Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis

Anas.Majeed, Miss Laiha Mat Kiah, Hayan .T. Madhloom, B.B Zaidan,A.A Zaidan

***Abstract*— Steganography is the idea of hiding private, sensitive data or information within something that appears to be nothing but normal. If a person views the digital object that the information is hidden inside, he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information, this is the main objective behind steganography. In this paper we extend a work approved two approaches from LSB algorithm; the 3-3-2 approach without any limitations on the type of images being used and can reach up to 33.3% of size of hidden data, and the second one is the 4-4-4 approach which increase the amount up to 50 % of hidden data from the size of image but with certain limitations on the type of images, the new approach features will increase the data hidden in the image by merge the above approaches. Image texture and edge detection has been involve to appoint the appreciate sample from the image with the suitable approach.**

Keywords:.steganography, LSB, image texture.

I. INTRODUCTION

Steganography is the art of concealing the presence of information within an innocuous container. Steganography has been used throughout history to protect important information from being discovered by enemies. A very early example of Steganography comes from the story of Demartus of Greece. He wished to inform Sparta that Xerces the King of Persia was planning to invade.

Anas Majeed Hamid - Master Student / faculty Computer System & Information Technology /University of Malaya /Kuala Lumpur/Malaysia, phone: +60166201502, Postcode: 58000 Email: hart2hartes@perdana.um.edu.my.

Dr. Miss Laiha Mat Kiah Lecturer & Head Department of Computer System & Technology/ faculty of Computer System & Information Technology /University of Malaya /Kuala Lumpur/Malaysia, Email: misslaiha@um.edu.my.

Hayan .T. Madhloom - Ph.D candidate on the department of A.I Faculty of Computer Science and Information Technology/University of Malaya / Kuala Lumpur/Malaysia phone: +60169146972, Email: hayan.tariq@gmail.com.

Bilal Bahaa Zaidan - PhD candidate, Department of Electrical & Computer Engineering, International Islamic University Malaya, Kuala Lumpur, Malaysia , phone: +60173577866, Postcode: 58000, Email:bilal_bahaa@hotmail.com.

Aos Alaa Zaidan - PhD candidate, Department of Electrical & Computer Engineering, International Islamic University Malaya, Kuala Lumpur, Malaysia, phone: +60172452457, Postcode: 58000 and Email: aws.alaa@yahoo.com.

In ancient Greece wax covered wooden tablets were used to record written text. In order to avoid detection by the Persians, Demartus scraped the wax from a tablet, etched the message into the underlying wood, then recovered the tabled with wax. This concealed the underlying message from the sentries who inspected the tablets as they left Persia by courier for Greece.

Another historical example of Steganography is the use of invisible inks. A common experiment conducted by young kids everywhere is to use a toothpick dipped in vinegar to write a message on a piece of paper. Once the vinegar dries, the presence of the message is not obvious to a casual inspector (aside from the smell). Upon slight heating of the paper, a chemical reaction occurs which darkens the vinegar and makes the message readable. Other, less smelly, invisible inks have been used throughout history similarly even up until World War II.

A more recently developed Steganography technique was invented by the Germans in World War II, the use of microdots. Microdots were very small photographs, the size of a printed period, which contain very clear text when magnified. These microdots contained important information about German war plans and were placed in completely unrelated letters as periods.

Although Steganography is related to Cryptography, the two are fundamentally different.

II. CRYPTOGRAPHY VS. STEGANOGRAPHY

Cryptography is the practice of 'scrambling' messages so that even if detected, they are very difficult to decipher. The purpose of Steganography is to conceal the message such that the very existence of the hidden is 'camouflaged'. However, the two techniques are not mutually exclusive [2],[3].

Steganography and Cryptography are in fact complementary techniques. No matter how strong algorithm, if an encrypted message is discovered, it will be subject to cryptanalysis. Likewise, no matter how well concealed a message is, it is always possible that it will be discovered. By combining Steganography with Cryptography we can conceal the existence of an encrypted message. In doing this, we make it far less likely that an encrypted message will be found. Also, if a message concealed through Steganography is discovered, the discoverer is still faced with the formidable task of deciphering it [3].

III. CURRENT STEGANOGRAPHY TECHNIQUES AND USES

The historical examples given earlier show that the use of Steganography is not limited to a new medium. It should therefore come as no surprise that techniques have been developed to work with digital media. It is now possible to hide any sort of digital media inside any other type of digital media. For example, it is possible to hide a text message, encrypted or plain text, inside of a digital picture or sound file. It is also possible to conceal one type of digital media inside of the same type of digital media. For example an image of a famous painting could be used to conceal a photograph of schematics of some type.

