Effect of Optimization Algorithm on Image Security and Reliability

Shaliza Kaushal, Dr.Vikas Thada, Ms.Aman Jatain

Abstract— Due to continuous developments in Internet and other communication technologies, major portionof information is kept electronically which has led to information security concern. Cryptography and steganography are two well-known techniques for information security. Both these techniques offer their own set of advantages but the present scenario suggests the need of an extraordinary security scheme. Due to the increasing quantity of information being shared over the internet, the security of network is turning out to be more significant. This paper presents a review of the numerous techniques proposed for image security with their contributions. In addition to this the paper proposes a technique using optimized AES and GA which helps in the security of an image. Strong steganographic technique is proposed which helps to achieve high security.

Index Terms— Image encryption, Steganography, AES, GA

I. INTRODUCTION

In this information technology driven era, the most vital part of communication and information sharing is internet. The advancement in information technology and Internet has made the digital media as one of the well-known tools utilized to transfer data. This digital data includes text, images, audio, video and software which are transferred over open public network. The major portion of this digital media is in the image form and it has become an important part in different applications, for instance, chats, news, websites, e-commerce, email and e books etc. Despite being in wide spread use, the digital content still faces many challenges, including authentication issues, tampering and protection of copyright. There are many techniques that are available for protection of this digital data, such as encryption (cryptography), authentication and steganography. The latest developed encryption techniques are the most capable answer for the vast class of issues. Recently, tamper detection, protection, image content authentication has attracted attention of researchers [1].

Nowadays since more and more sensitive information is transmitted over the Internet, hence there is a need to ensure information security and safety to defend against unauthorized access. This has led to development

Manuscript received May,2016.

Shaliza kaushal, CSE, Amity university, Haryana,Gurgaon, 09971219667

Dr. Vikas Thada, CSE,,Amity University Haryana , Gurgaon, India, 09958324522.

Ms. Aman Jatain, , CSE,,Amity University Haryana , Gurgaon, India,, 09711050859.

ofnumerous solutions in the areaof hiding of information that covers Steganography, digital media, fingerprinting, digital watermarking and cryptography. All these solutions for hiding of information are truly diverse in their working. Steganography and cryptography are generally related to data hiding and have got much consideration from both academia and industry in the past [2]

Cryptography and Steganography are two essential tools to secure and protect information. Cryptography involves converting an understandable message text into an unreadable cipher. But the ciphered text can be seen by anyone and by applying cryptanalysis; anyone can recover the original text.
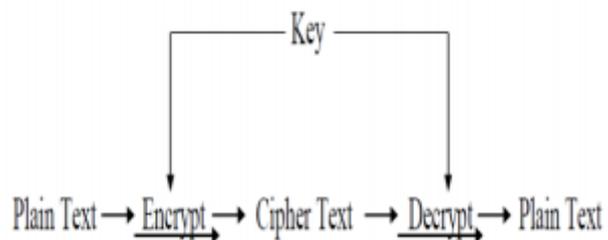

Figure 1: Cryptography concept

On the other hand, steganography is the science and art of concealing information under any other digital media. It conceals information so that it creates an impression that there exists no data.
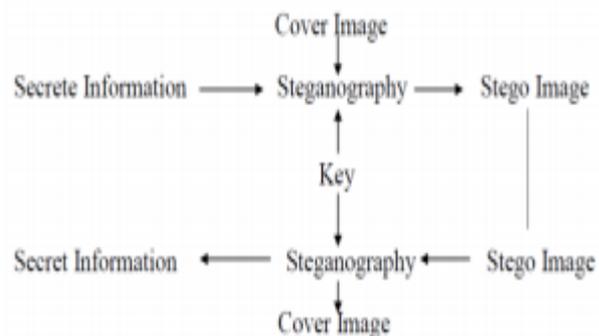

Figure 2: Steganography concept

Though Steganography and Cryptography both aim to achieve same objective of attaining security, but they differ in the way they are evaluated. Both techniques offer different advantages as encryption encrypts the information so that an unintended beneficiary cannot identify its original significance while steganography endeavour's to keep unintended recipient from expecting that information is there. In this paper, both the techniques cryptography and

Steganography have been combined into one system aiming for better confidentiality and security[3].

