SECURE PARTIAL IMAGE ENCRYPTION SCHEME USING SCAN BASED ALGORITHM

Parameshachari B D[1], K. M. Sunjiv Soyjaudah[2] and Sumithra Devi K A[3]
[1]Department of Electronics & Communication Engineering, JSS Academy of Technical Education, Vacoas, Mauritius. (Research Scholar, Jain University, Bangalore, India).
[2]Department of Electrical & Electronic Engg., University of Mauritius, Reduit, Mauritius.
[3]Department of Master of Computer Applications, R V College of Engineering, Bangalore, Karnataka, India.

ABSTRACT

Today data security is very important and high priority topic. With rapid growth in communication and computer technologies, there is a huge data transaction interment, teleconferencing and military applications. For all these applications we need a security. Encryption is the primary solution to provide security to the data, which is travelling on a communication link between any pair of nodes, but Partial encryption is a technique to save computational power, overhead, speed, time and to provide quick security by only encrypting a selected portion of a bit stream. The focus of this paper is on selecting the important part of the image that can efficiently achieve by conceptually selecting the important part of the image. This paper proposes a new approach for partial image encryption using SCAN algorithm. The main idea behind the present work is to select the part of the image is performed by SCAN based permutation of pixels and substitution rule which together form an iterated product cipher. The issue in traditional cryptosystem in many different areas such as wireless networking, mobile phone services and applications in homeland security is energy consumption for encryption of the large volume visual data. So we are dealing with partial encryption.

KEYWORDS: *Data confidentiality, decryption, partial encryption, scan patterns, symmetric key*

I. INTRODUCTION

In recent digital world, the security of multimedia data like images/videos becomes more and more important since the communications of multimedia products over network occur more and more frequently. In addition, special and reliable security in storage and transmission of digital images/videos is needed in many digital applications, such as broadcasting, confidential video conferencing and medical imaging systems, etc. Various encryption algorithms have been proposed in recent years as possible solutions for the protection of the video data. Normal data, such as program code or text are comparatively less complex to encode or decode. Large volume of the image data makes the encryption difficult as we need the encryption to be done in real-time. The main approach for image encryption is to treat image data as text and encrypt it using standard encryption algorithms like AES (Advanced Encryption Standard) or DES (Data Encryption Standard) [2]. The basic problem with these encryption algorithms is that they have high encryption time making them unsuitable for real-time applications. As a wireless devices is equipped with battery as their power supply, they have limited computational capabilities and one of them main concern is energy saving But it cannot be achieved if the encryption and decryption is applied on the complete message [1]. In the digital domain, distribution networks need to address two fundamental problems for real time data of large volume: (i) Reduction of huge communication requirements for multimedia data, and (ii) Protection of copyrighted multimedia data [3]. This paper mainly concentrates on the first problem in order to

reduce the communication requirements for multimedia data. As a result an efficient partial encryption algorithm is the efficient solution to save power for wireless devices and at the same time to sufficiently secure the data. In this article we mainly concentrate on two issues –

i) How to conceptually select the message as it is partial approach to conserve time of data transmission and overhead of the network.

ii) To apply an encryption algorithm to encrypt the important part of the original image.

Through applying this method our proposed scheme enhances the features of partial encryption and avoid the relevance between different messages [4]. Thus we present the solution for the issue of applying traditional symmetric key algorithm for data protection in dynamic environment, such as MANET, WANET etc.

The rest of this paper is organized in the following ways: In Section 2, we discuss the features of symmetric key algorithms. Section 3 we present a Partial encryption theory along with the issues in data selection of message partially, In Section 4 existing selection schemes are shown, In Section 5 we gives solution approach by our proposed SCAN method for Partial encryption scheme. The flow chart of proposed algorithm is given in Section 6 and Section 7includes experimental results and discussions. Finally, in Section 8 conclusions and future works are given.

II. SYMMETRIC KEY ALGORITHMS

Symmetric key algorithms have served as a traditional approach to data protection for a long time, as they can protect a message in a convenient way. The sender and receiver of the message only need a shared key to encrypt and decrypt the message. Here, symmetric keys are often referred to as secret keys [5]. According to the functions of symmetric keys, they are also sometimes used as group keys or session keys. A secure communication channel is required to be established between the communicating parties in advance to securely distribute their symmetric key. Though there are many favorable strengths about symmetric keys, one of their crucial imperfections is the short length of the key, which leads to concerns about security. Thus, we think a symmetric key algorithm should be used along with other security mechanisms to enhance its security.

