ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Comparison of Information Hiding by LSB Using Arithmetical Sequence on different image Format

Bassam Hasan Saghir[1], Elsamani Abd Elmutalib Ahmed [2], Abdelmajid H. Mansour[3], Gafar Zen A. Salh[4]

Lecturer, Computer Science, Alneelain University, Khartoum, Sudan [1]

Professor, Computer Science, Alneelain University, Khartoum, Sudan [2]

Assistant professor, Information Technology, University of Jeddah, Jeddah, Saudi Arabia [3,4]

Abstract: Information hiding recently become an important area in many applications, and the large demand of internet implementations requires data to be transferred in a secure state, there are many techniques of Information hiding exist for the securing process. The aim of this paper is to compare the hiding of information in images by the least significant bit 'LSB'. This done through inclusion of the secret message inside the image file in a complex form, so that as to make the finding of scattered information inside the image difficult, by using BMP, PNG and JPEG image format. In order to increase the security of the algorithm.

Keywords: Steganography, Information hiding, Cover image, Least Significant Bit (LSB), Stego image, spatial domain, security.

I. INTRODUCTION

Data or information is very crucial to any organization or any individual person. None of us likes our conversation being overheard as it contains the potential of being misused. Same is the case with the data of any organization or of any person. The exchange of data among two potential parties must be in done in a secured method so as to avoid any tampering. Two types of threats exists during any information exchange. The unintended user who may try to overhear this conversation can either tamper with this information to change its original meaning or it can try to listen to the message with intention to decode it and use it to his/her advantage. Both these attacks violated the confidentiality and integrity of the message passed [1].

Information hiding is a general term encompassing many sub disciplines. One of the most important sub disciplines is steganography [2]. Steganography aims to hiding information in a cover data in such a way that non-participating persons are not able to detect the presence of this information by analysing the information detection. Unlike watermarking, steganography does not intended to prevent the hidden information by opponents of removing or changing the hidden message, which is embedded in the cover data but it emphasizes on remains it undetectable. Steganography is particularly interesting for applications in which the encryption cannot used to protect the communication of confidential information. Largest amount of information that can be embedded in a coverage data without producing either statistical or visual distortion up to a certain degree is called the steganographic capacity. Generally the steganographic techniques are developed such that it will be able to maximally utilize the hiding capacity of the cover image. Compared to digital watermarking, another branch of information hiding, steganography stresses more on preserving the secrecy of the information instead of making the hidden information robust to attacks. The digital images appealing for steganographic applications because they have a high degree of redundancy in the presentation and pervasive applications in daily life. This results a growing interest in research on image steganography [3].

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data, the word Steganography literally means covered or hiding writing as derived from Greek. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with Steganography methods reduces the chance of a message being detected. If the message is also encrypted then it provides another layer of protection. Therefore, some Steganographic methods combine traditional Cryptography with Steganography; the sender encrypts the secret message prior to the overall communication process, as it is more difficult for an attacker to detect embedded cipher text in a cover. It has been used through the ages by ordinary people, spies, rulers, government, and armies [4].

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding [5].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

II. LEAST SIGNIFICANT BIT (LSB) CODING

A very popular methodology is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data [6]. That's usually an effective technique in cases where the LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps. In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position [7].

LSB coding is the simplest way to embed information in a digital audio file by substituting the least significant bit of each sampling points with a binary message. In. In referencing specific bits within a binary number, it is common to assign each bit a bit number, ranging from zero upwards to one less than the number of bits in the number. The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By contrast, the three most significant bits stay unchanged (000 to 000). Least significant bits are frequently employed in pseudorandom number generators checksums [6].