IV. MOTIVATION

In the paper "An Empirical Study of Impact of the Increment of the size of Hidden Data on the Image Texture", the author has described on how can use the human vision system and pure Steganography to increase the size of the data embedded in the images, the study cover two type of images "Gray Level, Color", in the "BMP", "JPEG", the study also shows the highest amount of data hidden in the 24 bit-image without conditions is 33.3%, this research paper has also approved if the texture is complex and there are not smooth areas in the image; its passable to embed 50% from the size of the image, although our experiment shows it is passable to hid data without conditions for more than 33.3% by adding another factor; this factor is the texture analysis.

Image processing is involved in the texture analysis, it is important to quantitatively evaluate such differences using texture features. This paper also discuss the impact of increasing the size of hidden data on the image texture for colour and gray level image, in fact this paper will provide a new study discuss a new approach for data hidden more secure, indeed we are towards from enhance the capacity of data hidden in images without conditions, this enhance carry many benefits, more secure for the data hence there will not be a pure steganography, in other word we will prevent the statistic attacking; it will be more difficult if it is not impassable to estimate statically the protecting data in the images,

V. EXPEREMENT RESULT

In this part we will expires some of the result for the study, for giving more understanding to the new approach let review some of the result after applying a high rate data hidden approach

Texture analysis refers to the characterization of regions in an image by their texture content. Texture analysis attempts to quantify intuitive qualities described by terms such as rough, smooth, silky, or bumpy as a function of the spatial variation in pixel intensities. In this sense, the roughness or bumpiness refers to variations in the intensity values, or gray levels.

Texture analysis is used in a variety of applications, including remote sensing, automated inspection, and medical image processing. Texture analysis can be used to find the texture boundaries, called texture segmentation. Texture analysis can be helpful when objects in an image are more characterized by their texture than by intensity.

This image below involve a flat area bounded by red color this areas if we apply the high rate data hidden regarding to that paper which we has talk about in the beginning, the result will be around 33.3%, and we cannot apply the hidden operation on the 4-bit, figure 1 below shows the flat area in the image

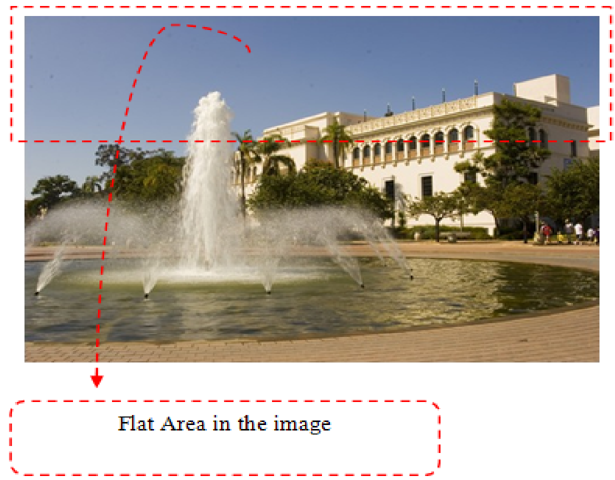

Figure 1 appoint the flat areas in the image

In fact if we apply the Least Significant Bit (LSB) up to the 4-bit data hidden the distortion in the flat areas being clear as shows in figure 2, in this case data hidden will be not more than 33.3% from the size of the images

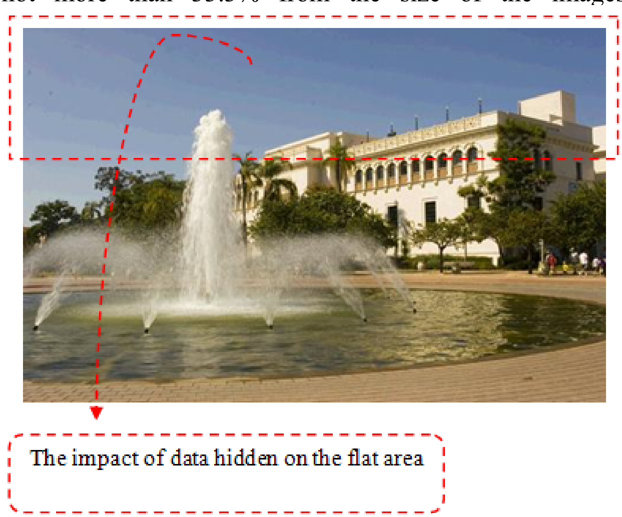

Figure 2 the impact of apply 4-bit LSB in the flat areas.