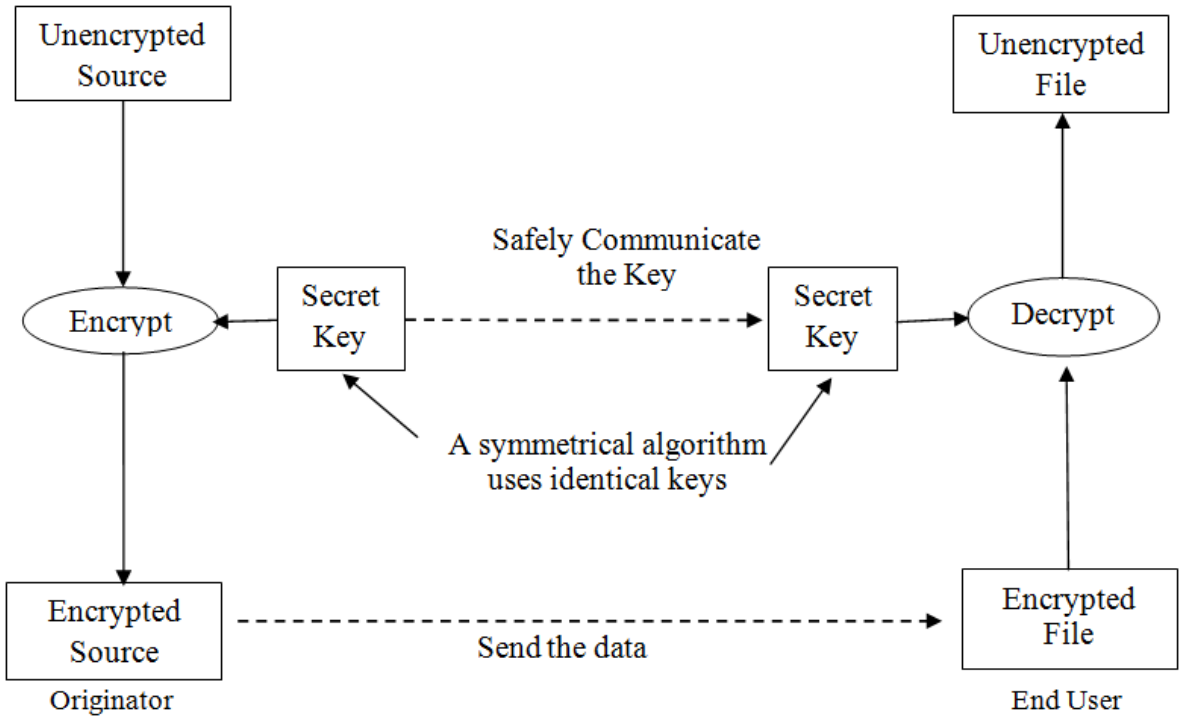


Figure 1: Scheme Diagram of Symmetric Key Algorithm

III. PARTIAL ENCRYPTION THEORY

The purpose of Partial encryption is to encrypt an important portion of messages with less overhead consumption but at the same time data should be encrypted in order to secure data sufficiently. In this concept no need to encrypt entire data, only the segments are encrypted. The data should be segmented in a standard pattern which involves sufficient uncertainty. The more uncertainty is involved, more effective is the cryptosystem. Multimedia communications often requires real-time data transmission. So tremendous audio and video data need to be transferred securely. Given that all multimedia data are encrypted, this will consume a great deal of overhead, so that multimedia data is difficult to transmit timely and the quality of communication cannot be guaranteed. As such, in a Wireless network, each device uses battery as its power supply and thereby has constrained computational ability, so a sensor cannot spend too much computational cost on data encryption and decryption [6]. Under such circumstances, the design of a partial encryption algorithm with less processing time but with relatively high security level is extremely significant.

A major recent trend is to minimize the computational requirements for secure of an image by "*partial encryption*" where only parts of the data are encrypted. Partial encryption is the algorithm that encrypts only a part of the image while leaving other parts unchanged. Image is first partitioned into two parts, then, one part is encrypted by traditional or novel ciphers under the control of the key, and the other part is not changed, and finally, the two parts are combined together. The decryption process is symmetric to the encryption process.