III. RELATED WORKS

Information hiding based on Least Significant Bit has been gaining widespread implementation in a number of security systems. It can be applied in either verification or identification mode, there are many researches on this area. Anjali Tiwari, Seema Rani Yadav, N.K Mittal, were presented some recent development in the field of image to image steganography the particular field is selected because of its large data hiding capability and difficulties in identification. Also provided greater scope because of its large sharing over social networks [3]. Zaidoon Kh, AL-Ani, A.A.Zaidan, B.BZaidan and Hamdan.O.Alanazi, were proposed of recognize the researchers for the main fundamentals of steganography. And provided a general overview of the following subject areas: Steganography types, General Steganography system, Characterization of Steganography Systems and Classification of Steganography Techniques [4]. The new method of information hiding in digital image in spatial domain. And using Plane Bit Substitution Method (PBSM) technique in which message bits are embedded into the pixel value(s) of an image, was proposed by Ms.G.S.Sravanthi, Mrs.B.Sunitha Devi, S.M.Riyazoddin and M.Janga Reddy [5]. Abikoye Oluwakemi C., Adewole Kayode S, Oladipupo Ayotunde J, were proposed a data hiding system that is based on audio steganography and cryptography to secure data transfer between the source and destination. Audio medium is used for the steganography and a LSB (Least Significant Bit) algorithm is employed to encode the message inside the audio file [6]. Mehdi Hussain and Mureed Hussain, have critically analyzed various steganographic techniques and also they have covered steganography overview its major types, classification, applications [8]. Pooja Kausshik and Yuvraj Sharma, were compared the different image enhancement techniques by using their quality parameters (MSE & PSNR) and proposed a new erosion enhancement technique [9]. Arvind Kumar, Km.Pooja, were discussed how digital images can be used as a carrier to hide messages. Also analyzed the performance of some of the steganography tools [10]. The good IQM must be accurate and consistent in predicting the quality. Most IQ metrics are related to the difference between two images (the original and the distorted image), were proposed by Yusra A.Y.Al-Najjar, Dr.Der Chen Soong [11]. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, were provided a state-of-the-art review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature. They concluded with some recommendations and advocates for the object-oriented embedding mechanism [12]. In this paper we compare the information hiding in images by using the least significant bit 'LSB', through the inclusion of the secret message inside the image file in a complex form.

IV. PROPOSED SCHEME

This paper propose the comparing of hiding information in images by using the Least Significant Bit 'LSB'. This done through inclusion of the secret message inside the image file in a complex form, so that as to make the finding of scattered information inside the image difficult, by using BMP, PNG and JPEG image format.

The type of hiding used in this algorithm is the Secret key steganography, and the hiding process depends on two secret keys. Key difference between sequence boundary (the difference between a place and nearby place was used in the inclusion process), and another key is used as a starting point for inclusion on the matter may begin embedding of bytes 12444 of the byte image matrix). Improving the least significant bit through including binaries of the secret message by using sequential computational, by identifying their first boundary and the difference between the two consecutive boundary. Then the binaries of the secret message included in the pixels of the image cover. We used several mathematical criteria for measuring the quality of the images after hiding process such as Peak Signal-to-noise ratio (PSNR), Mean Squared Error (MSE), Structural Content (SC), Matthews Correlation Coefficient (MCC), Average Difference (AD), Normalized absolute error (NAE), the structure of information hiding process as shown in the Figure 1.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

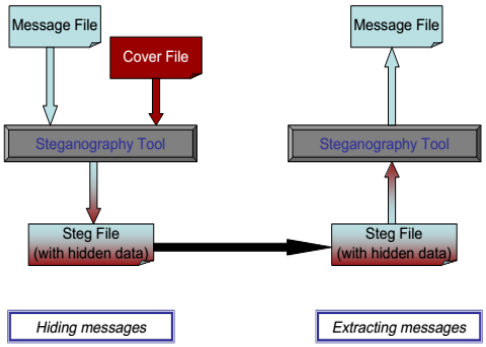

Fig 1. General structure of the information hiding process

The hiding algorithm move through the following steps:

1. Identify the hide cover image (BMP, PNG and JPEG).
2. Convert the cover image to matrix of byte type.
3. Identify the secret message and convert it into a byte type.
4. Identify the byte from the image by using sequential computational, that their first boundary and the difference between the two consecutive boundary determined by the user, and the sequence boundary is the number of secret message binaries.
5. Inclusion of the secret message binaries in the image cover bytes that selected in the previous step.
6. The inclusion done by switching least significant bit of the cover image byte by one byte of the secret message.
7. Saving the cover image that included the secret message on it as stego image.

The following steps show the process of extracting the secret message.

1. Identify stego image (BMP, PNG and JPEG).
2. Convert the stego image to matrix of byte type.
3. Extract the information of secret data size from the image.
4. Identify the first boundary from sequential computation, and the difference between the two consecutive boundaries. Note that the consecutive boundary is the size of the secret message in byte.
5. Extract the binaries of secret message from the image.
6. Save and print the binaries of the secret message and convert it into text file.

The secret message is a text file with size of 9.10 kb, has been hidden on 6 image of all type (BMP, PNG, JPEG). The image quality was tested after the hiding process by mathematical measurements. The inclusion of the message done by choosing the places of hiding randomly using sequential arithmetic, and the difference between their boundary equal 2 in different formats of images. The testing performed on 6 images for each type. These measurements has been calculated to evaluate the quality of the images after the hiding process by MATLAB program. The following table shows some of stego and cover image in different formats.

