

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Information Hiding Using Secret Particle Visible Mosaic Image With Magnify Security

B Sundarraj

Asst.Professor, Department of Computer Science & Engineering, Bharath University, Chennai, India

ABSTRACT : Information hiding was initially done by techniques like Steganography, Digital Watermarking, etc. A new type of digital art called the Secret Fragment Visible Mosaic Image has been discussed in this paper for information hiding. The information that is to be sent secretly is sent as an image, embedding it into another image called the target image. Small fragments of both the target image and the secret image are composed and embedded into each other resulting in the formation of a mosaic image. To create mosaic image, the target and the secret image are fragmented into blocks of equal size. The pixel color values of all the pixel in a block is computed by the 1-D Histogram Transformation Technique and saved. By using the greedy algorithm, the similar image for the secret image is found out and a secret key is generated using Randomized algorithm. The tiles are embedded into the blocks by Lossless LSB Replacement Algorithm and the mosaic image is generated. The recovery is done by the secret recovery sequence.

KEYWORDS:Steganography, Digital Watermarking, Secret Fragment Visible Mosaic Image, Histogram Transformation..

I. INTRODUCTION

In computer science, information hiding is the principle of segregation of the design decisions in a computer program that are most likely to change, thus protecting other parts of the program from extensive modification if the design decision is changed. The protection involves providing a stable interface which protects the remainder of the program from the implementation (the details that are most likely to change). Written another way, information hiding is the ability to prevent certain aspects of a class or software component from being accessible to its clients, through an explicit exporting policy and through reliance on the short form as the primary vehicle for class documentation.

1.1 Overview

The term encapsulation is often used interchangeably with information hiding. Not all agree on the distinctions between the two though; one may think of information hiding as being the principle and encapsulation being the technique. A software module hides information by encapsulating the information into a module or other construct which presents an interface.

A common use of information hiding is to hide the physical storage layout for data so that if it is changed, the change is restricted to a small subset of the total program. For example, if a three-dimensional point (x,y,z) is represented in a program with three floating point scalar variables and later, the representation is changed to a single array variable of size three, a module designed with information hiding in mind would protect the remainder of the program from such a change.

In object-oriented programming, information hiding reduces software development risk by shifting the code's dependency on an uncertain implementation onto a well-defined interface. Clients of the interface perform operations purely through it so if the implementation changes, the clients do not have to change.

1.2 Mosaic Images

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

To create a mosaic photo, you need only a computer and a collection of photographs. A photo-mosaic is an image made from multiple photos. The thing to remember about photo-mosaics is that the more photos you load to make them, the more spectacular the result. Up close, you can pick out all of the photographs that make up the mosaic photo, but from afar, you see a single photo.

A photo-mosaic from numerous photographs is a great tool for design. Imaging mosaicing is being done in this project such that images taken by normal camera can be used to create a larger field of view using a image mosaicing program. Image mosaicing not only allow you to create a large field of view using normal camera, the result image can also be used for texture mapping of a 3D environment such that users can view the surrounding scene with real images. The most common mosaicing applications include constructing high resolution images that cover an unlimited field of view using inexpensive equipment, creating immersive environments for effective information exchange through the internet.

In the field of photographic imaging, a photographic mosaic is also known under the term Photo-mosaic. When viewed at low magnifications, the individual pixels appear as the primary image, while close examination reveals that the image is in fact made up of many hundreds or thousands of smaller images. Most of the time, they are a computer-created type of montage.

There are two kinds of mosaic, depending on how the matching is done. In the simpler kind, each part of the target image is averaged down to a single color. Each of the library images is also reduced to a single color. Each part of the target image is then replaced with one from the library where these colors are as similar as possible. In effect, the target image is reduced in resolution, and then each of the resulting pixels is replaced with an image whose average color matches that pixel.

