A Fast and Secure Selective Encryption Scheme using Grid Division Method

Priyanka Agrawal
Department Of Computer Science and Engineering,RCET,Bhilai

Manisha Rajpoot
Department Of Computer Science and Engineering,RCET,Bhilai

ABSTRACT

“Encryption is the primary solution to provide security to the data, which is travelling on a communication link between any pair of nodes, but Selective 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. Securing the visual and multimedia data like images requires specific design consideration for use in different applications. The focus of this paper is on selecting the important part of the image that can efficiently achieve by conceptually selecting the part of the image which is further used in its normal mode of operation for encryption. Once encryption is done, the encrypted data is sent along with remaining original part of the message, ensuring its secured transmission and distribution over public networks.. This paper proposes a new approach for image encryption using matrix or grid conversion of image. The main idea behind the present work is to select the part of the image by the arranging the bit stream in grid form and choosing the diagonal of the grid. 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 a partial encryption algorithm of images.”

Keywords :

Data confidentiality and protection, symmetric key, selective encryption and grid method.

1. 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[1]. 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)[3]. 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 & decryption is applied on the complete message[2]. In the digital domain, distribution networks need to address two fundamental problems for real time data of large volume: (1) Reduction of huge communication requirements for multimedia data, and (2) Protection of copyrighted multimedia data[4]. This paper mainly concentrates on the first problem in order to reduce the communication requirements for multimedia data. As a result an efficient selective 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 –

1. How to conceptually select the message as it is selective approach to conserve time of data transmission and overhead of the network.

2. To apply an encryption algorithm to encrypt the selected part of the original message.

Through applying this method our proposed scheme enhances the features of selective encryption and avoid the relevance between different messages[5]. 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-II, we discuss the features of symmetric key algorithm. Section-III we present a Selective encryption scheme along with the issues in selection of message partially, In Section-IV existing algorithms are shown, In Section-V we gives solution approach by our proposed gird method for selective encryption scheme. The flow chart of proposed algorithm is given in Section-V and Section-VI includes expected result. Conclusion is drawn in Section-VII and At last in Section-VIII References is given.

2. SYMMETRIC KEY ALGORITHM

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. According to the functions of symmetric keys, they are also sometimes used as group keys or session key[4].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 [12]. Thus, we think a symmetric key algorithm should be used along with other security mechanisms to enhance its security.

3. SELECTIVE ENCRYPTION THEORY

The purpose of selective encryption is just to encrypt a certain portion of messages with less overhead consumption but at the same time data should be encrypted in order to secure data sufficiently. The data should be segmented in a standard pattern which involves sufficient uncertainty. Here, uncertainty can enhance the security of data transmission, as all messages are assumed to own equal importance. Thus, uncertainty becomes one of the paramount factors when designing a selective-based cryptosystem. The more uncertainty is involved, more effective is the cryptosystem. Multimedia communications, often requires real-time data transmission [11].So tremendous image, 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 [13]. Under such circumstances, the design of a selective encryption algorithm with less processing time but with relatively high security level is extremely significant.

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] [2]. 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 [6].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.

4. THE EXISTING SELECTION SCHEME

*S*elective 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.* [2] 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*[6] 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.* [8] 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*.[14] 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.

5. OUR PROPOSED APPROACH

In this section, we will present a concept of selective 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 message. In order to select the message conceptually it uses the grid conversion of bits and then selecting the diagonal of the grid then encrypt it. This assures that every wireless node has enough computational energy to finish this operation.

5.1 Grid Division and Diagonal Selection

Here we propose a selective approach which uses the advantages of grid method aiming to obtain sufficient complexity in the selection of some parts of a multimedia message after conversion it into the bitstream. During the process of sending messages, the sender will convert the visual data into binary form.this binary bit stream is then arranged in grid structure,then transpose of each sub grid (which is obtained by dividing the main grid) will be done. If the bits on any sub grid is same then compliment the bits. These are selected bit to be encrypted. In next step encrypted cipher will be merged with the remaining original bits in the grid and transmitted over the transmission channels to the receiver. Moreover this proposed selective encryption by grid method is comprised of following steps –

- The sender 'S' will first convert the image into binary form i.e. bit stream B_s.
- Bit steam B_s is now arranged in the form of n×n grid, leave remaining bits as original.
- Subdivide the main grid again, the sub grid(S_g) size should be of m×m where m=2, (While n>2 do n=n/2).
- Transpose each sub grid. If any S_g having same bits then compliments the bit and put in the same position in the respective sub grid.
- Select the right diagonal of each transposed sub grid and compliment it.
- Encrypt the operated grid (O_g) by symmetric encryption and convert O_g into bit stream again.
- Transmit the encrypted bits stream encr(B_s) along with the remaining original bit(O_{bs}).

