Scientific Research and Essays Vol. 5(21), pp. 3254-3260, 4 November, 2010
Available online at http://www.academicjournals.org/SRE
ISSN 1992-2248 ©2010 Academic Journals

Full Length Research Paper

Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study

Gazi Mahabubul Alam[1]*, M. L. Mat Kiah[2], B. B. Zaidan[3], A. A. Zaidan[3] and Hamdan O. Alanazi[2,4]

[1]Department of Educational Management, Planning and Policy, Faculty of Education, University of Malaya, 50606 Kuala Lumpur, Malaysia.
[2]Department of Computer System and Technology, Faculty of Computer Science and IT, University of Malaya, 50603 Kuala Lumpur, Malaysia.
[3]Faculty of Engineering, Multimedia University Jalan Multimedia, 63100 Cyberjaya, Selangor, Malaysia.
[4]Faculty of Applied Medical Science, King Saud University, King Saud University, P. O. Box 2454, Riyadh 11451, Kingdom of Saudi Arabia.

Accepted 8 October, 2010

Mosaic image approaches have been successfully proposed to solve different problems in the image processing such as image segmentation. As it becomes a well known art, there are thousands of mosaic images available in the internet galleries. In addition, there is quite a big number of free mosaic creation software available in the markets. In this paper we will study the features of the mosaic images which can help to implement undetectable data hidden approach (that is steganography approach). Through the research, we found that mosaic image texture is capable to hide up to five LSB layers. Furthermore, there are several papers stated clearly "secure steganography application should be engaged with cryptography". Thus, AES/Rijndael algorithm has been proposed together with the five LSB steganography to ensure the highest rate of data hidden side by side with high level of security. The evaluation of steganography approaches required either objective test (that is passing the SNR, PSNR, MSE or RMSE exam) or subjective test (that is using survey). Many researches conducted to approve the failure of the objective exam. Therefore, we evaluated our approach using the subjective test. Our survey shown the approximate of 99% is the success rate for the mosaic cover, comparing with approximately 50% the success of normal images.

Key words: Mosaic image, high rate data hiding, steganography and data hidden, AES cryptography.

INTRODUCTION

With the increase usage of digital multimedia, the protection of intellectual property rights problem has become very important issue (Findik et al., 2010). Several researchers defined the term security as the confidentiality, integrity, authenticity, non-repudiation, privacy and data protection (Yass et al., 2010; Alanazi et al., 2010; Haque et al., 2009). (Hashim et al., 2010; Alam, 2009b) said "Privacy and security are very important issues being discussed in the literature of the ICT". According to (Qabajeh et al., 2009; Alam and Khalifa, 2009a; Raad et al., 2010) conclude that privacy, copyright and security are very important issues. Mosaic image is an image which consists of hundreds or thousands of other images (Zaidan et al., 2010g). Mosaic images created with a set number (specified by the user) of mosaic pieces wide and high with each piece being of the same size. The image that is part of a mosaic is called mosaic piece. Creating a mosaic image required database of hundreds or thousand of images; these images have the same size. When an image is created

*Corresponding author. E-mail: gazi.alam@um.edu.my, gazimalamb@yahoo.com. Tel: + 603-7967 5077. Fax: + 603-7967 5010.

into a mosaic piece, it will resize following the size of that section. Each of the mosaic pieces reminded a section of the overall mosaic image. One of the most noticeable features of the mosaic images is the disparity in size. According to one of the internet Galleries, they publish mosaic image with size 324 MB, 12.000 * 9.000 pixels (Dali, 2009), other example has exceed the 9.4 Gigabytes with number of pixels: 3,366,400,000 (Gogh, 2010). This variation in size made the mosaic image as the best choice to be a cover for the data hidden According to (Zaidan et al., 2010g) steganography in the mosaic image is more successes and less detectable comparing with the normal images.

RESEARCH AIMS AND OBJECTIVES

Generally Data hidden has two techniques, Digital Watermark and Steganography (Zaidan et al., 2010a). According to (Hmood et al., 2010a,c). Data hidden approaches are suffering from the limitation of the size. In this research we will try to achieve the following objectives:

1. To analyze the features of mosaic images that can help to apply the high rate data hidden.
2. To design investigate the effect of increasing the amount of data hidden on the image texture.
3. To implement a gathering approach based on the analysis of mosaic image, and AES/Rijndael cryptosystem.