I. RELATED WORK

Plenty of research work has been done in the area of image security using cryptography techniques and genetic algorithms. Many methods have been proposed for security of images. Some important work in this area is as follows:

Ankita Aggarwal et.al [3] presents a new generalized model involving the combination of cryptographic and steganographic technique. These two techniques contribute in encrypting the data and further hiding it insome another medium to achieve the concealing of the message. To achieve cryptography, a Simplified Data Encryption Standard (S-DES) algorithm has been used to cipher the confidential message followed by the use of alteration component method to hide the obtained ciphered message. The use of both techniques increase the security of confidential data to two tier and a high quality stego image is achieved

Nandu Krishnan J et.al [4] shows the important role of encryption in image security. The paper involves the digital image encryption using Advanced Encryption Standard Algorithm (AES 128 bit). AES is a symmetric key block cipher that involves several rounds. There occur four transformations in each round of encryption: SubBytes, Shift Rows, Mix Columns and Add Round Key, while Mix Columns transformation is not considered in final phase. The AES has been made more secure with proposing a password along with normal AES.

R. Nivedhita et.al [7] came up with two techniques in which steganography and cryptography are consolidated for encoding the data and also for hiding the data in a medium. Steganography is the specialty of concealing the reality that communication is occurring. It is done by hiding data in some another data. Security of image by encryption is completed by algorithm of DES utilizing the key image. The image which is encoded can be covered in some another image by utilizing techniques of LSB in such a way that the presence of secrecy is covered. There could be decryption possible by same key image utilizing algorithm of DES.

Rajat Jhingran et.al [8] came up with an idea of involving GA into cryptography. In the process of key selection in public key cryptography, keys are categorized as per their fitness function which makes GA a better contend or for the key generation. A modified approach has been proposed to address the data security using Genetic algorithms Inspired Cryptography and RSA cryptography for encryption and decryption of the information.

Sonu Varghese K et.al [9] uses two techniques of security in steganography and cryptography. The matter of secret message is mixed in cryptography, where as in steganography the message which is secret is implanted into the cover medium. High security model is developed by consolidating security of cryptography and steganography. AES is utilized for encrypting secret image. The image which is encrypted is secured with another option of image with utilization of FS algorithm.

SaritaPooniaet.al [12] use the techniques of steganography and cryptography with watermarking so that to secure the specific information. Steganography is

proficient through concealing the information in some other information, along these lines by hiding the presence of conveyed information and enhancement of steganography can be done by joining it with the watermarking and cryptography. The fundamental idea of this proposed model is that it will give consent to a normal client for exchanging the information safely and hiding them in digital image file by using the local attributes inside the image, which will provide strong security.

Sandeep Bhowmik et.al [14] came up with a new technique regarding 'key' generation for encryption algorithms with the use of Genetic Algorithm (GA). The GA algorithm generates an encryption 'key' which can be used in any type of encryption. This paper proposes a hybridized technique called Blow GA which is an integration of Blowfish and GA where Blowfish Algorithm is a conventional method of encryption.

Jyotika Kapur et.al [16] discusses about the security in image processing. By utilizing image steganography and image stitching, security can be given to any type of an image which must be transmitted utilizing any electronic mode. The secret image is separated into parts. The first phase in the phase of Encryption handles the procedure of changing the real image into cipher text by using the algorithm of AES. The second phase is Embedding Phase, in which cipher text is inserted into any segment of the secret image which is to be sent. The third phase is Hiding Phase, in which steganography is implemented on the yield image of Embedding Phase and also different parts are disguised by some other image utilizing replacement of least significant bit. After all this, all these individual parts are sent to the recipient. At the end of recipient, Hiding phase decryption and Embedding phase decryption happens respectively. The obtained parts are stitched together by utilizing k nearest method. The quality of an image can be improved by using features of SIFT.

Manoj.B et.al [17] have discussed about image encryption and decryption using AES. For transferring block of data safely, Advanced Encryption Standard is acknowledged as standard of symmetric cryptography. The AES algorithm which is available is utilized for content information and it is additionally appropriate for encryption and decryption of an image to shield the data of a confidential image from an unapproved access. This paper proposes a methodology in which input to AES encryption is image data to acquire an encrypted image, and the input to decryption of AES is encrypted image to obtain the original image. 128 bit AES for encryption and decryption of an image is implemented which is simulated and synthesized on FPGA family of Spartan-6 (XC6SLX25) utilizing Xilinx ISE 12.4 tool as a part of very high speed integrated circuit Hardware Description Language (VHDL).

B.G. Priyanka et.al [20] attempts the study and usage of system of steganography with main objective of safe communication of images alongside related content. A model of image steganography which is already proposed is altered in such a manner that a confidential image is inserted alongside the private text scrambled into solitary cover image. Embedding of text alongside the image is done by disintegrating the cover image and inserting content in one of the fragments. Content information is implanted in spatial

domain using technique of Least Significant Bit Substitution (LSB) giving away one segment of stego. As spatial domain is more inclined to attacks, content information is encrypted by utilizing Advanced Encryption Standard (AES) to achieve high security. Payload image is implanted into other section, while Dual Tree Complex Wavelet Transform (DTCWT) and Lifting Wavelet Transform (LWT) are operated on other section of cover image and payload image respectively. Process of embedding an image is completed by technique known as adaptive scaling and coefficient replacement, and another section of stego is acquired.