3.1. Issues in data selection from original message

To apply selective encryption firstly we have to select the part of the messages and then encrypt the selected segment by using any appropriate encryption algorithm. For segmenting the message there are various existing methods like a fixed sequence. The fixed sequence of even bit position and odd bit positions are selected [1] [7]. In this concept of even-odd bit position selection firstly even bit positions are selected and in second round odd bit positions are selected sequentially and vice-versa. Another method is to apply chaos permutation by which bit stream is compressed and then replaced in order to shrink the image size [8].In the same order another method is to apply S-Box rotation technique on the data given in array form and then encode it. In these cases decryption may be easier if the sequence is predicted. So because of the fixed sequencing of bit positions data transmission is not enough secure as already complete messages is not encrypted. Figure 2, shows the message segmentation for selecting the important part of a message.

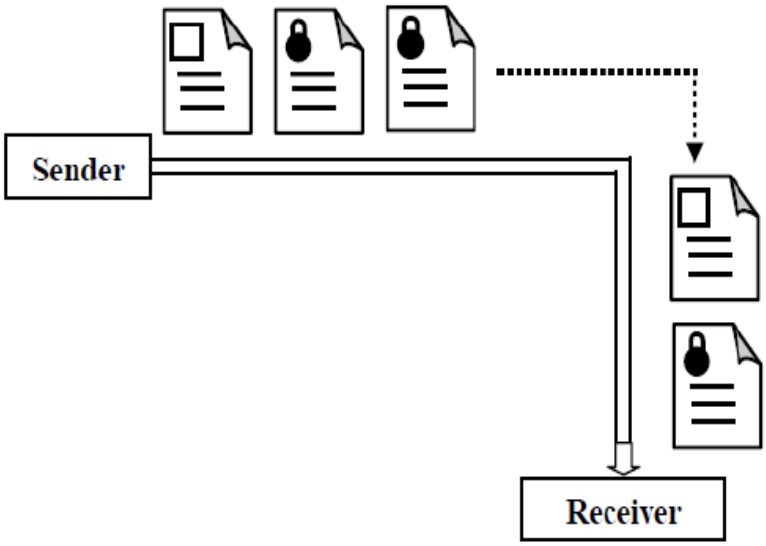


Figure 2: Selection and Encryption of Data

IV. THE EXISTING SELECTION SCHEME

Partial encryption algorithms are mainly applied in the field of secure multimedia communications, as the volume of multimedia data is huge to transmit and the cost will be overwhelmed if each packet is encrypted or decrypted. Yonglin *et al.* [1] presented a novel solution for selective encryption to achieve data protection effectively while with reasonably costs. The probabilistic and stochastic techniques in our proposed solution guarantee the security for data communications between the messages sender and receiver. The factor of encryption probability involves the uncertainty to data encryption. R.Gupta *et.al* [9] gives a shuffle scheme helps to remove the redundancy normally found in digital images and produce a flat histogram not normally possible with traditional data encryption schemes. Aikawa *et al.* [10] describe a rotation-based encryption algorithm called MX. This proposed algorithm is similar to DES and takes advantage of two sub keys without lookup tables, in order to simplify the key schedule step. For each rotation, the transformation of MX only makes changes in the parameters of rotation. Lian *et al.* [9] present a video encryption scheme for Advanced Video Coding (AVC) codec. In their algorithm, only those sensitive data are chosen to be encrypted, such as residue data and motion vector. Specifically, the intra-prediction mode is encrypted according to context-based adaptive variable length coding. M. Ahmad *et al*. [12] presented an algorithm is based on the concept of shuffling the pixels positions and changing the gray values of the image pixels in three different ways to achieve good shuffling. In [13] we enhance the Chung-Chang's scheme and then a more efficient and secure encryption scheme is obtained. Hence, the proposed scheme improves on Chung-Chang's scheme on the part of encryption time, compression ratio and security. Furthermore, image size affects the speed of encryption; that is, the higher the compression, the better the efficiency. In [14] we surveyed that the existing works on the partial encryption techniques and also analyze partial encryption schemes with respect to various parameters like tunability, visual degradation, compression friendliness, format compliance, encryption ratio, speed, and cryptographic security.

V. PROPOSED METHOD

In this section, we will present a concept of Partial encryption algorithm step by step, which not only reflects the idea of selection of part from original data but also uses symmetric key cryptography. Our propose algorithm aims to involve sufficient uncertainty into the encryption process, while providing satisfactory security of the image. The goal of partial encryption of a bit stream is to make the entire stream somehow useless for anyone that who cannot decrypt the ciphered subset. The main goal of proposed method is to reduce the amount of data to encrypt while achieving a required level of security. Partial encryption is a technique to save computational complexity or enable interesting new system functionality by only encrypting a portion of a compressed bitstream while still achieving adequate security. In order to select the original image conceptually it uses the encrypting Key including basic pattern and scan paths.

