2019 International Conference on Electrical, Computer and Communication Engineering (ECCE),
7-9 February, 2019

An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography

Chitra Biswas
Dept. of CSE, CUET
Chittagong, Bangladesh
chitra.biswas86@gmail.com

Udayan Das Gupta
Dept. of CSE, CUET
Chittagong, Bangladesh
udgupta05@live.com

Md. Mokammel Haque
Dept. of CSE, CUET
Chittagong, Bangladesh
malin405@yahoo.com

***Abstract*—Data/information is the most valuable asset for the modern electronic communication system. To secure data or information has become a challenge in this competitive world. There are many techniques for securing data/information such as cryptography, steganography etc. In this paper, hybrid cryptography has been applied using AES and RSA. In this hybrid cryptography, the symmetric key used for message encryption is also encrypted, which ensures a better security. An additional feature of this paper is to create a digital signature by encrypting the hash value of message. At the receiving side this digital signature is used for integrity checking. Then the encrypted message, encrypted symmetric key and encrypted digest are combined together to form a complete message. This complete message again has been secured using the steganography method, LSB. Here hybrid cryptography provides a better security, steganography strengthens the security. Message integrity checking is a special feature of this algorithm. Successful simulations have been shown to support the feasibility of this algorithm.**

Keywords—Cryptography, Hybrid cryptography, Algorithm, AES, RSA, Steganography, LSB

I. INTRODUCTION

In the modern electronic communication system, data and information security is a formidable challenge nowadays. To secure the information three security goals must be followed. They are confidentiality, integrity, and availability, also known as CIA triad for data, information and computing services [1]. That's why to conceal information from an unauthorized entity (confidentiality), to protect information from being illegally changed (integrity), to make information available to the authorized entity (availability) are the primary objectives for information security [2].

Some techniques are required for the application of security goals. The two most dominant techniques used today are cryptography and steganography [2][16]. Two Greek words 'Kryptos' meaning 'secret' and 'Graphein' meaning 'writing' derive the word 'Cryptography'. So Cryptography means 'secret writing', a science of transforming a message into an unintelligible form [3]. The unencrypted message is called 'plain text' and after encryption, it is converted into an unintelligible form which is called 'cipher text'[4]. The cipher text is then sent over an insecure channel with the presence of a third party called adversary or intruder and at the receiving end after decrypting the cipher text again the plain text is found. Fig.1. illustrates the general concept of cryptography using a block diagram.

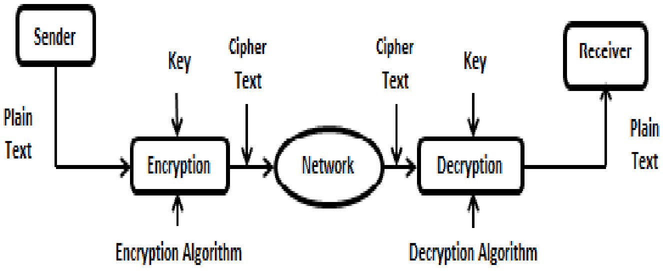


Fig.1. General concept of Cryptography

Cryptography introduces three different types of streams [2] [4]:

i) Symmetric-key (Shared secret key) Cryptography
ii) Asymmetric-key (Public-key) Cryptography
iii) Hashing

Symmetric-key cryptography uses a single secret key for both encryption and decryption purpose, whereas asymmetric-key cryptography uses two keys: one is the public key and another one is the private key. Receiver's public key is used by the sender for encrypting the message and receiver's own private key is used for decrypting the message at the receiver. Hashing provides a fixed-length message digest for a variable-length message to give check values [2]. In most of the cryptographic practical implementations, both the symmetric and asymmetric algorithms (sometimes hashing also) are used together which is called hybrid cryptography. To overcome one algorithm's weakness by another one's strength is the main purpose of using hybrid cryptography [5].

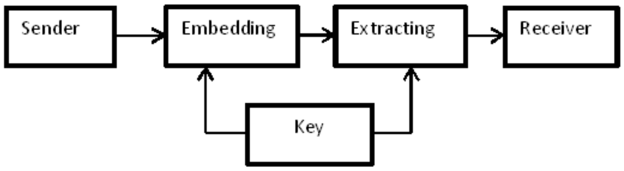


Fig.2. General concept of Steganography

978-1-5386-9111-3/19/$31.00 ©2019 IEEE

Sometimes to protect data/information, cryptography is not sufficient; it is also required to conceal the existence of the data/information. This process of hiding the existence of data/information is called steganography. Steganography is formed from the two Greek words 'Steganos' meaning 'Covered' and 'Graphein' meaning 'writing', which refers to 'Covered Writing'. It is the science of hiding the existence of information into another information [6]. The information is embedded into a cover or carrier object so that no one can understand the presence of information. A key is used for embedding procedure without which the adversary cannot be able to detect the embedded message [7]. The altered new object is called stego object. Image, audio, video etc. can be the cover objects [7] [8] [17]. Fig. 2. shows the general concept of steganography.