Certainly, there are many of the areas is suitable for the 4-bit LSB and some cannot work unless the LSB below the 4-bit, that was the 1st motive to consider there is missing factor, this factor is image texture analysis, in the beginning if we read the matrix of the original image pixels value it give no sense to extract any feature and find a way to apply the algorithm, figure 3 shows the matrix of image pixels.

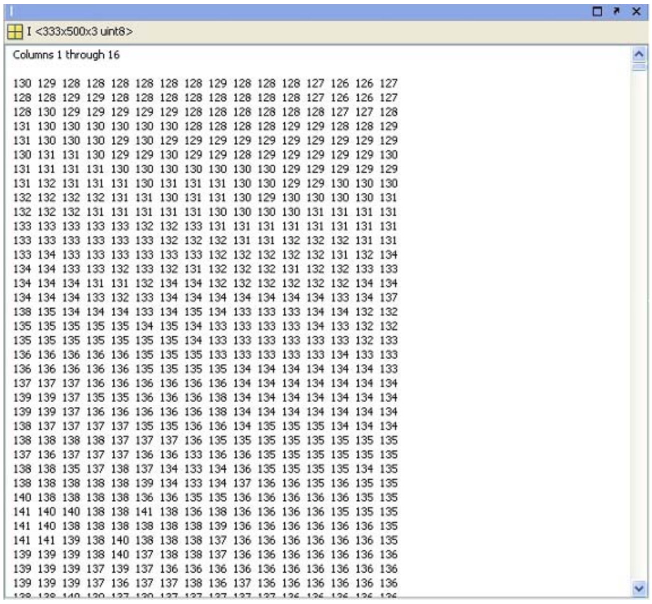

Figure 3 shows the image in a matrix

The 1st thing come to the mind is the image texture analysis where is extract many of the image texture, such us the complexity of the texture which is our necessitate in this project, figure 4 shows the flat areas using texture analysis

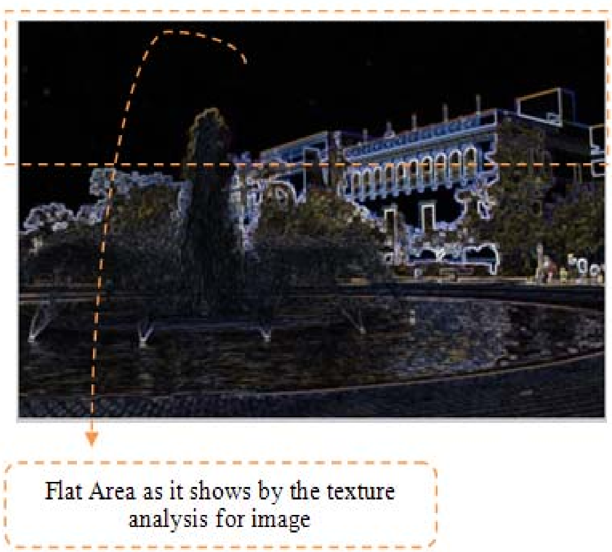

Figure 4 the flat area using image texture analysis

The matrix of the image texture shows how the flat areas represent at this matrix; actually we will use this factor to apply our algorithm.

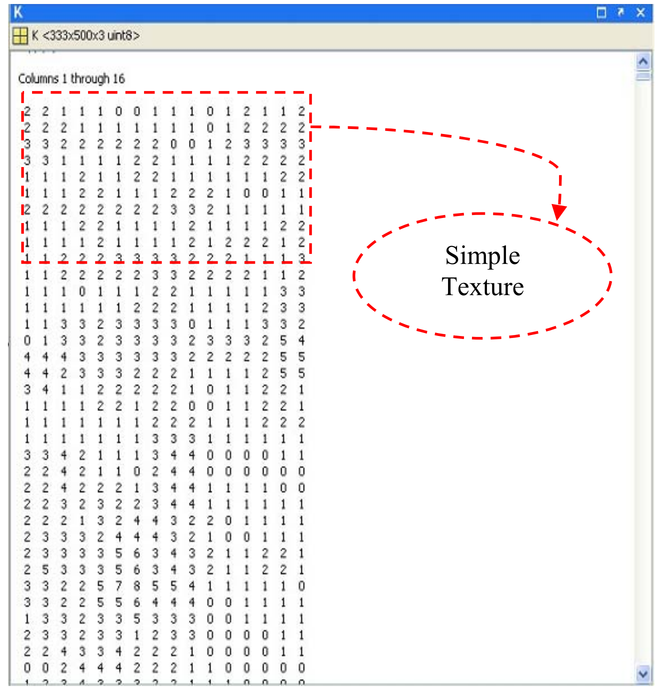

Figure 5 how the pixels presentation for the flat areas

For instant there are many methods for calculate the images texture or extract the images features, figure 6 is another method for calculate the images texture

