CRYPTOSAIC: CRYPTOGRAPHY FOR MOSAICING

Muhammad Barja Sanjaya[1], Ari Moesriami Barmawi[2], -[3]

[1]Magister Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Dewasa ini banyak data berupa gambar yang memerlukan pengamanan seperti mosaik, misalnya untuk data militer dan kesehatan. Salah satu kekurangan mosaik adalah bahwa mosaik sulit untuk dikembalikan menjadi gambar aslinya. Untuk mengatasi hal ini diusulkan untuk menggunakan algoritma enkripsi sebagai pengganti mosaik. Algoritma enkripsi yang pernah diusulkan terdahulu ditujukan untuk mengenkripsi bagian yang di "crop" (bagian yang dianggap penting untuk diamankan) dalam bentuk persegi. Dengan demikian terjadi ketidakefisienan enkripsi pada bagian yang tidak terlalu penting, karena bentuk crop tidak mengikut bentuk bagian yang akan dienkripsi. Pada tesis ini diusulkan metode yang menggunakan proses "crop" sesuai dengan bentuk bagian yang perlu diamankan dan memperkuat keamanannya. Proses "crop" dilakukan dengan memanfaatkan edge detection dan untuk memperkuat keamanannya digunakan Soft Encruption dan AES. Adapun cara mengamankan gambar dilakukan dengan mengubah nilai piksel berdimensi dua ke bentuk deretan satu dimensi untuk kemudian deretan tersebut dienkripsi menggunakan algoritma enkripsi seperti pada teks [1][4][5]. Dengan metode ini diperoleh waktu komputasi yang relatif rendah dengan kekuatan yang relatif tinggi dengan kebutuhan memori dan waktu proses enkripsi yang relatif rendah.

Kata Kunci : Mosaic, selective bitplane, experiment

Abstract

Recently, there are many data especialy image data which is necessary to be secured such as military and medical data. One method which is frequently used is mosaic. One of the disadvantages from mosaicing is that it is difficult to be reversed into the original image. For overcoming the problem then it is proposed to use encryption algorithm instead of mosaicing. Encryption algorithm which has been proposed to encrypt the part of image which have been cropped (a part which is considered confidental) in rectangle shape. However, the inefficiency occured while encrypting the unimportant part of the cropped image. In this study, a method which is using edge detection for segmenting the cropping area (such that the cropping area is similar to the image shape) and maintaining the security level. The cropping process is conducted by applying Sobel edge detection and Soft Encryption as well as AES for strengthening the security level. As for securing the image, it is done by altering the two dimensional pixel value into set of one dimensional pixel value, and further the pixel value set is encrypted using encryption algorithm such as in text [1][4][5]. By implementing this proposed method, lower computation while maintaining the strength is achieved.

Keywords : Mosaic, selective bitplane, experiment

CHAPTER I
INTRODUCTION

This chapter presents the background of the study; including the rationale, theoretical framework, conceptual framework, the problem, hypothesis, assumption, scope and limitation and the importance of the study.

1.1. Rationale

Nowadays the need for information security becomes so inevitable due to the rapid applications development on computer network and internet technology. There are specific informations need to be secured since they are valuable resources [3]. Security consists of some policies, rules, protocols and standards that help the organization to meet its objectives. Organizations need security to protect their assets from illegal and unauthorized access, also people in their personal life need to keep their private documents, family albums, and also confidential films. Physical security and access control are the solution but they are not enough to secure the data. Electronic data are still easy to access, steal or copy via networks. Therefore security system and methods are needed to keep them safe and secure [4].

Digital images are attractive data types with widespread range of use. There are many researchers who are interesting to protect the content against previewing, manipulation and copying. In many applications such as military image databases, confidential and top secret video conferencing, medical imaging system, cable tv, and online personal photograph album, security is significant and essential. The wide application of images in industrial process turns it into a resource and asset, so it is important to protect the confidential/top secret image data from unauthorized access. Most of today encryption algorithms are based on textual data, but images are different from text [4]. An idea for image encryption is to consider a 2D image as a 1D data stream and encrypt this stream with any textual based cryptosystem [3][4] and VEA. This approach is usually suitable for text, and sometimes for a small bit rate audio, image and video files that are being sent over a fast dedicated channel [7].

One method for securing it is by using mosaicing. However, it is hard to recover the image perfectly. For overcoming this problem cryptosystem may be used. However, since the size of image is greater than text, then for encrypting image, more time is needed compared to text.

