A New Tactic to Maintain Privacy and Safety of Imagery Information

Mohammad Alamgir Hossain
Department of Computer Science
Jazan University,
Kingdom of Saudi Arabia

Alwi Mohammad A Bamhdi
Department of Computer Science
JAZAN UNIVERSITY,
Kingdom of Saudi Arabia

Goutam Sanyal
Department of Computer Science and Engineering,
NIT, Durgapur, West Bengal, India

ABSTRACT
Privacy as well as Security is a burning issue to all the users in the field of Information Technology. With the perspective of socio, psychological, organizational, technical, economic and financial ground it is one of the most vital issues in our every day's life. Presently; security is a prime problem in domain of identification or authentication of any information that is delivered or conveyed for the reason of documentation, transaction in our life. There are various types of methodologies, algorithms, techniques available for the safeguard as well as smooth running of the system. Encryption is one among the methodologies that can solve the problem to ensure safety. A lot of encryption systems connected to images, texts, etc. have been proposed by different researchers, each one of them has its strong points as well as weak points. In this paper; a simpler method is proposed that will show a better image representation technique based on encryption. This method is simulated, investigated and executed based on permutation, value transformation and substitution. The selected and the proposed method is elaborated in a well-defined manner. Subsequently; it is assessed and equated based on the test data so that the degree of security and privacy in the encryption method is maintained.

General Terms
Secrecy, authentication, equated, obligates plaintext, encrypt, decrypt, data-image, mitigation.

Keywords
IEBTA, Authentication, HFA, Encryption, Decryption, permutation, block-based-image, image-object.

1. INTRODUCTION
Privacy preserving matter is regarded as an important research topic in a smart grid computing system as well as in many other areas of applications like e-transactions, e-commerce-banking, mobile banking, etc. To identify and formalize a new attack where the invader could exploit the information about the presence or absence of a specified pattern reading is a difficult task. This attack is known as human-factor-aware (HFA attack) cannot be addressed in existing secrecy-preserving collection protocols. It ensures that smart rhythms occasionally upload converted quantities to a supplier or aggregator such that the supplier or aggregator is in position to originate the supplied or aggregated statistics of all pattern quantities. But will be unable to learn anything about the human activities involved within this matter. Image encryption technique equipped information unconceivable. Therefore, no hacker or eavesdropper, including server administrators and others, have access to original message or any other type of conveyed material through public networks such as internet. But the followings are the difficulties those come across with the image encryption methodology. Presently, images are being digitized so that it can be compared through networks from a distance position. In this paper the elementary study of security services and basic design of image encryption systems that will provide security in banking sector, government sector or any other organization is presented. To be successful it is needed to follow that the images are essentially be in the encrypted form of source codes and it will help us to narrate the aforementioned functionality at the application level. This will lead to carry on the functionalities of encrypted image at the user level and the user will use it by the help of some presentable software. In this way it can be, therefore, guaranteed the guard of an image during communication. As a result of which we could achieve the digital data. Encryption technique can be the instant solution to protect information against hacker or eavesdroppers. This system obligates the encryption techniques of image data through some sort of mathematical method based on statistical/mathematical formula where only the actual party that shares the data could possibly be capable to decrypt the digital data in their useable form. Encryption uses a finite set of instruction depending on the conversion method of the original message in the form of plaintext into the cipher text in the encrypted form. Cryptographic technique needs a group of characters known as the key to perform the encryption or decryption of the original data. Based on key method we can encrypt as well as decrypt the original text (plaintext) into cipher text and vice versa.

In the present era, privacy of information is very important as data storage and transaction operation is totally depending on the secured information. Data in the form of image-object are widely used in unalike methods. Therefore for the safe guard of data-image from unauthorized uses is the prime concern nowadays. Data-image encryption method has an important role in the domain of information hiding. Data-image encryption method may vary from simpler to more complicated one. But their reliability and other characteristic will have to maintain in all circumstances. Almost all the encryption method available and are used for text data and may not be suitable for multimedia or image-data. We have discussed about that only and we have focused our ideas by the Section 2 presenting Literature review and problem formulation of various existing image encryption algorithm. Section 3 is presenting proposed work where we are developing new image encryption algorithm. Section 4 presenting results comparison between our propose algorithm and existing algorithm. Finally, Section-5 we have presented conclusion and references.