TABLE 1: COVER AND STEGO IMAGE IN BNP FORMATS

	**Cover image**
	**Stego image**

The following Table 2. Show the Evaluation of Natural image and the Stego image in BNP formats, the size of included data is 9.10 KB.

TABLE 2: EVALUATION OF NATURAL AND STEGO IMAGE IN BNP FORMATS

Image	Size H*W	Text length	Size after stego	MSE	PSNR	MCC	AD	SC	NAE
Image1	743 KB 718*353	9.10KB	530KB	0.0416	61.9389	1	-0.00000036	1	0.000000284
Image2	1.97 MB 960*720	9.10KB	724 KB	0.0159	66.1287	1.0001	-0.0081	0.9999	0.000000298
Image3	2.25 MB 1024*768	9.10KB	2.10 MB	0.0131	66.9481	1	0.0010	1	0.000000127
Image4	1.73 MB 900*675	9.10KB	1.26 MB	0.0173	65.7440	1	-0.0000000312	1	0.000000124
Image5	900 KB 640*480	9.10KB	771 KB	0.0344	62.7713	1.0000	0.0000004915	1	0.000000527
Image6	900 KB 640*480	9.10KB	754 KB	0.0332	62.9339	1	0.0013	1	0.000000434
Image7	854 KB 720*405	9.10KB	420 KB	0.0351	62.6833	0.9999	0.0022	1.0001	0.000000642

TABLE 3: COVER AND STEGO IMAGE IN BNG FORMATS

DOI 10.17148/IJARCCE.2015.44133

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

The following Table 4. Show the Evaluation of Natural image and the Stego image in BNG formats, the size of included data is 9.10 KB.

TABLE 4: EVALUATION OF NATURAL AND STEGO IMAGE IN BNG FORMATS

Image	Size H*W	Text length	Size after stego	MSE	PSNR	MCC	AD	SC	NAE
Image1	299 KB 1174*1029	9.10 KB	230 KB	0.0104	67.9552	0.9999	0.0063	1.0001	0.00000012
Image2	512 KB 820*1024	9.10 KB	515 KB	0.0129	67.0305	1.0000	0.000000026	1.0000	0.00000032
Image3	2.62 MB 900*1200	9.10 KB	2.44 MB	0.0109	67.7389	1.0000	0.0033	1.0001	0.000000085
Image4	2.36 MB 900*1200	9.10 KB	2.24 MB	0.0109	67.7459	0.9999	0.0040	1.0001	0.000000096
Image5	320 KB 1019*742	9.10 KB	327 KB	0.0164	65.9733	1.0000	-0.0020	1.0000	0.00000025
Image6	390 KB 573*339	9.10 KB	455 KB	0.0582	60.4824	1.0000	0.0031	1.0001	0.000000423
Image7	1.62 MB 1200 * 901	9.10 KB	1.78 MB	0.0110	67.7038	1.0000	0.00000047	1.0000	0.000000198

TABLE 5. COVER AND STEGO IMAGE IN JPEG FORMATS

The following Table 6. Show the Evaluation of Natural image and the Stego image in JPEG formats, the size of included data is 9.10 KB.

TABLE 6: EVALUATION OF NATURAL AND STEGO IMAGE IN BNG FORMATS

Image	Size H*W	Text length	Size after stego	MSE	PSNR	MCC	AD	SC	NAE
Image1	558 KB 752*489	9.10 KB	806 KB	0.0279	63.6738	1.0000	0.000000902	1.0000	0.00000026
Image2	407 KB 752*502	9.10 KB	677 KB	0.0278	63.6919	1.0000	0.00000015	1.0000	0.00000028
Image3	269 KB 752*564	9.10 KB	532 KB	0.0217	64.7655	1.0000	-0.0072	0.9999	0.00000012
Image4	549 KB 752*490	9.10 KB	792 KB	0.0285	63.5806	1.0000	0.0024	1.0000	0.000000203
Image5	265 KB 752*500	9.10 KB	379 KB	0.0330	62.9418	1.0000	0.0031	1.0001	0.000000314
Image6	422 KB 752*501	9.10 KB	600 KB	0.0259	64.0022	1.0000	-0.0054	0.9999	0.00000034
Image7	433 KB 752*503	9.10 KB	744 KB	0.0258	64.0133	1.0000	-0.0057	0.9999	0.000000213

The following tables representing the Result of basic requirement for hiding system in a different formats.