In the more advanced kind of photographic mosaic, the target image is not down-sampled, and the matching is done by comparing each pixel in the rectangle to the corresponding pixel from each library image. The rectangle in the target is then replaced with the library image that minimizes the total difference. This requires much more computation than the simple kind, but the results can be much better since the pixel-by-pixel matching can preserve the resolution of the target image.

1.3 Mosaic Image Principle

A new type of art image, called secret-fragment-visible mosaic image, which contains small fragments of a given source image is proposed in this study. Observing such a type of mosaic image, one can see all the fragments of the source image, but the fragments are so tiny in size and so random in position that the observer cannot figure out what the source image looks like. Therefore, the source image may be said to be secretly embedded in the resulting mosaic image, though the fragment pieces are all visible to the observer and this is the reason why the resulting mosaic image is named secret-fragment-visible.

Because of this characteristic of the new mosaic image, it may be used as a carrier of a secret source image in the disguise of another—a target image of a different content. This is a new technique of information hiding, not found in the literature so far. It is useful for the application of covert communication or secure keeping of secret images.

II. PREVIOUS RESEARCH

Amit Phadikar and Santi, published their research in “ROI Based Error Concealment of Compressed Object Based Image Using QIM Data Hiding and Wavelet Transform” VOL.56,no 2,pp.971-979,IEEE TRANSACTIONS on Consumer Electronics, May 2010. Transmission of digital data through radio mobile experiences fading effect. To improve this, algorithms like integer wavelet, data hiding and ROI (Region Of Interest) are used. The ROB (Region Of background) is embedding into the ROI and retrieval is done by QIM (Quantization Index Modulation). The disadvantage is that it is not possible for high burst error condition.

Lixin Luo, Zhenyong Chen, et. al. “Reversible Image Watermarking Using Interpolation Technique”, VOL.5,no1,pp.187-193 ,Ieee Transactions on Information Forensics and Security, March 2010 stated that the Interpolation technique is used for embedding imperceptibly. Interpolation error is used for embedding the bits into images. Watermarking helps in embedding digital information. The disadvantage is it not applicable for sending side

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

The purpose of the paper "Inpainting Assisted Self Recovery With Decreased Embedding Data" authored by Zhenxing Qian and Guorui Feng in November 2010 is to reduce the amount of embedding data while maintaining good recover quality. This also used to encode different types of blocks with varied number of bits. The Inpainting method is used to aid the recovery. The disadvantage is performance of quality is less.

In February 2010, Feng Li,Jie Wu, published their analysis in "Fast Matrix Embedding by Matrix Extending", VOL.7. In that, the Referential columns are appended to parity check.ME(Matrix Embedding) algorithm is used for embedding process. The disadvantage is that its computation complexity is high.

III. EXISTING SYSTEM

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. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphei meaning "writing". 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. Cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

The disadvantage includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time. Paul Levinson Future of the Information Revolution where he called for the use "smart patent numbers", or the embedding of electronic chips in every piece of technology, which would give an updated listing of all of its inventors. A disadvantage of digital watermarking is that a subscriber cannot significantly alter some files without sacrificing the quality or utility of the data. This can be true of various files including image data, audio data, and computer code.

The existing system has less security measures and the secret image that gets embedded can be hacked. Moreover, the time taken for reconstructing the secret image is also more.

IV. PROPOSED WORK

The proposed system focuses on hiding of information by embedding a secret image into a target image by embedding the tiles of the secret image into blocks of the target image. Since the fragments are visible to the observer but they are secretly embedded into the target image, the system is named as Secret Fragment Visible Mosaic Image.

4.1 Methodology

The general methodology that is involved in hiding the information is explained here. A new type of art image, called secret-fragment-visible mosaic image, which contains small fragments of a given source image is proposed in this study. Observing such a type of mosaic image, one can see all the fragments of the source image, but the fragments are so tiny in size and so random in position that the observer cannot figure out what the source image looks like. Therefore, the source image may be said to be secretly embedded in the resulting mosaic image, though the fragment pieces are all visible to the observer. This is the reason why the resulting mosaic image is named secret-fragment-visible.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Because of this characteristic of the new mosaic image, it may be used as a carrier of a secret source image in the disguise of another—a target image of a different content. This is a new technique of information hiding, not found in the literature so far. It is useful for the application of covert communication or secure keeping of secret images.

