A NEW APPROACH TO IDENTIFY THE STEGNO IMAGE USING EIGEN VALUE AND EIGEN VECTOR METHOD

Dr.S.S Dinakaran[#1], M.Sc., M.Phil., Ph.D.,
Associate Professor
Department of Computer Science & Engineering
Alagappa University
Karaikudi – 630 003.

A.Ruby[#2]
Research Scholar
Department of Computer Science & Engineering
Alagappa University
Karaikudi – 630 003.

***Abstract*: In this paper we propose a new BMP based Steganography image identification using Eigen values and Eigen Vectors Technique. This is new approach and this method is different from normal and Steganography image comparison, the steganography technique is normally based on BMP images by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of steganography image identification using Eigen values and Eigen Vectors Technique. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.**

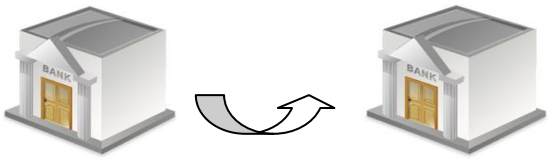
***Keywords:* Eigen values, Eigen Vectors and BMP based steganography technique**

I. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images. This paper's focus is on a relatively new field of study in Information Technology known as Steganography using Eigen values and Eigen Vectors Technique.

These techniques based on hidden data from the image processing. The messaged images have easy to identify by using matrix concept. We used this spare matrix Eigen value and Eigen vectors method for normal image to steganography image color value comparison. The data has hidden by changing to confidential data employing. For using Eigen values and Eigen vectors manipulating method the image color value is used to identify it, the RGB color is very important from the image; it can be easy to retrieve from the values, used to this technique.



Normal Image **Stegno Image**

II. LITERATURE STUDY

A. Eigen values and Eigen vectors:

A1. Definitions of Eigen value and Eigenvector

Eigenvalues are a special set of scalars associated with a linear system of equations (i.e., a matrix equation) that are sometimes also known as characteristic roots, characteristic values (Hoffman and Kunze 1971), proper values, or latent roots (Marcus and Minc 1988, p. 144)

The determination of the eigenvalues and eigenvectors of a system is extremely important in physics and engineering, where it is equivalent to matrix diagonalization and arises in such common applications as stability analysis, the physics of rotating bodies, and small oscillations of vibrating systems, to name only a few. Each eigenvalue is paired with a corresponding so-called eigenvector (or, in general, a corresponding right eigenvector and a corresponding left eigenvector; there is no analogous distinction between left and right for eigenvalues)

A2. Identifying eigenvalues:

The computation of eigenvalue/eigenvector can be realized with the following algorithm.Consider an n-square matrix *A*

1. Find the roots of the characteristic polynomial of *A*. These are the eigenvalues.

If n different roots are found, then the matrix can be diagonalized.

2. Find a basis for the kernel of the matrix given by $A - \lambda_n I$. For each of the eigenvalues. These are the eigenvectors

The eigenvectors given from different eigenvalues are linearly independent.

The eigenvectors given from a root-multiplicity are also linearly independent.

Let us determine the eigenvalues of the matrix

$$A = \begin{bmatrix} 0 & 1 & -1 \\ 1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$$

which represents a linear operator $\mathbf{R}^3 \to \mathbf{R}^3$.

We first compute the characteristic polynomial of *A*:

$$p(\lambda) = \det(A - \lambda I) = \det \begin{bmatrix} -\lambda & 1 & -1 \\ 1 & 1-\lambda & 0 \\ -1 & 0 & 1-\lambda \end{bmatrix} = -\lambda^3 + 2\lambda^2 + \lambda - 2.$$

This polynomial factors to

$$p(\lambda) = -(\lambda - 2)(\lambda - 1)(\lambda + 1).$$

Therefore, the eigenvalues of *A* are 2, 1 and −1.

