Global Journal of Computer Science and Technology
Volume 12 Issue 1 Version 1.0 January 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Digital Watermarking: Digital Data Hiding techniques for BMP Images

By Tripat Deep Singh Dua
Guru Nanak Institute Of Management And Technology Model Town Ludhiana , Punjab India

Abstract - Purpose: This research evaluates the digital watermarking technology further for hide/retrieved data into the BMP file by manipulating the contents their pixel value using least significant bits (LSB) approach. Methodology: Various experiments have been applied on the pixel value of the BMP file to hide/store the maximum data. With a condition the size and the quality of the BMP file will not change. The trail and error methods have been used or applied to check the various sizes with various qualities. Findings: The study finds that the any digital data can be hiding into the BMP file by manipulating the contents of the Red Green Blue (RGB) value by applying least significant approach. Originality/Value: Due to the growing usage of multimedia content on the internet, serious issues have emerged. Counterfeiting, forgery fraud and pirating of this content are rising. The research is a mechanism which can help resolve the ownership issues for digital data.

Keywords : *Digital watermarking, Digital Data, 24 bit BMP Image, Red Green Blue (RGB) pixel Value, Least Significant Bit (LSB), lower order bits, Copy right, Tracking,*

GJCST Classification: *D.2.11*

Strictly as per the compliance and regulations of:

Digital Watermarking: Digital Data Hiding techniques for BMP Images

Tripat Deep Singh Dua

Abstract - Purpose: This research evaluates the digital watermarking technology further for hide/retrieved data into the BMP file by manipulating the contents their pixel value using least significant bits (LSB) approach.

Methodology: Various experiments have been applied on the pixel value of the BMP file to hide/store the maximum data. With a condition the size and the quality of the BMP file will not change. The trail and error methods have been used or applied to check the various sizes with various qualities.

Findings: The study finds that the any digital data can be hiding into the BMP file by manipulating the contents of the Red Green Blue (RGB) value by applying least significant approach.

Originality/Value: Due to the growing usage of multimedia content on the internet, serious issues have emerged. Counterfeiting, forgery fraud and pirating of this content are rising. The research is a mechanism which can help resolve the ownership issues for digital data.

*Keywords : Digital watermarking, **Digital Data**, 24 bit BMP Image, Red Green Blue (RGB) pixel Value, Least Significant Bit (LSB), lower order bits, Copy right, Tracking,*

I. Introduction

Due to the growing usage of multimedia content on the internet, serious issues have emerged. Counterfeiting, forgery fraud and pirating of this content are rising. Virtually anyone with a sound card, scanner, video frame grabbers or multimedia authoring systems allow them to incorporate copyrighted material into presentations, web designs and internet marketing campaigns. A simple search on any of the search engines returns hundreds and thousands of images which can be easily downloaded on to a personal computer. The desire for the availability of information and quick distribution has been a major factor in the development of new technology in the last decade. There is the increased use of multimedia across the internet. Multimedia distribution has become an important way to deliver services to people around the world. It is commonly applied in internet marketing campaigns and electronic commerce web sites.

Digital Watermarking describes methods and technologies that hide information on bmp images, for example a number, text, image, video in any digital media. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. For images this means that the modifications of the pixel values have to be invisible. In other words it is a pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.). The name comes from the faintly visible watermarks imprinted on stationery that identify the manufacturer of the stationery. The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format. Digital watermarks on the images are designed to be completely invisible, moreover, the actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated.

The left size picture is true 24 BMP 2.25 MB Image file and right size picture is 2.25 KB image Jpg picture that is to be inserted in left size image (True 24 bit bmp file)

BMP file 2.25 MB

Jpg file 2.25 KB

Author : Assistant Professor, Guru Nanal Institute of Mgt & Tech, Gujarkhan Campus, Model Town Ludhiana.

The picture shows half of the right picture has been inserted into the left picture that is original BMP file. When we insert the jpg 2.25 KB file into 2.25 MB file the by manipulating the pixels of the BMP file the size will remains same 2.25 MB and the image quality will also remains same.