SCAN method converts a 2D image into a 1D list, and employs a SCAN language to describe the converted result. In this language, there are several SCAN letters. Each SCAN letter represents one kind of scan order. Different kinds of combinations of SCAN letters may generate different kinds of secret images. After determining the combination of SCAN letters, the scheme then generates a SCAN string. This string defines the scan order of the original image. Next, this method scans the original image in the determined order and, moreover, encrypts the SCAN string by using commercial cryptosystems. Since the illegal users cannot obtain the correct SCAN string, the original image is therefore secure. There is no image compression in this method. Therefore, the size of the image is very large, and thus it is inefficient to encrypt or decrypt the image directly.

SCAN is the method for image encryption together with information hiding. This algorithm is based on permutations of the image pixels and replacement of the pixel values. The encryption power of the SCAN method is based on the very large number of private keys. The "SCAN" language includes an alphabet consisting of primitive scanning techniques, as letters, and a simple grammar to manipulate and combine the alphabet symbols by generating new scanning patterns (words) from simple ones. The development of SCAN provides an efficient approach to the problem of modeling and generating all accessing algorithmic patterns of an image of nxn. The SCAN is a family of formal languages such as Simple SCAN, Extended SCAN, and Generalized SCAN, each of which can represent and generate

a specific set of scanning paths. Each SCAN language is defined by a grammar and each language has a set of basic scan patterns, a set of transformation of scan patterns and a set of rules to recursively compose simple scan patterns to obtain complex scan patterns. Note that this set of basic scan patterns can be extended or reduced as needed by a specific application. There are 6 transformations of scan patterns. They are identity, horizontal reflection, and vertical reflection, rotation by 90, 180, and 270°, and compositions of these transformations. The rules for building complex scan patterns form simple scan patterns are specified by the production rules of the grammar of each specific language. The encryption specific SCAN language uses four basic scan patterns. They are continuous raster C, continuous diagonal D, continuous orthogonal O, and spiral S. The SCAN alphabet consists of SCAN items and is by the set ∑:

$$\sum = \{r, c, d, o, a, s, m, e, y, w, z, b, x\} \quad \ldots\ldots (1)$$

The symbols of ∑ are called SCAN *letters*, and correspond to scan orders (algorithms) which are illustrated in Figure 3 (for an image of size). For a complete specification of the underlying scan algorithms.

The basic partition patterns are shown in Figure 4. Since most images require different scanning indifferent sub regions, the encryption specific SCAN language allows an image region to be recursively partitioned into four sub regions, and each sub region to be scanned independently. When an image region is partitioned, the order in which the four sub regions are scanned is specified by a partition pattern. The partition patterns are letter B, letter Z, and letter X, each of which has eight transformations [15, 16].