RESEARCH QUESTIONS

Implementing a new approach of steganography or digital watermark needs to analyze the limitation of recent approaches. Thus, this research tries to spot the light and answer the following questions:

1. According to (Abomhara et al., 2010; Zaidan et al., 2010d) Symmetric cryptography is approved to be the suitable cryptosystem. How good is the symmetric cryptography with data hidden approaches?
2. Increasing the amount of data hidden within the multimedia file might affect the texture of image, video frame, and the signal of audio, therefore, the cover of data hiding would be affected and the distortion would be visible. (Al-Frajat et al., 2010). The question is; is there any type of multimedia files, where increasing the amount of data hidden might not be visible?
3. Steganography cannot stand alone (Zaidan et al., 2010e,f) the question is; is having a hybrid approaches (that is, consists of steganography and cryptography) is worthy?
4. Do you trust the metrics that used to evaluate the steganography object?

Literature review

A number of techniques have been implemented towards improving secure data hidden approaches. They tried to overcome two main problems which are the amount of data hidden and the security of the data against the attackers. The table below depicted the direct related work to our approach (Table 1).

General notes: The most popular application for data hidden has been implemented using LSB algorithm. In the previous research paper (s), they have discussed the capabilities of implement the low LSB encoding within the image (Zaidan et al., 2009), audio file (Ahmed et al., 2010) and video files (Taqa et al., 2009). They conclude that 4 LSB layers which mean embedding 50% from the size of the cover file are possible in some cases. Yet, an approach implement 5 LSB layer of data hidden has not appeared in the literature due to the texture problems. Another issues has been discussed in the literature is the security of data hidden, some research implement their own encryption methods such as (Zaidan et al., 2010d,g), while other research have used either symmetric or asymmetric cryptography such as (Por et al., 2009; Naji et al., 2009; Zaidan et al., 2010c; Taqa et al., 2009) to overcome the problems of the security.

LSB steganography

According to Hmood et al. (2010a,b,c), Ahmed et al. (2010), Zaidan et al. (2009), Taqa et al. (2009), Zaidan et al. (2010a,c,d,g), Hamid et al. (2009), Naji et al. (2009), Por et al. (2008), increase the amount of data hidden up to the 5 LSB layers will affect the texture of the image, audio and video files, therefore, implementing 5 LSB layer approach required a specific texture properties, this research mainly conducted to justify this finding and test the capabilities of the mosaic images to carry up to 62.5% from the size of original image.

Cryptography

Cryptography is the science of securing data from unwanted individuals by changing it into a form non-recognizable by its attackers while stored and transmitted (Naji et al., 2009). Data cryptography mostly is the scrambling of the content of data, such as text, image, audio, video and so on to make the data incomprehensible, invisible or meaningless during transmission or storage called Encryption (Abomhara et al., 2010a).

The main target of cryptography is keeping data protect form unauthorized attackers. Data decryption is the reverse of data encryption. Nowadays, cryptography is not to protect sensitive military information but known as one of the major components of the security policy of any organization and considered industry standard for provide

Table 1. The literature survey of the related work.