A3. Identifying eigenvectors:

With the eigenvalues in hand, we can solve sets of simultaneous linear equations to determine the corresponding eigenvectors. Since we are solving for the system $(A - \lambda I)v = 0$, if $\lambda = 2$then,

$$\begin{bmatrix} -2 & 1 & -1 \\ 1 & -1 & 0 \\ -1 & 0 & -1 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} = 0.$$

Now, reducing $(A - 2I)$

$$\begin{bmatrix} -2 & 1 & -1 \\ 1 & -1 & 0 \\ -1 & 0 & -1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

allows us to solve easily for the eigenspace E_2:

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} = 0 \to \begin{cases} v_1 + v_3 = 0 \\ v_2 + v_3 = 0 \end{cases}$$

$$\to E_2 = \operatorname{span} \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}.$$

We can confirm that a simple example vector chosen from eigenspace $E_2$is a valid eigenvector with eigenvalue $\lambda = 2$:

$$A \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ -2 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}.$$

If *A* is a real matrix, the characteristic polynomial will have real coefficients, but its roots will not necessarily all be real. The complex eigenvalues come in pairs which are conjugates, For a real matrix, the eigenvectors of a non-real eigenvalue *z* , which are the solutions of $(A - zI)v = 0$, cannot be real.If v_1, ..., v_m are eigenvectors with different eigenvalues λ_1, ..., λ_m,

then the vectors v_1, ..., v_m are necessarily linearly independent.The spectral theorem for symmetric matrices states that if A is a real symmetric n-by-n matrix, then all its eigenvalues are real, and there exist n linearly independent eigenvectors for A which are mutually orthogonal. Symmetric matrices are commonly encountered in engineering.

Our example matrix from above is symmetric, and three mutually orthogonal eigenvectors of A are

$$v_1 = \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \quad v_3 = \begin{bmatrix} 2 \\ -1 \\ 1 \end{bmatrix}.$$

These three vectors form a basis of $\mathbf{R}^3$. With respect to this basis, the linear map represented by A takes a particularly simple form: every vector x in $\mathbf{R}^3$ can be written uniquely as $x = x_1v_1 + x_2v_2 + x_3v_3$ and then we have $Ax = 2x_1v_1 + x_2v_2 - x_3v_3$.

B. Steganography:

B1. What is Steganography and why is it important?

Steganography or Stego as it is often referred to in the IT community, literally means, "covered writing" which is derived from the Greek language. Steganography is defined by Markus Kahn as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present".

In a digital world, Steganography and Cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security.

Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. Mainly because of their popularity on the Internet and the ease of use of the steganographic tools that use these data formats. These formats are also popular because of the relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message.

Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet. Steganographic research is primarily driven by the lack of strength in the cryptographic systems on their own and the desire to have complete secrecy in an open-systems environment. Many governments have created laws that either limit the strength of cryptosystems or prohibit them completely. This has been done primarily for fear by law enforcement not to be able to gain intelligence by wiretaps, etc. This unfortunately leaves the majority of the Internet community either with relatively weak and a lot of the times breakable encryption algorithms or none at all. Civil liberties advocates fight this with the argument that "these limitations are an assault on privacy". This is where Steganography comes in. Steganography can be used to hide important data inside another file so that only the parties intended to get the message even knows a secret message exists. To add multiple layers of security and to help subside the "crypto versus law" problems previously mentioned, it is a good practice to use Cryptography and Steganography together. As mentioned earlier, neither Cryptography nor Steganography are considered "turnkey solutions" to open systems privacy,but using both technologies together can provide a very acceptable amount of privacy for anyone connecting to and communicating over these systems.

B2. Encoding Secret Messages in Images:

Coding secret messages in digital images is by far the most widely used of all methods in the digital world of today. This is because it can take advantage of the limited power of the human visual system (HVS). Almost any plain text, cipher text, image and any other media that can be encoded into a bit stream can be hidden in a digital image. With the continued growth of strong graphics power in computers and the research being put into image based Steganography, this field will continue to grow at a very rapid pace.

Before diving into coding techniques for digital images, a brief explanation of digital image architecture and digital image compression techniques should be explained.

