Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057 OPEN ACCESS 2017 12 (4): 111-117

A Secure Transmission of Multiple Specialized Secret Sharing Scheme

G. Michael, R. Kavitha

Received: 06 December 2016 ▪ Revised: 09 January 2017 ▪ Accepted: 08 February 2017

Abstract: Medical imaging, though very advanced and widespread, has been facing drawbacks with regard to integrity and confidentiality. A relevant literature survey brings into notice that there is no single exhaustive method to deal with all the issues. In telediagnosis it is required that a medical image is distributed among a group of medical experts. However, disclosing all the information of an important patient's medical condition to each of the clinicians is a security issue. A specialized secret sharing scheme is proposed in which digitized, archived and compatible medical images are shared among n clinicians such that at least k of them must gather to reveal the diagnosable medical image. It also emphasizes on the process of hiding textual medical information in these images in order to meet not only the security issue but also suffices the storage requirements during transmission. It is a novel technique for a secure transmission of confidential and important medical information over an insecure network effectively.

Keywords: Visual Cryptography, Confidentiality, Text Hiding, Polynomial Interpolation.

Introduction

Security has become an inseparable issue as information technology is ruling the world now. Cryptography is the study of mathematical techniques and the related aspects of information security such as confidentiality, data security, entity authentication and data origin authentication.

The integrity and confidentiality issues have been satisfied by some of the researchers so far in literature findings. (Acharya et al., 2004; Luo et al., 2003; Shih and Ta Wu, 2005; Woo et al., 2005). Both fragile and robust watermarking techniques are used for integrity control and EPR hiding. The involvement of medical images call for satisfying important issues like that of the integrity and the confidentiality.

Another robust technique abased on genetic algorithms to embed the watermark or textual around the region of interest was proposed by Shih and Ta Wu in 2005. They embed the signature image and the fragile watermark into the frequency domain of non-ROI part of a medical image. Woo et al. (2005) used a multiple watermarking method consisting of an annotation part and a fragile part. In this the encrypted EPR can be embedded in an annotation watermark and tampering can be detected using a fragile watermark. Security can be improved by hash-block-chaining watermarking approach in the fragile watermarking. A method that attaches digital signature and EPR into the medical image was indicated by the works of Zhou et al. (2001). LSB replacing technique has been used to embed the signature. A secure data hiding technique based on the bipolar multiple-base conversion to allow a variety of EPR data to be hidden within the same mark image was presented by Chao et al in 2002. The mark of a hospital used to identify the origin of an EPR could be used as a mark image. There is a good scope of separation and restoration of hidden data by authorized users in this.

Another noted technique of reversible Steganography can be used to hide EPR in medical images. This work was published by Nayak in 2009. Their method doesn't evaluate confidentiality and authenticity of the medical image. Moreover, embedding capacity of their method depends the number of pixels of the medical image. Steganography can be used for EPR hiding and this was indicated by Lou in 2009. However, Integrity and confidentiality of the medical image is not satisfied by their work. Hu and Han in 2009 used Cryptography for transforming medical images into noise like form for protection.

G. Michael, Associate Professor, Department of Computer Science and Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai. E-mail: michaelcse@gmail.com

R. Kavitha, Associate Professor, Department of Computer Science and Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai.

However, noisy images have a great likelihood of attracting malicious user's attention and EPR hiding is not considered. Each method outlined above satisfies different security requirements (confidentiality, authenticity, EPR hiding) for medical image sharing. A method will be proposed for ensuring the secrecy of a medical image, which satisfies the following requirements.

1. Electronic patient records should be hidden in medical images thereby reducing storage requirements and network bandwidth.
2. Confidentiality of the medical images should be maintained.
3. A single individual should not be allowed to diagnose political leaders or high-ranking military officers since it is not adequate to trust only one.

PREVIOUS RESEARCH

Visual cryptography is a technique that enables us to encrypt data in a way that decryption can be done easily by human eye without any computer aid. This being the domain of this paper some related concepts have been discussed below.

