

PROPOSED AES FOR IMAGE STEGANOGRAPHY IN DIFFERENT MEDIAS

Yojna Goyal¹, Manmohan Sharma²

¹Department of computer science, Lovely Professional University, Phagwara, India

²Department of computer science, Lovely Professional University, Phagwara, India

Abstract

In this paper, the author presents an enhanced version of modified AES for image-audio steganography technique. The proposed technique improves the security level of encryption and steganography process. Digital image processing is a wide area for research. Images are widely used today. Processing on images means some editing, preprocessing, restoration, compression, steganography and encryption. Steganography is concealing secret information into cover information. Encryption is mainly used for encoding the content of an image into something that cannot be understandable by unauthorized persons. Authorized are those who have the legal access to the content. Nowadays everyone is after information so; it becomes the need today to secure the (confidential) information. The proposed AES technique is an enhancement of modified AES method, which focuses on improving the security of steganography images. Modified AES is described in four steps: first step is key expansion, second is sub bytes modification, third is new shift rows and at last mixing of columns is applied to the matrix. This technique will provide better security and good quality encryption and decryption. Results shows that this method takes less time with the high quality of encrypted image

Keywords – Steganography, Modified Advance Encryption Standard(MAES), Proposed Advance Encryption Standard(PAES), Image Steganography, Image Encryption.

1. INTRODUCTION

The need of transmission of data increases day by day due to the vast requirements over the world. Everything, every business depends upon data or information. So, the basic need is to securely transmit the digital information. An image can be described in terms of a two dimensional function with parameters x and y, here x and y are plane coordinates. Digital image processing means process digital images using digital computers. The main component of an image is a Pixel. Image consists of pixels and these elements (pixels) are processed in digital image processing.

The processes can be of 3 types in image processing a) low level processes b) mid level processes c) high level processes. Low level processes involve preliminary processes like noise reduction; contrast enhancement; sharpening images. Low level processing is distinguished by the fact that its input and output both are images. Mid-level processing engaged in segmentation of images tasks such as segmentation, depiction of objects those are appropriate for computer processing and classification of individual items. The input in mid level processing is images but its output is the features extracted from input images. At last higher-level processing engaged in making sense of a collected works of recognized elements (objects) like in image analysis.

Steganography, defined as the capacity of covering information or data in such way that avoid the exposure of covered data. It takes a huge collection of undisclosed communications procedures that wraps the message's

survival. The procedures are invisible inks, microdots, arrangement of characters and covert channels, digital signatures, and spread spectrum. Steganography is only used for security purpose of information that we want to send to another side safely. There are basic elementary classes of steganography

a) Subliminal communication: This type of communication hides that some information is transferred in a particular file. For passing the information from sender to receiver secretly hidden in one another type of information is wrapping as a single unit. The secret canal is a medium of transformation of information. There are number of ways to conceal a information: by adjusting least significant bit of pixel in a cover information.

b) Integrity and authentication: By using steganography technique we can say that our information is much more secure. Since nobody can alter any information till they can know the proper method of extracting the information. Integrity defines that our information is not altered by any other sources. Once you lock the data by sender key, it only provides the authentication to valid receiver to open and extract the original information from the file. In this paper, we present a technique which performs steganography with the help of encryption by using the image as following steps:

2. METHOD FOR IMAGE STEGANOGRAPHY

Image steganography permits the secret information to be concealed in a cover image. There are various techniques existing in the world by which we are able to hide the

information in the wrapper image. Information hidden in the image can only be regained by the authorized person who knows the proper method of extracting the information. Firstly, we will check that information entered in the image is image, audio, text. If the information is image then convert the RGB value of image into ASCII and consign into the vertical fusion of cover image. If the information is audio then convert the eight bits into pixel and replace into cover image RGB. If the information is text then translate the text into values and situate into the RGB channel of carrier image.