It includes three phases of works:

Phase 1- construction of a color image database for use in selecting similar target images for given secret images;

Phase 2 - creation of a secret-fragment-visible mosaic image using the tile images of a secret image and the selected similar target image as input;

Phase 3 - recovery of the secret image from the created secret- fragment- visible mosaic image.[1]

4.2 System Architecture

The system architecture has been designed in such a way that all the phases of work are included into it. The most effective feature of an image is color. Hence we focus on extracting the colors from an image. At first, the database is created. This database is as large as possible so all the possible images are uploaded into it. This finishes the first phase. Before being stored, they are divided into equal sized fragments and only then they are stored. The secret information that is to be sent is then uploaded into the system and also divided into many equal sized fragments. The (r,g,b) pixel average value for the secret image is calculated and compared. The most similar target image is generated and a secret key too. The tiles and the blocks are embedded into each other and they form the resultant mosaic image.

At the recovery side, the reverse version of the above algorithms is performed and the secret image is then extracted from the mosaic image. The result is the mosaic image back. [2]

4.2.1 Block Diagram

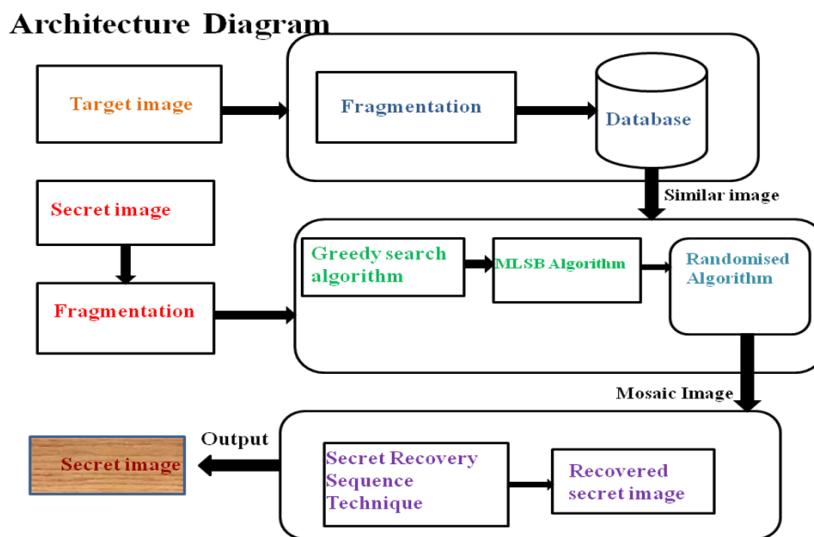


Figure 4.1 Block diagram

The above diagram represents the architecture of implementing secret fragment visible mosaic image for information hiding.

4.3 Module Explanation

4.3.1 Database Creation

The target image database plays an important role in the mosaic image creation process. If a selected target image from the database is dissimilar to a given secret image, the created mosaic image will be distinct from the target one, resulting in a reduction of the information hiding effect. To generate a better result, the database should be as large as

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

possible. Searching a database for a target image with the highest similarity to a given secret image is a problem of content-based image retrieval. In general, the content of an image may be described by features like shape, texture, color, etc. Due to the use of small tile images in the proposed method, which are the fragments of the secret image, it is found in this study that the most effective feature, which affects the overall visual appearance of the resulting mosaic image, is color. Therefore, we focus on extracting color distributions from images to define an appropriate image similarity measure for use in target image selection in this study.[3]

The technique used here is the 1-d Histogram Transformation Technique. An image histogram is a type of histogram that acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance.