DOI 10.17148/IJARCCE.2015.44133

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

TABLE 7: RESULT OF BASIC REQUIREMENT IN DIFFERENT FORMATS

	LSB in BMP	LSB in PNG	LSB in JPEG
Payload Capacity	High	High	High
Size after LSB	<= original	<= original	>original
Detectable	Difficult	Difficult	Low
Invisibility	High*	High*	High*
Robustness against Statistical Attacks	Low	Low	Low
Robustness against Image Manipulation	Low	Low	Low
Independent of File Format	Low	Low	Low
Unsuspicious Files	High*	High*	Low

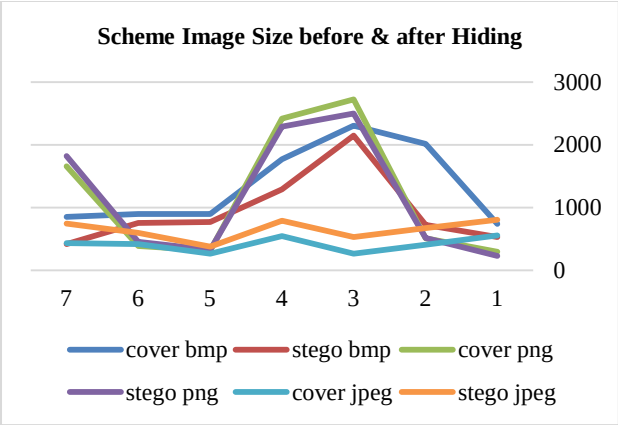

Fig 2. Image size before & after hiding process

From the Fig. 2 above we saw that the values of the files size is more stable with the file format BMP and PNG, while the size of the are files increasing in jpeg images, and this is a defect in a LSB method with JPEG files format .

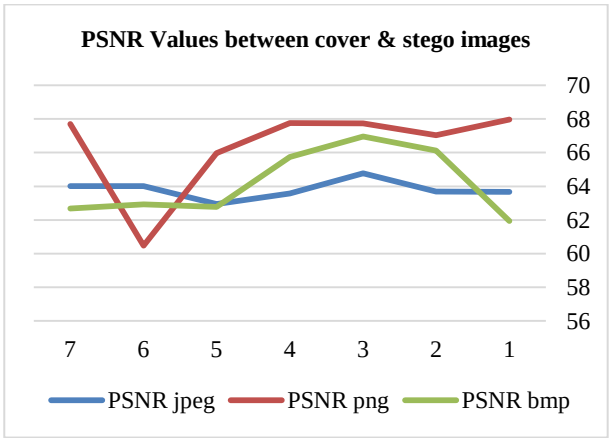

Fig 3. PSNR values of Cover and Stego images

From the Fig. 3 above we saw that the values of PNSR reflect the high quality the image that resulted after the hiding process, and this act as a feature of the algorithm.

From the Fig. 4 above we saw that the Error Rate Square showed very small values, and this act as a benefit for the

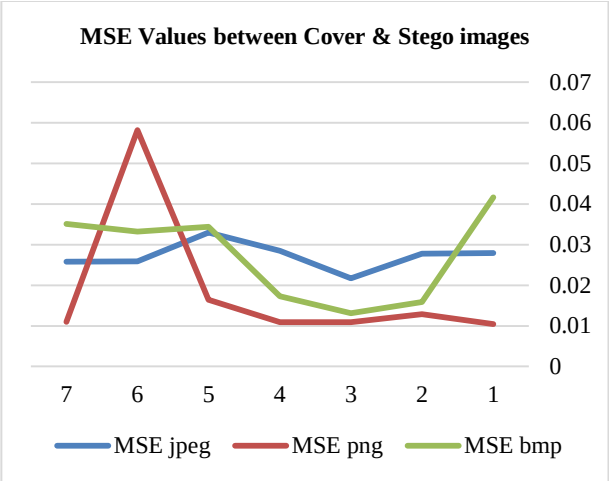

Fig. 4. MSE values of Cover and Stego images

algorithm, where small values of MSE is reverse the result of the PSNR. When the value of MSE increased then the value of PSNR will be decreased. The increasing of MSE value indicate the decreasing of image quality.

V. CONCLUSION

From the results of analysis and diagrams above we saw that when the value of PSNR is higher than 50 db the quality of image become better after the hiding process, and the size of the image decreasing on files with format PNG, BMP. While increasing significantly in JPEG file formats. So the hiding by least significant bit in JPEG may be noticeable because of their large size. So the preference come in the formats of BMP, PNG. Because JPEG suitable in hiding method by space domain methods, which rely on compression.

Where in the JPEG format significantly the file size increase relatively than the normal file size. Therefore will be difficult to upload it on the Internet to send it, and may be easy to detect it by the comparison between the normal image size and the stego image.