Shamir's Secret Sharing Scheme

Shamir, a pioneer in the field of visual cryptography, proposed a scheme back in year 1979. According to it a secret of any form is divided into n number of shares. Out of these n shares at least k or more shares when gathered are sufficient to get back the share intact. Its known as the (k, n) secret sharing scheme. In the present scenario a medical image is to be distributed among a set of clinicians hence the image is converted into noise like shares and distributed among all of them. In order to maintain the secrecy and in case of trust violation even if one less than k clinicians gather it would be impossible to retrieve the secret. This threshold value then depends on various internal factors as well.

Steganography

Steganography is a technique of hiding messages such that no one, apart from the sender and the recipient know about the message, a form of security through obscurity. Medical images are shared among n participants in this work. Since the main issue is hiding a text or an image in it, steganography plays a vital role of an efficient embedding technique. The embedding process encrypts the medical image and the shares that are generated are noisy giving out no hint of the hidden text. This is a reversible process since decryption is needed to get back the hidden contents. If any k or more participants gather, the medical image can be revealed. It is assumed that at least k clinician is an adequate security measure to view the medical image to diagnose.

Polynomial Interpolation

Shamir's method of (k, n) secret sharing is based on a polynomial approach. The image or the text that is being hidden is done so by generating polynomials for every share that is being created. Zhao's method to generate unique keys helps in providing unique shares to every participant. Interpolation of the keys values and the polynomial values would give back the polynomial during decryption and the constant part of the polynomial would be the secret. The pixel values of the medical image are used to generate the polynomial of (k-1) order or less.

The dealer selects a large prime number p and a (k−1) degree polynomial is constructed as in (1) to compute shares using the secret:

RESEARCH METHOD

Overview of this paper consists of the following modules:

a) KEY GENERATION
b) EMBEDDING
c) SHARING
d) RECONSTRUCTION

a) Key Generation

In order to maintain the uniqueness of the shares, every participant is provided with a unique key. This key is generated based on Zhao's method. This method ensures,

- Unique shares by using unique x values.
- x values are calculated independently by both the dealer and participants before the sharing procedure. Thus an insecure channel between the dealer and participants is sufficient.
- Even if one gathers any k shares from the network, one cannot recover the secret image unless corresponding x values for those shares are known.

Algorithm

1. A 'secret shadow' is chosen uniquely by each participant.
2. A dealer chooses primes p & q and computes N=pq.
3. Then the dealer chooses integer g from $[N^{1/2}, N]$ where g is relatively prime to p & q and publishes {g, N}.
4. The participant chooses randomly $s_i \in [2, N]$ and computes $Ri = g^{si} \bmod N$ and provide own R_i to dealer.
5. Now the dealer makes sure $R_i \neq R_j$ and chooses $S_0 \in [2, N]$ where S_0 is relatively prime to (p-1) & (q-1).
6. Then the dealer computes $R_0 = g^{s0} \bmod N$ and publishes $\{R_0\}$ and finally computes $X_i = R_i^{S0} \bmod N$ for each participant.

b) Embedding

The medical image is first embedded with the text i.e., EPR (Electronic Patient Record). EPR is taken from a text file which is read and every character is converted into the corresponding ASCII codes. The number of characters that can be embedded into an image depends on the size and the bit depth of the image. The next step is to generate a polynomial which incorporates both the image pixels and the ASCII code. This polynomial is generated randomly thereby creating a share that is different from the other. This can also be used for embedding an image into another image. Thus the encryption of this sort provides scope for hiding a considerably large amount of text into an image and also for hiding an image into another image.

c) Sharing

In the sharing phase the embedded image i.e., the image with the hidden text is divided into n noise like shares. All the shares are of the same size as that of the medical image. With the available attributes of an image i.e. bit depth and size the image pixels are taken as follows:

$$M = \{m_i \,|m_i \in [0, (2^b - 1)], i = 1,2 \ldots, W * H\}$$

The EPR values are ASCII characters of length L which are represented as follows:

$$E = \{e_i \,|e_i \in [0, 251], i = 1,2 \ldots, L\}$$

With both the image pixel values and the ASCII values of the Electronic Patient Record (EPR) the polynomial and shares are obtained (say) as follows:

$$F(x) = (1+2x) \bmod 257$$

The unique x values are used to obtain Shared pixels:

