamic range. The stretching of the histogram was actually performed on the luminance channel after converting the original image to HSL color space. Histogram equalization is a method for spreading the histogram of pixel levels more evenly.

Here it uses the Least Significant Bit (LSB) replacement for data embedding. LSB replacement replaces the least significant bits of pixels with secret data in a cover image. In LSB matching, it first converts the secret data into a stream of bits. Later the LSB of the cover pixel value is added or subtracted if the LSB of the next cover pixel does not match the next bit of secret data. It uses RGB color space for increasing the embedding capacity. An RGB color space is any additive color space based on the RGB color model. A particular RGB color space is defined by the three chromaticities of the red, green, and blue additive primaries and can produce any chromaticity that is the triangle defined by those primary colors. The complete specification of an RGB color space also requires a white point chromaticity and a gamma correction curve.RGB is a convenient color model for computer graphics because the human visual system works in a way that is similar though not quite identical to an RGB color space.

II. IMAGE ENCRYPTION BY XOR ALGORITHM

First of all, the three-dimensional color image has been taken as the input. Then split the image into its red, green and blue components. The image redundancy is the property that it utilizes here. The encryption process has to continue for all the three red, green and blue components. The XOR algorithm is utilized for encrypting the component images. In that, block permutation technique is utilized. In this technique, the image can be decomposed into blocks. A group of blocks is taken from the image and these blocks are permuted same as bit and pixel permutation. For better encryption the block size should be lower. If the blocks are very small then the objects and its edges don't appear clearly.

At the receiver the original image can be obtained by the inverse permutation of the blocks. The image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels keep their neighbour's. In this case the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the value of its neighbour's. At the receiver side, the original image can be obtained by the inverse transformation of the blocks.

The steps of the algorithm are as follows. First load the three dimensional input image. Then split into its red, green and blue components. Then input the 8 bit key. Convert each decimal pixel value into binary. After that repeat step for pixel in all three planes. Rearrange the bits according to the key entered. Then convert the permuted value back to decimal. Transfer a row of pixels into a temporary matrix. Permute the pixels according to the key entered. After that divide the image into 8 blocks, vertically and horizontally. Finally rearrange the blocks according to the key entered.

III. HISTOGRAM MODIFICATION AND RGB-LSB METHOD FOR DATA EMBEDDING

A histogram is a display of statistical information that uses rectangles to show the frequency of data items in successive numerical intervals of equal size. In the most common form of histogram, the independent variable is plotted along the horizontal axis and the dependent variable is plotted along the vertical axis. The data appears as colored or shaded rectangles of variable area. Histogram shifting could be explained as below. Each pixel contained in a digital photograph can have a value between 0 and 255. When the number of pixels having a value of 0, 1, 2…, 255, are plotted against the pixel value, it gets the histogram.

Pixels on the left of the graph represent the dark areas in the photograph, while the pixels on the right side of the graph represent the bright areas in the photograph. While allowing shifting the value of all the pixels to the right or left on the histogram graph, vacant spaces created to hide data. The brightness of the image change accordingly. The histogram is modified to create vacant spaces for hiding the data.

The Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-bit, 8-bit or gray scale format. In LSB technique, first select the message image that is to be hidden behind the cover image. Embed the required number of bits in order to hide the MSB (Most Significant Bit) of the message image behind the LSB (Least Significant Bit) of the cover image.

Since the MSB contains the most important information of the image and the LSB contains the message. This message can be retrieved only by that receiver who knows that it is a stego image sent by the sender. The data embedding technique of the system is RGB-LSB method. Here, the hidden data is embedded into the least significant bits of the red, green and blue components. In the Reversible data hiding scheme, it will first encrypt the original uncompressed red, green and blue components

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

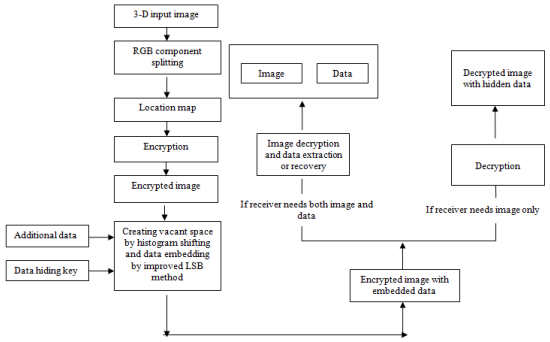

Fig.1: 3-D Difference Histogram Modification for Reversible Data Hiding

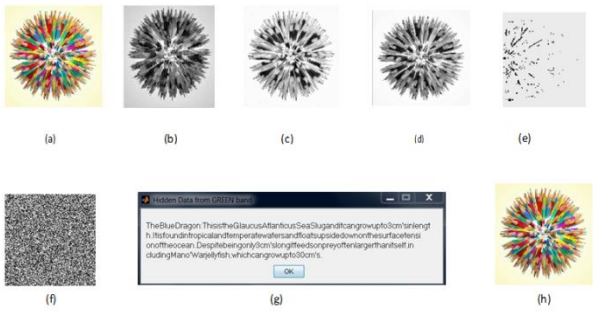

Fig. 2 : (a) 3-D input image (b) to (d) blue, red and green band images (e) location map (f) encrypted image (g)hidden data (h) recovered cover image

using an encryption key to produce an encrypted image and then follows the data-hiding process. In data-hiding, it embeds additional data into the encrypted image using a data-hiding key. Having an encrypted image containing additional data receiver firstly decrypts it using the encryption key and can further extract the embedded data. Thus there are mainly three processes, image encryption, data embedding and data extraction/ image recovery. Here after encrypting the image, the vacant spaces for hiding the data been created by histogram shifting and by the RGB- LSB method. In general, in LSB methods, hidden information is stored into a specific position of LSB of image. In the proposed method, it makes use of LSB of red color value, green color value and red color value. Thus it gets more space for data hiding and thus the embedding capacity is improved. The main aim of the work could be attained with the help of this technique. Moreover, here it uses a pixel pair selection strategy in our mapping stage. This is to represent the three dimensional points on a two-dimensional plane. By using this selection strategy, only those pixels on the smooth image regions are used.

