A Review Paper of Improvement in Security of Images using Genetic Technique

Er. Shekharan Deep Bindra[1] Er. Navneet Bawa[2]
[1,2]Department of Computer Science and Engineering
[1,2]Amritsar College of Engineering & Technology (Manawala)

Abstract— In the world of digital communication data is the heart of worldwide economy and computer networks. In this review paper the two techniques are combined to form a hybrid technique. Cryptography and steganography are two essential branches of information security. The purpose of both these is same but both are different. It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The main goal(s) of this research is To do communication in a secure manner and also to avoid drawing suspicion to the transmission of hidden data and To create a strong steganographic technique that can achieve high security & embedding capacity while maintaining image quality & imperceptibility.

Key words: Steganography, Cryptography, AES, LSB techniques

I. INTRODUCTION

With the expanding utilization of the Internet and other effective technologies of communication, the computerized media have turned into the most well-known tools which are utilized to exchange information. The majority of these advanced media is in the form of an image and utilized as a part of different applications. For example, email, eBooks, websites, e-commerce, news, chats etc. But still digital content is still faced with many difficulties, for example, authentication, tampering and protection of copyright. The modern techniques of encryption have been viewed as the most effective answer for the vast majority of these issues. Authentication of content and detection of tamper of digital image, audio and video have caught enthusiasm of the researchers. In the last ten years, study on the schemes of image security concentrated mostly on the problems of the protection of copyright, yet gave less consideration to speed, distortion and lossless data. The conventional algorithms of image encryption grew in the most recent couple of years may not fit for different formats of digital image, due to the large size of data, unknown environment and real time constraints. Likewise, few of them have been recognized as unreliable, the methods of encryption permit to change digital images to some from which is unreadable and difficult to comprehend, and inverse change feasibility of the digital image encryption to the target image. Every one of these problems emerge the requirement for reliable techniques for encryption.

In the growing prospect of communications system need the exceptional means of security especially in computer network communication. In the world of digital communication, data is the heart of worldwide economy and computer communication. So to guarantee the data security, the idea of hiding is the best way to provide the security to the data. The internet gives a technique for communication to convey information to big group. We have two diverse technique of hiding the information: -

Steganography: Expects to send a message on channel, in which some other sort of data is now being transmitted. The objective of steganography is to hide a message with in another. The key concept behind steganography is that the message to transmitted is not detectable to the casual eyes. Steganography does not change the structure of private message, rather conceals it in a medium so that the change is not observable. As it were, steganography keeps an unintended receiver from expecting that the information exists as the privacy of the system of steganography depends on privacy of the system of data encoding. When the system of encoding is known, the system of steganography is crushed.

A. Cryptography

Cryptography shrouds the private message contents from an unapproved individual yet the message content is visible. in this Message structure is jumbled in such a manner so as to make it insignificant and incomprehensible. Generally, cryptography offers the capacity of transmitting data between individuals in a manner that keeps an outsider from reading it.

We have methods that are extremely secure for both Steganography and Cryptography that is AES algorithm is a technique which is very secure for cryptography and the methods of steganography that uses frequency domain, are very secured and safe. Regardless of the fact that we join these strategies straight forwardly, there is a risk that the intruder may distinguish the initial message.

B. Steganography Vs Cryptography

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secrete message from a malicious people, whereas steganography even conceal the existence of the message. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganography system need the attacker to detect that steganography has been used. It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged.

II. Review of Literature

Gowtham M.G.V et al. (2013) in this paper the authors described AES based steganography in biometrics and biometric feature have been used to implement steganography as skin tone region of images. In this paper here secret data is encrypted by AES (Advanced Encryption Standard) and embedded within skin region of image that will provide an excellent secure location for data hiding.

Hussein Al-Bahadili (2013) in this paper aurthor gave detailed description of a new secure Block Permutation

Image Steganography (BPIS) algorithm. In this research the algorithm amalgamates the simple concept of permutation with steganography to provide a relatively fast, reliable, and high information security approach.