Image histograms are present on many modern digital cameras. Photographers can use them as an aid to show the distribution of tones captured, and whether image detail has been lost to blown-out highlights or blacked-out shadows.[4]

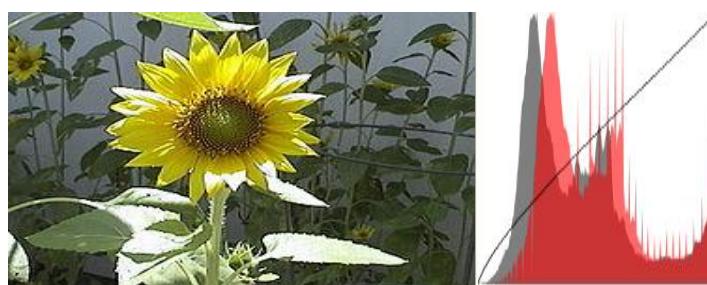


Fig4.2: Histogram of sunflower

In fig4.2, the horizontal axis of the graph represents the tonal variations, while the vertical axis represents the number of pixels in that particular tone. The left side of the horizontal axis represents the black and dark areas, the middle represents medium grey and the right hand side represents light and pure white areas. The vertical axis represents the size of the area that is captured in each one of these zones. Thus, the histogram for a very dark image will have the majority of its data points on the left side and center of the graph. Conversely, the histogram for a very bright image with few dark areas and/or shadows will have most of its data points on the right side and center of the graph.[5]

$$h(r', g', b') = (b - N_b) + (N_b * (r - N_r)) + (N_b * N_r * (g - N_g))$$

- r, g, b are the channel values
- N_r, N_g, N_b are the levels, set to 8
- $b = 1$ (smallest weight)
- $g = N_b * N_r$ (largest weight)

The numbers of levels are all set to be 8, and the largest weight, g, namely, the value , is assigned to the green channel value and the smallest weight, the value 1, is assigned to the blue channel value . This way of weight assignment is based on the fact that the human eye is the most sensitive to the green color and the least sensitive to the blue one, leading to a larger emphasis on the intensity of the resulting mosaic image. In addition, with all of and set to be 8, the proposed mosaic image creation process can be speeded up according to our experimental experience. Subsequently, we will say that the new color function proposed defines a 1-D colorscale.[6]

4.3.2 Creation of Mosaic Image

It includes three stages of operation

Stage 2.1—searching the database for a target image the most similar to the secret image;

Stage 2.2—fitting the tile images in the secret image into the blocks of the target image to create a mosaic image;

Stage 2.3—embedding the tile-image fitting information into the mosaic image for later secret image recovery. An example is given in fig 4.3.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

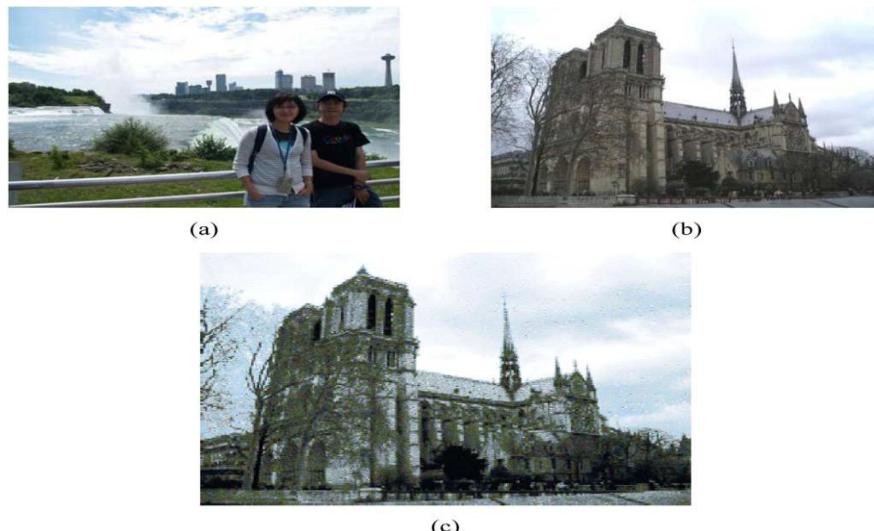


Fig4.3: Experimental result of mosaic image creation using Algorithm
(a) Secret image. (b) Target image. (c) Created mosaic image.