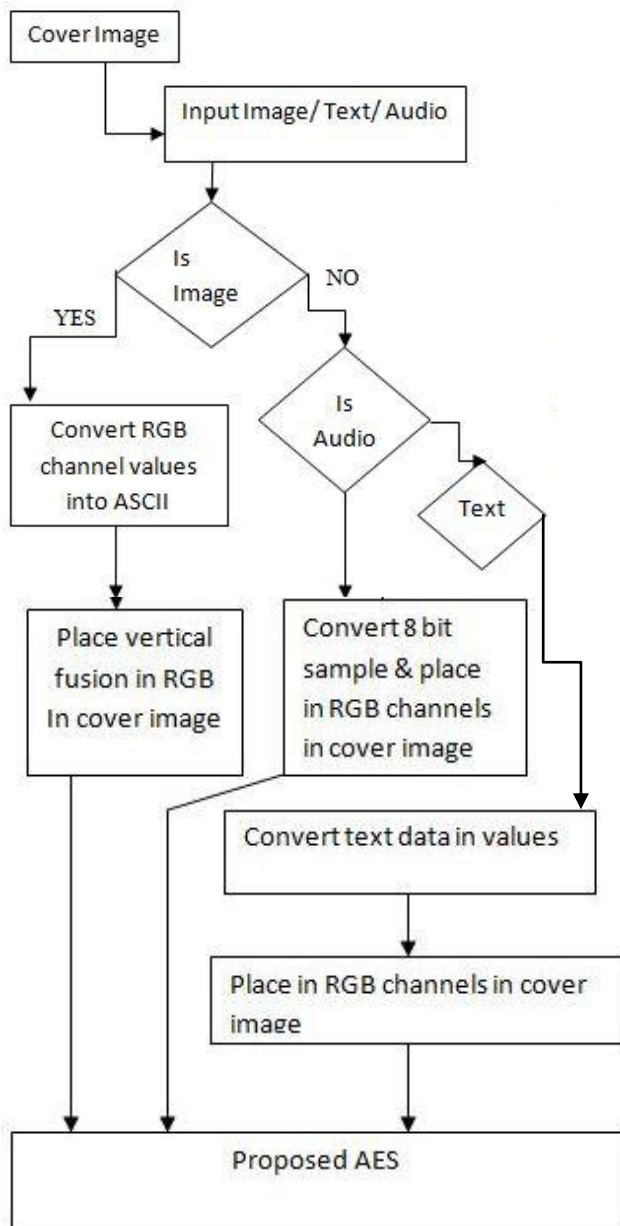


Fig 1 Information hiding

For hiding the information we use the encryption process as modified AES in following steps:

- Key Expansion: generation of a number of keys.
- Sub Bytes modification: values are altered using s boxes values.

- New Shift Row: rows are cyclically shifted according to first value existing in the matrix even or odd.
- Mix Column: mixing of columns takes place by vector method..

3. METHODOLOGY USING PROPOSED AES FOR IMAGE ENCRYPTION

3.1 Key Expansion

In this step, firstly we choose the image of size pxq , where p and q are the pixels of image. We encrypt as a password which is further used in Bit Rotate the 16 pixels by using the two round keys. Formation of Rcon values takes place which is not constant but formed by initial key and transpose of values will give better results. Using s-boxes and Inverse of s-box will develops the non linearity in expansion of the key.

Sub Bytes Modification: In the sub byte modification we will alternate the every single byte in the state with the help of s-box.

3.2 New Shift Row

The Shift Rows step is performed on the rows of the state. It cyclically Shifts the bytes of each row depending upon the first element of state.

If the value is even rotate first row first column to left. Second column second row to left no change in the method, but rotate third row third column to left will not be performed.

If odd rotate first row first column to left. Second row second column to will not be performed. Third row third column are shifted to the left. This means that when state table element has even and odd values one step will not be performed hence it saves the time.

3.3 Mixing Columns

In the Mix Columns step, we will define the reducible polynomial.

- Find the inner vector product with the sum of correct row vector.
- Multiply ($G F(2^8)$) as polynomial multiplication such as the polymultiple (inner vector, state of in matrices, column state)
- Finally, Bit XOR (temp state, poly state)

3. DECRYPTION PROCESS

In this section, the decryption process of algorithm is discussed. The decryption process is just opposite of the encryption procedure. One should follow the encryption steps in reverse order

4. BLOCK DIAGRAM OF REVERSE MECHANISM

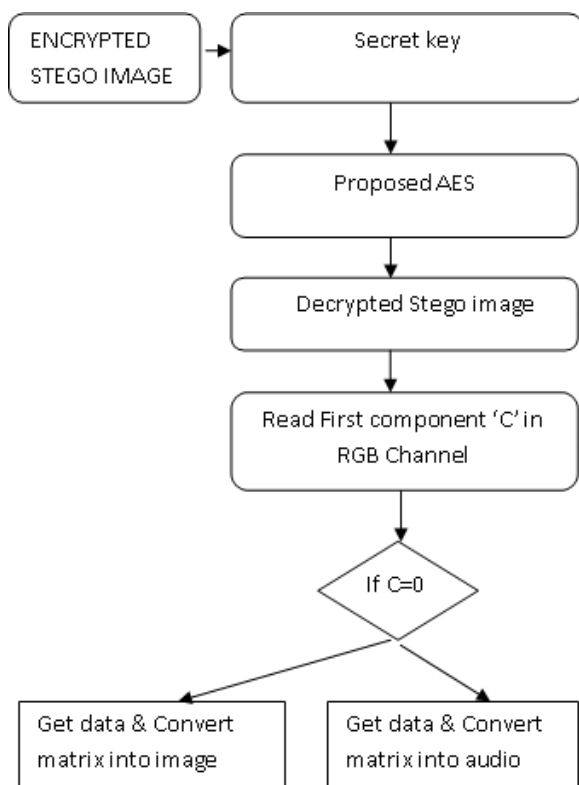


Fig. 2: Decryption of information

5. RESULT AND DISCUSSION

This section explores the various results of Enhances AES mechanism when applied to some plain images. The results are shown below in the form of encrypted images.