1.2. Theoretical Framework

This research proposes new approaches to modify the method for obtaining secure mosaic with more secure and robust. The improvement of this study combined with soft encryption (also known as selective bitplane) can also reduce the time computation regardless of the boundary of input in the previous research [8].

The idea of the proposed method for mosaicing is applying cryptography instead of blurring method and minimizing the area of the mosaic using image processing. For reducing the time and memory needed by the process, the combination of selective bitplane [1] based cryptosystem and AES [3] is introduced. To achieve stronger security, the mosaic has also message on it embedded using method Modified Dynamic Cell Spreading [13]

For investigating the visibility of the proposed method proposed method compared to blurred images, investigating by people is conducted as well as for investigating the invisibility of the embeded image.

1.3. Conceptual Framework/Paradigm

This study introduces new method proposed to achieve the optimal objectives. There are several processes to be conducted, they are the image preprocessing, encrypting with soft encryption, embedding the message into mosaic. There are some parameters analysed related to the previous studies for securing the information. Those parameters and criterions are

a. Data source,
b. Image processing; including: cropping image, edge detection, selecting area the most needed.
c. Cryptography; including: generating plaintext, key generating, encrypting selective bitplane.
d. Steganography; including: random number generating, bit stream generating, and embedding the message.
e. Performance of cryptography; including: memory usage and time computation.
f. Performance of robustness of the steganography; including the values result of MSE, PSNR for the theoretically objective criterion, and the invisibility between the mosaic and stego-mosaic for the subjective one.

1.4. The Problem

The problem identified is that recently the mosaic until this time can be carried out by blurring the signal on the image such as lowering the probability to recover the original one. In order to overcome the problem, recently cryptography is introduced as a method for mosaicing. One method for mosaicing image using cryptography is conducted in [12]. But, this method still has drawback because it needs large computation.

1.5. Objectives and Hypothesis

Due to those problems, then this objective of this research is for decreasing the computation while maintaining the strength of mosaicing process.Thus, the mosaic can be read only by the authorized party.

The hypothesis for securing a mosaic with minimum computation is implemented using cryptosaic. Cryptosaic is a method for generating a mosaic by encrypting the object which will be procesessed by applying selective bitplane encryption which is frequently called as Soft Encryption (SE) [1]. This method is used to reduce the encryption computation because by applying SE it is not necessary to encrypt the whole pixels. Morover, for decreasing computation, it is conducted process edge detection based on cropping method.

For strengthening the security level in implementing SE, AES [3] is used instead of RC4 in [12]. AES is stronger than RC4 and this has been discussed in [14].

Furthermore, the key seed for decrypting ciphertext will be inserted into the mosaic.

1.6. Assumption

The assumption proposed in this study is that no problem occurs during the process (such as interrupted running time).

1.7. Scope and delimitation

This thesis discusses the implementation of the cryptosaic algorithm and the scope this study are:

a. The format image to encrypt is in JPG and to embed is in Bitmap.
b. There are three categories of images as input to process.
c. The time performance of processing image will not be considered.
d. The image size is 500x313 pixels.
e. The cropped image is in large (50..100) x (50..100) pixels, with addition 10 pixel.
f. The key length is 128 bit.

1.8. The importance of the study

This research can be used for securing confidential information (such as military and health infomation), since it proposes a method for securing data partially with less computation while maintaining the security strength.

CHAPTER V
CONCLUSIONS AND FUTURE WORK

This chapter concludes the overall scenario and each testing concerning to the terms in parameter explained in previous. Here, it also explains the future work which can be conducted as improvement.

5.1. Conclusion

Based on the analysis of the experimentation result, the proposed Cryptosaic method Cryptosaic can reduce the memory usage up to 55%. It also shows that encryption speed is up to 93% faster than the previous research [12].

This proposed method surprisingly presents that the invisibility between the mosaic and stego-mosaic image based on human perception is similar. Since the PSNR is relatively low, then it can be concluded that the randomness of the Cryptosaic result is relatively high. Thus, Cryptosaic is better than the previous method [12].

In the term of strength, the proposed method still holds the strength against the known-plaintext attack.

Based on the experimentation result, it can also be concluded that the best performance is achieved if the selected area covers the important data and its size is approximately the half of the cropped area size.

5.2. Future Work

The study of this proposed method indeed gives many improvements, but still has some limitation and also drawback. The drawback is failure in cropping the intended area selection. Therefore, a method for cropping area can be proposed as the future work. Furthermore a method for generating random numbers can be proposed for strengthening the security of Cryptosaic.