Philijon T.L.J and Venkateshvara R.N. (2011) in this paper the new technique was presented which encrypts the message with image and generates a cipher image; this cipher image is manipulated with the cover image and generates an intermediate text. Also the size of cover image should be at least equal to size of cipher image. The main problem with this technique is that it can easily be detected by naked eyes that something is hidden in cover image because direct manipulation with the cover image degrades the quality of stego image.

Ramaiya M. et al. (2013) in this paper the approach AES is used to secure the steganography. The conventional steganography algorithem does not provide the preprocessing required in image for better security. All of the cryptographic algorithms presented so far have some problems. The earlier ciphers can be broken with ease on modern computation systems. The DES algorithm was broken in 1998 and Triple DES turned out to be too slow for efficiency as the DES algorithm was developed for mid-1970's hardware and does not produce efficient software code

Ramaiya M. K. et al. (2013) in this paper unique technique for image steganography based on Data Encryption Standard using the strength of S Box mapping. In this paper, authors have modified the DES algorithms and used this algorithm to encrypt the secret image pixel before hiding it behind the cover image file.

Ramaiya M. K. et al. (2013) in this paper a unique technique for Image steganography based on the Data Encryption Standard (DES) using 64 bit block size of plain text & 56 bits of Secrete key. The preprocessing provide high level of security as extraction of image is not possible without the knowledge of mapping rules of S –Box and secrete key of the function.

Varghese S. K et al. (2014) in this paper the contents of secret message are scrambled in cryptography, where in steganography the secret message is embedded into the cover medium. In this proposed system they developed high security model by combining cryptographic and steganography security. In cryptography they used advanced encryption standard (AES) algorithm to encrypt secret image.

III. Approches Used

The approach used in previous work is AES which is as follow:

A. AES (Advanced Encryption Standard)

The algorithm is based on Rijndael algorithm which permits different block and key sizes. AES is an algorithm with iterations i.e. it is an iterative algorithm. Every iteration is known as round. Every round of processing incorporates one step of single byte based on substitution, a permutation step which is row wise, a mixing step which is column-wise and then addition of the round key. The arrangement in which all these four steps are performed is distinctive for encryption as well as for decryption. The four transformations are as below:

B. Sub Bytes

It works in each byte of the state separately. Every byte is substituted by relating byte in the S-box.

C. Shift Row

It consistently moves the rows of the state over distinctive offsets.

D. Mix Column

In this transformation, the column of the state is taken as polynomials over GF (28) and are increased with an altered polynomial. The component Mix Column does not work in the last round of AES algorithm.

E. Add Round Key

It involves operation of XOR bitwise.

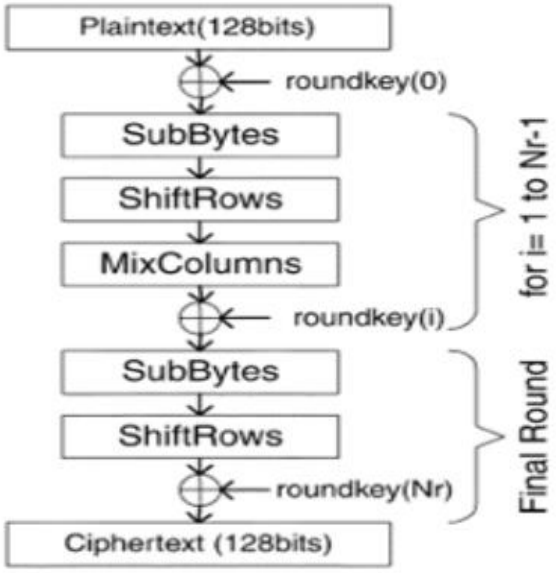

Fig. 1: Block diagram of encryption part of AES.

But AES algorithm is very difficult to implement because the usage of keys make it very complex and moreover it has very complex algebraic structure. If we use the keys then there are number of iterations which we have to implement in AES that make it very complex and also time consuming.