Table 1 Result of Enhanced AES


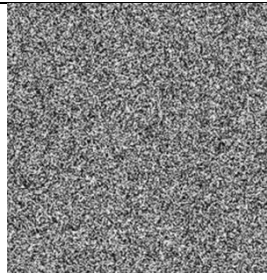

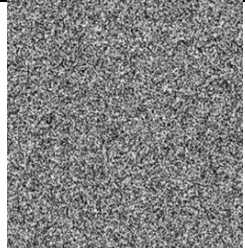
Cover Image	Encrypted Image
	
	



Table2: SteganographyBy using Proposed AES

Cover Image	Information to Embed	Time Taken
	We embed Text ABC	17.342
	Cat.jpg	8.7424
	Filewatermark.ark.wav	14.239

6. CONCLUSION AND FUTURE SCOPE

The image encryption algorithms provide security to different media at acceptable level. The proposed algorithm improves the security at two different levels. This complex relationship provides more security to image encryption. It helps us to reduce the time to some extent. In future we will embed the information in any of three medias as we have done in image media

ACKNOWLEDGMENTS

Author would like to thank Mr. Manmohan Sharma for continues support and valuable suggestions.

The author is grateful to Lovely Professional University for overall guidance.

REFERENCES

- [1]. Adil Haouzia & Rita Noumeir, "Methods for image authentication: a survey", *Multimedia Tools and Applications*, Vol.39, p. 1–46, August, 2007
- [2]. Benyamin Norouzi and Seyed Mohammad Seyedzadeh and Sattar Mirzakuchaki and Mohammad Reza Mosavi, "A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos", *Multimedia Tools and Applications*, New York, Vol. 20, p. 45-69, 2013.
- [3]. Bibhudendra Acharya, Sambit Kumar Shukla, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "H-S-X Cryptosystem and Its Application to Image Encryption", *International Conference on Advances in Computing, Control, and Telecommunication Technologies*, p. 720-724, 2009.
- [4]. C.K. Huang, C.W. Liao, S.L. Hsu, Y.C. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system", *Telecommunication Systems*, Vol. 52, pp 563-571. 29, February, 2013.
- [5]. Gyan Singh Yadav and Aparajita Ojha, "A Fast and Efficient Data Hiding Scheme in Binary Images", *Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, p. 79 – 84, 2012.
- [6]. I. Shatheesh Sam. P. Devaraj, Raghuvul S. Bhuvaneswaran, "A novel image cipher based on mixed transformed logistic maps", *Journal of Multimedia Tools and Application*, Vol. 56, p. 315-330, November, 2010.
- [7]. Jawad Ahmad and Fawad Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes", *International Journal of Video & Image Processing and Network Security*, Vol. 12, No. 04, 2012.
- [8]. Ke Qin, Mingtian Zhou, Yong Feng, "A Novel Multicast Key Exchange Algorithm Based on Extended Chebyshev Map", *IEEE Computer Society*, p. 643-648, 2010.
- [9]. Liang Zhao, Di Xiao and Kouichi Sakurai, "Image Encryption Design Based on Multi-dimensional Matrix Map and Partitioning Substitution and Diffusion-Integration Substitution Network Structure", *Information Science and Applications, International Conference*, Vol. 4, p 1-8, 2010.
- [10]. LIU Bin, LI Zhitang, TU Hao, "An Image Encryption Method Based on Bit Plane Hiding Technology", *Wuhan University journal of Natural Sciences*, Vol.11 No.5, 1283-1286, 2006.
- [11]. Mahmood Al-khassaweneh and Selin Aviyent, "Image Encryption Scheme Based on Using Least Square Approximation Techniques", *Electro/Information Technology, EIT IEEE International Conference*, p. 108-111, 2008.
- [12]. Modified Keys Exchange, Sami A. Nagar and Saad Alshamma, "High Speed Implementation of RSA Algorithm with", *6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications*, P. 639-642, 2012.
- [13]. Mr. Prashant Rewagad, Ms. Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", *International Conference on Communication Systems and Network Technologies*. p. 437-439, 2013.
- [14]. Philip P. Dang and Paul M. Chau, "Image Encryption for Secure Internet Multimedia Applications", *IEEE Transactions on Consumer Electronics*, Vol. 46, p. 3, 2000.
- [15]. Rajinder Kaur, Er. Kanwalpreet Singh, "Comparative Analysis and Implementation of Image Encryption Algorithms", *IJCSMC*, Vol. 2, Issue. 4, p. 170-176, April, 2013.
- [16]. Sandeep Bhowmik and Sriyankar Acharyya, "Image Cryptography: The Genetic Algorithm Approach", *Computer Science and Automation Engineering (CSAE)*, IEEE International Conference on Vol. 2, p. 223-227, 2011.
- [17]. Shi Runhua, Zhong Hong, Huang Liusheng and Luo Yonglong, "A (t, n) Secret Sharing Scheme for Image Encryption", *Congress on Image and Signal Processing*, Vol.3, p. 3-6, 2008.
- [18]. Somdip Dey, Sriram S. Ayyar, S.B. Subin and P .K. Abdul Asis, "SD-IES: An Advanced Image Encryption Standard- Application of Different Cryptographic Modules in a New Image Encryption System", *7th International Conference on Intelligent Systems and Control*, p. 285-289, 2012.