ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 7, March 2018

EMBEDDING THE DATA IN IMAGE BY USING REVERSIBLE TEXTURE SYNTHESIS FOR DATA SECURITY

SOWMIYA P[1], ARCHANA E[2], JANANI S[3], MENAKA P[4], MONISHA V[5]

ASSISTANT PROFESSOR[1], UG SCHOLAR[2, 3, 4, 5]

***ABSTRACT*-The steganography is an art of hiding existence of the data in another transmission medium to achieve the secret communication. The reversible texture synthesis method can be used to resamples a texture image, which synthesizes a new texture image with a similar appearance and size. Existing system is much expensive and not so robust because if the size of the secret message increases it results into distortion of the image. A texture synthesis process provides embedding capacity so that to hide the large message. With this process the blank image is constructed from input image and it can be divided into number of different patches. These patches are indicated by a patch ID and randomly pasted on the blank image. This system can embed the size of the image and provide high quality image which avoids the distortion. The proposed system is much more robust against any kind of attack and provides high degree of security to the confidential data hidden inside the image patches.**

Key terms-*Encryption, Decryption, Data Hiding*

I. INTRODUCTION

Steganography is to hide text, audio, video behind the image. The main purpose is to hide information in such a way that attacker cannot detect hidden messages. The term steganography is derived from the Greek words "Steganos" (covered) and "graphia" (writing). The intention of steganography is to provide the secret transmission of data. Steganalysis provides a way of detecting the presence of hidden information. In contrast to steganography, cryptography change the secret message from one from another, where the message is scrambled, unreadable, and the existence of message is often unknown. Encrypted message can be located and intercepted but can't be decoded easily. This nature hiding information in cipher protects the message, but the interception of the message can just be as damaging because it give clue to an opponent or enemy that someone is communicating with someone else. Steganography brings out the opposite approach and tries to hide all evidence during communication [3]. Image steganography is defined as to covert embedding data into digital pictures. Though steganography hides information in any one of digital Medias, digital images are most popular as carrier due to their frequency usage on the internet. Since the size of the image file is large, it can be conceal large amount of information. HVS cannot differentiate the normal image and includes large amount of redundant bits, images became the most popular cover objects for steganography. Hence this research uses image as cover file .Different image formats such as JPEG, BMP, TIFF, PNG or GIF files can be used as cover objects.

A bitmap or BMP format is a simple image file format [8]. Data is easy to manipulate, since it is uncompressed. It uses lossy compression technique; the quality of the image is excellent. The size of the file is also smaller. TIFF format uses lossless compression. The file is reduced without affecting the image quality.GIF has color palette to provide an indexed colors image. It uses lossless compression. Since it can store only 256 different colors it is not suitable for representing complex photography with continuous tones, PNG file format provides better color support, best compression, and gamma correction in brightness control and image transparency. PNG format can be used as an alternative to GIF represent web images.

II.PROPOSED METHOD

The objective of steganography is to hide information in such a way that existence of communication is unknown by an attacker. This paper introduces steganography in texture images. Texture synthesis process synthesizing a large texture image from a smaller texture image, which has same local appearance. We combine texture synthesis and steganography to conceal secret messages... [6], [11].

INPUT IMAGE

We call the input image as source texture image. This image may be captured in a photograph or drawn by an artist to create synthesized texture image which is having similar appearance.

COLOR BAND SEPARATION

Color Separation is the process of converting an image, such as photograph, into a set of colors that can be printed. Color separations for screen printing can be made using Adobe Photoshop. When an image is brought into Adobe Photoshop, it is usually in a color mode compatible with the device that it was created. This is often the RGB color mode, which is a common mode for digital cameras and computer monitors. The RGB mode is based on the blending of Red, Green and Blue light. To screen print an image, the colors must be converted to a combination of colors compatible with screen printing. The resulting set of colors is called a Color Separation.

GRAY SCALE TO RGB CONVERSION

Now we will convert a color image into a gray scale image. There are two methods to convert it. Both have their own merits and demerits. The methods are:

- Average method
- Weighted method or luminosity method

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 7, March 2018

Average Method

Average method is the simplest one. You just have to take the average of three colors.
Since it's an RGB image, so it means that you have added r with g with b and then divide it by 3 to get your desired gray scale image. It's done in this way.

Gray scale = (R + G + B / 3)

Weighted Method or Luminosity Method

Weighted method has a solution to that problem. Since red color has more wavelengths of all the three colors, and green is the color that has not only less wavelength then red color but also green is the color that gives more soothing effect to the eyes. It means that we have to decrease the contribution of red color, and increase the contribution of the green color, and put blue color contribution in between these two.

So the new equation that forms is:
New gray scale image = ((0.3 * R) + (0.59 * G) + (0.11 * B)).

According to this equation, Red has contributed 30%, Green has contributed 59% which is greater in all three colors and Blue has contributed 11%.