For steganography algorithms, three concepts are required that contend with each other [9]:

i) Capacity: indicates the information quantity that the cover object can hide.
ii) Security: indicates to the protection so that an intruder cannot be able to understand the existence of hidden information.
iii) Robustness: refers to the amount of modifications that a stego object can withstand before hidden information destruction.

On the basis of cover object, steganography is classified as image, audio, text, video, and protocol steganography [7]. Among them, image steganography is a popular one as it can achieve the three concepts which contend with each other: capacity, imperceptibility, and robustness [10]. The image steganography methods are of two types depending on domain type: spatial domain based techniques and frequency domain based techniques. In spatial domain based technique, the message is embedded in the intensity of pixels of the images straightly while in frequency domain based technique, images are converted into the frequency domain and then the messages are embedded in the transform coefficients [11]. Among many spatial domain based techniques, LSB (Least Significant Bit) method is the widely applied method. In this technique, messages are embedded in the least significant bit of the pixel of the cover image. To embed more messages, two or more pixels of the cover image can be allocated, but this kind of allocation can degrade the image fidelity as well as imperceptibility [11]. The available frequency domain based techniques are Discrete Cosine Transformation (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT) etc. [12]. Fig. 3. shows the classification of image steganography.

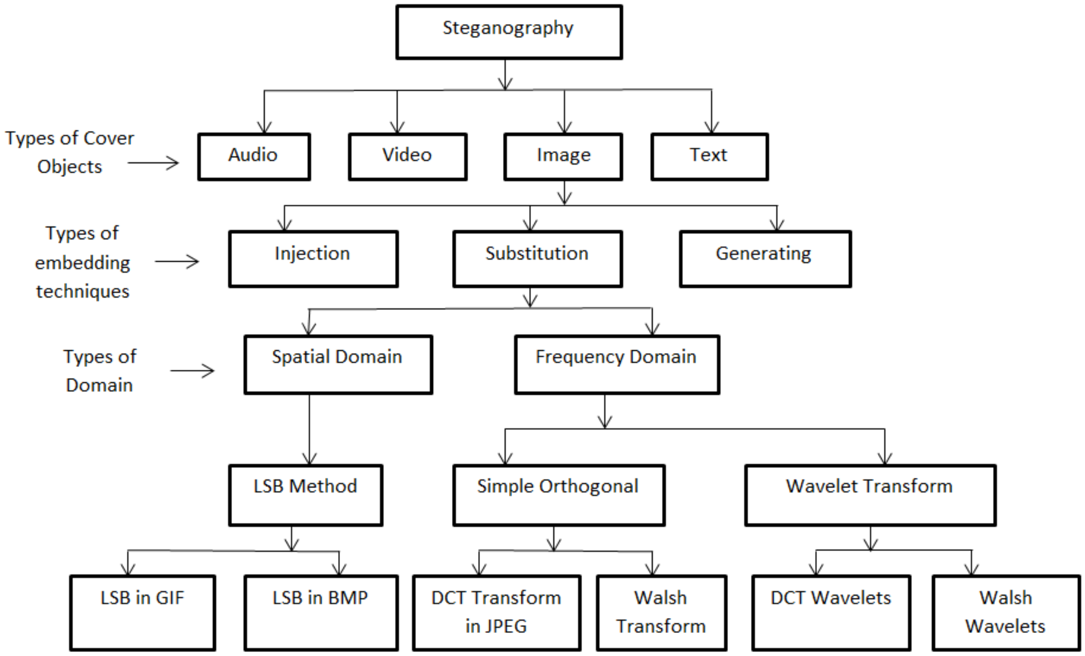


Fig. 3. Classification of Image Steganography [8]

In this paper, a hybrid cryptography is applied using both the symmetric key cryptography algorithm, AES (Advanced Encryption Standard) and the public-key cryptography algorithm, RSA [13] [14]. Cryptography hides the contents of information but steganography hides the presence of information [15]. So to increase the security one step forward, a steganography technique, LSB (Least Significant Bit) has also been applied. An additional feature of this algorithm is, for integrity checking, a digest has been generated. This digest is also encrypted using the public key of RSA, which is called digital signature (DS). At the receiver side, this digital signature is decrypted with the help of the private key of the receiver to regenerate the digest. This digest is compared with the hash value of the message. As both the values are equal, the integrity of the message has been checked.