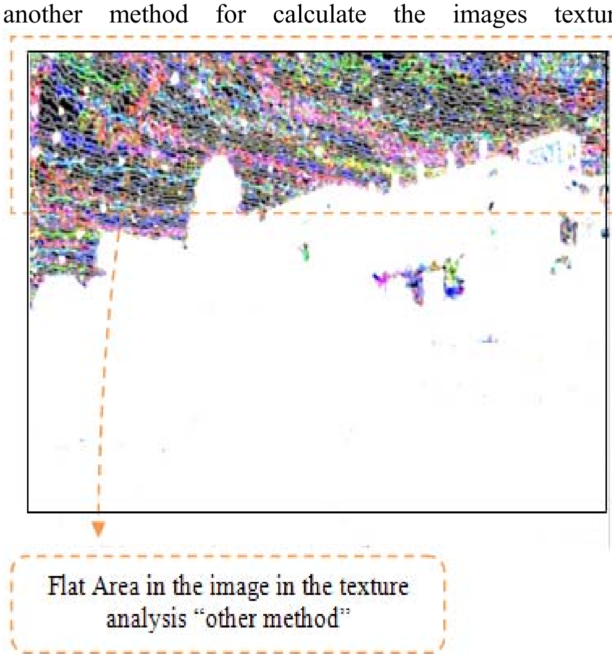

Figure 8 below shows the matrix or complex texture, it's clearly showing how we can differentiate between the simple texture and the complex texture.

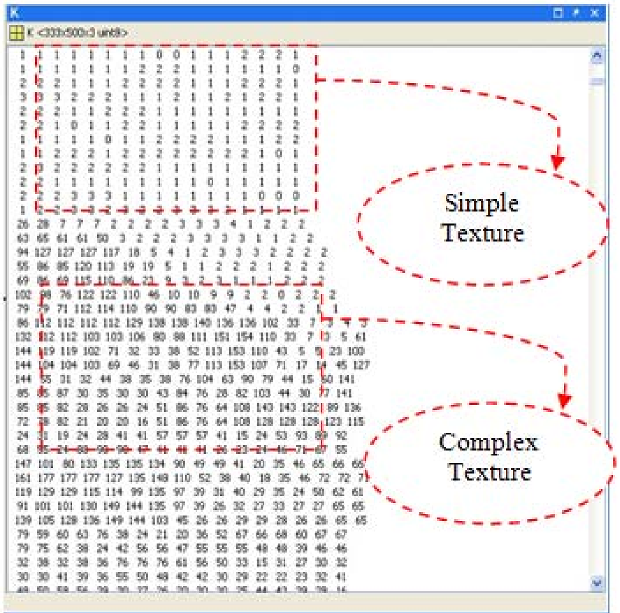

Figure 8 simple texture and complex texture in the texture analysis matrix

In conclusion there are some features in the image texture will be change after augment the data hidden, in this study we will focus on the image texture regarding to the data hidden, in other hand there are some feature we are going to use intended for make the data hidden being stronger.

VI. Image Texture Methods

We recognize texture when we see it but it is very difficult to define. This difficulty is demonstrated by the number of different texture definitions attempted by vision researchers. Coggins [1] has compiled a catalogue of texture definitions in the computer vision literature and we give for examples here, "Texture is an apparently paradoxical notion. On the one hand, it is commonly used in the early processing of visual information, especially for practical classification purposes. On the other hand, no one has succeeded in producing a commonly accepted definition of texture. The resolution of this paradox, we feel, will depend on a richer, more developed model for early visual information processing, a central aspect of which will be representational systems at many different levels of abstraction. These levels will most probably include actual intensities at the bottom and will progress through edge and orientation descriptors to surface, and perhaps volumetric descriptors. Given these multi-level structures, it seems clear that they should be included in the definition of, and in the computation of "texture descriptors." , through this definition it become clear what is the meaning of texture analysis, however there are many methods we can use for our new approach, texture analysis is a statistical functions, these statistics can characterize the texture of an image because they provide information about the local variability of the intensity values of pixels in an image. For example, in areas with smooth texture, the range of values in the neighborhood around a pixel will be a small value; in areas of rough texture, the range will be larger. Similarly, calculating the standard deviation of pixels in a neighborhood can indicate the degree of variability of pixel values in that region.