2. LITERATURE REVIEW

Privacy preservative mitigation matter is regarded as an important research topic in a smart grid computing technique. To identify and formalize a new attack, in which the invader could exploit the information about the presence or absence of a specified pattern, is a difficult task. This attack created as human-factor-aware (HFA) attack, cannot be addressed in existing secrecy-preserving collection protocols. It ensures that smart rhythms; occasionally; upload converted quantities to a supplier or aggregator such that the aggregator is in position to originate the aggregated statistics of all meter quantities but is unable to learn anything about the human activities. Image encryption technique is equipped with information incomprehensible. Therefore, no hacker or eavesdropper, including server administrators and others, have the access permission to original message or any other type of conveyed material through public networks such as internet. But the following are the difficulties those come across related with image encryption methods. The speedy growth of computer depended systems allows numerous files, such as digital-images are to convey easily over the internet [3]. Encryption of data is extensively used in various applications to ensure security in many ways. However, most of the available encryption methods are used for encrypting text-data. Due to huge size of data and cost of processing time, some methods that are good for text-data may not be suitable in case of hypermedia data [5]-[7].

There are so many image encryption methods available and those had been used by different researchers. Those techniques would be used to protect confidential image-data's from illegal access. Various encryption techniques have been used to protect text-data. But those might not be very appropriate for hypermedia data. However, there is the necessity of block-based conversion methodology that will be a mixture of image alteration and a well-known algorithm called Blowfish is presented. Here the original image is separated into blocks, which are regrouped into a converted image with a well-defined alteration method and then the converted image is encrypted by Blowfish method. The results prove that the relationships between images are significantly reduced by using the proposed method. In [3] is also existing image security over internet through encryption/decryption. In this they used offered encryption procedures for text-data. Due to huge size of data and time limits, the system is compatible for text-data. But it may not be well suited for multimedia data. The value of an assumed pixel might be wisely forecast the standards of its neighborhood pixel. In this way an image encryption procedure which is following rearrangement method would be a mixture of an image rearrangement method and a very popular encryption method called AES is presented.

It is obvious that the entropy of an encoded image feasibly will be produced followed by a well-organized encryption method. Another thing has been surveyed which is associated with two pixels and it produces the resultant pixel-image in a reduced form. With the help of entropy and associated values the capability of any suggested process is accelerated. Moreover it is suggested that attainable alteration process has very difficult to follow. Another cause of poor effectiveness is the number of round used in the procedure. It is already known that rounds of any procedure is directly united with the time frame that means execution time of any algorithm is in a straight line and will be contingent to total circles executed over the speculated time.

3. PROPOSED WORK

In order to proliferation the security level of the encrypted images, block-based conversion architecture is proposed in our work. Different researchers have been used different types of their ideas for the sack of gradation and make their work unique one. So block-based idea is not the new one but our proposal is to get better result with the simpler way of conversion and as well as by following an established algorithm.

3.1 Outline of Imagery Encryption

Here we have tried to represent the method we followed in step by step. Our proposal encryption technique for Imagery Images is Encapsulated with Block-Based Transformation Algorithm(IEBTA) which has been applied in the subsequent phases of application to achieve the desired result. This is a figurative description or presentation as follows in Figure (i).