S.H. Kamali et.al in [21] presents a technique of modified AES. Advanced Encryption Standard (AES) is block cipher which is well known and has many advantages in encryption of information. But it is not appropriate for the applications of real time. For achieving security at higher level and better encryption of an image, a modification to the Advanced Encryption Standard (AES) is discussed in this paper. This modification is completed by changing the Shift Row Transformation. The results of the experiment demonstrate that this proposed methodology is very secure from the perspective of cryptosystem. This method also gives better results in encryption.

Pye Pye Aung et.al [22] demonstrated a new system with the combination of cryptography and steganography upgraded with new features of security for producing a new system. The two prevalent means for the transmission of secure data is Cryptography and Steganography. Cryptography modifies the message in such a manner so that the message is not readable. But steganography shrouds a message so that it is not visible. In cryptography, advanced encryption standard (AES) algorithm is utilized for encrypting the private message and after that there are differentiated keys; one of which is utilized to conceal in cover image. In steganography, some portion of encrypted message is utilized to conceal in discrete cosine transform (DCT) of an image which is exceedingly secured and safe. This sort of framework is presented in applications, for example, exchanging secret information which can be validation of different fields.

Hussein Al-Bahadili in [23] explains an algorithm for image steganography based on secure block permutation. Steganography is the technique of concealing secret information inside any cover media to develop an amalgamated private cover media known as stego media, so that the secret can't be perceived or recouped by unapproved recipients. The proposed algorithm changes the private message to binary sequence, partitions the sequence of binary into blocks, permutes the block by utilizing arbitrarily produced permutation which is based on key, connects the permuted blocks framing the sequence of permuted binary and at last uses the approach of Least Significant Bit (LSB) to insert the sequence of permuted binary into BMP image file. The performance of an algorithm is examined after executing numerous experiments and for every experiment the PSNR (Peak Signal-to-Noise Ratio) between the cover and stego images is computed. This algorithm offers high quality of an image and invisibility and also security at high level.

Shubhangini P.Nichat et.al in [24] talked about image encryption using hybrid genetic algorithm. In this paper, a best hybrid model for encryption of an image made out of

genetic algorithm and chaotic function. In the first phase, numerous encrypted images are developed by utilizing secret key and chaotic function. In the following stage, these encrypted images are utilized as initial population for genetic algorithm. Genetic algorithm is utilized to acquire ideal results in this proposed methodology and in the end phase, image of best cipher is chosen in light of coefficient of correlation and entropy. The image which has highest entropy and lowest coefficient of correlation is chosen. Entropy and coefficient of correlation acquired by utilizing this technique are 7.9978 and -0.0009 respectively.

Table 1: Comparison of various proposed techniques

Author	Proposed approach	Contributions
Ankita Aggarwal et.al	S-DES with Alteration approach	2-tier security and high quality stego image
Nandu Krishnan et.al	Password enabled AES	More secure than normal AES
R. Nivedhita et.al	DES with LSB technique	Cryptography and steganography attained
Rajat Jhingran et.al	Genetic algorithms Inspired Cryptography and RSA cryptography	Modified approach to data security
Sarita Poonia et.al	Watermarking with cryptography	Data hiding using local attributes in image and strong security
Sandeep Bhowmik et.al	Hybridised technique BlowGA	Combination of Blowfish and GA provides better way of key generation
S.H. Kamali et.al	Modified AEs with changed shift row transformation	Secure from cryptosystem.
PyePyeAung et.al	AES cryptography with DCT inspired hiding	Exchanging secret information which can be validation of different fields.
Hussein Al-Bahadili	Block permutation steganography with LSB	high quality image invisibility and high level security
Shubhangini P.Nichat et.al	Hybrid form of GA and chaotic functions for cryptography	Image with highest entropy and lowest coefficient of correlation

II. PROPOSED APPROACH

Steganography and cryptography are the two braches essential for security of information. Though both these technique fulfil the same purpose but both are different. It is conceivable to join the strategies by message encryption using cryptography and then hiding the message which is encrypted utilizing steganography. The paper aims to achieve a communication which is secure and furthermore to abstain from attracting suspicion to the hidden data transmission. For this, the paper presents an AES optimized with genetic algorithm to get higher PSNR and data hiding capacity.

III. CONCLUSION

This paper presents a review of the techniques proposed by many scholars for image security, highlighting their contributions. Despite much work done in this domain, there is still scope of developing more secure schemes to meet the continuous rising security demands. The cryptography and steganography concepts can be combined to achieve superior results. In this regard, paper proposes an optimized AES inspired cryptography with GA to attain steganography.