(1, F (1)) = 3

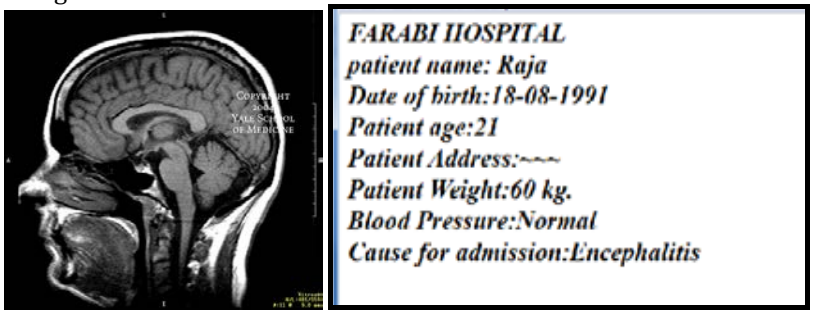
(2, F (2)) = 5

d) Reconstruction

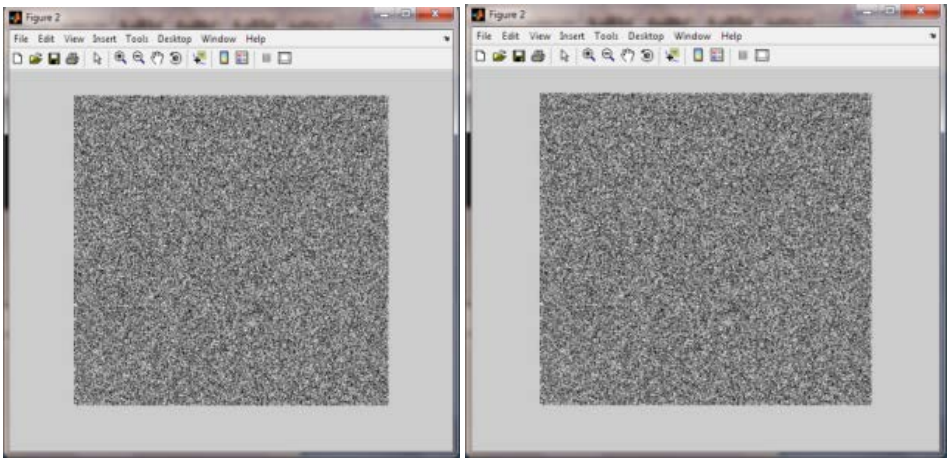
With the individual and unique keys and the shares given to the participants the original image and EPR can be retrieved. Lagrange's interpolation technique extracts the secret by getting back the polynomial. The constant part of the polynomial is the secret. Every part of the image and the text in every share created so it is convenient to interpolate the polynomials of at least k shares to get back the secret. Even in the case of embedding an image into another image both the images can be retrieved separately.