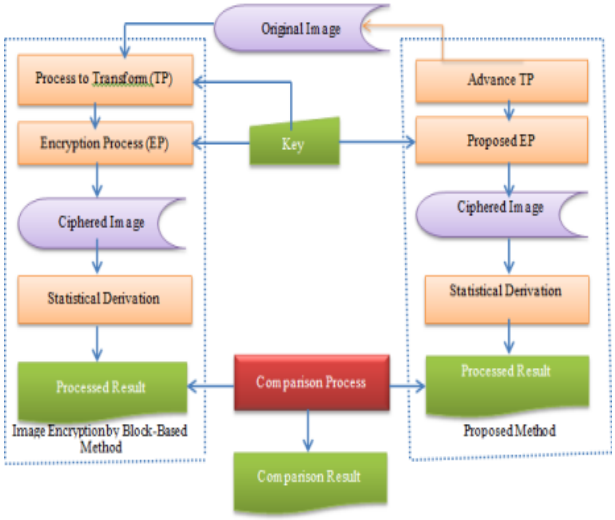

Fig-(i). An overview diagram of the Advance IEBTA

3.2 Projected Method of Architecture

Here we have selected constraint to be calculated and various images are selected. Those images are passed simultaneously over the existing and proposed methods to achieve the comparative results sets. The architecture is shown here with the help of figure (ii) in a very simpler form.

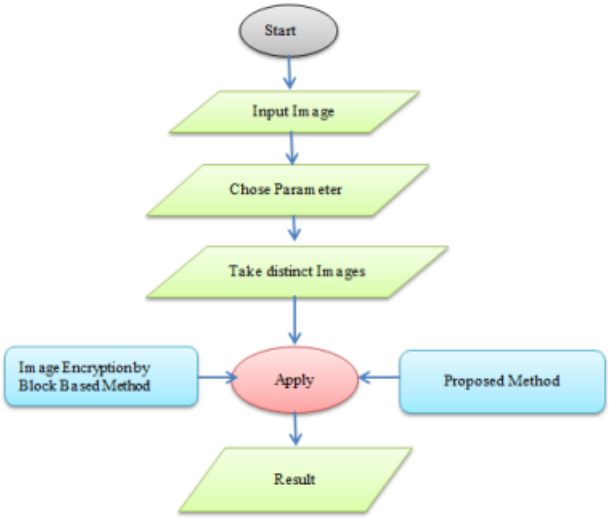

Fig. (ii) Proposed System Architecture

3.3 Create Transformation Block

The Steps of the existing transformation table with some modification are formulated in the form of executable notation is shown as follows.

1. Input image
2. Split it into pixel blocks
3. Compute Horizontal and Vertical Pixel Block
4. Compute Number of Pixel Blocks = Horizontal Pixel Block * Vertical Pixel Block
5. If Count=(Pixel Blocks / 2 != 0)
6. Then set Count = Count + Extra Pixel Block
7. Divide Count into two equal Sub- Block (Sub-Block1 and Sub-Block2).
8. Select variable I =0 and R=0 (R□ Random Variable)
9. While I < Sub-Block1
10. RN = Random Number of (0, Sub-Block1-1)
11. Set New Block
12. RN □ PBi (Selection of Pixel Block (PB)from Sub-Block1 Serially)
13. I = I + 1
14. End of While
15. Equally for Sub-Block2. I =0 and RN=0
16. While I < Sub-Block2
17. RN = Random Number of (0, Sub-Block2-1)
    R □ PBi Choose PB from Sub-Block2 Serially)
18. I = I + 1
19. End of While
20. Lastly we achieve PB location in Sub-Block1 and Sub-Block2.

After formation of the conversion frame work we have applied the proposed encryption algorithm in our experimental result.

The proposed encryption algorithm has been divided into three phases. The phases are compiled with the help of simulation to achieved the desired result and so that we can reuse our previous result to the next step of simulation. So it makes a cyclic order to gain the accurate resultant sets. Resultant of the conversion process is again passed as an input in the subsequent phases to achieve the refined and rectified accurate result. Firstly; phase one and then phase two and finally phase three.

3.4 Proposed Algorithm: Third Phase

1. Select Cipher Image from first phase.
2. Select Cipher Image from second phase.
3. Now combining both images we get final cipher image (FCI).

3.5 Characteristic of Proposed Algorithm

Straightforwardness: Our proposed algorithm is very simple and straightforward. Each partner will use same encryption algorithm. The method is so secret that there is no need to develop and use other method for security.