As Duncan Sellars explains "To a computer, an image is an array of numbers that represent light intensities at various points, or pixels. These pixels make up the images raster data." When dealing with digital images for use with Steganography, 8-bit and 24-bit per pixel image files are typical. Both have advantages and disadvantages, as we will explain below. 8-bit images are a great format to use because of their relatively small size. The drawback is that only 256 possible colors can be used which can be a potential problem

during encoding. Usually a gray scale color palette is used when dealing with 8-bit images such as (.GIF) because its gradual change in color will be harder to detect after the image has been encoded with the secret message. 24-bit images offer much more flexibility when used for Steganography. The large numbers of colors (over 16 million) that can be used go well beyond the human visual system (HVS), which makes it very hard to detect once a secret message, has been encoded. The other benefit is that a much larger amount of hidden data can be encoded into a 24-bit digital image as opposed to an 8-bit digital image. The one major drawback to 24-bit digital images is their large size (usually in MB) makes them more suspect than the much smaller 8-bit digital images (usually in KB) when sent over an open system such as the Internet.

Digital image compression is a good solution to large digital images such as the 24-bit images mentioned earlier. There are two types of compression used in digital images, lossy and lossless. Lossy compression such as (.JPEG) greatly reduces the size of a digital image by removing excess image data and calculating a close approximation of the original image. Lossy compression is usually used with 24-bit digital images to reduce its size, but it does carry one major drawback. Lossy compression techniques increase the possibility that the uncompressed secret message will lose parts of its contents because of the fact that lossy compression removes what it sees as excess image data. Lossless compression techniques, as the name suggests, keeps the original digital image in tact without the chance of loss. It is for this reason that it is the compression technique of choice for steganographic uses. Examples of lossless compression techniques are (.GIF and .BMP). The only drawback to lossless image compression is that it doesn't do a very good job at compressing the size of the image data.

We will now discuss a couple of the more popular digital image encoding techniques used today. They are least significant bit (LSB) encoding and masking and filtering techniques.

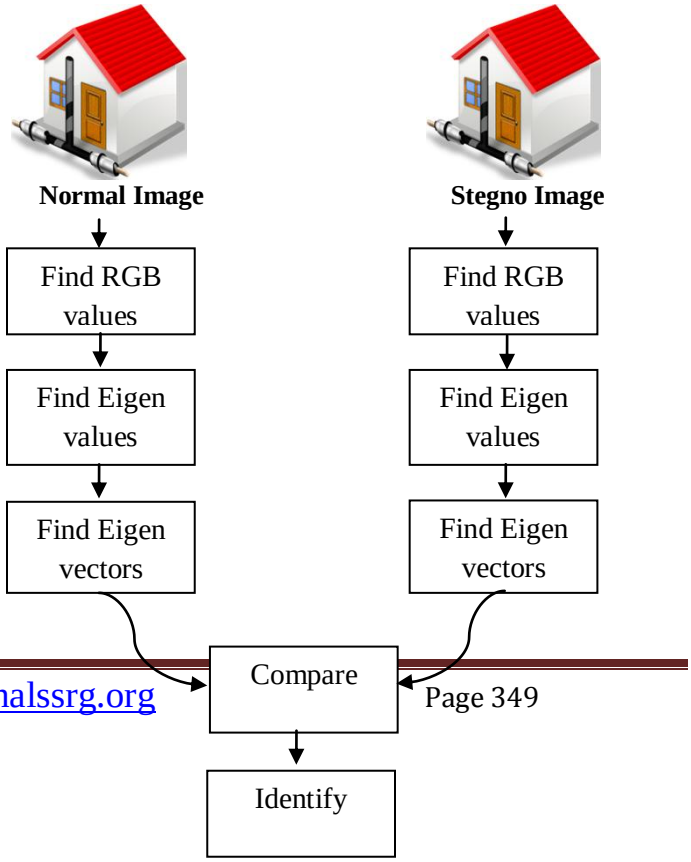
Least significant bit (LSB) encoding is by far the most popular of the coding techniques used for digital images. By using the LSB of each byte (8 bits) in an image for a secret message, you can store 3 bits of data in each pixel for 24-bit images and 1 bit in each pixel for 8-bit images. As you can see, much more information can be stored in a 24-bit image file. Depending on the color palette used for the cover image (i.e., all gray), it is possible to take 2 LSB's from one byte without the human visual system (HVS) being able to tell the difference. The only problem with this technique is that it is very vulnerable to attacks such as image changes and formatting (i.e., changing from .GIF to .JPEG).