Author, data	Contribution
Por et al. (2008)	They combine three steganography algorithms on GIF image through StegCure system, they success on implementing StegCure which hide around 33% with high level of security using PKI.
Naji et al. (2009), Zaidan et al. (2009c)	They have implemented high rate and high secure data hidden using PE-file with AES encryption method, they conclude that AES present a very good algorithm to secure the data; moreover, PE-file is the best cover comparing with multimedia files.
Zaidan et al. (2009)	The author (s) tried to test the largest amount of data that might be hidden in the image using pure steganography. The obtained result was 50% from the size of the images with a condition that “no flat area from the same color density” (that is, simple texture).
Hamid et al. (2009)	They implemented a solution to solve the problem of simple texture by filtering the images into complex and simple texture; they used only the complex texture to hide the data. they overcome the problems that mentioned at (Zaidan et al., 2009).
Taqa et al. (2009)	They implement a frame work to secure the hidden data within the video file, both LSB algorithm and AES has been implemented over the MPEG video to ensure the robustness and the security of the data hidden.
Zaidan et al. (2010d)	They implemented multi-cover steganography using remote sensing image and general recursion neural cryptosystem; they used a non standard method to secure the data before hide it, moreover, they create a multi-cover technique to ensure the robustness of their approach.
Ahmed et al. (2010)	They used the audio file to implement a high rate, robust and secure data hidden, this novel embedding method is invented mainly for the purpose of increasing the capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm.
Hmood et al. (2010a), Hmood et al. (2010c)	The author (s) illustrated the relation between the quantity of data hidden and quality of image using human vision system property and pure Steganography. The main purpose of these papers is to evaluate the effect of increasing the amount of the data and the quality of image. They come with two recommendations, firstly: the images that include a simple texture can hide only 33.3% from the size of image. secondly: images that not include any simple texture can hide up to 50% from the size of the image.
Zaidan et al. (2010g)	They implement StegoMos, StegoMos is a secure approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem, however, they hide only 50% from the size of the image and they used non-standard method (that is ANN-BMP cryptosystem) to secure the data.

information security, confidence, controlling access to resources, and electronic financial business. The first usage of cryptography known in ancient Egypt, it has passed through different stages and was affected by many major events that influenced the way people controlled information. In the Second World War, cryptography played an important role and was a key factor that gave the allied forces the upper hand, and enables them to succeed the war, when they were able to solve the Enigma cipher machine which the Germans used to encrypt their military secret communications (Abomhara et al., 2010a,b).

Cryptography algorithms are either symmetric algorithms, which use symmetric keys (also called secret keys), or asymmetric algorithms, which use asymmetric keys (also called public and private keys). Asymmetric algorithms are used for complex systems to do some other security objectives such as, Non repudiation, Digital Signature, etc. The confidentiality can be achieved using symmetric algorithms. DES, 3DES and AES are examples of symmetric algorithms. AES is much better than others in term of nine factors, which are key length, cipher type,

block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys and time required to check all possible key at 50 billion second (Naji et al., 2010).

Advanced encryption standard (AES) rijndael

At the end of 1990s, National Institute of Standards and Technology (NIST) in U.S.A conducted a competition to develop a replacement for DES. The winner, announced in 2001, is the Rijndael (pronounced "rhine-doll") algorithm, intended to become the new Advanced Encryption Standard. Rijndael mixes up the SPN model by including Galios field operations in each round. It is similar to RSA modulo arithmetic operations; the Galios field operations generate visible nonsense, but can be mathematically reversed. AES have Security is not an absolute; it's a relation between time and cost. Any question about the security of encryption should be asked in terms of time and cost (Abomhara et al., 2010a; Abomhara et al., 2010c).

Nowadays, there are speculations that military intelligence services probably have the technical and economic means to attack keys equal to about 90 bits. However, no civilian researcher has actually seen or reported of such a capability. Actual and demonstrated systems today, within the bounds of a commercial budget of about 1 million dollars can control key lengths of about 70 bits. An aggressive estimate on the rate of technological progress is to suppose that technologies will double the speed of computing devices every year at a fixed cost. If correct, 128 bit keys would be in theory is in range of a military budget within 30 to 40 years. An illustration of the current status for AES is given by the following example, where we suppose an attacker with the ability to build or purchase a system that tries keys at the rate of one billion keys per second. This is at least 1000 times faster than the fastest personal computer in 2009. Under this assumption, the attacker will need around 10 000 000 000 000 000 000 000 years to try all possible keys for the weakest version, AES-128. The key length should thus be chosen after deciding for how long security is necessary, and what the cost must be to brute force a secret key. In some military circumstances a few hours or days security is sufficient - after that the war or the mission is completed and the information uninteresting and without value. In other cases a lifetime may not be long enough. Till this moment, there is no any evidence that AES has any weaknesses making any attack other than exhaustive search that is brute force, possible. Even AES-128 provides a sufficiently large number of possible keys, making an exhaustive search impractical for many decades, provided no technological breakthrough causes the computational power available to rise dramatically and that theoretical research does not find a short cut to avoid the need for exhaustive search. There are many pitfalls to avoid when encryption is implemented, and keys are generated. It is necessary to make sure each and every implementation of security, but hard since it requires careful examination by experts. An important aspect of an evaluation of any specific implementation is to settle on that such an examination has been made, or can be conducted (Abomhara et.al, 2010a; Zaidan et al., 2010b).