Digital Watermarking describes methods and technologies that hide information on bmp images, for example a number, text, image, video in any digital media. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. For images this means that the modifications of the pixel values have to be invisible. The research will be able to water mark the BMP images with bmp, jpeg, video, audio or any other format files. Digital Watermarking, which is used to transfer or pass information in a manner that the very existence of the message is unknown. With this study we can hide any type of file with any format into a 24 Bit True BMP with password protection (password can be encrypted using any of the existing encryption technology). For example we can hide or insert a video file or an audio file into a given BMP file without changing the image or its size. 24 Bit BMP format has been chosen because of its large pixel data. More the number of pixels in the image more data we can embed in it. This manipulation neither changes the image nor its size. i.e. the Image quality and its original size is maintained.

The first part of this study depicts the overview of the digital watermarking and defined the problem. Second part discusses the objectives of the study. The third part review the findings of the scholars who studied the watermarking in the past. Fourth chapter discusses the methodology used for the research purpose. The fifth part shows the analysing of the data and experiments. The sixth part shows the findings and colclusion.

II. Objective of the Study

The study aims the following objectives

The objective of our study would be to develop a technique which would embed some kind of information into the digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control and will help us to address some of the challenges faced by the rapid proliferation of digital content.

- Watermark should remain invisible
- Use of any digital content as watermark
- Copy/Copyright protection

III. Review of Literature

There is no dearth of literature on watermarking. A number of scholars investigated the diffrents aspects of the topic. *Zhao and Koch (1995), Cox et al (1997), Hartung, Eisert, and Girod (1998), Hsien Fu (1998), Hsu and Wu (1998, 1999), Zhao et al. (1998), Unzign and Stirmark (1999), Fei et al (2001), Hasslacher (2004), Saryazdi & Hossein (2005) and Agrawal (2007)* evaluated the topic digital watermarking.

An interface has been defined in the watermark agent to the external watermark retrieval library.

This interface employs Java's native interface technology to allow Java objects to call watermark retrieval functions written in C. At present, SysCoP *(Zhao and Koch 1995)* is the only digital watermarking mechanism that has been supported in the watermark agent. However, the watermark agent can easily support any other watermarking system.

Cox et al (1997) describe a method for embedding a binary watermark sequence in the highest magnitude DCT coefficients.

Hsien Fu (1998) conducts a literature survey of digital watermarks used for images. It describes the previous work done on digital watermarks, including the analysis of various watermarking schemes and their results. Potential applications are discussed, and an implementation plan of the project is presented. Hsien Fu uncovers the fact that recent work has shown that digital watermarks can be fairly successful in achieving the desired properties mentioned in section 2. These watermarks, however, are not perfect, and more could be done to improve a watermark's robustness or accuracy in detection. Furthermore, the question of copyright infringement remains a legal issue. Courts need to determine which methods may or may not be used. Until these legal standards are set, the Internet continues to be unsafe for images.

Hartung, Eisert, and Girod (1998) studied the methods for digital watermarking of MPEG-4 facial animation parameter data sets. They used a model-based approach for the estimation of the facial parameters that combines a motion model of an explicit 3D textured wireframe with the optical flow constraint from the video data. This leads to a linear algorithm that is robustly solved in a hierarchical framework with low computational complexity. Experimental results confirm the applicability of the presented watermarking technique.

Hsu and Wu (1998, 1999) use the middle frequency coefficients of DCT/Wavelet transform to embed a binary watermark. These mentioned methods are robust against image processing. Their main drawback is requiring the original image to extract the watermark.

Digital watermark has found a multitude of potential applications other than the originally motivation for copyright protection *(Zhao et al. 1998).* Similarly, the various types of uses of the watermark agents create many spectrums and great business opportunities.

Zhao and Luo (1998) presents a complete

digital watermark agent system to effectively put the digital watermark technology into practice. This system enables an agency to dispatch digital watermark agents to agent servers and agent can perform various tasks on the server. Once all the actions have been taken, a report will be sent to an agency's database and an agent can continue to travel to another agent server.

Unzign and Stirmark (1999), integrate a variety of geometric attacks. Unzign introduces local pixel jittering and is very efficient in attacking spatial domain watermarking schemes. Stirmark introduces both global and local geometric distortions. We give a few more details about these attacks later in this paper. However, most recent watermarking methods survive these attacks due to the use of special synchronization techniques. Robustness to global geometric distortions often relies on the use of either a transform in variant domain (Fourier-Melline) or an additional template or of specially designed periodic watermarks whose auto covariance function (ACF) allows estimation of the geometric distortions.

Fei et al (2001) attempt to find a suitable transform domain to watermark images robust against JPEG compression attack. They show that the choice of the transform domain depends on the type of the embedded information. If the watermark is embedded by repetition coding, then the Hadamard transform gives the best results.