6. FLOW CHART

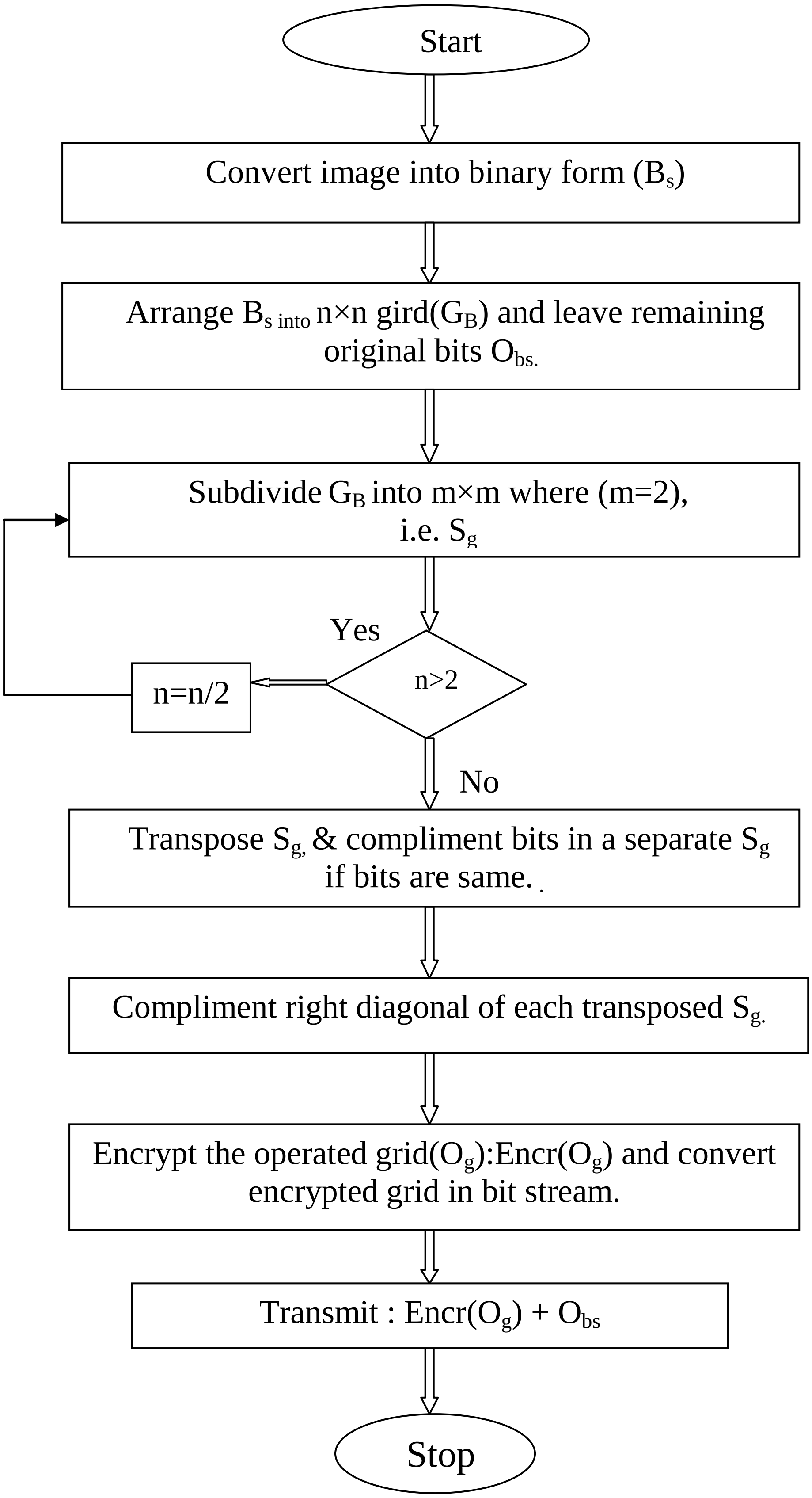
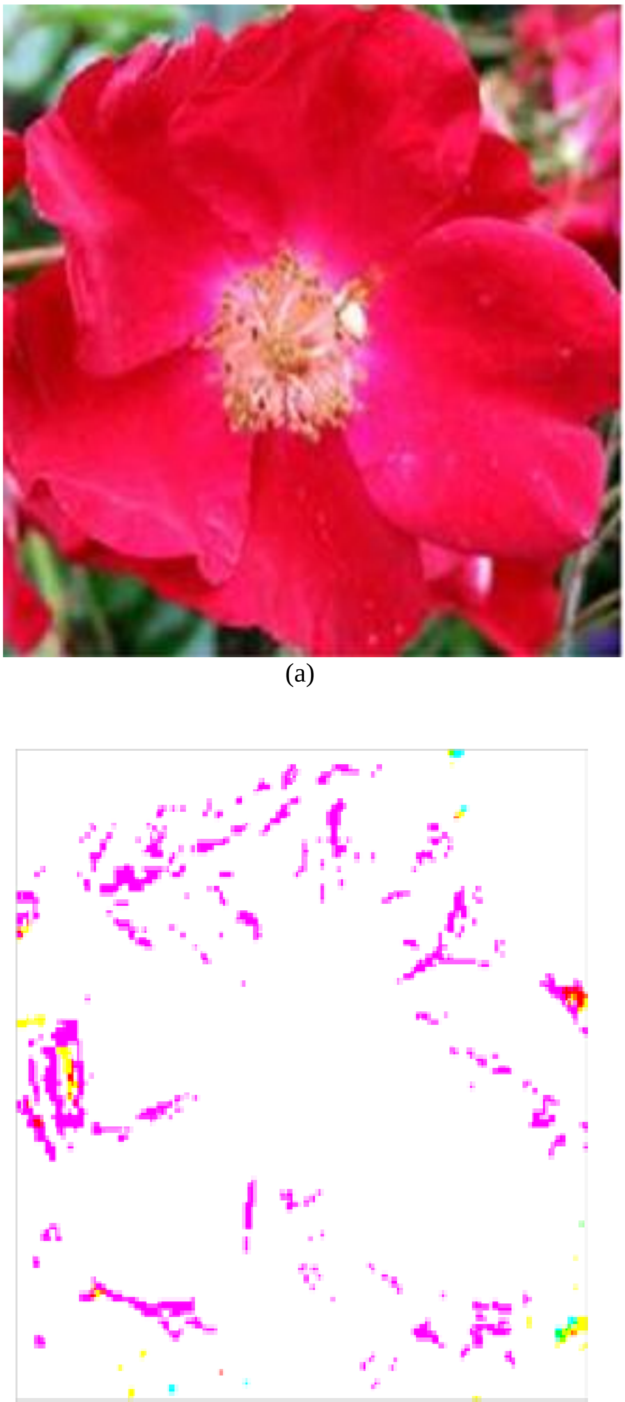