F. Digital Watermarking

A digital watermark is a piece of information which is embedded in the digital media and hidden in the digital content in such a way that it is inseparable from its data. This piece of information known as watermark, a tag, or label into multimedia object such that the watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video, or text. This paper is focused on noteworthy work and techniques used for images during preliminary and principal development stage of digital watermarking by various researchers with the utility of giving a fundamental understanding of the basic principles of digital watermarking as it has evolved. This may serve as the concrete foundation and the base for understanding further advances in this technology in later years. This paper gives a summary of different innovative techniques in this emerging area. Watermarking is the process of inserting a digital signal or pattern (indicative of the owner of the content) into digital content. The signal, known as a watermark, can be

used later to identify the owner of the work, to authenticate the content, and to trace illegal copies of the work.

G. Des Technique

DES algorithm, an encryption algorithm, used keys of smaller sizes (64bit key) hence it was easy to decode it using computations. Algorithms using keys of these sizes are easily cracked by any intruder. So it is better if one goes for algorithms using keys of larger size which are difficult to decrypt and provide better security. Where stitching is concerned, multiband blending, gain compensation, automatic straightening makes the image smooth and more realistic.

H. Genetic Algorithm

The genetic algorithm is a search algorithm depending on the procedure of natural genetics and natural selection. Genetic algorithm is the optimization problem solver. Optimization is performed through natural exchange of genetic material between parents. The principle idea is that in place for individual's population to adjust to some environment, it ought to act like characteristic framework. The reproduction and survival of an individual being is advanced by the end of pointless characteristics and by developing the valuable conduct. Generally, genetic algorithm starts with set of individuals that are generated randomly.

1) Generate random population of n chromosomes (suitable solutions for the problem).
2) Evaluate the fitness f(x) of each chromosome x in the population.
3) Create a new population by repeating following steps until the new population is complete

Select two parent chromosomes from a population according to their fitness (the bigger fitness, the bigger chance to be selected).With a crossover probability cross over the patterns to form a new offspring (children). If no crossover was performed, offspring is an exact copy of parents.

With a mutation probability mutate new offspring at each locus (position in chromosome).

Place new offspring in a new population.

4) Use generated population for a further run of algorithm.
5) If the end condition is satisfied, stop, and return the best solution in current population.

IV. Conclusion

The two main problems that arise in image encryption are With respect to time it takes for its computation and Its security. For real time image encryption, only those ciphers are preferable which takes lesser amount of computational time without comprising security. Cryptography and steganography are two essential branches of information security. The purpose of both these is same but both are different. It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The main goal(s) of this research are:

To do communication in a secure manner and also to avoid drawing suspicion to the transmission of hidden data.

To create a strong steganographic technique that can achieve high security & embedding capacity while maintaining image quality & imperceptibility.

V. Future Scope

The developing prospects of the system of communications require the uncommon methods for security particularly in communication in networks of computer. The security in the network is picking up importance as the information which is exchanged or shared on the internet enhances. The main objectives to ensure for the security in images are:

1) The authenticity or possession of the sender or creator of an image.
2) The integrity of the data of an image, and the capacity to get knowledge about the image if it has been modified.
3) Privacy, in the words of possession or content of the information.

In this manner, integrity and confidentiality are needed to provide security against unapproved access. This has brought about an unstable development in the area of hiding information, which also wraps applications, for example, Digital Watermarking, protection of copyright for digital media, fingerprinting, Steganography and Cryptography. But all these applications of hiding information are very different. Cryptography gives a technique for authenticating and securing the transmission of information over the channels which are not secure. It empowers us to store delicate data or transmit it over networks which are not secure so that unapproved persons are not able to read it. Steganography is the art of concealing and sending information through obviously inoffensive transformers with an end goal to hide the data existence. If a message is concealed with Steganography, it decreases the possibility of message being noticed. Hence some methods of Steganography join traditional cryptography with steganography.