RESULT TESTING

In this part, we will present the result of the new approach. Three standard images has been selected for the test, the result of this test has been presented in Figure 1: A, B, C and D. the test below depicted the capabilities of the mosaic image over the normal image on hiding more than 62.5% (5 LSB layers) from the size of the original cover.

System evaluation

Regarding to measurements metrics, the author will use the subjective evaluation since PSNR, SNR, MSE and RMSE is not functional. Regardless to (Kanvel and Monie, 2009) where the author mentioned that the peak signal-to-noise ratio (PSNR) and root mean square error (RMSE) offer a more objective way to compare various algorithms' performance. According to (Hmood et al., 2010b) the well-known objective metrics (that is PSNR, SNR, MSE and RMSE) is not functional. This metrics have been widely criticised with perceived quality measurement.

As we can, it has been depicted from Figures 1, 2 and Table 2, the average success of the normal images were respectively 94.36111, 33.61111, 39.02778, for Figures 1B, 2B and 3B. While the mosaic images 99.88888, 96.44444, 95.47222 for Figure 1 D, 2 D and 3 D respectively, which means that mosaic images texture is the best comparing with the normal images. Thus, mosaic images perform a good cover for data hidden since using 5 LSB bits is undetectable. This evolution support our finding on increasing the amount of the data hidden depend on the complexity of texture.

Conclusion

The mosaic is an image that is consists of hundreds or maybe thousands of other images to create one image. The complex texture of the mosaic image helped to create an extremely high rate of data hidden using five LSB layers without any detectable distortion. The experiment above showed the capability of the mosaic image to hide a high rate of data hidden without any distortion. Our survey shown the approximate of 99% is the success rate for the mosaic cover, comparing with approximately 50% the success of normal images. Moreover, we selected AES/ Rijndael to implement a secure hybrid

Table 2. Evolution table.

Picture no.	Evaluators									Average (%)
	Person 1	Person 2	Person 3	Person 4	Person 5	Person 6	Person 7	Person 8	Person 9	
Picture 1 B	90	100	89	95	85	80	90	100	100	94.36111
Picture 1 D	100	100	95	100	100	98	100	100	100	99.88888
Picture 2 B	50	0	35	51	40	0	59	27	33	33.61111
Picture 2 D	100	99	98	100	85	89	100	100	100	96.44444
Picture 3 B	55	0	45	65	45	0	66	30	40	39.02778
Picture 3 D	100	100	98	99	85	90	99	98	100	95.47222