Hasslacher (2004) evaluates the watermarking and its uses. He reveals that the scaling factor is a critical system parameter. If ais too small. The image is not distorted but the robustness of the scheme is low. He also unearth that Modification of low-frequency coefficients distorts the image and Gives the hacker a clue about where the watermark is embedded.

Wang et al. (2004) describe a kind of blind watermarking based on relative modulation of the DCT coefficient value by referring to its estimated one. In their method, the DC values of a 3×3 neighborhood of 8×8 blocks are used to estimate the AC coefficients of central block. In each group of nine 8×8 blocks, five bits of watermark are embedded by modulating the first five DCT AC coefficients, in central block, with the following rule:

Set ACi □ AC'i □□ to embed bit "1"

Set ACi □ AC'i □□ to embed bit "0"

Where, ACi and AC'i are the real and estimated value of the AC coefficients, respectively. The watermark recovery is done by comparing ACi and its estimated value. If ACi □ AC'i , then the extracted bit is "1", otherwise, it is "0".

Saryazdi & Hossein (2005) propose a blind scheme for gray-level data embedding in Hadamard Domain. In the proposed algorithm, the host image is first divided into 4×4 non-overlapping blocks. Their embedding procedure contains two parts. The first part is estimating the first two Hadamard low frequency AC coefficients (i.e. H(0,2) and H(2,0)) in each block, using its neighbor blocks. We use the following equations, to estimate the low frequency AC Hadamard coefficients of a block using the DC values of its 3×3 neighbor blocks. *Saryazdi & Hossein (2005)* concludes that For most watermark application, it is desired to recover the embedded data without using host image. In this paper, such a watermarking scheme for embedding gray-level watermarks is presented. In the proposed method, the two first Hadamard AC coefficients are estimated by their neighbor blocks. Then, a number proportional to the gray-level watermark value is added to each estimated AC coefficient. The recovery procedure consists of comparing the estimated values with actual ones.

Agrawal (2007) propose a robust perceptual digital video watermarking procedure to embed a watermark image in digital video frames using the variable-temporal length 3-D DCT technique. He finds that in many existing video watermarking schemes, the raw video is needed for detection of watermark logo. This is refered to as non-blind method and is not convenient in many cases. In this thesis we propose a new blind watermark detection algorithm. The performance of the blind detection technique was evaluated for several types of video sequences. The watermarking is also done for color video samples in the YUV domain. We used only the luminance (Y-Component) to embed the watermark to make the watermarking scheme more robust since the chrominance (U and V) components is perceptually less sensitive to human visual system compared to the luminance (Y-Component).

Research scholars evaluated the different aspects of the digital watermarking and revealed a number of facts about the technology but not much research has been done on the watermarking on BMP files and on the method to hiding an BMP image in other without changing its view. This research will concentrate on the said topic.

IV. Research Methodology

Digital watermarking techniques can be used successfully with digital content in various forms like still images of bmp format using their least significant bit (LSB). In LSB substitution the lower order bits of selected pixels in the image are used to store watermarks. Techniques like flipping the lower order bits, replacing the lower order bits of each pixel with higher order bits of a different image (for e.g., a company logo), superimposing a watermark image over an area of image to be watermarked and adding some fixed intensity value are used to embed watermarks in spatial domain.

In Least Significant Bits substitution the lower order bits of selected pixels in the image are used to

store watermarks or the LSB's are replaced with the higher order bits of the data that is to be inserted in the image that will effect the slightest change in the colour value of the pixel but non noticeable in colour point of view. The 24 bit BMP data has been chosen because of large pixel value more the file size the more data can de hide into the file. Any logo, signature, company name, bmp image or nay image or any audio/ video file can be hide into BMP file. More over the size of the original image will remain same after embedding the other data into the image. Because the data that is to be hide into the BMP file that is not any extra data or not any embedded data but the original data that will be replaced with the original lower bits of the BMP file. The idea behind this technique is that modifying the LSB will not make much difference to the color of the pixel.