BIBLIOGRAPHY

[1] Podesser, Martina. Schmidt, Hans-Peter. dan Uhl, Andreas. *Selective bitplane encryption for secure transmission of image data in mobile environments*. School of Telematics & Network Engineering. Carinthia Tech Institute, 2002.

[2] T. Maples and G. Spanos. *Performance study of a selective encryption scheme for the security of networked real-time video*. In *Proceedings of the 4th International Conference on Computer Communications and Networks (ICCCN '95)* Las Vegas, NV, 1995.

[3] Shah, Jolly. and Saxena, Vikas. *Performance Study on Image Encryption Schemes*. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011. ISSN (Online): 1694-0814. Department of CS & IT, Jaypee Institute of Information Technology. Nodia, Uttar Pradesh 201307, India. 2011.

[4] Soleymani, Ali. Md Ali, Zulkarnain. and Nordin, Md Jan. *A Survey on Principal Aspects of Secure Image Transmission*. World Academy of Science, Engineering and Technology 66. 2012.

[5] Puech, W. and Rodrigues, J. M. *A New Crypto-Watermarking Method for Medical Images Safe Transfer*. In The 12th European Signal Processing Conference, pp. 1481-1484.

[6] A. M. Alattar, G. I. Al-Regib, and S. A. Al-Semari. *Improved selective encryption techniques for secure transmission of MPEG video bit streams*. In *Proceedings of the 1999 IEEE International Conference on Image Processing (ICIP'99)*. IEEE Signal Processing Society, 1999.

[7] C. J. Skrepth and A. Uhl. *Selective Encryption of Visual Data: Classification of application scenarios and comparison of techniques for lossless environments*. In *Advanced Communications and Multimedia Security, IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, CMS '02*, Portoroz, Slovenia, Sept. 2002. Kluver Academic Publishing. To appear.

[8] T.-L. Wu and S. F. Wu. *Selective encryption and watermarking of MPEG Video (extended abstract)*. In H. R. Arabnia, editor, *Proceedings of the International Conference on Image Science, System, and Technology, CISST '97*, Las Vegas, USA, Feb. 1997.

[9] Sethi, Nidhi. and Vijay, Sandip. *Comparative Image Encryption Method Analysis Using New Transformed – Mapped Technique*. Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013). Dehradun Institute of Technology. Dehradun-248001. 2013.

[10] H. Cheng and X. Li. *Partial Encryption of compressed images and videos*. *IEEETransactions on Signal Processing*, 48(8):2439-2451, 2000.

[11] Septian, Dean. 2011. *Modification of Steganography Methods Dynamic Cell Spreading (DCS) In Digital Image*. Bandung. IT Telkom.

[12] Dharmaadi, I Putu Arya. 2012. *Tugas Akhir*: *Partially Image Encryption with Combination Method of RC4 Stream Cipher and Chaotic Function*. Bandung. IT Telkom.

[13] J. Daemen and V. Rijmen. *The Design of Rijndael: AES – the advanced encryption standard*. Springer Verlag, 2002.

[14] Singhai, Nidhi. and Raina, J.P.S. *Comparative Analysis of AES and RC4 Algorithm for Better Utilization*. International Journal of Computer Trends and Technology. Department of Electronics & Communication, BBSB engineering college, Fatehgarh Sahib, Punjab, India. 2011.

[15] Forouzan, Behrouz A. *Cryptography and Network Security*. International Edition. New York. MacGraw-Hill Companies, Inc. 2008.

[16] Stinson, D. R. 1995. *Cryptography: Theory and Practice*. Florida: CRC Press, Inc.

[17] Menezes, A. and Van Oorschot, P. and Vanstone, S. 1997. *Handbook of Applied Cryptography*. Florida: CRC Press Inc.

[18] Schneier, B. 1996. *Applied Cryptography*. _____: John Wiley and Sons Inc.

[19] Matsumoto, Makoto. and Nishimura Takuji. *Mersenne Twister*: *A 623-Dimensionally Equidistributed Uniform Pseudorandom Number Generator*. ACM Transactions on Modeling and Computer Simulations: Special Issue on Uniform Random Number Generation. Keio University. 1988.

[20] Junod, Pascal. *Cryptography Secure Pseudorandom Bits Generation*:*The Blum-Blum-Shub Generator*. August 1999.

[21] Sidorenko, Andrey. and Schoenmakers, Berry. *Concrete Security of the Blum-Blum-Shub Pseudorandom Generator*. Cryptography and Coding: 10th IMA Interntional Conference. Springer-Verlag: Computer Science 3796. 2005. Eindhoven University of Technology. P.O. Box 513, 5600 MB Eindhoven. The Netherlands.