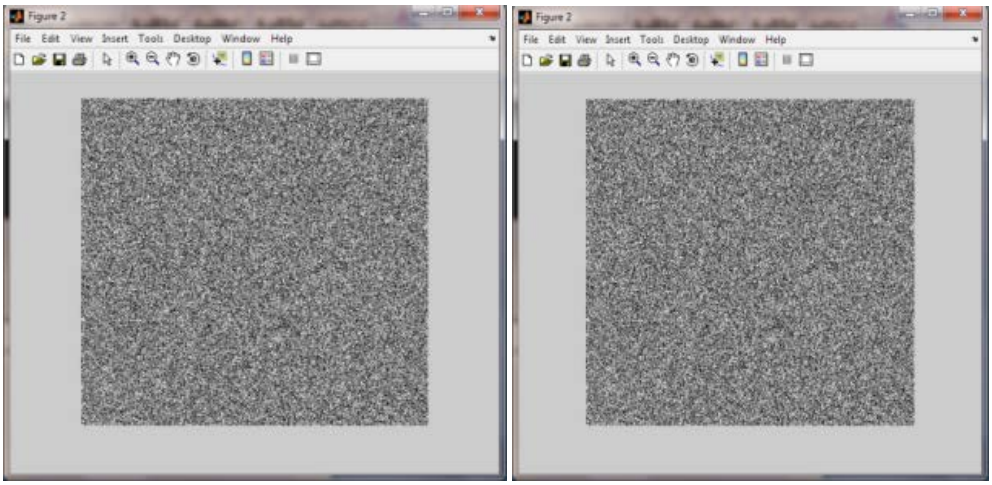
SIMULATION RESULTS

In this section examples are provided to illustrate the effectiveness of the proposed method. A medical 2D X-Ray medical image has been taken and an EPR has been hidden inside it.

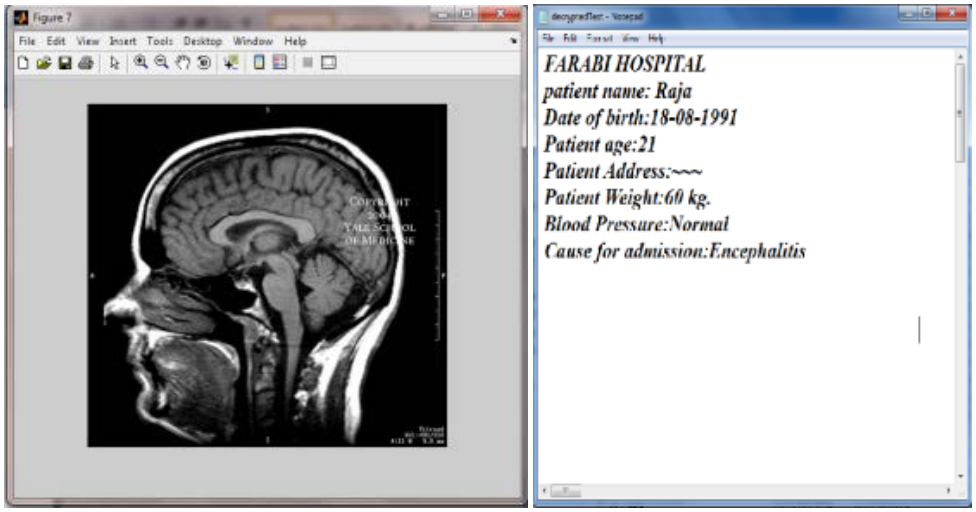


Medical Image EPR





Obtained Shares



Reconstructed secret image Decrypted EPR

During decryption process the secret medical image and the text are retrieved without much distortion to it.

SUMMARY AND CONCLUDING REMARKS

In this paper important medical information in textual form (EPR) are hidden into a secret medical image. This image is then divided into n noise like shares which are unique. In order to avoid any adverse security threats only k or more such shares are sufficient to recover the original text and the image. In case of image embedded in an image both the images can be retrieved efficiently. The recreated image and the recovered text have almost no change from that of the original.

REFERENCES

[1] Das, J., Das, M. P., & Velusamy, P. (2013). Sesbania grandiflora leaf extract mediated green synthesis of antibacterial silver nanoparticles against selected human pathogens. *Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy*, *104*, 265-270.

[2] Umanath, K.P.S.S.K., Palanikumar, K., & Selvamani, S. T. (2013). Analysis of dry sliding wear behaviour of Al6061/SiC/Al2O3 hybrid metal matrix composites. *Composites Part B: Engineering*, *53*, 159-168.

[3] Udayakumar, R., Khanaa, V., Saravanan, T., & Saritha, G. (1786). Cross layer optimization for wireless network (WIMAX). *Middle-East Journal of Scientific Research*, *16*(12), 1786-1789.