4.3.2.1 Searching the most similar image

4.3.2.1.1 Greedy Search Algorithm

This is a type of the algorithm that searches for an optimal solution. It searches for the solution in a greedy way. Using this technique of greedy search, a block similarity value is defined that helps in searching the most optimal target blocks for the secret block.[7]

Actual Largest Path Greedy Algorithm

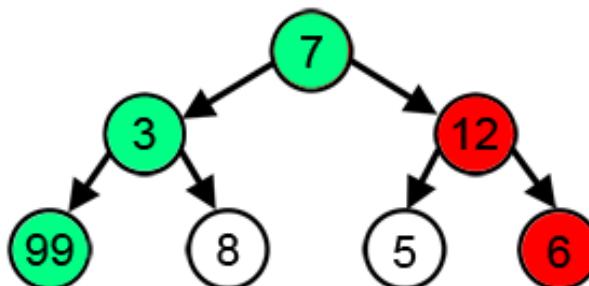


Fig 4.4: Greedy search

From fig 4.4, with a goal of reaching the largest-sum, at each step, the greedy algorithm will choose what appears to be the optimal immediate choice, so it will choose 12 instead of 3 at the second step, and will not reach the best solution, which contains 99.

Before generating the secret-fragment-visible mosaic image for a given secret image with the preselected size , we have to choose from the database DB a target image which is the most similar to . For this, first we divide into blocks of the preselected size , compute the -feature values of all the resulting blocks by (3), and generate the -feature histogram of . Then, we define an image similarity value between and each candidate target image with -feature histogram in DB in the following way. It is calculated using following formula[9]

$$m(s,d)=1/(|h_s - h_d|)$$

- h_s is the average pixel value of the tile in secret image.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

- h_d is the average pixel value of the block in target image.

4.3.2.2 Generation of the secret key

4.3.4.2.1 Randomized Algorithm

A randomized algorithm is an algorithm which employs a degree of randomness as part of its logic. The algorithm typically uses uniformly random bits as an auxiliary input to guide its behavior, in the hope of achieving good performance in the "average case" over all possible choices of random bits. Formally, the algorithm's performance will be a random variable determined by the random bits; thus either the running time, or the output (or both) are random variables.

4.4.2.3 Embedding Tiles into Blocks

4.4.2.3.1 Lossless Replacement Scheme LSB (Least Significant Bit)

LSB can also stand for least significant byte. The meaning is parallel to the above: it is the byte in that position of a multi-byte number which has the least potential value.

Image compression is the process of encoding image data into lesser number of symbols such that after decoding, the original image information can be retrieved. The compression procedure facilitates optimized space utilization for storage purposes and also enhances network utilization by using lesser bandwidth. Fig 4.6 depicts this.[10]

With the ever-increasing growth of multimedia applications over a network, on-line compression has become a necessity. Lossless image compression utilizes statistical redundancy in the uncompressed image.

The frequency of occurrence of a particular pixel value is used to encode the image pixel information using variable size bit-words. This process is also known as entropy encoding. The dictionary maintenance procedure postulates that image pixel information should be stored in a dictionary, and

4.4.3 Secret Image Recovery

Another issue which should be dealt with in creating the mosaic image is how to embed the information of tile-image fitting so that the original secret image can be reconstructed from the created mosaic image. Each fitting of a tile image into a target block forms a mapping. The way we propose for dealing with the issue is to record these mappings into a sequence , called the secret recovery sequence, and embed into randomly-selected blocks in the created mosaic image using a technique of lossless least-significant-bit (LSB) . In more detail, to get the mappings, we start from the top leftmost target block in the selected target image and find for it the most similar tile image in the secret image in the sense of, and form the first mapping to be included in . Next, in a raster-scan order, we process the target block to the right of to find the most similar tile image in the remaining tile images to form the second mapping for. Then, we do similarly to find the third mapping , and so on. We continue this greedy search process until the last target block at the bottom-rightmost corner in the target image is processed. The resulting may be regarded to include two block-index sequences, and with mappings , and so on. Since is a well-ordered sequence we can ignore it and take to include data volume of to be embedded.