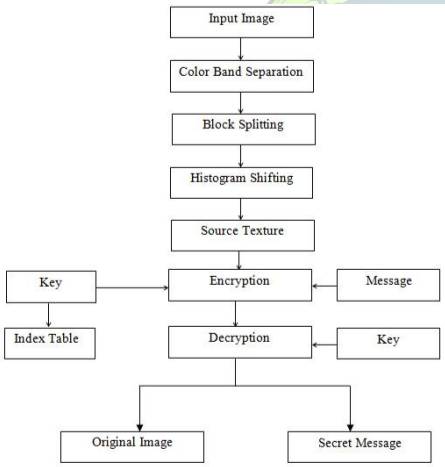

Fig 1. WORKING METHODOLOY

After, the color separation process, the image is splitted into two equal numbers of planes. i.e. A-plane and B-plane.

.

HISTOGRAM SHIFTING TECHNIQUE

In histogram sliding, we just simple shift a complete histogram rightwards or leftwards. Due to shifting or sliding of histogram towards right or left, a clear change can be seen in the image. It improves the brightness and contrast.

Brightness

Brightness is a relative term. Brightness can be defined as intensity of light emit by a particular light source.

Contrast

Contrast can be defined as the difference between maximum and minimum pixel intensity in an image.

The reversible data hiding schemes based on histogram shifting were proposed. In these schemes, peak point in the histogram of the cover image is used to select the embedding area for the secret data, then the part [Peak point +1, Zero point] is shifted to get the embedding area. It improves the brightness and contrast.

These schemes were improved by using the histogram of the difference image or predict error image instead of the original image to get a higher peak point. If the peak point is high, the hiding capacity will be large.

INDEX TABLE

The index table allows us to access the synthetic texture and retrieve the source texture completely. While generating index table we need to provide the secret key for the authentication purpose. We have to write the encrypted secret message into the patch. To do this the appropriate patch must be selected. This selection is based on the entry into the index table which tells which patch to select and where to paste the patch into the blank image. [7]

ENCRYPTION

In this module it allows user to enter the user name and password in order to restrict the user to access the system. Then it validates the entered user name and password, it is correct it will allow the user to access the application. Authentication process is always occurred prior to mobility management process included locations registration and service delivery. Ensures network resources are accessed by authorized clients and prevents resources from any illegal client or damage.

Bitwise XOR Operation

The exclusive or operation - a logical function applied to binary bits, like AND, OR, and NOT - is a fundamental encryption technique. It is often used in stream ciphers, which are widely used in web browsers when connecting to secure web servers. When used properly, this technique provides strong protection. In fact, it is the basis for the one-time pad, the only provably uncrackable encryption. However, this protection is easily eroded if the cipher is not used correctly. XOR is a trivial operation for computer logic to perform show the table. The operation often appears as a built-in machine instruction so that software can perform it in a single machine operation.

A	B	⊕
0	0	0
0	1	1
1	0	1
1	1	0

Table 1. XOR operation transforms individual bits

The above table shows how the XOR operation transforms individual bits. Let A be a bit from the plain text message, and B be a bit from the key. The ⊕ column shows the resulting bit.

DECRYPTION

In this module it allows to pick the encrypted image received from the owner side encrypting data and then to enter the password key to decrypt. If the image and the key are

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 7, March 2018

correct then the corresponding message will be displayed. To decrypt any file one has to know exactly what is the key matrix and to find the random matrix theoretically one has to decrypt the cryptography image data. The keyless method can be applied for data encryption and decryption in any type of application for sending confidential data. [11] Finally, separately to get a secret message and original image.