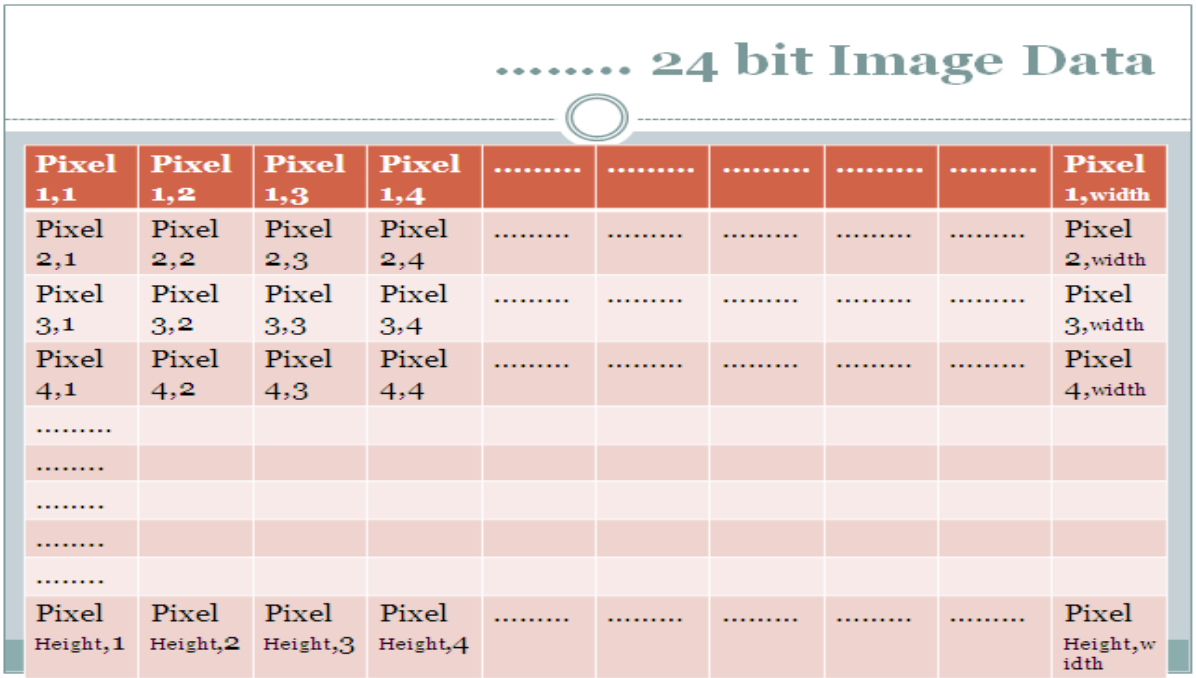
a) Methods used for the study

Experimentations refer to the used of the new techniques to innovate/implement new idea for experiment based. The research refers to the experiments to hide any digital data into the BMP file format so that it can be easily inserted into the 24 BMP file. The hidden data will be into the BMP file with its original form and will not loose its originality. On the other side the size of the BMP file will remains same because it will not increase in any case because the BMP has given the full space to the data that is to hide in the BMP file by replacing its contents or called pixels. The experiment is successful because the BMP file can store large data because of its large file size. And experiment is again successful when the quality/colour of the BMP file will remains same to normal human eye after modifying the contents of the pixel value in the BMP file.

First convert the file to be hidden into a binary stream and then read the BMP file pixel by pixel and substituting the LSB's of R, G, B component of each pixel with the bits from the binary stream until the entire binary stream had been substituted into the image. The binary stream that is substituted also has a format for easy and fast retrieval. We use a 12 Byte or 96 Bit headers, which is prefixed, to the Binary Stream before being substituted.

V. Experiments & Analysis

Figure 1 : shows the actual 24 bit BMP image data



The figure 1 shows how the pixels are stored in the form of BMP file. The data is stored in the form of the matrix of height and width. The RGB pixels are stored in the BMP file which describes the overall description of the image. The pixel value starts from (1,1) to until the size and the width of the picture.