V. RESULTS

Many images are uploaded into the database. After fragmenting the images and calculating the average pixel value of each block, it is stored in the database. The images are inserted into the database. The image is resized into blocks of 9 as 3x3. The (r,g,b) pixel values of each block is computed and saved into the database.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015



Fig 5.1 Original Image

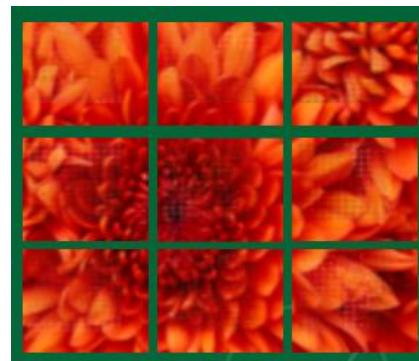


Fig 5.2 Uploaded Fragmented Image

The creation of mosaic image includes 3 stages of operations. The secret image is uploaded and its h-feature is also calculated. The most similar target image is selected at random and it is embedded into the target image resulting in the formation of a mosaic image.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015



Fig 5.3 Secret Image



Fig 5.4 Fragmented Secret Image

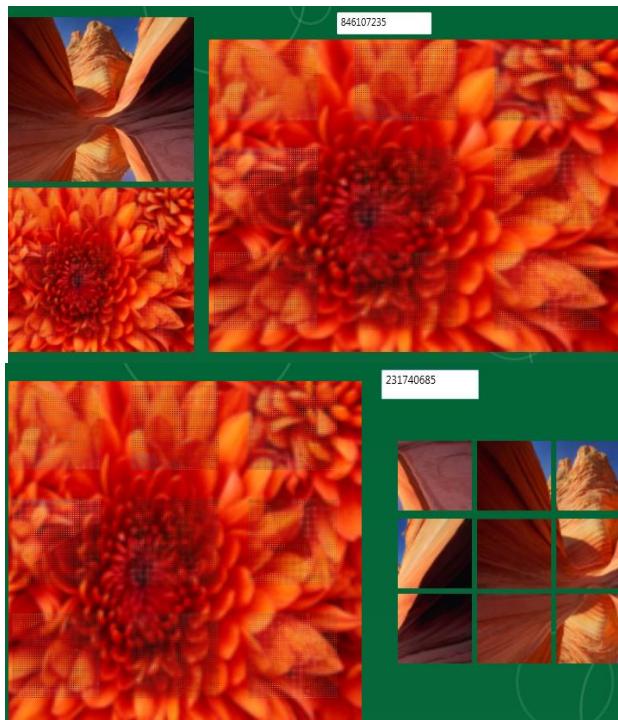


Fig 5.5 Mosaic Image with the generated key

Fig 5.5 Recovery of Secret Image Image with Key

The image that is to be sent is uploaded and also its average (r,g,b) pixel value is computed and saved. The mosaic image is uploaded and the secret key is given as the input. The secret image is finally extracted from it.

VI. SUMMARY AND CONCLUDING REMARKS

In this paper, we have used Secret fragment visible mosaic image for the secured hiding of information by various techniques. An additional security enhancement measure was also proposed by the generation of a secret key.

A new type of digital art, called secret-fragment-visible mosaic image, has been proposed, which can be used for secure keeping or covert communication of secret images. This type of mosaic image is composed of small

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

fragments of an input secret image; and though all the fragments of the secret image can be seen clearly, they are so tiny in size and so random in position that people cannot figure out what the source secret image looks like.