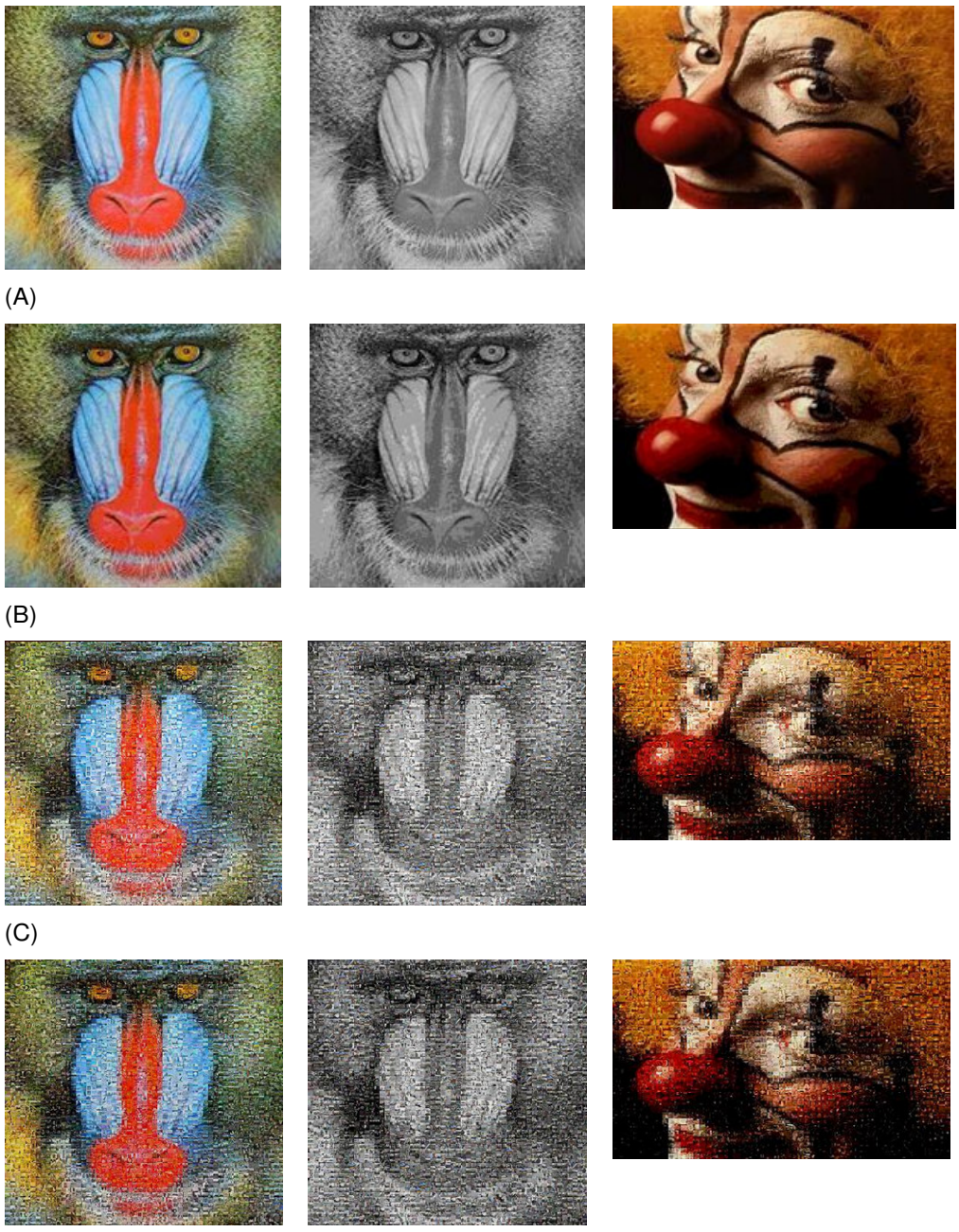

Figure 1. The tested images.