Figure 2 : of BMP Image Data in the form of array

Image Data PixelArray [x,y]					
Pixel[0,h-1]	Pixel[1,h-1]	Pixel[2,h-1]	...	Pixel[w-1,h-1]	Padding
Pixel[0,h-2]	Pixel[1,h-2]	Pixel[2,h-2]	...	Pixel[w-1,h-2]	Padding
			⋮		
Pixel[0,9]	Pixel[1,9]	Pixel[2,9]	...	Pixel[w-1,9]	Padding
Pixel[0,8]	Pixel[1,8]	Pixel[2,8]	...	Pixel[w-1,8]	Padding
Pixel[0,7]	Pixel[1,7]	Pixel[2,7]	...	Pixel[w-1,7]	Padding
Pixel[0,6]	Pixel[1,6]	Pixel[2,6]	...	Pixel[w-1,6]	Padding
Pixel[0,5]	Pixel[1,5]	Pixel[2,5]	...	Pixel[w-1,5]	Padding
Pixel[0,4]	Pixel[1,4]	Pixel[2,4]	...	Pixel[w-1,4]	Padding
Pixel[0,3]	Pixel[1,3]	Pixel[2,3]	...	Pixel[w-1,3]	Padding
Pixel[0,2]	Pixel[1,2]	Pixel[2,2]	...	Pixel[w-1,2]	Padding
Pixel[0,1]	Pixel[1,1]	Pixel[2,1]	...	Pixel[w-1,1]	Padding
Pixel[0,0]	Pixel[1,0]	Pixel[2,0]	...	Pixel[w-1,0]	Padding

Figure 2 shows the 24 bit BMP Image pixels are stored in the form of Pixel Array or Matrix. The height and the width of the pixels are adjusted according to the size of the image. The lowermost left pixel of the image describes the starting point or the starting pixel values of the height and the width of the pixel. For example in the image 2 it is clearly shown that the lower most value of in the pixel array is pixel (0, 0). As the size of the picture grows the values in the array grows according to the size of the image.

Figure 3

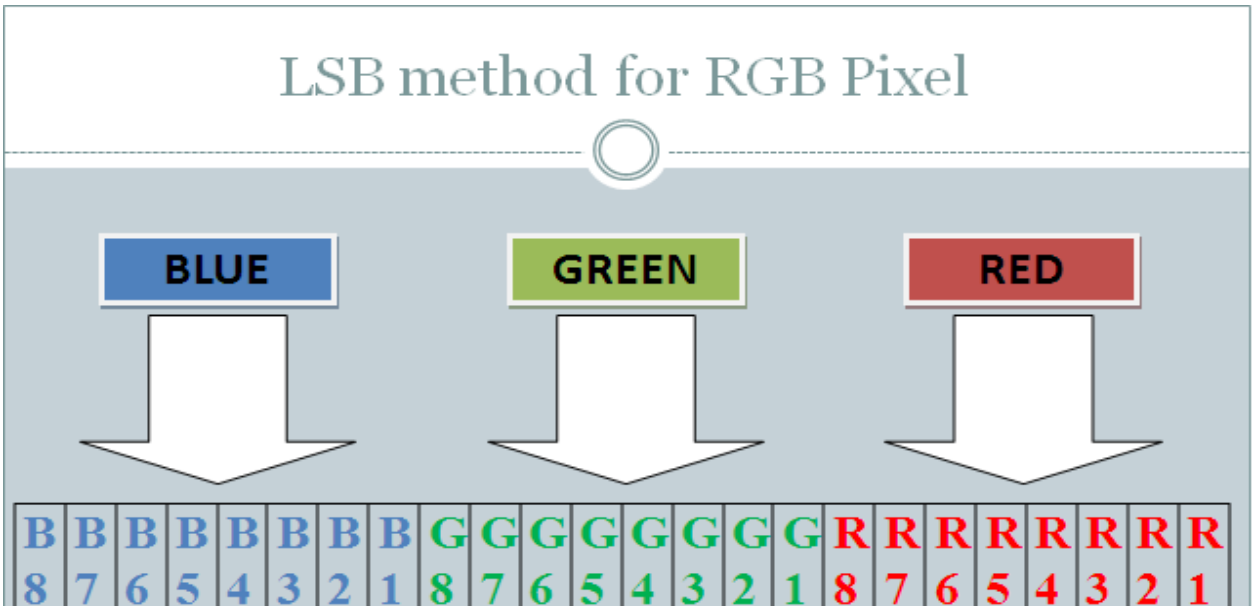


Figure 3 shows **pixel** Method of a 24 bit BMP file, the data is stored in the form 3 pixel RGB. The format of BMP file id 24 bit and each pixel has been assigned a colour value 8 for RGB. This is the colour combination of each pixel where all the colours in the colour palette designed by the combination of RGB.

Figure 4

The figure 4 shows that the left picture is true BMP format picture with a size of 2.25 MB and the right side picture Jpg picture with a size of 225 KB that is to be inserted in BMP file. The insertion takes place with the BMP file.

Figure 5 : shows to hide some text and a ring tone of a song into 2.25 MB file.