Safety: The length of the key and as well as block taken herewith is standard sufficient for maintaining security and privacy.

Proficiency: The simplicity of our proposed method shows its level of efficiency. We have used symmetric key so that we can produce stronger ciphers and we can get proficient result.

Robustness: With the improvements in knowhow it is of vital importance that encryption system is robust sufficient to endure the progresses in technology. The comparison study and the achieved resultants with the help of test image set and the required processing time compared to other researchers proves the robustness of our proposed algorithm.

Time-Efficacy: We have applied very simple method so as to save the processing time. The processing time measured herewith in different ways by comparing with the other similar technique followed by different researchers so that we can get accurate and good result compared to others proposed one. Since time is a vital one in this regard so we have given the prime importance on the required time of execution. The time efficiency of proposed encryption technique is measured in second to encrypt and decrypt information.

Flexibility: We have tried to establish it in a very flexible way by using simple method of encryption and decryption algorithm because we are using the images as our inputs. So if the process of accepting an input becomes time consuming it will create a lot of complexity and the flexibility will be reduced automatically. The use of keys and its lengths are set to be different with respect to its usability.

4. RESULTS COMPARISON

We have used the method and tried to implement by using sophisticated algorithm and formula. The evaluation system of the whole process is also robust since we have used the algorithms in a simplier way and we have applied them in a formulated simulation mechanism so that our result sets can be reused in the subsequent phases of application. We applied the methods and the related algorithm by using laptop Pentium® Core i7 @3.00Ghz and 32-bit Operating System. We have achieved the performance matrix based on the comparison results. We focus on two factors entropy and correlation value one is numeric value and second is percentage ratio as shown in table 1and table 2. Here it is calculated in respect to execution time as shown in table 3. Finally, the results of the calculation scheme are entropy correlation and execution time, and measured in numeric form.

4.1 Result Comparison

To calculate results we have select 32 byte key length which is mention below

Key:

Welcometoourcollegewelcometoourcollge

And this key has applied on various selected images which are also shown below:

Table 1 based on BBTM, PCT and PM

Images (Size in Kb)	IE by BBTM	IE with PCT tracked by Encryption Method	Proposed Method(PM)
E:\simi\IMG-JU\1.jpeg	0.4225	0.7789	0.0766
E:\simi\IMG-JU\3.jpeg	0.5244	0.8151	0.0821
E:\simi\IMG-JU\5.jpeg	0.3335	0.8235	0.0832
E:\simi\IMG-JU\9.jpeg	0.0216	0.3509	0.2107
E:\simi\IMG-JU\11.jpeg	0.2855	0.5671	0.1103
E:\simi\IMG-JU\17.jpeg	0.0215	0.4109	0.1021

IE (Image Encryption)

BBTM (Block Based Transformation Method)

PCT(Permutation Combination Technique)

4.2 Graphical Representation

From the above data as given above table it is clear that our proposed method is more sophisticated in respect of the other simulation techniques. Now we have been able to draw the following Fig-1based on the Table-1 that proves the superiority and robustness of our proposed method (PM).