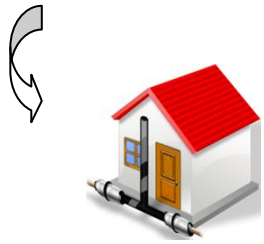
Masking and filtering techniques for digital image encoding such as Digital Watermarking (i.e.- integrating a companies logo on there web content) are more popular with lossy compression techniques such as (.JPEG). This technique actually extends an images data by masking the secret data over the original data as opposed to hiding information inside of the data. Some experts argue that this is definitely a form of Information Hiding, but not technically Steganography. The beauty of Masking and Filtering techniques are that they are immune to image manipulation which makes there possible uses very robust.

As a side note, there are many other techniques that are not covered in this paper that should be researched by anyone interested in using digital images for steganographic purposes. Techniques that use complex algorithms, image transformation techniques and image encryption techniques are still relatively new, but show promise to be more secure and robust ways to use digital images in Steganography.

III. PROPOSED ALGORITHM

1. Calculate RGB color of the Normal image
2. Calculate RGB color of the Stegno image
3. Assign RGB valve of the Normal image in 200*200 Matrix
4. Assign RGB valve of the Stegno image in 200*200 Matrix
5. Find Eigen values of the Normal image from 200*200 Matrix





Stegno Image

6. Find Eigen values of the Stegno image from 200*200 Matrix
7. Find Eigenvector of the Normal image form obtained Normal image Eigen values
8. Find Eigenvector of the Stegno image form obtained Stegno image Eigen values
9. Compare the Eigenvector of Normal image & Stegno image
10. Identify the Stegno image from high pixel value

IV. PROPOSED RESEARCH WORK

We are proposing this valuable method for differentiating the stegno images from the normal images, Normal imagers are actual images without having any hidden information but stegno images are having some hidden information.

Normal images are high pixel resolution images in all the places but stegno images are low pixels only in hidden place (this will be in black color).

If we see the normal & stegno image, both will look same and we can't differentiate the image, to identify the difference we propose to use Eigen values and Eigen Vectors mathematical Technique.

These techniques based on hidden data from the image processing. The messaged images can easy to identify by using matrix concept. We used this spare matrix Eigen value and Eigen vectors method for normal image to stegno image color value comparison. The data has hidden by changing to confidential data employing. For using Eigen values and Eigen vectors manipulating method the image color value is used to identify it.

RGB color is very important from the image; We used to identify the normal image and stegno image from the RGB color, both the images are having certain RGB color in every pixel, we get the image pixel size from each coordinate color values. The color values are converted to matrix method for calculating Eigen values and Eigen vectors, after that it can be easy to retrieve from the each image.

V. SIMULATION RESULTS

Here with we are showing 200*200 two images, one is normal image another one is stegno Image. We will calculate the RGB value of two 200*200 images and we will consider in 200*200 matrix, then we will calculate the Eigen values and Eigen vectors of 200*200 RGB value.

If we see the final result after Eigen values and Eigen vectors calculation stegno image value will be more than normal images only in hidden area.

Modules:

- Normal Image
- Stegno Image

Algorithm:

1. If we see the Figure 1, It was shown the normal and stegno image without any difference but the images are differentiated from the RGB Color.

Figure 1

2. Calculate the RGB color of the Normal image and store it in the row (R1) and column (C1) of the matrix A, then do the same for stegno image and store it in the row(R2) and column (C2) of the matrix B (see the matrix row and column valve of normal and stegno image in Figure2)

Figure 2

3. If we see the Figure 3, before calculating the Eigen values and Eigen vectors, the pixel of the Normal image is higher than the stegno image, so we can't identify the actual stegno image

4. For Identifying the actual stegno image, We will use Eigen values (λ_1, ..., λ_m) and Eigen vectors(v_1, ..., v_m) algorithm of the two matrix A & B (It was shown in the Figure 3 after calculation).