REFERENCES

[1] Gamil R.S. Qaid, Sanjay N. Talbar, "Bit-Level Encryption and Decryption of Images Using Genetic Algorithm: A New Approach", IPASJ International Journal of Information Technology (IIJIT), Vol.1, Issue 6, December 2013.

[2] ManojRamaiya, Naveen Hemrajani, Anil Kishore Saxena, "Secured Steganography Approach Using AES", Intenational Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol.3, Issue 3, Aug 2013.

[3] AnkitaAggarwal, "Security Enhancement Scheme for Image Steganography using S-DES Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue 4, April 2012.

[4] Nandu Krishnan J, Roshny G. Kumar, "Security Enhanced Image Encryption usingPassword based AES Algorithm", International Journal of Engineering Research & Technology (IJERT)ISSN: 2278-0181, IJERTV4IS061106 , Vol. 4 Issue 06, June-2015

[5] Lokesh Kumar, "Novel Security Scheme for Image Steganography using Cryptography Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue 4, April 2012.

[6] Anil Kumar, M.K. Ghose, "Information Security using Genetic Algorithm and Chaos", Sikkim Manipal University of Technology, Sikkim.

[7] R.Nivedhitha, Dr. T. Meyyappan, "Image Security Using Steganography And Cryptographic Techniques", International Journal of Engineering Trends and Technology, Vol.3, Issue 3, 2012.

[8] RajatJhingran, VikasThada, Shivali Dhaka, "A Study on Cryptography using Genetic Algorithm", International Journal of Computer Applications (0975 – 8887), Volume 118 – No.20, May 2015

[9] Sonu Varghese K, Faisal K K, Vinayachandran K K, "Image Security using F5 and AES Algorithm", Proceedings of IRF International Conference, Chennai, April 2014

[10] SaifHasan, SagarChordia, Rahul Varshneya, "Genetic Algorithm", Februray 2012.

[11] P.Karthigaikumar, SoumiyaRasheed, "Simulation of Image Encryption using AES Algorithm", IJCA Special Issue on "Computational Science-New Dimensions & Perspectives", NCCSE, 2011.

[12] SaritaPoonia, MamteshNokhwal, Ajay Shankar, "A Secure Image Based Steganography and Cryptography with Watermarking", International Journal of Emerging Science and Engineering (IJESE), Vol.1, Issue 8, June 2013.

[13] AnkitaAggarwal, "Secret Key Encryption Using Genetic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol.2, Issue 4, April 2012.

[14] SandeepBhowmik, SriyankarAcharyya, "Image Cryptography: The Genetic Algorithm Approach", 978-1-4244-8728-8/11, 2011 IEEE

[15] Shamim Ahmed Laskar, KattamanchiHemachandran, "Secure Data Transmission Using Steganography and Encryption Technique" International Journal on Cryptography and Information Security (IJCIS), Vol.2, No. 3, September 2012.

[16] JyotikaKapoor, Akshay. J. Baregar, "Security using Image Processing", International Journal of Managing Information Technology (IJMIT), Vol.5, No.2, May 2013.

[17] Manoj. B, Manjula N Harihar, "Image Encryption and Decryption using AES", International Journal of Engineering and Advanced Technology (IJEAT), Vol.1, Issue 5, June 2012.

[18] Kundan kumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, "Text and Image Encryption Decryption Using Advanced Encryption Standard", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol.3, Issue 3,May-June 2014.

[19] P. Radhadevi, P. Kalpana, Secure Image Encryption using AES", IJRET: International Journal of Research in Engineering and Technology, Vol. 1, Issue 2, Oct- 2012.

[20] B.G. Priyanka, S.V. Sathyanarayana, "A steganographic system for embedding image and encrypted text", International Conference on Contemporary Computing and Informatics (IC3I), November 2014.

[21] S.H. Kamali, R. Shakerian, M. Hedayati, M. Rahmani, "A new modified version of Advanced Encryption Standard based algorithm for image encryption", International Conference on Electronics and Information Engineering (ICEIE), Vol. 1, August 2010

[22] PyePyeAung, Tun Min Naing, "A Novel Secure Combination Technique of Steganography and Cryptography", International Journal of Information Technology, Modeling and Computing (IJITMC), Vol. 2, No. 1, February 2014

[23] Hussein Al-Bahadili, "A Secure Block Permutation Image Steganography Algorithm", International Journal on Cryptography and Information Security (IJCIS), Vol. 3, No. 3, September 2013

[24] ShubhanginiP.Nichat, Prof. Mrs.S.S. Sikchi, "Image Encryption using Hybrid Genetic Algorithm", International Journal of Advanced Research on Computer Science and Software Engineering, Vol. 3, Issue 1, January 2013