Start
Convert image into binary form (B_s)
Arrange $B_{s\ into}$ n×n gird(G_B) and leave remaining original bits $O_{bs.}$
Subdivide G_B into m×m where (m=2), i.e. S_g
Yes
n>2
n=n/2
No
Transpose $S_{g,}$ & compliment bits in a separate S_g if bits are same. .
Compliment right diagonal of each transposed $S_{g.}$
Encrypt the operated grid(O_g):Encr(O_g) and convert encrypted grid in bit stream.
Transmit : Encr(O_g) + O_{bs}
Stop

Figure 2: Flow Chart for proposed Algorithm

EXPECTED RESULT

The proposed result of our selective encryption algorithm will be like images given below in figure 3, here is the original image which is to be transmitted over the network so selective encryption will be done on the selected part of the image and then selected part will be encrypted.



(a)

(b)

Figure 3. Selectively Encrypted Image, (a) is the original image, (b) is the encrypted image by grid conversion

7. CONCLUSION

Selective 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 selective 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. We make two fold contribution to achieve data protection in less time to save computational energy. On one hand the application of grid division and diagonal selection, 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. This scheme’s security against some special attacks and its hardware-implementation will be further studied in future work. For securing voluminous visual data with requirements of real-time communication and use in resource constrained applications such schemes would be in demand in the future as well.

8. REFERENCES

[1] P.Agrawal & M.Rajpoot, 2012. Partial Encryption Algorithm for Secure transmission of Multimedia messages. In proceedings of *Int. J.Comp. Sci.*, **3**(1), . 467-70.

[2] 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.

[3] 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.

[4] 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*.

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

[6] 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.

[7] L. Jun, L. Zou, and C. Xie, *Eds.*,J.2006. A two-way selective encryption algorithm for MPEG video, *Proceedings of International Workshop onNetworking, Architecture, and Storages*.

[8] M. Aikawa, and K. Takaragi, *Eds,J.1998.* A Lightweight Encryption Method Suitable for Copyright Protection,In proceedings of *IEEE Transactions on Consumer Electronics*, Vol. 44, pp. 902–910.

[9] 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.

[10] A.J. Prakash, and V. R. Uthariaraj,J.2009. Multicrypt: A Provably Secure Encryption Scheme for Multicast Communication,In *Proceedings of 1st*

[11] *Int'l Conference on Networks and Communications*, pp. 246–253.

[12] X. Yi, C. Tan, C. Siew, and S. Rahman,J.2001. Fast encryption for multimedia,In proceedings of *IEEE Transactions on Consumer Electronics*, Vol. 47, No. 1, page(s): 101 – 107.

[13] L. Tang,J.1996. Methods for encrypting and decrypting MPEG video data efficiently, In Proceedings of *the Fourth ACM International Multimedia Conference (ACM Multimedia'96)*, pp. 219-230.

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

[15] M.Ahmad and M. Shamsher Alam, J.2009.A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping, In proceedings of International Journal on Computer Science and Engineering, Vol.2(1), 2009, 46-50.

[16] C. Wu, and C. Jay Kuo,2001.Efficient multimedia encryption via entropy codec design,In proceedings of *SPIE International Symposium on Electronic Imaging*.

[17] S.Agaian,A.Jassim,J.2009.*MobileMultimedia/Image Processing, Security, and Applications*, Proceedings of SPIE, 0277-786X, v. 7351