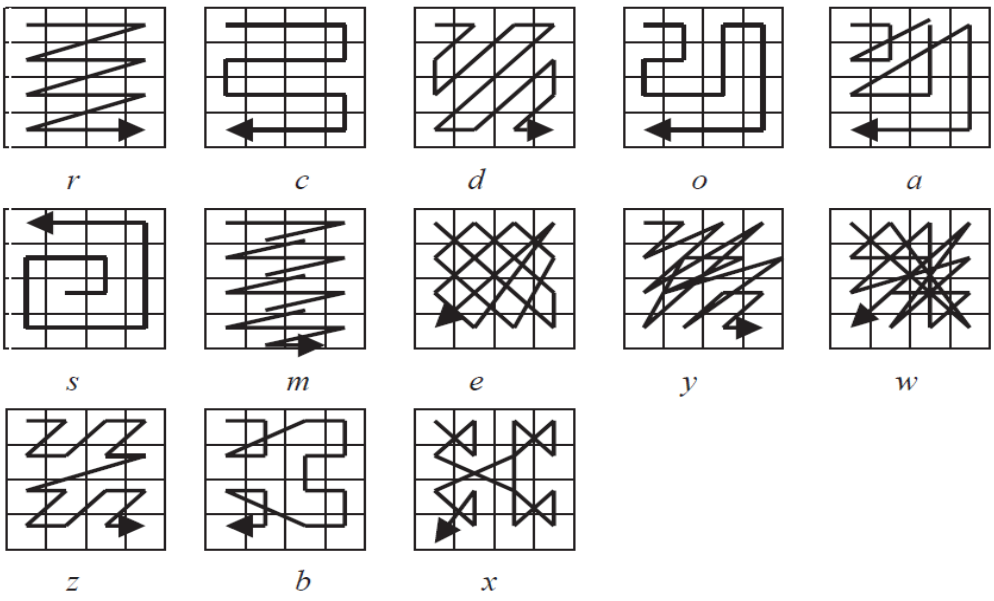


Figure 3. Scan Patterns

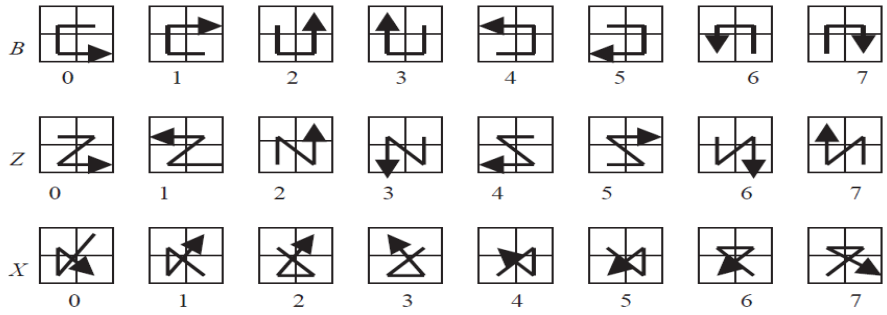


Figure 4. Partition Patterns

VI. FLOWCHART

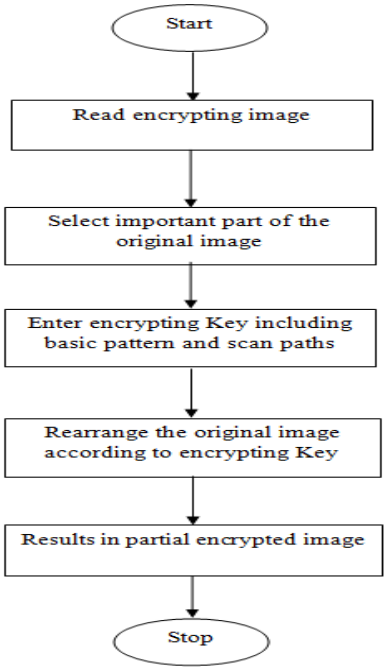


Figure 5: Flow chart for proposed method

VII. EXPERIMENTAL RESULTS AND DISCUSSIONS

The proposed result of our partial encryption technique will be like images given below, here is the original image which is to be transmitted over the network so partial encryption will be done on the important part of the image and then important part will be encrypted. Once encryption is done, the encrypted data is sent along with remaining original part of the image.