III. RESULT

Fig 2: Input Image

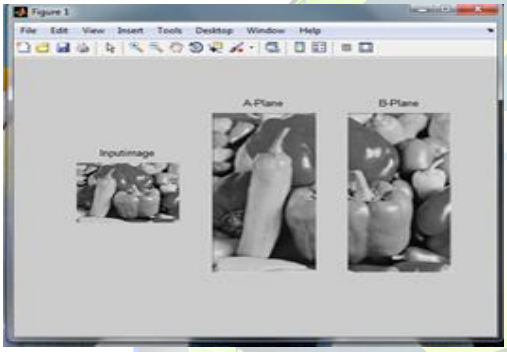

Fig 3: Color band separation

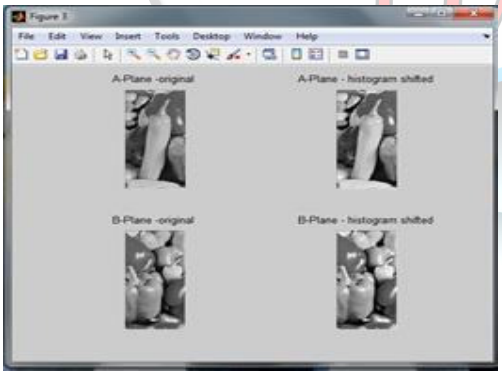

Fig 4: Histogram shifted image

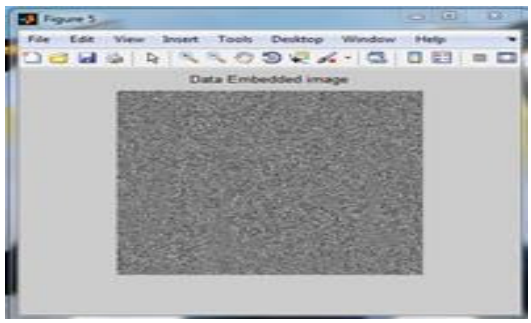

Fig 5: Data embedded image

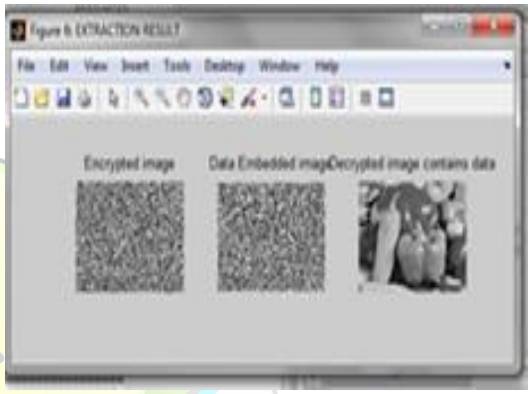

Fig 6: Data decrypted image

IV. PERFORMANCE ANALYSIS

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs.

The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; when it is used to compare results from the same codec (or codec type) and same content.

PSNR is most easily defined via the MSE. Given a noise-free $m \times n$ monochrome image I and its noisy approximation K, MSE is defined as:

$$MSE = \frac{1}{m n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

The PSNR (in dB) is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$PSNR = 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 7, March 2018

$$20.\log_{10}(MAXi) - 10.\log_{10}(MSE)$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

More generally, when samples are represented using linear PCM with B bits per sample, MAX_I is 2^B-1. For color images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three.

COVER IMAGE	SIZE OF THE COVER IMAGE	DATA INSERTED	MSE	PSNR
Baboon	135KB	Basilisk lizard	3.1378	50.8712
Lena	89KB	Basilisk lizard	3.1543	49.5194
Peppers	117KB	Basilisk lizard	3.1683	49.1712

Table 2.MSE and PSNR

Alternately, for color images the image is converted to a different color space and PSNR is reported against each channel of that color space, e.g.,YCbCr or HSL.

V. Conclusion

In this an original source texture produces a large stego synthetic texture in which secret messages are embedded. The system also provides reversibility to retrieve the original source texture from the stego synthetic textures. It offers some advantages such as the reversible capability of texture synthesis provide the functionality to allow recovery of the source texture and to avoid image distortion. We believe our proposed scheme offers substantial benefits and provides an opportunity to extend steganographic applications.

REFERENCES

1. A. A. Efros and W. T. Freeman, "Image quilting for texture synthesis and transfer," in Proc. 7th IEEE Int. Conf. Comput. Vis., Sep. 1999, pp. 1033–1038.

2. Anjali Tiwari et al, "Different Image Steganography Techniques,"International Journal of Engineering and Innovative Technology (IJEIT) vol 3, Issue 7, January 2014.

3. Arvind Kumar and Km. Pooja, "Steganography- A Data Hiding Technique," International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

4. H. Otori and S. Kuriyama , "Data-embeddable texture synthesis," in Proc. 8th Int. Symp. Smart Graph. Kyoto, Japan, 2007, pp. 146–157.

5. J. Fridrich, M. Goljan, "**Detecting** LSB steganography in color and gray scale images," IEEE MultiMedia, vol. 8, no. 4, pp. 22–28, Oct. /Dec. 2001.

6. L. Liang, C. Liu, Y.-Q. Xu, B. Guo, and H.-Y. Shum, " Real-time texture synthesis by patch-based sampling, " ACM Trans. Graph., vol. 20, no. 3, pp. 127–150, 2001.

7. M. F. Cohen, " Wang tiles for image and texture generation," ACM Trans. Graph., vol. 22, no. 3, pp. 287–294, 2003.

8. N. Provos and P. Honeyman, —Hide and seek, " An introduction to steganography," IEEE Security Privacy, vol. 1, no. 3, pp. 32–44, May/Jun. 2003.

9. R. Rejani,D. Murugan and Deepu V. Krishna, "Pixel pattern based steganography on images, journal on image and video processing, " feb 2015, volume: 05, issue: 03.

10. Y. Guo, G. Zhao, "Video texture synthesis with multi-frame LBP-TOP and diffeomorphic growth model," IEEE Trans. Image Process. vol. 22, no. 10, pp. 3879–3891, Oct. 2013.

11. Z. Ni, Y.-Q. Shi, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.