Specifically, a new color-scale and a new grayscale have been proposed to define a new -feature and a new -feature, which then are used to define appropriate similarity measures for images and blocks for generating secret-fragment-visible mosaic images more effectively. A greedy search algorithm has also been proposed for searching the tile images in a secret image for the most similar ones to fit the target blocks of a selected target image more efficiently. Tile-image fitting information for secret image recovery is embedded into randomly selected tile images in the resulting mosaic image controlled by a secret key. An additional security enhancement measure was also proposed. The method has been extended to generate grayscale mosaic images with grayscale secret images as input. Good experimental results have been shown to prove the feasibility of the proposed method. Good mosaic image creation results are guaranteed only when the database is large in size so that the selected target image can be sufficiently similar to the input secret image.

Future works may be directed to allowing users to select target images from a smaller-sized database or even freely without using a database, as well as to developing more information hiding applications using secret fragment technique.

REFERENCES

- [1] Amit Phadikar and Santi, et. al. "ROI Based Error Concealment of Compressed Object Based Image Using QIM Data Hiding and Wavelet Transform" VOL.56,no 2,pp.971-979,IEEE TRANSACTIONS on Consumer Electronics, May 2010.
- [2] Jebaraj S., Iniyam S., Kota H., Forecasting of commercial energy consumption in India using artificial neural network", International Journal of Global Energy Issues, ISSN : 0954-7118, 27(3) (2007) pp.276-301.
- [3] Lixin Luo, Zhenyong Chen, et. al. "Reversible Image Watermarking Using Interpolation Technique", VOL.5,no 1,pp.187-193 ,IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, March 2010.
- [4] Sharmila S., Jeyanthi Rebecca L., "GC-MS Analysis of esters of fatty acid present in biodiesel produced from Cladophora vagabunda", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(11) (2012) pp.4883-4887.
- [5] Zhenxing Qian and Guorui Feng, et. al. "Inpainting Assisted Self Recovery With Decreased Embedding Data", VOL.17,no 11,pp.929-932 ,IEEE SIGNAL PROCESSING LETTERS, November 2010.
- [6] Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., 'Highly secured online voting system over network", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp.4831-4836.
- [7] Jun Zhang and Dan Zhang, et. al. "Detection of LSB Matching Steganography in Decompressed Images", VOL.17,no 2,pp.141-144 ,IEEE SIGANL PROCESSING LETTERS ,February 2010.
- [8] Kiran Kumar T.V.U., Karthik B., 'Improving network life time using static cluster routing for wireless sensor networks", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S5) (2013) pp.4642-4647.
- Feng Li,Jie Wu, et. al. "Fast Matrix Embedding by Matrix Extending", VOL.7,no 1,pp.346-350 ,IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, February 2010.
- [10]Jeyanthi Rebecca L., Susithra G., Sharmila S., Das M.P., Isolation and screening of chitinase producing *Serratia marcescens* from soil", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 5(2) (2013) pp.192-195.
- [11] Jemima Daniel,The world of illusion in Tennessee William's "The Glass Menagerie",International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 6183-6185 ,Vol. 2, Issue 11, November 2013.
- [12] Jemima Daniel,Themes of Violence, Horror, Death in Hemingway,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 4500-4503,Vol. 2, Issue 9, September 2013.
- [13] Jemima Daniel,Role of Technology in Teaching Language,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753, pp 2287-2283,Vol. 2, Issue 6, June 2013.
- [14] Jemima Daniel,Optimism in Samuel Beckett's Waiting for Godot,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 5467-5470,Vol. 2, Issue 10, October 2013.
- [15] Jemima Daniel,Treatment of Myth in Girish Karnad'S Play the Fire and the Rain,International Journal of Innovative Research in Science, Engineering and Technology ,ISSN: 2319-8753, pp 1115-1117 ,Vol. 2, Issue 4, April 2013.
- [16] Jemima Daniel,Audio-Visual Aids in Teaching of English,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753, pp 3811-3814,Vol. 2, Issue 8, August 2013.