Figure 6. Original Coffeemaker image and corresponding partial C SCAN pattern

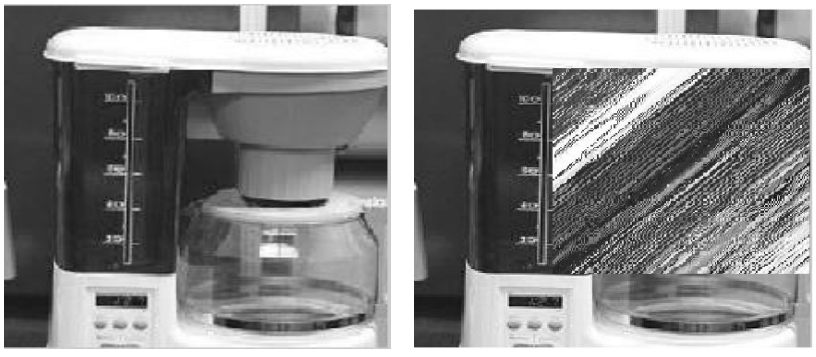


Figure 7. Original Coffeemaker image and corresponding partial D SCAN pattern

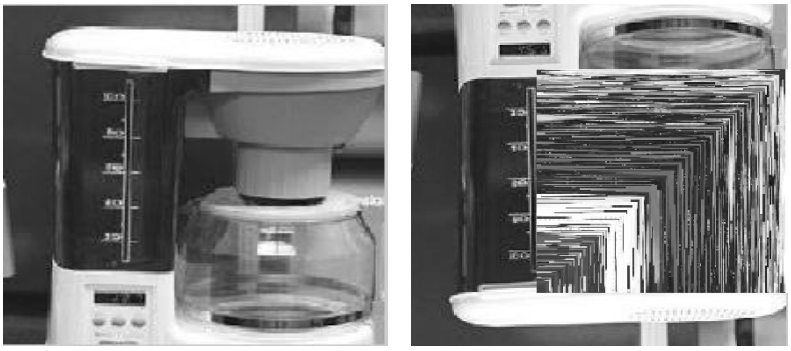


Figure 8. Original Coffeemaker image and corresponding partial O SCAN pattern

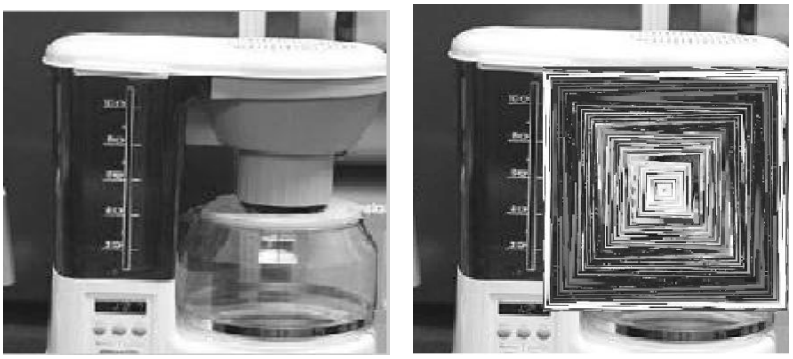
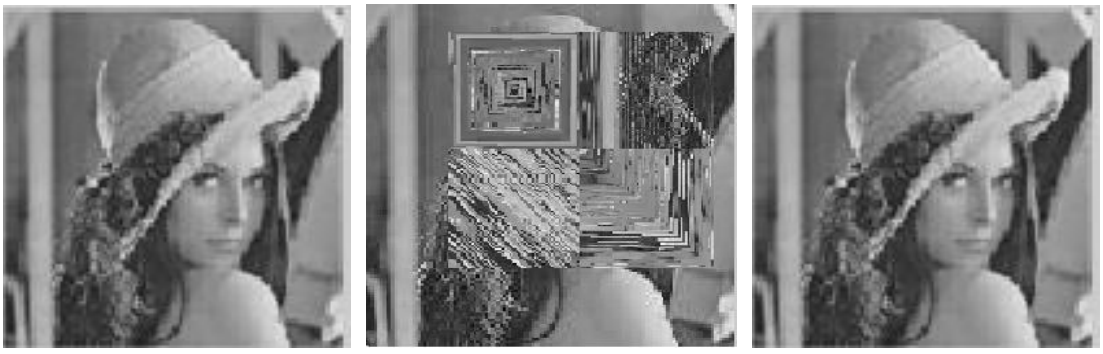
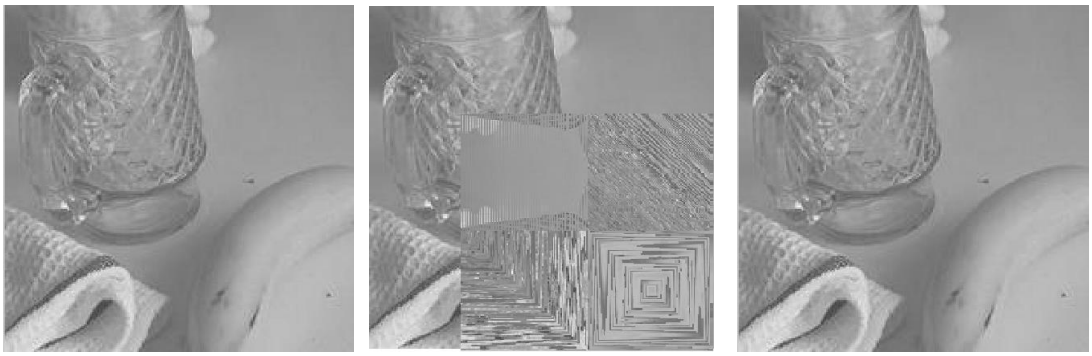