The most of previous results were suitable, and the stego image versus normal image have high quality, and very little variation. Almost no in most of the images, although the number of bytes of the secret message 9.10 kb is equivalent to 9318 bytes. From the results of the previous standards, the Average Differences, Normalized absolute

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

error, high variation, and the correlation represents that the quality of the image is high compared with the original image, and the similarity rate is high, and the differences between the structure of the original image and the image after hiding process became more little and small values.

REFERENCES

[1] Richa Gupta," Information Hiding and Attacks: Review", International Journal of Computer Trends and Technology (IJCTT), ISSN: 2231-2803, volume 10, number 1, Apr 2014, pp.21-24.
[2] L. Y. POR, B. Delina," Information Hiding: A New Approach in Text Steganography", 7th WSEAS Int. Conf. on APPLIED COMPUTER & APPLIED COMPUTATIONAL SCIENCE (ACACOS '08), Hangzhou, China, ISSN: 1790-5117, April 6-8, 2008, pp. 689-695.
[3] Anjali Tiwari, Seema Rani Yadav, N.K Mittal, "A Review on Different Image Steganography Techniques", International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume 3, Issue 7, January 2014, pp. 121-124.
[4] Zaidoon Kh, AL-Ani, A.A.Zaidan, B.BZaidan and Hamdan.O.Alanazi, "Overview: Main Fundamentals for Steganography", Journal of Computing, HTTPS://SITES.GOOGLE.COM/SITE/JOURNALOFCOMPUTING/, Vol.2, Issue 3, March 2010, ISSN: 2151-9617, pp. 158-165.
[5] Ms.G.S.Sravanthi, Mrs.B.Sunitha Devi, S.M.Riyazoddin and M.Janga Reddy, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", Global Journal Of Computer Science And Technology Graphics & Vision, Global Journals Inc(USA), ISSN: 0975-4172, Volume 12, Issue 15, Version 1.0, Year 2012, pp. 1-9.
[6] Abikoye Oluwakemi C., Adewole Kayode S, Oladipupo Ayotunde J, "Efficient Data Hiding System using Cryptography and Steganography", International Journal of Applied Information Systems(IJAIS), Foundation of Computer Science FCS, New York, USA, ISSN: 2249-0868, Vol. 4, No.11, December 2012, pp. 6-11.
[7] Jayaram P, Ranganatha H R, Anupama H S," INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011, pp. 86-96.
[8] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography techniques", International Journal of Advanced Science and Technology, Vol. 54, may 2013, pp.113-124.
[9] Pooja Kausshik and Yuvraj Sharma, "Comparison of Different Image Enhancement Techniques Based upon Psnr & Mse", International Journal of Applied Engineering Research, http://www.ripublication.com/ijaer.htm, ISSN: 0973-4562, Vo1.7, No.11, 2012, pp. 1-5.
[10] Arvind Kumar, Km.Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications, ISSN: 0975 – 8887, Volume 9, No. 7, November 2010, pp. 19-23.
[11] Yusra A.Y.Al-Najjar, Dr.Der Chen Soong, "Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI", International Journal of Scientific & Engineering Research, ISSN 2229-5518, Vol 3, Issue 8, August-2012, pp.1-5.
[12] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methodsm", signal processing, volume 90, Issue 3, March 2010, pp. 727-752.

BIOGRAPHIES

Bassam Hasan Saghir Al-Malhani, Lecturer, Department of Computer Science, Faculty of computer Science and Information Technology, Alneelain University, Khartoum, Sudan.
Permanent Address: Department of Computer Science, Faculty of computer and Information Technology, Sana'a University, Sana'a, Yemen.

Prof. Elsamani Abd Elmutalib Ahmed Abd Elmutalib, Professor, Department of Computer Science, Faculty of computer Science and Information Technology, Alneelain University, Khartoum, Sudan.

Dr. Abdelmajid Hassan Mansour Emam, Assistant Professor, Department of Computers and Information Technology, University of Jeddah, Faculty of Computers and Information Technology, Khulais, Jeddah, Saudi Arabia.
Permanent Address: Department of Information Technology, Faculty of computer Science and Information Technology, Alneelain University, Khartoum, Sudan.

Dr. Gafar Zen Alabdeen Salh Hassan, Assistant Professor, Department of Computers and Information Technology, University of Jeddah, Faculty of Computers and Information Technology, Khulais, Jeddah, Saudi Arabia..
Permanent Address: Department of Information Technology, Faculty of computer Science and Information Technology, Alneelain University, Khartoum, Sudan.