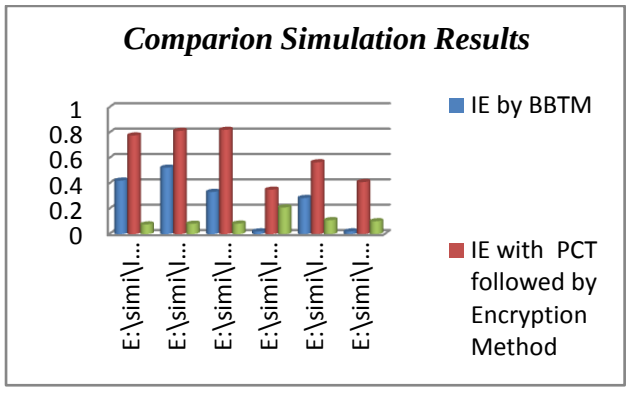

Fig1. Simulation Chart of Proposed Method

A. Original Image Entropy

Table 2. Comparison table of OIE of EM with PM

Images (Size in Kb)	IE by BBTM	IE with PCT tracked by Encryption Method	Proposed Method (PM)
E:\simi\IMG-JU\1.jpeg	423689.6	389452.3	27491071
E:\simi\IMG-JU\3.jpeg	57273.43	926318.51	39217921
E:\simi\IMG-JU\5.jpeg	234333.1	932731.31	8735723
E:\simi\IMG-JU\9.jpeg	324016.7	421083.5	2739117
E:\simi\IMG-JU\11.jpeg	342601.31	737230.9	1654521
E:\simi\IMG-JU\17.jpeg	258019.5	535173.13	1531593

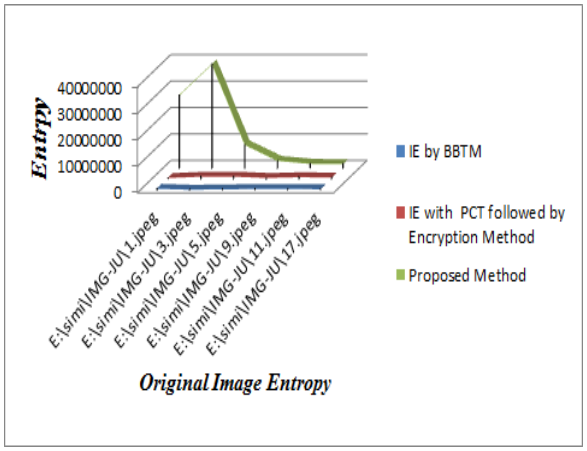

Fig 2:- Comparison graph of OIE, EM with PM

B.Encrypted Image Entropy of Original Image

Now we got the encrypted Image Entropy (EIE) and it is produced as follows in the following Fig 3 as shown below. It shows how much better result we have been able to achieve from our simulation based on the test data/image that we have taken for our experiment.

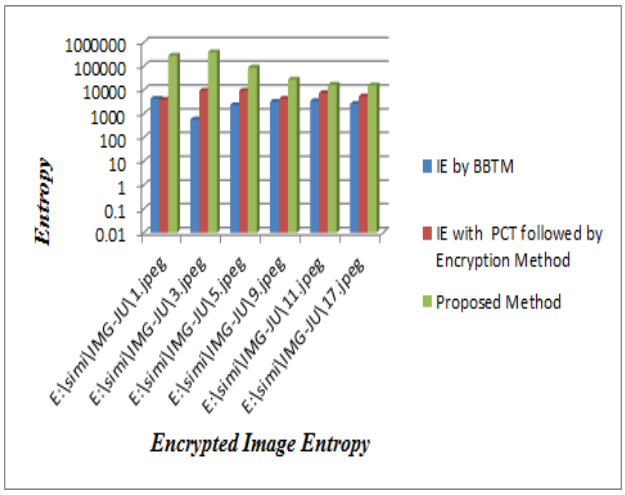

Fig 3: Comparison chart of EIE, EM with PM

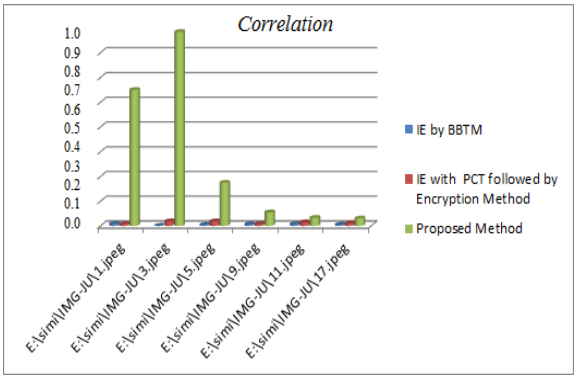

Fig-4: Comparison graph based on Correlation of EIE, EP with PM

The experiment results show the supremacy of our proposed method over the existing methods with respect to entropy, correlation and time required to execute the image. Since the execution time is remarkably very less than other existing method so power consumption and throughput will also be better than the EM. There is some typical results obtained by the simulation technique as shown in the table 1 and table 2 which shows the superiority of our proposed method than other existing one. However, it should not at all be very difficult to solve the problem if we can take the data size larger than the used one. Because it is obvious that as much as the size of data increased the level of security will also be increased subsequently. We know that the entropy algorithm depends on the size of images, key structure method and generated random number, too.