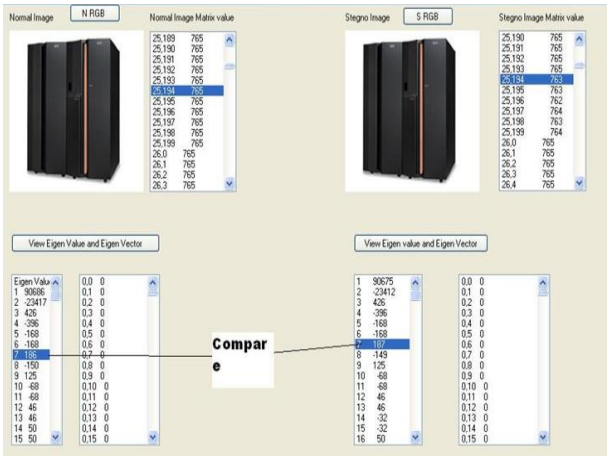


Figure 3

5. If we see the Figure No 4, this will show us the pixel difference for normal and stegno images. So, We Can find the stegno image by using Eigen values and Eigen vectors method.

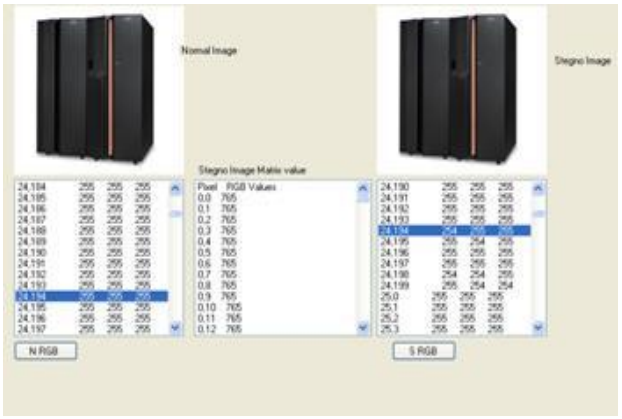


Figure 4

VI. CONCLUSION

In this article, a new algorithm is submitted to find the hidden BMP image which performs the least variations in normal image. Compared to other existing methods, this method can easily identify the stegno images using the mathematical calculation and this will save up to one third of other method. With due attention to the submitted method and less alterations in image, image detection is much more difficult than the previous methods.

VII. REFERENCES

[1] StegoArchive, "Steganography Information, Software and News to enhance your Privacy" 2001, URL: www.StegoArchive.com

[2] Petitcolas, Fabien A.P., "The Information Hiding Homepage: Digital Watermarking and Steganography", URL:http://www.cl.cam.ac.uk/~fapp2/steganography/

[3] Johnson, Neil F., "Steganography", 2000, URL: http://www.jjtc.com/stegdoc/index2.html

[4] Sellars, D., "An Introduction to Steganography", URL:http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html

[5] The WEPIN Store, "Steganography (Hidden Writing)", 1995, URL: http://www.wepin.com/pgp/stego.html

[6] Krinn, J., "Introduction to Steganography", 2000, URL:http://rr.sans.org/covertchannels/steganography.php

[7] Noto, M., "MP3Stego: Hiding Text in MP3 files", 2001, URL:http://rr.sans.org/covertchannels/mp3stego.php

[8] Smith, B.T.; J.M. Boyle; J.J. Dongarra; B.S. Garbow; Y. Ikebe; V.C. Klema; and C.B. Moler."Matrix Eigensystem Routines--(EISPACK) Guide" Springer-Verlag, Berlin. 1976

[9] Garbow, B.S.; J.M. Boyle; J.J. Dongarra; and C.B. Moler. Matrix Eigensystem Routines-- (EISPACK) Guide Extension" Springer-Verlag, Berlin. 1977

VII. BIOGRAPHY

[1]Dr.S.S.Dhenakaran:

Prof.Dr.SS.DHENAKARAN is working as an associate professor in the department of Computer Science and Engineering Alagappa University, Karaikudi, Tamilnadu. He has received his Ph.D in Computer Science and Engineering from Alagappa University, Karaikudi, Tamilnadu, India. He has published many papers in international journals and presented in the national and international conferences.

[2]A.Ruby:

Ms. A.RUBY is a Research scholar in the Department of Computer Science and Engineering, Alagappa University, Karaikudi, Tamilnadu, India. She has received her B.Sc. degree in Information Technology from Madurai Sivakasi Nadar's Pioneer Meenakshi womens college, Poovanthi, Sivagangai Dist in 2008 under Alagappa university, Karaikudi, the MCA Degree from Mohamed Sathak Engineering College, Kilakarai, Ramnad Dist in 2011 under Anna university-Tirchy, She has presented her work in International and National level conferences. Her areas of research interests include Image processing & security.