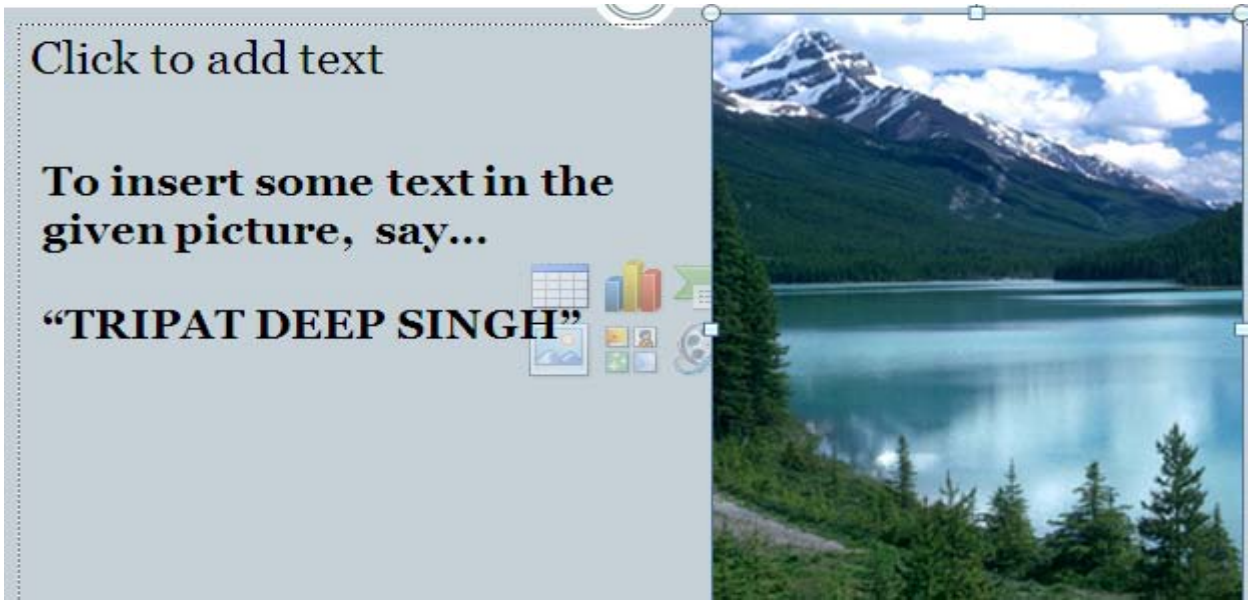
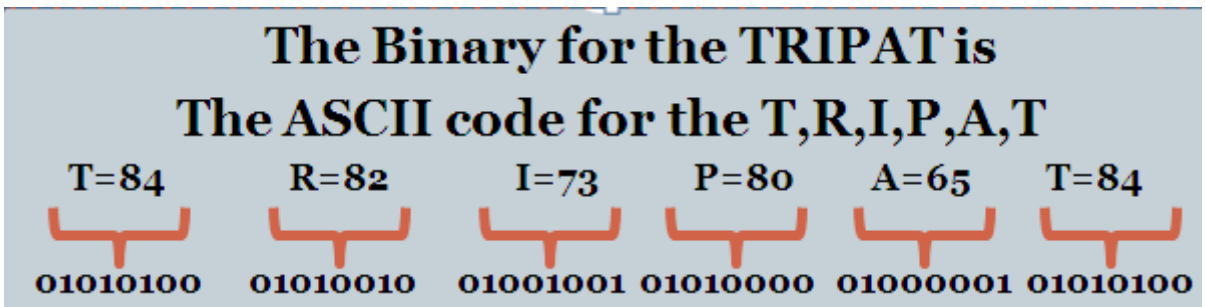


Figure 6



To hide something into BMP file, first covert the Binary for the TRIPAT into ASCII CODE, Than 24 bit RGB pixel value for the sample colour for the starting image is

VI. Findings and Conclusion

Digital watermarks for BMP images on the images are designed to be completely invisible, moreover, the actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated.