5. CONCLUSION

In our work we tried to implement and prosed modest and robust method for image security by the help of a permutation of block based image conversion and proposed encryption method. From the proposed method we have derived the correlation and we measure the performance matrix to produce a clear comparative study and establish our method's supremacy. From the correlation among the result set shows that whether we have achieved the better result or not. In the experimental results of our proposed method we have been able to prove the better performance than the other method used by the researchers before. From our experiment and achieved result we can firmly conclude that our proposed method is capable to produce best performance with the highest entropy and lowest correlation. In the future we will focus on how we could achieve the better result taking the multiple images at a time.

6. ACKNOWLEDGMENTS

We are thankful to the Prof (Dr) G Sanyal, Dean of Faculty, NIT, Durgapur, West Bengal, India. Without his help and proper guidance it was not possible to complete this versatile work covering different types of domain. It is also my pleasure to say that the Deanship of Research is encouraging a lot for our research work.

7. AUTHORS PROFILE

Mohammad Alamgir Hossain has received his M. Tech and MCA degree from University of North Bengal and M.Tech degree from Bengal Engineering and Science University, Shibpur (BESUS), West Bengal. He possesses an experience of more than 16 years in the field of teaching and research. He has published more than 13 papers in International Journals and Conferences. He is pursuing his PhD in Computer Science and Engineering from National Institute of Technology, Durgapur, India in the area of Image Processing. His areas of interest are Artificial Intelligence, Natural Language Processing and Image Processing. He has guided more than 25 PG and 50 UG projects and thesis. He is presently working as a Lecturer, Department of Computer Science, College of Computer Science & Information Systems Jazan University, Jazan P.O. Box -114, Kingdom of Saudi Arabia.

Dr Alwi M. Bamhdi Studied MSc Information Technology (Software Systems) at Heriot-Watt University, and PhD in Computer Sciences at **Heriot-Watt University** London. Presently he is working as an Assistant Professor,

Department of Computer Science, College of Computer Science & Information Systems Jazan University, Jazan P.O. Box -114, Kingdom of Saudi Arabia. His Research interest is in the area of Mobile Computing, Communication Systems, Information Security and Computer Vision.

Goutam Sanyal received B.E and M.Tech degree from National Institute of Technology (NIT), Durgapur, and PhD (Engg.) from Jadavpur University, Kolkata, India, in the area of Robot Manipulator path Planning. He possesses an experience of more than 28 years in the field of teaching and research. He has published more than 140 papers in International and National Journals / Conferences. Five (05) scholars has been supervised under his guidance and awarded PhD degree. Presently Six PhD's scholars are working in the field of Information Security, Computer Network, Computer Vision, Natural language Processing. He has guided more than 20 PG and 100 UG theses. Also he has examined the PhD thesis of other Universities. He has written book in Computer Graphics and Multimedia and Book chapters in Discrete Wavelet Transform in Biomedical Applications. He has served in Various International Conferences Program / Technical Committee Member and reviewer of Journals & Conferences. He has visited abroad in different Universities for research collaboration. He is teaching Computer Graphics, Computer Vision, Image processing, VLSI, Computer Architecture to UG and PG students. He has visited abroad for research collaboration in different Universities. Currently he is working as Professor in the Department of Computer Science & Engineering, National Institute of Technology, Durgapur and also holding the post of Dean (Faculty welfare) of the Institute. He was earlier served as Dean (Students Welfare) and Dean (AA and Resource Generation). He is a regular Member of IEEE and Fellow of IEI. Recently his biography has been selected for inclusion in Marquis Who's Who in the World 2015.