VII. Rangefilt

In this research we are going to use rangefilt for texture analysis, in fact we need to understand how this filter work

Let J = rangefilt (I) returns the array J, where each output pixel contains the range value (maximum value - minimum value) of the 3-by-3 neighborhood around the corresponding pixel in the input image I. I can have any dimension. The output image J is the same size as the input image I.

J = rangefilt (I, NHOOD) performs range filtering of the input image I where you specify the neighborhood in NHOOD. NHOOD is a multidimensional array of zeros and ones where the nonzero elements specify the neighborhood for the range filtering operation. NHOOD's size must be odd in each dimension.

By default, rangefilt uses the neighborhood true (3). Rangefilt determines the center element of the neighborhood by floor((size(NHOOD) + 1)/2). For information about specifying neighborhoods, for example we have this N is matrix for random image

VIII. Proposed Solution

The proposed solution key for the predicament exceeding is study the nature of texture, actually, texture analysis give all the image texture properties, in fact, it may shows where is most excellent areas in the image to hide data.

The hidden procedure will be act on the images depend on the texture where there will be two functions for data hidden one for high rate data hidden use complex texture and the other use for simple texture, figure 7 is the flowchart for the new algorithm where P_c represent the Pixels in on the complex texture and P_s represent the Pixels in on the simple texture region.

A. LSB 4-bit

If we try to increase the size of data hidden to the fourth LSB (as shown in Figure 7), changes have been aware in the texture of image and the reason was "flat areas". These obvious differences can be seen in Figure 8

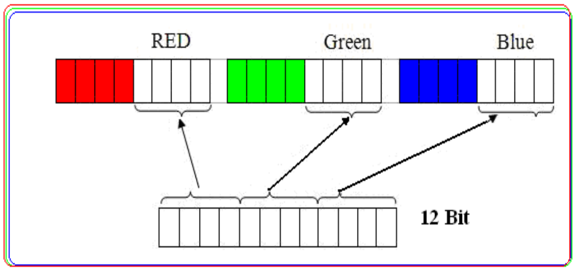

Figure7. One pixel from 24-bit image.

Let $I = \{X_i,\ i \in \Omega\}$ where Ω is an index set denote the mean subtracted cover image. The set Ω can be partitioned into three subsets A 1, A2, and A3, where, $\Omega = \cup_{i=1}^{3} A_i$ A_i and $A_i \cap A_j = \emptyset$ for $i \neq j$ Then, the pixel values in a LSB based stego-image $I_s = \{Y_i,\ i \in \Omega\}$ can be represented as

$$Y_i = \begin{cases} X_i + S, S\epsilon\{1,2 \ldots\ldots 15\} & if\ i\epsilon A1 \\ X_i - S, S\epsilon\{1,2 \ldots\ldots 15\} & if\ i\epsilon A2 \\ X_i & if\ i\epsilon A3 \end{cases} \quad \ldots. (1)$$

B. LSB 3-3-2 bit

Taking the advantage of the first characteristics of human vision system can overcome the problem of the sensitivity of the blue, using two bit while using three bit from each other colours green and blue. This means we have been able to hide byte in each pixel of true colour image (24-bit), as shown by Figure 3, and so is to increase the proportion of concealment by 33.33% from the size of file cover, without suspected to the concealment, even if they were chosen at random file cover.

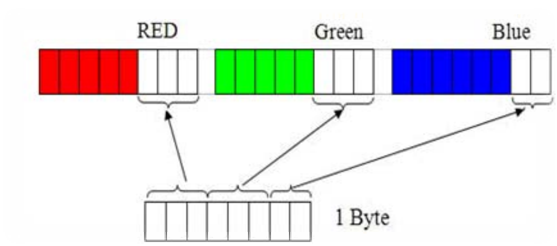

Figure 8 Showing the New Approach (3-3-2)

The new system will classify the texture into two sample, where in the first sample (include the complex texture) we will use the 4- bit LSB, while 3-3-2 approach will be use in the simple texture, by using this technique, we can increase the quantity of data hidden in the image, and the way of encoding will make the possibility of extract the data by the attacker even more difficult, below is the chart of the new approach