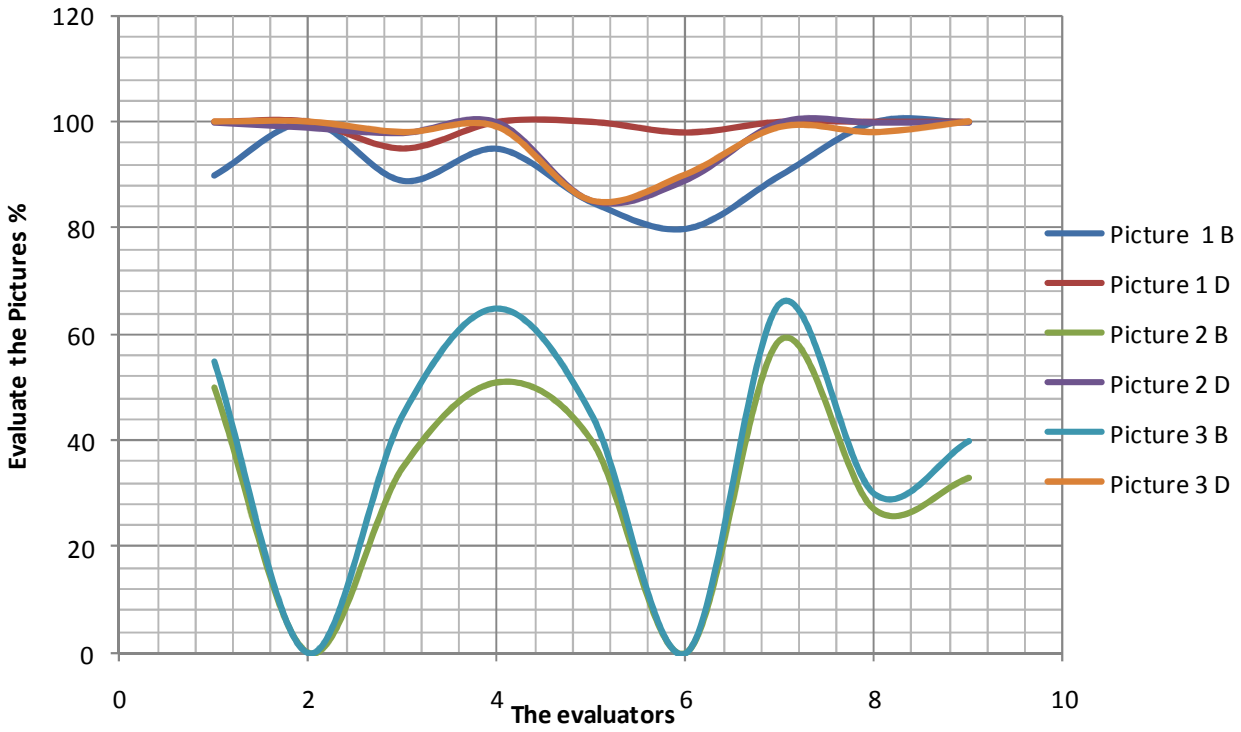

Figure 2. The result of the survey.

approach for data hidden.

ACKNOWLEDGEMENTS

This research has been funded in part from University of Malaya under No. UM.C/625/1. The Authors would like to acknowledge Multimedia University as the Co-funder for this research.

REFERENCES

Abomhara M, Khalifa OO, Zakaria O, Zaidan AA, Zaidan BB, Alanazi HO (2010a). Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview. J. Appl. Sci., 10(15): 1656-1661.

Abomhara M, Khalifa OO, Zakaria O, Zaidan AA, Zaidan BB, Rame A (2010b). Video compression techniques: An overview. J. Appl. Sci., 10: 1834-1840.

Abomhara M, Zakaria O, Khalifa OO, Zaidan AA, Zaidan BB (2010c). Enhancing selective encryption for H.264/AVC using advance encryption standard. Int. J. Comput. Theory Eng., 2(2): 223-229.

Ahmed MA, Kiah MLM Zaidan BB, Zaidan AA (2010). A Novel Embedding Method to Increase Capacity and Robustness of Low-bit Encoding Audio Steganography Technique Using Noise Gate Software Logic Algorithm., J. Appl. Sci., 10(1): 59-64.

Alam GM, Khalifa MTB (2009). The impact of introducing a business marketing approach to education: A study on private HE in Bangladesh. Afr. J. Bus. Manage., 3(9): 463-474.

Alam GM (2009b). Can governance and regulatory control ensure private higher education as business or public goods in Bangladesh? Afr. J. Bus. Manage., 3(12): 890-906.

Alanazi HO, Jalab HA, Zaidan BB, Zaidan AA, Alam GM (2010). Securing Electronic Medical Records Transmissions over Unsecured Communications: An Overview for Better Medical Governance., J. Med. Plants Res. (Accepted).

Al-Frajat AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB (2010). Hiding Data in Video File: An Overview., J. Appl. Sci., 10(15): 1644-1649.

Dali S (2009). Landscape with Butterflies Mosaic Creator Gallery, http://www.aolej.com/mosaic/gallery.htm

Findik O, Babaoglu I, Ülker E (2010). A digital robust image watermarking against desynchronization attacks, Sci. Res. Essays, 5(16): 2288-2294.

Gogh V (2010). Starry Night. Mosaic Creator Gallery, http://www.aolej.com/mosaic/3giga.htm.

Hashim F, Alam GM, Siraj S (2010). Information and communication technology for participatory based decision-making-E-management for administrative efficiency in Higher Education. Int. J. Phys. Sci., 5(4): 383-392.

Haque A, Tarofder AK, Rahman S, Raquib MA (2009). Electronic transaction of internet banking and its perception of Malaysian online customers. Afr. J. Bus. Manage., 3(6): 248-259.