The well-known method for securing transmission of data or storage is Encryption. Many methods of encryption are already available, for example, RSA, DES (Data Encryption Standard), AES (Advanced Encryption Standard). These methods jumble the private message so that no one can understand the message. But it makes the message so doubtful to pull in attention of eavesdropper. There are some techniques which are already available for the security of images is as follows:

- Steganography
- Water Marking Technique
- Visual Cryptography
- Without Sharing Keys Technique.

VI. References

[1] Gowtham M.G.V., Senthur T., Sivasankaran M., Vikram M.,Bharatha S.G. "AES based steganography", International Journal of Application , ISSN 2319 – 4847,Vol 2, 2013.
[2] Hussein Al-Bahadili. "A secure block permutation image steganography algorithm", International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 3, 2013.

[3] Philjon T. L. J and Venkateshvara R. N. "Metamorphic Cryptography -A Paradox between Cryptography and Steganography Using Dynamic Encryption", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011.
[4] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishor Saxena, Monika Sharma "Image Stenography: Self Extraction Mechnanism", UACEE International Journal of Advances in Computer Science and its Applications-IJCSIA, ISSN 2250-3765, Vol-3 , pp 145-148, 2013.
[5] Ramaiya M. K., Hemrajani N. and Saxena A. K. "Security Improvisation in Image Steganography using DES", 3rd IEEE Trans. International Conference IACC -2013, pp 1094 – 1099. 2013
[6] Ramaiya M. K., Hemrajani N. and Saxena A. K., "Security Improvisation in image Steganography applying DES", International Conference on Communication Systems and Network Technologies, IEEE pp 431-436. 2013
[7] varghese S. K., Faisal K. K. and Vinayachandran K K. "Image security using f5 and AES algorithm", Proceedings of IRF International Conference, Chennai, India, 2014
[8] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Parta Pratim Sarkar " An Image Steganography Technique using X-Box Mapping", IEEE Trans. International Conference Advances in Engineering, science and Management (ICAESM-2012) pp 709 -713. 2012
[9] Donovan Artz " Digital Steganography: Hiding Data within Data ", Los Alamos National Laboratory, IEEE Trans.2001, pp 75-80. 2001
[10] Federal Information Processing Standard Publication (FIPS 197), "Advance Encryption Standard (AES) ", 2001.
[11] Ge Huayong, Huang Mingsheng, Wang Qian, "Steganography and Steganalysis Based on Digital Image", IEEE Trans. International Congress on Image and Signal Processing. pp 252-255., 2011
[12] Guilliang Zhu, Weiping Wang, "Digital Image Encryption algorithm based on pixel", ICIS – 2010, IEEE International Conference, pp 769 – 772, 2010.
[13] J. Mielikainen, LSB Matching Revisited, IEEE Signal Process. Lett. 13 (5),pp 285-287. 2006.
[14] Jasmin Cosic, Miroslav Bacai, " Steganography and Steganalysis Does Local web Site contain "Stego" Contain",52th IEEE Trans. International Symposium ELMAR-2010, pp 85 – 88. 2010.
[15] M. Zeghid, M. Machhout, L. Khriji, A.Baganne, and R. Tourki, World Academy of Science and Technology, pp 526-531, 2007.
[16] N Provos and P. Honeyman, "Hide and seek: An Introduction to Steganography", IEEE Security and Privacy, pp 32-44,2003.
[17] Saeed R. Khosravirad, Taraneh Eghlidos and Sharokh Ghaemmaghami, "Higher Order Statistical of Random LSB Steganography", IEEE Trans., pp 629 – 632, 2009.
[18] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans.Inf. Forens. Security 5 (2) pp 201-214,2010.
[19] Yambin Jina Chanu, Themrichon Tuithung, Kh Manglem singh," A Short Survey on Image Steganography and Steganalysis Technique ", IEEE Trans. ,2012 .
[20] Zhang Yun-peng , Liu Wei " Digital Image Encryption Algorithm Based on chaos and improved DES ", System, man and Cybernatics ,SMC 2009 , IEEE International Conference 11-14, pp 474-479., 2009.