II. Proposed Algorithm

At first, both the hybrid cryptography and steganography are applied to create the stego image at the sender side. Fig.4 illustrates the encryption and embedding process. At the receiving end, the complete message is extracted from the stego image and then all the encrypted messages are decrypted. Integrity of the message is also verified. The extraction and decryption process is shown in Fig.5.

A. Encryption and Embedding Process

i) Sender will receive public key (PK) from the receiver.

ii) It will generate a random number, X.

iii) Using the random number X as a symmetric key, it will encrypt the message using AES.

iv) Sender will generate a hash value from the message using SHA256 that is denoted here as digest, DG.

v) Applying the public key, PK of RSA sender will encrypt the digest, DG. This encrypted digest is called the digital signature, DS.

vi) The random number, X is encrypted using the public key, PK of RSA. This encrypted key is denoted as Y.

vii) All the encrypted data i.e. encrypted message (C), encrypted digest (DS), encrypted key (Y) are combined together to form a complete message, CM.

viii) Using steganography technique, LSB, the whole message CM will be hidden in the cover image and the output image is referred to as stego image.

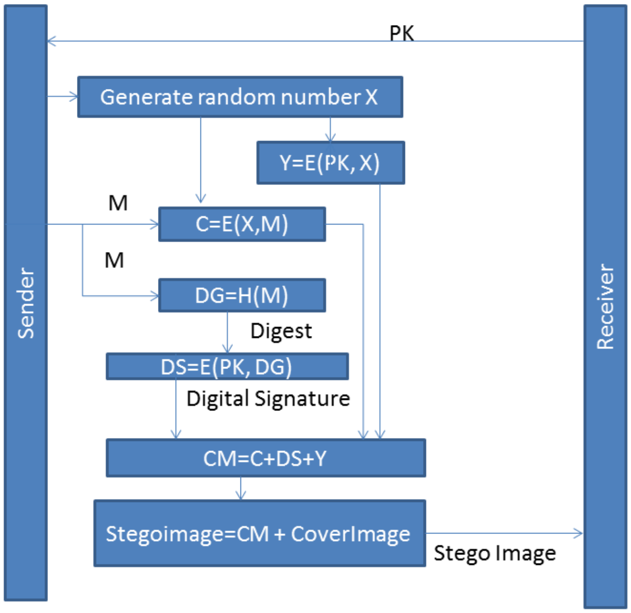


Fig. 4. Encryption and Embedding Process of Proposed Algorithm

B. *Extraction and Decryption Process*

i) Receiver will receive the stego image from the sender. The complete message is extracted from the stego image and then all the encrypted data, i.e. encrypted message (C), encrypted digest (DS), encrypted key (Y) are separated from the complete message (CM).

ii) Using the private key (SK), the receiver will decrypt the Y to generate the random number X which will be applied as a key to decrypt the cipher (C).

iii) Using X as a key, the cipher (C) is decrypted and the message is found.

iv) The digital signature (DS) is also decrypted using the private key, SK and the digest (DG) will be found.

v) The hash value from the message is generated which has been denoted as digest (DG).

vi) If the digest from the message and the digest from the digital signature are equal, the message integrity is verified. Otherwise the message integrity is violated.