[4] Kumaravel, A., & Rangarajan, K. (2013). Algorithm for automaton specification for exploring dynamic labyrinths. *Indian Journal of Science and Technology*, *6*(5S), 4554-4559.

[5] Pieger, S., Salman, A., & Bidra, A.S. (2014). Clinical outcomes of lithium disilicate single crowns and partial fixed dental prostheses: a systematic review. *The Journal of prosthetic dentistry*, *112*(1), 22-30.

[6] Vijayaraghavan, K., Nalini, S.K., Prakash, N.U., & Madhankumar, D. (2012). One step green synthesis of silver nano/microparticles using extracts of Trachyspermum ammi and Papaver somniferum. *Colloids and Surfaces B: Biointerfaces*, *94*, 114-117.

[7] Khanaa, V., Mohanta, K., & Satheesh, B. (2013). Comparative study of uwb communications over fiber using direct and external modulations. *Indian Journal of Science and Technology*, *6*(6), 4845-4847.

[8] Khanaa, V., Thooyamani, K. P., & Udayakumar, R. (1798). Cognitive radio based network for ISM band real time embedded system. *Middle-East Journal of Scientific Research*, *16*(12), 1798-1800.

[9] Vijayaraghavan, K., Nalini, S.K., Prakash, N.U., & Madhankumar, D. (2012). Biomimetic synthesis of silver nanoparticles by aqueous extract of Syzygium aromaticum. *Materials Letters*, *75*, 33-35

[10] Caroline, M.L., Sankar, R., Indirani, R.M., & Vasudevan, S. (2009). Growth, optical, thermal and dielectric studies of an amino acid organic nonlinear optical material: l-Alanine. *Materials Chemistry and Physics*, *114*(1), 490-494.

[11] Kumaravel, A., & Pradeepa, R. (2013). Efficient molecule reduction for drug design by intelligent search methods. *International Journal of Pharma and Bio Sciences*, *4*(2), B1023-B1029.

[12] Kaviyarasu, K., Manikandan, E., Kennedy, J., Jayachandran, M., Ladchumananandasiivam, R., De Gomes, U. U., & Maaza, M. (2016). Synthesis and characterization studies of NiO nanorods for enhancing solar cell efficiency using photon upconversion materials. *Ceramics International*, *42*(7), 8385-8394.

[13] Sengottuvel, P., Satishkumar, S., & Dinakaran, D. (2013). Optimization of multiple characteristics of EDM parameters based on desirability approach and fuzzy modeling. *Procedia Engineering*, *64*, 1069-1078.

[14] Anbuselvi S., Chellaram, C., Jonesh S., Jayanthi L., & Edward J.K.P. (2009). Bioactive potential of coral associated gastropod, Trochus tentorium of Gulf of Mannar, Southeastern India. *J. Med. Sci,* 9(5), 240-244.

[15] Kaviyarasu, K., Ayeshamariam, A., Manikandan, E., Kennedy, J., Ladchumananandasivam, R., Gomes, U. U., & Maaza, M. (2016). Solution processing of CuSe quantum dots: Photocatalytic activity under RhB for UV and visible-light solar irradiation. *Materials Science and Engineering: B*, *210*, 1-9.

[16] Kumaravel, A., & Udayakumar, R. (2013). Web portal visits patterns predicted by intuitionistic fuzzy approach. *Indian Journal of Science and Technology*, *6*(5S), 4549-4553.

[17] Srinivasan, V., & Saravanan, T. (2013). Reformation and market design of power sector. *Middle-East Journal of Scientific Research*, *16*(12), 1763-1767.

[18] Kaviyarasu, K., Manikandan, E., Kennedy, J., & Maaza, M. (2015). A comparative study on the morphological features of highly ordered MgO: AgO nanocube arrays prepared via a hydrothermal method. *RSC Advances*, *5*(100), 82421-82428.