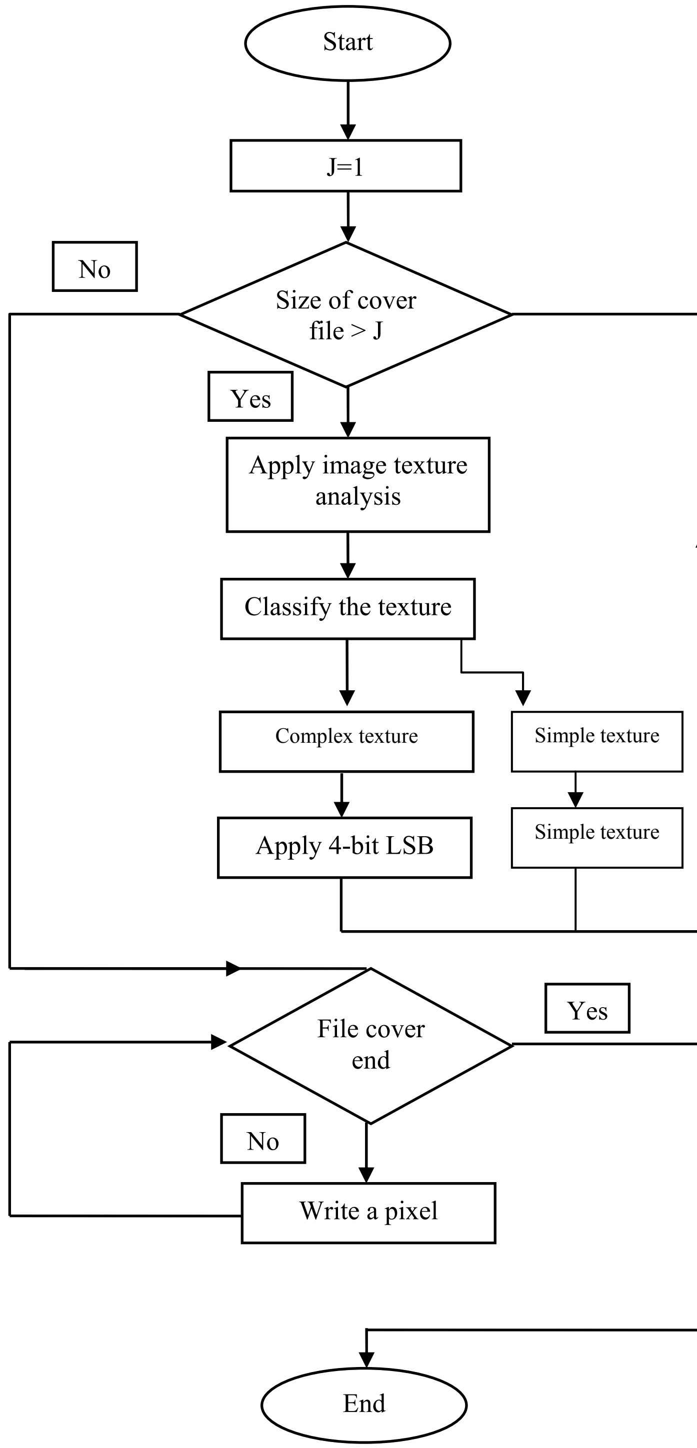

Figure 9 The New Approach Algorithm

We can summarize the new method as it will show below in the block chart.