8. REFERENCES

[1] Wafa Ben Jaballah, Mauro Conti, Mohamed Mosbah, Claudio E. Palazzi, "A secure alert messaging system for safe driving", Computer Communications 46 (Elsevier 2014)

[2] Weiwei Jia, Haojin Zhu, Xiaolei Dong, and Chengxin Xiao, "Human-Factor-Aware Privacy-Preserving Aggregation in Smart Grid", IEEE SYSTEMS JOURNAL, VOL. 8, NO. 2, JUNE 2014.

[3] Sean M. Randall, Anna M. Ferrante, James H. Boyd, Jacqueline K. Bauer, James B. Semmens, "Privacy-preserving record linkage on large real world datasets", Journal of Biomedical Informatics 50 (Elsevier 2014) pp-205–212.

[4] Abraham Cherfi, Michel Leeman, Florent Meurville, Antoine Rauzy, "Modeling automotive safety mechanisms: A Markovian approach", Reliability Engineering and System Safety 130 (Elsevier -2014) pp-42–49.

[5] Jun Yang, Bin Wang, Xiaochun Yang, Hongyi Zhang and Guang Xiang, "A secure K auto morphism privacy preserving approach with high data utility in social networks", SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 2014; 7:1399–1411 Published online 30 September 2013, DOI: 10.1002/sec.840.

[6] Weiwei Jia, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, and Chengxin Xiao, "Human-Factor-Aware Privacy-Preserving Aggregation in Smart Grid", IEEE SYSTEMS JOURNAL, VOL. 8, NO. 2, JUNE 2014.

[7] Issa Khalil, Abdallah Khreishah, Muhammad Azeem, "Consolidated Identity Management System for secure mobile cloud computing", Computer Networks 65 (Elsevier -2014) 99–110.

[8] Zhiwei Wang, Guozi Sun, DanweiChen, "A new definition of homomorphic signature for identity management in mobile cloud computing", Journal of Computer and System Sciences 80 (Elsevier -2014) pp-546–553.

[9] Ackerman, Mark S., Lorrie Cranor, and Joseph Reagle. 1999. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. Proceedings of the ACM Conference in Electronic Commerce : 1-8.

[10] Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior. Proceedings of the ACM Conference on Electronic Commerce: 38-46.

[11] Bernard, H. Russell. 2000. Social Research Methods: Qualitative and Quantitative Approaches. Newbury Park, CA: Sage.

[12] Rivest, Ron, A. Shamir, and L. Adelman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21 (2) : 120-126.

[13] Cranor, Lorrie, and Joseph Reagle. 1998. The Platform for Privacy Preferences. Communications of the ACM, 42 (2) : 48-55.

[14] Chaum, David. 1985. Security Without Identification: Transaction Systems To Make Big Brother Obsolete. Communications of the ACM, 28 : 1030-1044.

[15] Dierks, T., and C. Allen. 1999. The Transport Layer Security Protocol. Internet RFC 2246. Diffie, W., and M. Hellman. 1976. New Directions in Cryptography. IEEE Transactions on Information Theory, 22 (6) : 644-654.

[16] A SENGUPTA, C MAZUMDAR and MSBARIK, "e-Commerce security – A life cycle approach", Sadhana Vol.30, Parts-2&3, April/June 2005, pp. 119–140. © Printed in India.

[17] S.W. Smith, " WebALPS: A Survey of E-Commerce Privacy and Security Applications"- Hanover, New Hampshire 03755 USA, sws@cs.dartmouth.edu.

[18] Hamid Jebur, Hamed Gheysari, Parastoo Roghanian," E-Commerce Reality and Controversial Issue ", IJFPSS, Vol 2, No.4, pp. 74-79, Dec , 2012.

[19] MR. HARDIK NARIYA, PROF. CHIRAG GOHEL," E-COMMERCE SYSTEM: A REVIEW ON SECURITY CHALLENGES AND INDIAN PERSPECTIVE", JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN COMPUTER ENGINEERING, ISSN: 0975 – 6760| NOV 12 TO OCT 13 | VOLUME – 02, ISSUE – 02 Page 451-57.