IV. DATA EMBEDDING AND EXTRACTION PROCEDURE

After completed with the RGB component splitting, next comes the location map creation. The location map is used to solve the overflow and underflow problems. Location map is a binary sequence of particular length. It needs to losselessly compress the location map using arithmetic coding. The basic steps of reversible data hiding data embedding are as follows. First divide the cover image into non- overlapping pixel pairs. Then embed the secret message into part of the cover image, represented as A. Next, record the least significant bits of some of pixels of A, represented as B, to get a binary sequence, and embed this sequence into the rest of the part of cover image. Finally, by using LSB replacement, embed the auxiliary information and the compressed location map into B. In this process, it will not take the last two columns and last two rows, from left to right and top to bottom. This is because the embedding data into the edge, cause losing the cover image. The auxiliary information will contain the pixel-pair selection threshold, index of the last embedded pixel-pair, Length of the compressed location map and index of the last embedded pixel pair.

The data extraction and image restoration process is reverse to the embedding procedure. By reading the least significant bits of the marked image to determine the values of the pixel-pair selection threshold, index of the last embedded pixel pair, length of the compressed location map and index of the last embedded pixel-pair. By reading the least significant bits, determine the compressed location map. Finally generate the location map by decompressing the compressing the compressed location map. The next step is extracting the LSB sequence. Here also, it will leave the last two columns and last two rows left to right and top to bottom. While recovering the image there is a chance of noise in the pixel values. There are two types of non-functioning pixels. They are dead pixels and stuck pixels. Dead pixel is a pixel that reads zero or is always off on all exposures. This state produces a black pixel in the final image. A stuck pixel is a pixel that always reads high or is always on to maximum on all exposures. This produces a white pixel in the final image. These problems could be avoided and recovered by choosing a noisy level. Here it uses the GAP predictor to deal with the noise.

V. EXPERIMENTAL RESULTS

We implemented the proposed three dimensional difference histogram modifications for reversible data hiding with the help of MATLAB simulink. The version of this jsimulator is R2013a.We run the proposed system on a Windows 8 platform with h Simulator is R2013a.The proposed system run on a 32 bit Windows 8 platform with 4 GB RAM. MATLAB is a matrix oriented computing engine. Thus it is almost perfect for image processing because images can be thought of as matrices. The MATLAB works with various toolboxes to attain the functionalities. The input image is a three dimensional color image of size 512* 512.Then the image is split into its red, green and blue components. Then on each component location map is found and encrypted that image component. RGB-LSB replacement carried out to create vacant spaces and data is hidden. By using a data hiding key, it is possible to embed the data. While extracting the data and recovering the image, the same data hiding key is utilized. Thus, the data is obtained and image is recovered. It can be shown that the PSNR value is improvised and thus the embedding capacity is increased.

VI. CONCLUSIONS

The three dimensional difference histogram modification for reversible data hiding could improve the embedding capacity and quality. Thus more data could be embedded. This ca n be used in medical image processing where the cover image and the hidden data is important. This could also used for multimedia archive management and image trans-coding etc. The future works lies on embedding Multimedia data into the cover image. Thus other than text data, it could hide more forms of data.

REFERENCES

[1] A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference–Histogram Modification., Xialong Li, Weiming Zhang, Xinlu Gui and Bin Yang, Ieee Transactions On Information Forensics And Security, Vol. 8, No. 3, July 2013.

[2] V. K Agham and T.M Patteewar, "Separable Reversible Data Hiding Technique based on RGB-LSB Method," International Journal of Research in Advent Technology, vol. 1, no. 3, Oct. 2013.

[3] H.B Kekre, D. Mishra, R. Khanna, S. Khanna and A. Hussaini, "Comparison between the basic LSB Replacement Technique and Increased Capacity of Information Hiding in LSB's Method for Images", International Journal of Computer Applications , vol. 45, no. 1, May 2012.

[4] A. Dixit, p. Dharuve and D. Bhagwan, "Image Encryption using Permutation and Rotational XOR Technique," CS & IT Open-Access Computer Science Conference Proceedings, vol. 6, no. 3, pp. 01–09, 2012.

BIOGRAPHIES

MEERA K completed her B.Tech degree course in Information Technology from Nehru College of engineering and research centre, pambady which is affiliated to Calicut University. She is currently perusing her M.tech degree in Computer Science from Jawaharlal College of engineering and technology which is affiliated to Calicut University.

MANU G THOMAS received Bachelor Degree in Computer Science and Engineering from RVS College of Engineering and Technology, Dindikal., and the M.E degree in Computer Science and Engineering from Annamalai University, Chidambaram.