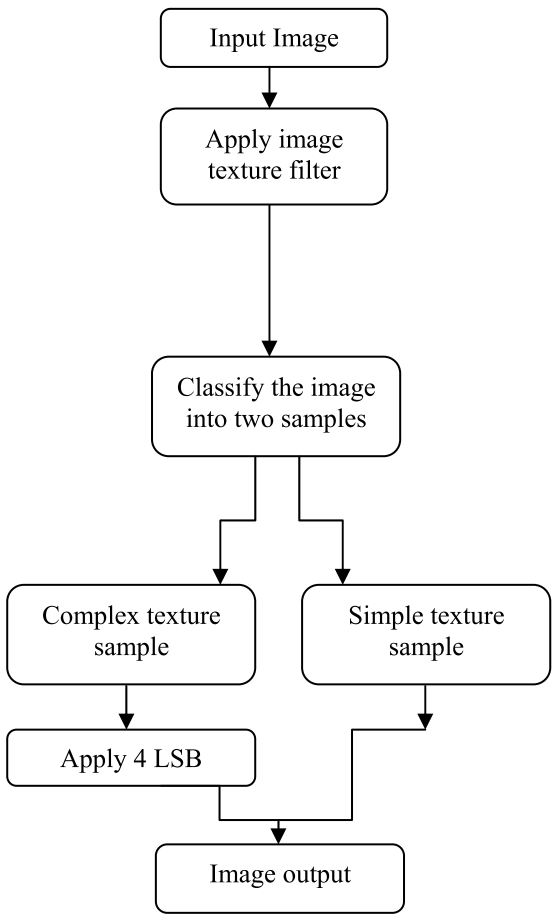

Figure 10 The Flow of the Algorithm

IX. DISSCUSION

Several approaches for data hidden nowadays approved, all these approaches meet up on a sole purpose which is protecting the data from the third party, with the enormous progress in the world of software and information security yet the attackers attempt didn't stop, on the contrary they increase those capabilities, possibilities, conducts, for a different purpose, money awful habits, etc, for that reason any new technique is required, the main purpose from hidden information and encryption is to protect the data from against, although it represents a real challenge, this paper review many principle of protecting data, in fact, we tried to Marge between different approaches, perhaps three methods to come with a new approach for high rate data hidden, high security through two ways to reduce the suspected level from the fabrication in the image through the human eyes, also prevent the traditional methods from found out there is data hidden, indeed the way that we depend on for the 1st stage is the image texture, the benefit of the image texture to appoint the appreciate pixels on which the attacker will not suspect there is data hidden over the image, yet there is not attacker could destroyed this method, with the appreciate pixels for embedding data, the algorithm will be extremely secure, the experiment result shows the applicability of the algorithm and the successful of applying the two methods with the hidden data in the images

X. ACKNOWLEDGEMENT

This work was supported in part by the University of Malaya, Kuala Lumpur Malaysia.

REFERENCES

[1] B.B Zaidan A.A Zaidan, Fazida Othman "Quality of Image vs. Quantity of Data Hidden in the Image File" The 2009 International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV'09: July 13-16, 2009, USA) World Academyof Science, 2009, USA

[2] A.A.Zaidan, B.B.Zaidan, Anas Majeed, "High Securing Cover-File of Hidden Data Using Statistical Technique and AES Encryption Algorithm", Directory of Open Access Journals (DOAJ), Electronic Journals Library (Elektronische Zeitschriftenbibliothek, EZB), 2009, Paris, France.

[3] A.A.Zaidan, Fazidah.Othman, B.B.Zaidan, R.Z.Raji, Ahmed.K.Hasan, and A.W.Naji," Securing Cover-File without Limitation of Hidden Data Size Using Computation between Cryptography and Steganography ", The International Association of Engineers journal (IAENG), ISBN: 978-988-17012-5-1, 2009, London, UK.

[4] A.A.Zaidan, B.B.Zaidan, M.M.Abdulrazzaq, R.Z.Raji and S.M.Mohammed ," Implementation Stage for High Securing Cover-File of Hidden Data Using Computation Between Cryptography and Steganography", International Association of Computer Science and Information Technology (IACSIT), 2009, Manila , Philippines

[5] A.A.Zaidan, B.B. Zaidan, Fazida Othman, , A.W. Naji and Shihab A. Hameed, " Approved Undetectable-Antivirus Steganography for Multimedia Information in PE-File ",International Conference on IACSIT Spring Conference 2009 (IACSIT-SC09), 2009, Singapore.

[6] A.W. Naji, B.B Zaidan, A.A Zaidan, Teddy S. Gunawan and Shihab A. Hameed, "Stego-Analysis Chain, Session One" Investigations on Steganography Weakness Vs Stego-Analysis System for Multimedia File ", International Conference on IACSIT Spring Conference 2009 (IACSIT-SC09), 2009, Singapore.

[7] A.W. Naji, A.A.Zaidan, B.B Zaidan, Shihab A. Hameed, Md Rafiqul Islam and Teddy S.Gunawan," "Stego-Analysis Chain, Session Two" Novel Approach of Stego-Analysis System for Image File ", International Conference on IACSIT Spring Conference(IACSIT-SC09) , 2009, Singapore.

[8] Mohamed Elsadig Eltahir, Laiha Mat Kiah, B.B.Zaidan and A.A.Zaidan," High Rate Video Streaming Steganography", International Conference on Information Management and Engineering (ICIME09), 2009, Kuala Lumpur, Malaysia

[9] Fazida.Othman, Miss.Laiha.Maktom, A.Y.Taqa, B.B.Zaidan, A.A.Zaidan, "An Extensive Empirical Study for the Impact of Increasing Data Hidden on the Images Texture", International Conference on Future Computer and Communication (ICFCC 09), 2009, Kuala Lumpur, Malaysia.