[19] Kumaravel, A., & Udhayakumarapandian, D. (2013). Consruction of meta classifiers for apple scab infections. *International Journal of Pharma and Bio Sciences*, *4*(4), B1207-B1213.

[20] Sankari, S. L., Masthan, K. M. K., Babu, N. A., Bhattacharjee, T., & Elumalai, M. (2012). Apoptosis in cancer-an update. *Asian Pacific journal of cancer prevention*, *13*(10), 4873-4878

[21] Harish, B. N., & Menezes, G. A. (2011). Antimicrobial resistance in typhoidal salmonellae. *Indian journal of medical microbiology*, *29*(3), 223-229.

[22] Manikandan, A., Manikandan, E., Meenatchi, B., Vadivel, S., Jaganathan, S. K., Ladchumananandasivam, R., & Aanand, J. S. (2017). Rare earth element (REE) lanthanum doped zinc oxide (La: ZnO) nanomaterials: synthesis structural optical and antibacterial studies. *Journal of Alloys and Compounds*, *723*, 1155-1161.

[23] Caroline, M. L., & Vasudevan, S. (2008). Growth and characterization of an organic nonlinear optical material: L-alanine alaninium nitrate. *Materials Letters*, *62*(15), 2245-2248.

[24] Saravanan T., Srinivasan V., Udayakumar R. (2013). A approach for visualization of atherosclerosis in coronary artery, Middle - East Journal of Scientific Research, 18(12), 1713-1717.

[25] Poongothai, S., Ilavarasan, R., & Karrunakaran, C.M. (2010). Simultaneous and accurate determination of vitamins B1, B6, B12 and alpha-lipoic acid in multivitamin capsule by reverse-phase high performance liquid chromatographic method. *International Journal of Pharmacy and Pharmaceutical Sciences*, *2*(4), 133-139.

[26] Udayakumar, R., Khanaa, V., & Saravanan, T. (2013). Synthesis and structural characterization of thin films of SnO 2 prepared by spray pyrolysis technique. *Indian Journal of Science and Technology*, *6*(6), 4754-4757

[27] Anbazhagan, R., Satheesh, B., & Gopalakrishnan, K. (2013). Mathematical modeling and simulation of modern cars in the role of stability analysis. *Indian Journal of Science and Technology*, *6*(5S), 4633-4641.

[28] Caroline, M.L., & Vasudevan, S. (2009). Growth and characterization of bis thiourea cadmium iodide: A semiorganic single crystal. *Materials Chemistry and Physics*, *113*(2-3), 670-674.

[29] Sharmila, S., Jeyanthi Rebecca, L., & Das, M. P. (2012). Production of Biodiesel from Chaetomorpha antennina and Gracilaria corticata. *Journal of Chemical and Pharmaceutical Research*, *4*(11), 4870-4874.

[30] Thooyamani, K.P., Khanaa, V., & Udayakumar, R. (2013). An integrated agent system for e-mail coordination using jade. *Indian Journal of Science and Technology*, *6*(6), 4758-4761.

[31] Caroline, M. L., Kandasamy, A., Mohan, R., & Vasudevan, S. (2009). Growth and characterization of dichlorobis l-proline Zn (II): A semiorganic nonlinear optical single crystal. *Journal of Crystal Growth*, *311*(4), 1161-1165.

[32] Caroline, M.L., & Vasudevan, S. (2009). Growth and characterization of L-phenylalanine nitric acid, a new organic nonlinear optical material. *Materials Letters*, *63*(1), 41-44.

[33] Kaviyarasu, K., Xolile Fuku, Genene T. Mola, E. Manikandan, J. Kennedy, and M. Maaza. Photoluminescence of well-aligned ZnO doped CeO2 nanoplatelets by a solvothermal route. *Materials Letters*, *183*(2016), 351-354.

[34] Saravanan, T., & Saritha, G. (2013). Buck converter with a variable number of predictive current distributing method. *Indian Journal of Science and Technology*, *6*(5S), 4583-4588.