Hamid AM, Mat Kiah ML, Madhloom HT, Zaidan BB, Zaidan AA (2009). Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis, Int. J. Eng. Technol. (IJET), 1(2): 63-69.

Hmood AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB (2010a). On the Capacity and Security of Steganography Approaches: An Overview., J. Appl. Sci., 10(16): 1825-1833.

Hmood AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB (2010b). On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates, Int. J. Phys. Sci., 5(7): 1054-1062.

Hmood AK, Zaidan BB, Zaidan AA, Jalab HA (2010c). An overview on hiding information technique in images. J. Appl. Sci., 10(18): 2094-2100.

Kanvel N, Monie EC (2009). Adaptive lifting based image compression scheme for narrow band transmission system. Int. J. Phys. Sci., 4(4): 194-164.

Naji AW, Hameed SA, Zaidan BB, Al-Khateeb WF, Khalifa OO, Zaidan

AA, Gunawan TS (2009). Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standard and Distortion Techniques, International Journal of Computer Science and Information Security (IJCSIS), 3(1): 73-78.
Por LY, Lai WK, Alireza Z, Ang TF, Su MT, Delina B (2008). StegCure: a comprehensive steganographic tool using enhanced LSB scheme. W. Trans. on Comp. 7(8): 1309-1318.
Qabajeh LK, Mat Kiah ML, Qabajeh MM (2009). A Scalable and Secure Position- Based Routing Protocol for Ad-Hoc Networks, Malaysian J. Comput. Sci., 22(2): 99-120
Raad M, Alam GM, Yeassen NM, Zaidan BB, Zaidan AA (2010). Impact of spam advertisement through email: A study to assess the influence of the anti-spam on the email marketing, Afr. J. Bus. Manage., (Accepted).
Taqa A, Zaidan AA, Zaidan BB (2009). New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm, Int. J. Comput. Elect. Eng. (IJCEE), 1(5): 566-571.
Yass AA, Yaseen NM, Zaidan BB, Zaidan AA, Jalab HA (2010). SSME Architecture Design in Reserving Parking Problems in Malaysia. Afr. J. Bus. Manage., (Accepted).
Zaidan AA, Zaidan BB, Al-Fraja AK, Jalab HA (2010a). Investigate the Capability of Applying Hidden Data in Text File: An Overview, J. Appl. Sci., 10(17): 1916-1922.
Zaidan AA, Zaidan BB, Al-Frajat AK, Jalab HA (2010b). An overview: Theoretical and mathematical perspectives for advance encryption standard/rijndael. J. Appl.Sci., 10(18): 2161-2167.
Zaidan AA, Zaidan BB, Alanazi HO, Gani A, Zakaria O, Alam GM (2010c). Novel approach for high (secures and rate) data hidden within triplex space for executable file, Sci. Res. Essays, 5(15): 1965-1977.
Zaidan AA, Zaidan BB, Taqa AY, Jalab HA, Mustafa KMS, Alam GM (2010d). Novel Multi-Cover Steganography Using Remote Sensing Image and General Recursion Neural Cryptosystem, Int. J. Phys. Sci., (Accepted).
Zaidan AA, Karim HA, Ahmed NN, Alam GM, Zaidan BB (2010e). .A New Hybrid Module for Skin Detector Using Fuzzy Inference System Structure and Explicit Rules, Int. J. Phys. Sci. (in Press).
Zaidan BB, Zaidan AA, Al-Frajat AK, Jalab HA (2010f). On the Differences between Hiding Information and Cryptography Techniques: An Overview J. Appl. Sci., 10(15): 1650-1655.
Zaidan BB, Zaidan AA, Taqa A, Jalab HA, Alam GM, Kiah MLM (2010g). StegoMos: A Secure Novel Approach of High Rate Data Hidden Using Mosaic Image and ANN-BMP Cryptosystem, Int. J. Phys. Sci. (Accepted) pp. ??????.
Zaidan BB, Zaidan AA, Taqa A, Othman F (2009). Stego-Image Vs Stego-Analysis System, Int. J. Eng. Technol. (IJET), 1(5): 596-602.