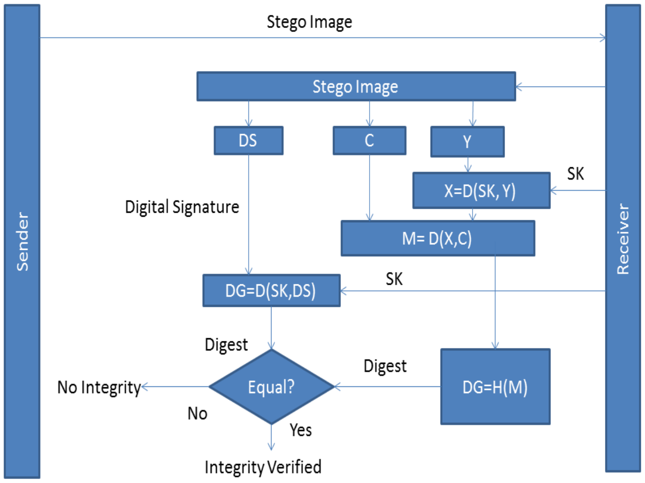


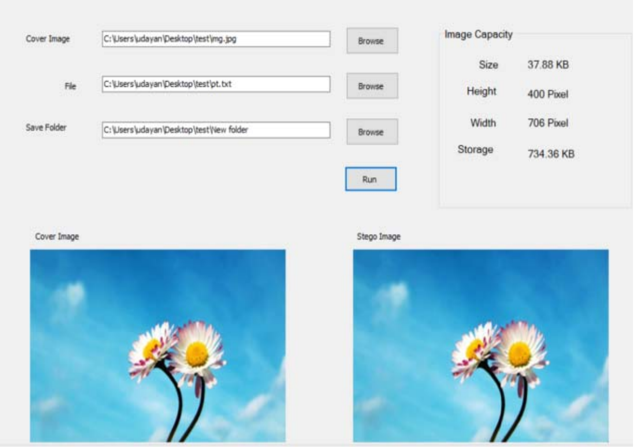
Fig. 5. Extraction and Decryption Process of Proposed Algorithm

III. Simulation Result

C# implementation of this technique gives good results and performance. Here, we need a cover image and a file to encrypt and embed which can be of any type, then a folder location as file saving directory where several files of encryption-decryption process to be generated. In Encryption process digest is generated using SHA256 which gives a byte[] of length 32. Then, we converted it into a string of hexadecimal to make a 64byte digest. After that, RSA algorithm is used to encrypt the digest which produces the digitalsignature.txt of the file to be encrypted. Then a 64byte hexadecimal number is derived from a random number's digest . First 32bytes of 64bytes are used as key and second 16 bytes are used as IV (Initial Vector) as the parameter of AES algorithm. After completion of AES encryption, encrypted text is saved in the ct_pt.txt file. Finally, AES 64byte key and IV deriving number is encrypted by RSA algorithm which is stored in the rnd_number.txt. After that, all rnd_number.txt, ct_pt.txt and digitalsignature.txt bytes are combined and forwarded to embed into the cover image, which generates a stego image.

Extraction and Decryption process is opposite to the encryption & embedding process where digital signature, encrypted random number and cipher text are extracted from stego image. Then, RSA algorithm decrypt the random number which contain key and IV parameters. These parameters reveal the plain text from cipher text using AES algorithm. After that, plain text is hashed to produce a digest. Then digital signature is decrypted using RSA decryption process produces a digest which is the same of decrypted plain text digest. As the condition is satisfied, then integrity of message is checked.

Fig.6 shows the GUI (Graphical User Interface) of hybrid cryptography and steganography. In fig.7 and fig.8, cover image and stego image histograms have been illustrated respectively. Both the histograms are very close to each other which prove the efficiency of the embedding algorithm.