[35] Parthasarathy, R., Ilavarasan, R., & Karrunakaran, C. M. (2009). Antidiabetic activity of Thespesia Populnea bark and leaf extract against streptozotocin induced diabetic rats. *International Journal of PharmTech Research*, *1*(4), 1069-1072.

[36] Hanirex, D. K., & Kaliyamurthie, K. P. (2013). Multi-classification approach for detecting thyroid attacks. *International Journal of Pharma and Bio Sciences,* 4(3), B1246-B1251

[37] Kandasamy, A., Mohan, R., Lydia Caroline, M., & Vasudevan, S. (2008). Nucleation kinetics, growth, solubility and dielectric studies of L-proline cadmium chloride monohydrate semi organic nonlinear optical single crystal. *Crystal Research and Technology: Journal of Experimental and Industrial Crystallography*, *43*(2), 186-192.

[38] Srinivasan, V., Saravanan, T., Udayakumar, R., & Saritha, G. (2013). Specific absorption rate in the cell phone user's head. *Middle-East Journal of Scientific Research*, *16*(12), 1748-50.

[39] Udayakumar R., Khanaa V., & Saravanan T. (2013). Chromatic dispersion compensation in optical fiber communication system and its simulation, Indian Journal of Science and Technology, 6(6), 4762-4766.

[40] Vijayaragavan, S.P., Karthik, B., Kiran, T.V.U., & Sundar Raj, M. (1990). Robotic surveillance for patient care in hospitals. *Middle-East Journal of Scientific Research*, *16*(12), 1820-1824.

[41] Gupta, T., & Sharma, A. (2014). Search Accuracy in Web information Retrieval. *International Journal of Communication and Computer Technologies, 2*(2), 98-105.

[42] Kakavand, Z.M., & Chalechale, A. (2015). Comparison of Two Different Distance Functions of Image Retrieval for Detecting Species of Microscopic Fungi in Medical Mycology Laboratory. *International Academic Journal of Science and Engineering, 2*(4), 39-44.

[43] Ramya, V., Ranjitha, S., Sathya Sofia, A., & Ganesh Kumar, P. (2014). Load Balancing of Tasks in Cloud Computing Environment Using Honey Bee Behavior. *International Journal of System Design and Information Processing, 2*(2), 25-53.

[44] Brindha, M.S. (2017). A Survey on Cross Layer Distributed Topology Control in Mobile Adhoc Network. *Bonfring International Journal of Networking Technologies and Applications, 4*(1), 1-3.

[45] Kumar, P. (2014). Load Characteristics of Electric System for Distributing Power on Locality Based Criterion. *Bonfring International Journal of Power Systems and Integrated Circuits, 4*(4), 39-43.

[46] Rama Rao, G., Purna Prakash, J., & Rama Raju, M. (2014). Designing High to Low Cost Solution for Crash Recovery of Servers through Virtualization using Cloud Computing. *International Scientific Journal on Science Engineering & Technology, 17*(5), 549-555.

[47] Arul Jothy, K., Sivakumar, K., & Delsey, M.J. (2018). Distributed System Framework for Mobile Cloud Computing. *Bonfring International Journal of Research in Communication Engineering, 8*(1), 5-9.

[48] Kabeer, V., & Zainul Abid, T.P. (2013). Automated Face Recognition using Artificial Light Receptor Model and SVM Classifier. *The SIJ Transactions on Computer Science Engineering & its Applications, 1*(3), 36-41.

[49] Yasvanthkumaar, V., Sabitha, S., & NithyaKalyani, S. (2018). Parallel and Multiple E-Data Distributed Process with Progressive Duplicate Detection Model. *Bonfring International Journal of Software Engineering and Soft Computing, 8*(1), 23-25.

[50] Kanaga Sundar, R., Joe Paul, J., Krishna Kumar, M., & Laser, L. (2014).Secured POR for Flooding Attack Prevention in Extremely Dynamic Ad Hoc Networks. *The SIJ Transactions on Computer Networks & Communication Engineering (CNCE), 2*(2), 5-9.