[10] A.A.Zaidan, B.B.Zaidan, Anas Majeed, "High Securing Cover-File of Hidden Data Using Statistical Technique and AES Encryption Algorithm", International Conference on Cryptography, Coding and Information Security (ICCCIS09), 2009, Paris, France.

[11] A.A.Zaidan, Fazidah.Othman, B.B.Zaidan, R.Z.Raji, Ahmed.K.Hasan, and A.W.Naji," Securing Cover-File without Limitation of Hidden Data Size Using Computation between Cryptography and Steganography ", International Conference of Computer Science and Engineering (ICCSE09), 2009, London, UK

[12] B.B.Zaidan, A.A.Zaidan, Fazidah Othman "Enhancement of the Amount of Hidden Data and the Quality of Image", Malaysia Education Security (MyEduSec08), Grand Continental Hotel, 2008, Kuala Trengano, Malaysia.

AUTHORS PROFILE

Anas Majeed Hamid has obtained his bachelor in the computer science/ mustansria University/ Baghdad- Iraq currently he is Master candidate at faculty of Computer System & Information Technology /University of Malaya /Kuala Lumpur/Malaysia, his research interest on network security, steganography, he has publish many papers on steganography and WIMAX.

Dr. Miss Laiha Mat Kiah B.Sc. Comp. Sc. (Hons) (Malaya), M.Sc. (London) Ph.D. (London), joined the Faculty of Computer Science & Information Technology, University of Malaya, Malaysia as a tutor in 1997. She was appointed as a lecturer in 2001. She received her B.Sc. (Hons) in Computer Science from the University of Malaya in 1997, a M.Sc. from Royal Holloway, University of London UK in 1998 and a Ph.D. also from Royal Holloway, University of London in 2007. Between 1999 and 2003 before pursuing her study, she was primarily involved in academic teaching and research in University of Malaya. She was appointed as a senior lecturer in 2008 and currently she is the Head of Computer Systems and Technology Department. Her current research interests include key management, secure group communication and wireless mobile security. She is also interested in routing protocols and ad-hoc networks.

Hayan .T. Madhloom He obtained his bachelor degree in computer science from Al-Mustansyria University 2001, followed by master from master of computer Science from University of Technology 2004 . Currently he is Ph.D candidate on the department of A.I Faculty of Computer Science and Information Technology/University of Malaya / Kuala Lumpur/Malaysia, His research interest in image and computer vision, pattern recognition, A.I application in medicine, information security, steganography and cryptography.

Bilal Bahaa Zaidan He obtained his bachelor degree in Mathematics and Computer Application from Saddam University/Baghdad followed by master from Department of Computer System & Technology Department Faculty of Computer Science and Information Technology/University of Malaya /Kuala Lumpur/Malaysia, He led or member for many funded research projects and He has published more than 40 papers at various international and national conferences and journals. His research interest on Steganography & Cryptography with his group he has published many papers on data hidden through different multimedia carriers such as image, video, audio, text, and non multimedia careers such as unused area within exe. file, he has done projects on Stego-Analysis systems, currently he is working on Quantum Key Distribution QKD and multi module for Steganography, and he is PhD candidate on the Department of Electrical & Computer Engineering, International Islamic University Malaya / Faculty of Engineering / Kuala Lumpur /Malaysia. He is members IAENG, CSTA, WASET, and IACSIT. He is reviewer in the (IJCEE, IJCSNS, IJCSN and IJCSE).

Aos Alaa Zaidan He obtained his 1st Class Bachelor degree in Computer Engineering from university of Technology / Baghdad followed by master in data communication and computer network from University of Malaya. He led or member for many funded research projects and He has published more than 40 papers at various international and national conferences and journals, he has done many projects on Steganography for data hidden through different multimedia carriers image, video, audio, text, and non multimedia carrier unused area within exe. File, Cryptography and Stego-Analysis systems, currently he is working on the multi module for Steganography, Development & Implement a novel Skin Detector. He is PhD candidate on the Department of Electrical & Computer Engineering, International Islamic University Malaya/ Faculty of Engineering / Kuala Lumpur / Malaysia. He is members IAENG, CSTA, WASET, and IACSIT. He is reviewer in the (IJSIS, IJCSNS, IJCSN and IJCSE).