Cover Image: C:\Users\udayan\Desktop\test\img.jpg

File: C:\Users\udayan\Desktop\test\pt.txt

Save Folder: C:\Users\udayan\Desktop\test\New folder

Image Capacity

Size	37.88 KB
Height	400 Pixel
Width	706 Pixel
Storage	734.36 KB

Fig. 6. GUI of hybrid cryptography and steganography

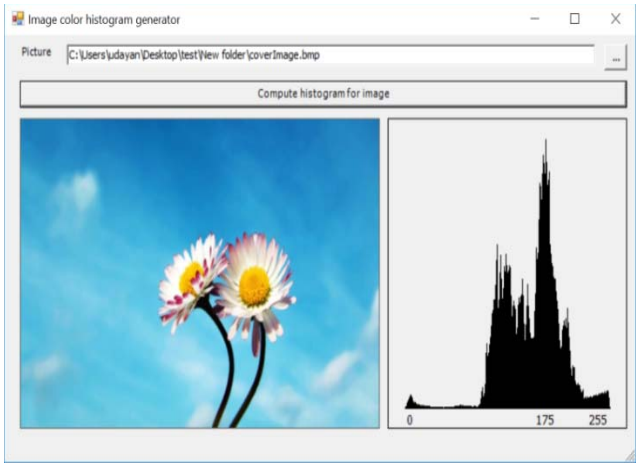


Image color histogram generator

Picture: C:\Users\udayan\Desktop\test\New folder\coverImage.bmp

Fig. 7. GUI of cover image histogram

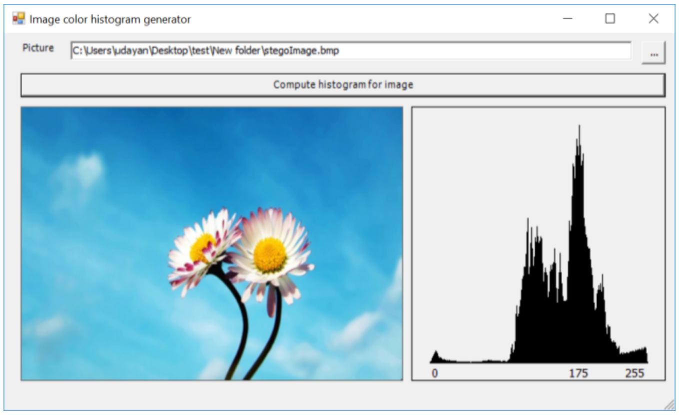


Image color histogram generator

Picture: C:\Users\udayan\Desktop\test\New folder\stegoImage.bmp

Fig. 8. GUI of stego image histogram

IV. Conclusion

In this paper both the hybrid cryptography and steganography have been applied, and a stego image has been generated. Here, the message is encrypted using AES. The symmetric key used for message encryption has also been encrypted using the public key of RSA, which increases the security level. A hash value of the message is generated that is encrypted again with the help of the public key of RSA to produce a digital signature. At the receiving side this digital signature helps to check the integrity of the message. All these encrypted files, i.e. the encrypted message, encrypted key and the encrypted digest have been combined together to form a complete message. This complete message has been embedded using the steganography technique, LSB. The histograms for both the cover image and the stego image have been displayed. As both the histograms are almost same, the resistivity of the proposed system against attack has been ensured. Thus this algorithm provides confidentiality, integrity and authentication together.

References

[1] W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice-Hall, New Jersey, 1999.

[2] Behrouz A. Forouzan, "Cryptography and Network Security", Tata McGraw-Hill Education, 2011.

[3] Chitra Biswas, Udayan Das Gupta and Md. Mokammel Haque" A Hierarchical Key Derivative Symmetric Key Algorithm using Digital Logic", IEEE International Conference on Electrical, Computer and Communication Engineering (ECCE), February 16-18, 2017, Cox's Bazar, Bangladesh.

[4] Rajani Devi. T, "Importance of Cryptography in Network Security", 2013 IEEE International Conference on Communication Systems and Network Technologies", 6-8 April 2013, Gwalior, India.

[5] Christof Paar, Jan Pelzl, "Understanding Cryptography", Springer-Verlag Berlin Heidelberg 2010, pp-3-4.

[6] V. Lokeswara Reddy, Dr. A. Subramanyam and Dr.P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications,Volume: 02, Issue: 05, Pages: 868-872 (2011).

[7] Ross J. Anderson and Fabien A.P. Petitcolas, "On the Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 98, Special Issue on Copyright & Privacy Protection. ISSN 0733-8716, pp 474-482.

[8] Sumeet Kaur, Savina Bansal, and R. K. Bansal, "Steganography and Classification of Image Steganography Techniques'', 2014 IEEE International Conference on Computing for Sustainable Global Development (INDIACom), 5-7 March 2014, New Delhi, India.

[9] N. Provos and P. Honeyman, "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003, pp 32-44.

[10] Nadeem Akhtar, Shahbaaz Khan, Pragati Johri " An improved inverted LSB image steganography", 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 7-8 Feb. 2014, Ghaziabad, India.

[11] Lee, Y.K. and Chen, L.H., "High capacity image steganographic model", Visual Image Signal Processing, 147:03, June 2000.

[12] A. Cheddad, J. Condell, K. Curran, & P. Mc Kevitt, (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, Vol 90, Issue 3, March 2010, pp. 727-752.

[13] Federal Information Processing Standards, Advanced Encryption Standard (AES). Federal Information Processing Standards Publications (FIPS PUBS), Nov 2001.

[14] R. Rivest,A Shamir, L. Aldeman, "A Methoed for Obtaining Digital Signatures and Public-key Cryptosystems," J. Communications of the ACM, 1978, 21(2) 120-126.

[15] Jaspal Kaur Saini, Harsh K Verma, "A Hybrid Approach for Image Security by Combining Encryption and Steganography", Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013), Dec. 2013, Shimla, India.

[16] May H. Abood, " An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms", Annual Conference on New Trends in Information & Communications Technology Applications-(NTICT'2017), 7-9 March, 2017, Baghdad,Iraq.

[17] Lipi Kothari, Rikin Thakkar, Satvik Khara, "Data hiding on web using combination of Steganography and Cryptography", 2017 International Conference on Computer, Communications and Electronics (Comptelix), 1-2 July 2017, Jaipur, India.