Figure 9. Original Coffeemaker image and corresponding partial S SCAN pattern



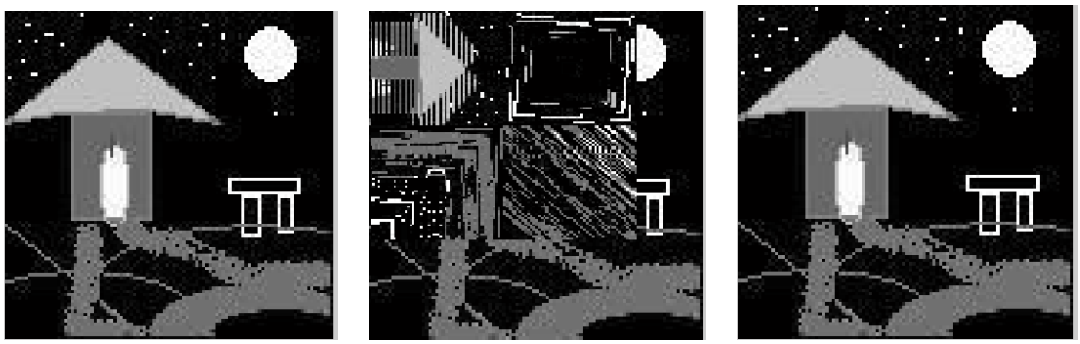
(a) Original image (b) Encrypted image (c) Decrypted image

Figure 10. Partially encrypted Image: *encryption key **'Z1(s1c2d3o1)'***



(a) Original image (b) Encrypted image (c) Decrypted image

Figure 11. Partially encrypted Image: *encryption key **'B0 (c1d3o1s4)'***



(a) Original image (b) Encrypted image (c) Decrypted image

Figure 12. Partially encrypted Image: *encryption key* ***'B3(c5s3o7d6)'***

VIII. CONCLUSIONS

Partial encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile network. In this paper, we have presented a novel solution for Partial encryption to achieve data protection, confidentiality and integrity effectively while with reasonably cost specially when the data is of large volumes like multimedia message and to be transmitted on wireless environment.The proposed algorithm has the best performance; the lowest correlation and the highest entropy. We make two fold contributions to achieve data protection in less time to save computational energy. On one hand to select the part of the image is performed by SCAN based permutation of pixels and substitution rule which together form an iterated product cipher, which provides uncertain segmentation of multimedia data by reducing the encrypted data volumes. On the other hand we take the advantage of symmetric key algorithm to reduce the complexity of the operation and protect the data in a reasonable computational cost. These properties make the scheme suitable for real-time applications.

8.1 Future Scope of Work

Extensions of this work could be the investigation of new scanning patterns applied efficiently to image processing. Such texture synthesis using SCAN words matrix elements rearrangement for parallel storage and manipulation. In future work will hardware implement using DSP chip, and accelerate the process speed.

REFERENCES

[1]. Yonglin Ren, A. Boukerche and L. Mokdad, J.,(2011) "Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks", *In proceedings of IEEE* Wireless communications and networking conference,pp. 1038-1043.

[2]. A.Massoudi, F. Lefebvre, and C. De Vleeschouwer, Eds.J.,(2008) "Secure and Low Cost Selective Encryption for JPEG2000", In *Proceedings of 10th IEEE International Symposium on Multimedia*, pp. 31–38.

[3]. M. Podesser, H. Schmidt, and A. Uhl,J, (2002) "Selective bitplane encryption for secure transmission of image data in mobile environments", In Proceedings of *the 5th IEEE Nordic Signal Processing Symposium*.

[4]. F. Bao, and R. H. Deng,J., (2007), "Light-Weight Encryption Schemes for Multimedia Data and High-Speed Networks", In p*roceedings of IEEE Global Telecommunications Conference*, pp. 271–350.

[5]. Y.Ren, A. Boukerche, R.W.N.Pazzi, (2010),"Performance Analysis of a Hybrid Cryptosystem with Authentication for Wireless Ad- Hoc Networks", Global Telecommunications Conference, pp. 1-5.

[6]. M. Aikawa, K. Takaragi, Eds.,(1998), "A Lightweight Encryption Method Suitable for Copyright Protection", IEEE Transactions on Consumer Electronics, Vol. 44, pp. 902–910.

[7]. F. Bao, R. H. Deng, (2007),"Light-Weight Encryption Schemes for Multimedia Data and High-Speed Networks", Proceedings of IEEE Global Telecommunications Conference, pp. 271–350.

[8]. L. Jun, L. Zou, C. Xie, Eds.,(2006),"A two-way selective encryption algorithm for MPEG video", Proceedings of International Workshop on Networking, Architecture, and Storages.