The development will be able to water mark the BMP images with bmp, jpeg, video, audio or any other format files. The research is based on a Technique known as Digital Watermarking, which is used to transfer or pass information in a manner that the very existence of the message is unknown. With this study we can hide any type of file with any format into a 24 Bit True BMP with password protection (password can be encrypted using any of the existing encryption technology). For example we can hide or insert a video file or an audio file into a given BMP file without changing the image or its size. 24 Bit BMP format has been chosen because of its large pixel data. More the number of pixels in the image more data we can embed in it. This manipulation neither changes the image nor its size. i.e. the Image quality and its original size is maintained. Our study is based on a Digital Watermarking Technique known as Least Significant Bit (LSB's)

In this technique the LSB's of the Pixels are modified to store the information. The idea behind this technique is that modifying the LSB will not make much difference to the colour of the pixel. Multimedia distribution has become an important way to deliver services to people around the world. It is commonly applied in internet marketing campaigns and electronic commerce web sites. Due to the growing usage of multimedia content on the internet, serious issues have emerged. Counterfeiting, forgery fraud and pirating of this content are rising. Virtually anyone with a sound card, scanner, video frame grabbers or multimedia authoring systems allow them to incorporate copyrighted material into presentations, web designs and internet marketing campaigns. A simple search on any of the search engines returns hundreds and thousands of images which can be easily downloaded on to a personal computer.

An important point that arises in these applications is the protection of ownership rights. Anybody and everybody can download digital content from the internet and can reuse or redistribute that as his own thus depriving the rightful owner of royalty or recognition for his/her work. Hence the need for developing new copy deterrence and protection mechanisms for digital content is felt.

We need to have a mechanism which can help resolve the ownership issues for digital content. The owner should be able to mark his work in some way which should later help in resolving the ownership in case of dispute. Moreover the mark should not affect the quality or the meaning of the image or should not change it. This process on hard copy of images is known as watermarking and when applied to digital content is known as digital watermarking. Consequently, copyright abuse is rampant among multimedia users who are rarely caught. This copyright abuse is the motivating factor for this study.

References References Referencias

1. Frank Hartung, Peter Eisert, and Bernd Girod (1998) *"Digital Watermarking of MPEG-4 Facial Animation Parameters"* Computers & Graphics, Vol. 22, No. 3
2. Alexander Hasslacher (2004) *"Digital Watermarking"*, EMT-Institut, JKU-Linz
3. Agrawal vinod (2007) "*Perceptual Watermarking Of Digital Video Using The Variable Temporal Length 3d-Dct"* Thesis M-tech, IIT Kanpur.
4. Fu Hsien (1998) *"Literature Survey on Digital Image Watermarking",* Multidimensional Signal Processing
5. Saryazdi Saeid, Nezamabadi-pour. Hossein (2005) *"A Blind Digital Watermark in Hadamard Domain"* World Academy of Science, Engineering and Technology 3.
6. Cox, I. J., Kilian, J., Leighton, F. T., Shamoon, T., "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. On Image Processing, No. 6, Vol. 12,pp 1673-1687, 1997.
7. Wang, Y., Pearmain. A., "Blind Image Data Hiding Based on Self Reference", Pattern Recognition Letters, Vol. 25, Issue 15, pp. 1681-1689, November 2004.
8. Fei, C., Kundur, D., Kwong, R. H., "The Choice of Watermark Domain in the Presence of Compression", Proc. Of IEEE Int. Conf. On Information Technology: Coding & Computing, pp 79-84, Las Vegas, Nevada, April 2001.
9. Hsu, C. T., Wu, J. L., " Multi-resolution Watermarking for Digital Images", IEEE Trans. On Circuits & Systems: Analog & Digital Signal Processing, Vol. 45, No. 8, 1998.
10. Hsu, C. T., Wu, J. L., " Hidden Digital Watermarks in Images", IEEE Trans. On Image Processing, Vol.8, No. 1, 1999.
11. M. Kutter and F. Petitcolas, "A fair benchmark for image watermarking systems," *Electronic Imaging 199: Security and Watermarking of Multimedia Content*, Vol. **3657** of SPIE Proceedings, San Jose, California USA, 25-27 January 1999.
12. Zhao Jian & Luo Chenghui *"Digital Watermark Mobile Agents"* Fraunhofer Center for Research in Computer Graphics, Inc.
13. Zhao, J. and Koch, E. (1995). *Embedding Robust Labels Into Images For Copyright Protection*. In: Proc. of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna, Austria, August 21-25, 1995.
14. Zhao, J., Koch, E. and Luo, C. (1998). *Digital Watermarking In Business Today and Tomorrow.* In: Communications of ACM, pp. 67-72, Vol. 41, No. 7, July 1998.