[20] Suresh Chari, Parviz Kermani, Sean Smith and Leandros Tassiulas, "Security Issues in M-Commerce: A Usage Based Taxonomy", Liu and Y. Ye (Eds.): E-Commerce Agents, LNAI 2033, pp. 264-282, 2001. Springer-Verlag, Berlin Heidelberg 2001.

[21] Himani Grewal, Shivani," A Study of Ethical and Social Issues in E-Commerce"- International Journal of Advanced Research in Computer Science and Software Engineering- Volume 2, Issue 7, July 2012 ,ISSN: 2277 128X.

[22] Raghav Gautam, Sukhwinder Singh, "Network Security Issues in e-Commerce", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014.

[23] M. Jos. Capkovic," INFORMATION SECURITY & PRIVACY NEWS"- Publication of the Information Security Committee ABA Section of Science & Technology Law, AUT UMN 2013 VOL UME 4 I SSUE 4.

[24] N. Doukas, A. Drigas, N. G. Bardis and N. V. Karadimas," Accessible Secure Information Society Applications via the Use of Optimised Cryptographic Calculations", Journal of Applied Mathematics & Bioinformatics, vol.3, no.4, 2013, 181-206.

[25] Peter Stavroulakis," Communications and information security: Case study military systems",Journal of Applied Mathematics & Bioinformatics, vol.3, no.4, 2013, 207-211 ISSN: 1792-6602 (print), 1792-6939 (online),Scienpress Ltd, 2013.

[26] Richard M. Escalante," Socio-Legal Issues Affecting the Use of Digital Signatures for Secure E-commerce Transactions: A Caribbean Perspective", 20th Sep, JIBC-2014.

[27] Shazia Yasin, Khalid Haseeb, Rashid Jalal Qureshi, "Cryptography Based E-Commerce Security: A Review", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012 ISSN (Online): 1694-0814.

[28] Ashish Wadhaval, Rugved Mehta, Ashlesha Gawade, "Mobile Commerce and Related Mobile Security Issues "International Journal of Engineering Trends and Technology (IJETT) – Vol 4 Issue 4- April 2013.

[29] Pradnya B. Rane , B.B.Meshram , "Transaction Security for E-commerce Application" International Journal of Electronics and Computer Science Engineering, SSN 2277-1956/V1N3-1720-1726.

[30] Sen-Tarng Lai," A SECURITY REQUIREMENT QUALITY MEASUREMENT MODEL FOR REDUCING ECOMMERCE SECURITY RISK",

International Journal of Software Engineering & Applications (IJSEA), Vol.5, No.1, January 2014.

[31] K. Sakthidasan and B. V. Santhosh Krishna," A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011.

[32] Godwin J. Udo, "Privacy and security concerns as major barriers for e-commerce: a survey study", Information Management & Computer Security 9/4 [2001] 165-174, MCB University Press [ISSN 0968-5227].

[33] Alexandra Michota," Digital security concerns and threats facing women entrepreneurs", Michota Journal of Innovation and Entrepreneurship 2013, 2:7,Springer Open Journal.

[34] Neetu Kawatra, Vijay Kumar, "Analysis of E-Commerce Security Protocols SSL and SET", Recent Trends in Mathematics and Computing (RTMC) 2011, International Journal of Computer Applications® (IJCA).

[35] Dimitrios Poulakis," On the Cryptographic Long Term Security", Journal of Applied Mathematics & Bioinformatics, vol.3, no.1, 2013, 1-15.

[36] George Marinakis, "Minimum key length for cryptographic security", Journal of Applied Mathematics & Bioinformatics, vol.3, no.1, 2013, 181-191.

[37] Melita Charitou ,"THE ROLE OF LONG RETURNS IN SECURITY VALUATION: INTERNATIONAL EMPIRICAL EVIDENCE", The International Journal of Business and Finance Research, Volume 5, Number 3, 2011.