[9]. R.Gupta, A. Aggarwal, and Saibal K.,J., (2012), "Design and Analysis of New Shuffle Encryption Schemes for Multimedia",In proceedings of Defense Science Journal, Vol. 62, No. 3, May 2012, pp. 159-166.

[10]. M. Aikawa, and K. Takaragi, *Eds,J., (199),* "A Lightweight Encryption Method Suitable for Copyright Protection",In proceedings of *IEEE Transactions on Consumer Electronics*, Vol. 44, pp. 902–910.

[11]. S. Lian, Z. Liu, and Z. Ren, *Eds.*,J,(2006), "Secure advanced video coding based on selective encryption algorithms", In proceedings of *IEEE Transactions on Consumer Electronics*, Vol. 52, pp. 621–629.

[12]. C. Shi, and B. Bhargava,J.(1998), "A fast MPEG video encryption algorithm", In Proceedings of *the 6th ACM International Multimedia Conference*, Bristol, UK.

[13]. Parameshachari B D and Dr. K M Soyjaudah, (2012), "A Study of Binary Image encryption using Partial Image Encryption Technique" International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.3, pp-955-959.

[14]. Parameshachari B D, Panduranga H T and Dr. K M S Soyjaudah,(2012), "A Overview on Partial Image Encryption Approaches", International Journal of Engineering Research and Development (IJERD), Volume 1, Issue 2, pp. 49-54.

[15]. C. Kachris et. el., " A reconfigurable logic based processor for the SCAN image and video encryption algorithm", IJPP, vol. 31, no. 6, Dec 2003, pp. 489-506.

[16]. Parameshachari B D, Chaitanyakumar M V, (2011), "Image Security using SCAN Based Encryption Method", *42nd IETE Mid-term symposium on Telecom Paradigms - Indian Scenario*, pp 115-118.

AUTHORS

Parameshachari B D working as a Senior Lecturer in the Department of Electronics and Communication Engineering at JSS Academy of Technical Education, Mauritius. He is working at JSSATE, Mauritius since from July 2010 and worked as a Lecturer at Kalpatharu Institute of Technology, Tiptur for Seven years. Parameshachari obtained his B.E in Electronics and Communication Engineering from Kalpatharu Institute of Technology, Tiptur and M. Tech in Digital communication Engineering from B M S college of Engineering, Bangalore. He is pursuing his Ph.D in Electronics and Communication Engineering at Jain University, Bangalore, Karnataka, India. Parameshachari area of interest and research include image processing and cryptography. He has published several Research papers in international Journals/conferences. He is a Member of ISTE, IETE, IACSIT, IAEST, IAENG and AIRCC.

K M Sunjiv Soyjaudah received his B. Sc (Hons) degree in Physics from Queen Mary College, University of London in 1982, his M.Sc. Degree in Digital Electronics from King's College, University of London in 1991, and his Ph. D. degree in Digital Communications from University of Mauritius in 1998. He is presently Professor of Communications Engineering in the Department of Electrical and Electronic Engineering of the University of Mauritius. His current interest includes source and channel coding modulation, image processing, cryptography, voice and video through IP, as well as mobile communication. Dr. K M S Soyjaudah is a member of the IEEE, Director in the Multicarrier (Mauritius), Technical expert in the Energy Efficiency Management Office, Mauritius. Registered Ph.D Guide in University of Mauritius, Reduit, Mauritius and Jain University, Bangalore, Karnatka, India.

Dr. Sumithra Devi K A, Professor and Director, in Master of Computer Applications at R V College of Engineering, Bangalore, India. She received B.E. from Malnad College of Engineering, Hassan. She received M.E and Ph D from UVCE, Bangalore and Avinashilingam University for Women, Coimbatore, INDIA respectively. Reviewer for many International Journals / Conferences like WEPAN, WICT, EDAS, IACSIT, ISCAS, JEMS, Published 14 journals and 65 International/ National Conferences. Professional Member in many IEEE, IETE, CSI, ISTE. Member in BoS and BoE, for Visvesvaraiah Technological University, Belgaum, Karnataka. Registered PhD Guide in Visvesvaraiah Technological University, Belgaum; Jain University, Bangalore; Prist University, Sathyabhama University, Tamilnadu. Authored a chapter "CAD algorithm for VLSI design" in the book "VLSI Design ", published by In-Tech Publications, ISBN 979-953-307-512-8, 2011, and authored book on Operating System, published by Shroff Publisher India.