REVERSIBLE DATA HIDING IN IMAGES WITH ENHANCED SECURITY

Kiranjeet Kaur Sandhu[1], Prof. Shilpa Chougule[2], Dr. Shrikant Charhate[3]
[1]Research Scholar, [2]Assistant Professor, [3]Professor
Email:ksandhu@mes.ac.in[1], schougule@mes.ac.in[2], scharhate@mes.ac.in[3]

Abstract

Reversible Data Hiding (RDH) is a technique in which the original image can be recovered without any loss after the hidden message is retrieved. Thus, encryption is performed by the sender, by embedding the data-hider, and data extraction and/or image restored by the receiver. The novel scheme which is RDH in images using Blowfish Algorithm enhances the security level of image encryption. The actual cover image is sent to the data-hider where it compresses a sequence of preferred least significant bits chosen from the image to vacate the place for the secret data to be hidden. Then the data embedded image is being encrypted using the block cipher technique which is the blowfish algorithm. At the receiver end, the hidden message can be retrieved if the receiver has only the embedding key which is the private key. Suppose the receiver has only the encryption key i.e. the secret key, the receiver can redeem the actual image without any distortion. If the receiver has both the private and secret keys, the receiver can retrieve the hidden data and ideally retrieve the actual image with high security level. The proposed system ensures the enhancement of the security level of image encryption as well as the secret data encryption strongly.

Keywords: Reversible data hiding, image encryption, image recovery.

I. INTRODUCTION

Data hiding is the procedure to conceal the data (symbolizing few useful data) into actual media. That is, the data hiding procedure connects two groups of data, one is the group of the secret data and the other group is of the actual media information. The connection between these two groups of information identifies various implementations. For example, in stealthy transmissions [1], the secret information may usually does not relate to the actual media. In authentication, however, the hidden information is nearly related to the actual media [7]. From the above two types of applications, non visibility of secret information is the main necessity. In majority cases of hiding information, the actual media will come across some deformation due to hiding information and cannot be reversed back to the actual media. This is, some never ending deformation has taken place in the actual media still after the concealed information has been retrieved out.

In some applications, such as medicinal investigation and law constraint, it is crucial to reversing the noticeable media back to the actual media after the secret information is extracted for few lawful factors. In other implementations, such as remote sensing and high energy investigational examination, it is needed that the actual media can be retrieved because of the necessary high-accurate nature. The marking skills fulfilling this condition are declared as reversible, without any loss, deformation-free or inverse hiding information skills. Reversible data hiding provides a great probability of implementations to connect two groups of information in such a means that the actual media can be retrieved without any loss after the secret information have been retrieved out, therefore giving an extra venue of managing two various groups of information.

RDH[7] in images is a method, by which the actual image can be retrieved without any loss after the secret data is retrieved. This significant skill is widely used in medicinal images, armed images and law investigations, where no deformation of the actual image is sanctioned.

Securing data means securing data and data network from unauthenticated entrance, utilize, leak, interruption, alteration, examination, tape or destruction. In every field maintaining privacy in sharing information is needed and with the help of encryption technique it can be achieved. It was invented for the very same purpose. The technique of Reversible data hiding (RDH) is to conceal hidden data in an actual picture in a revert way [2]. At the receiver end, the secret data will be retrieved and flawlessly retrieve the actual image.

The rest of the paper is organized as follows. The proposed system is described in Section II. Section III presents the procedures of image encryption and data embedding. Section IV discusses the proposed method and the experimental results. Section V concludes the paper.

Hiding secret data in encrypted images are evaluated using the method of RDH. The RDH methods for encrypted image are usually planned for the applications where the data-hider and the figure proprietor are both different from each other. The data-hider is not able to retrieve the image information, and on the other hand the hidden information is owned by the data-hider. Thus, the sender does the encryption part, embedding part is executed by the data-hider and the receiver performs the final part which is information retrieving as well as image restoration.

For encrypted image, X .Zhang (April 2011) proposed a new reversible data hiding method [3]. Using a stream cipher technique the entire data is being encrypted of a decompressed picture, by altering a little amount of encrypted information, the extra information can be hidden in the picture. The existing RDH technique was in which data hider separates the encrypted picture into chunks by rolling over three LSB. At the receiver end, the noticeable encrypted picture is decrypted to an estimated picture. The receiver, roll over the three LSBs of pixels for the formation of a new chunk. At the time information retrieval and picture reconstruction mistakes may happen if an unsuitable chunk size is taken. W. Hong, T. Chen, and H. Wu (April 2012) has demonstrated that this scheme [4] was enhanced by utilizing spatial correlation among neighboring chunks with the help of a side match algorithm to minimize the error rates in image recovery. Though information retrieval are not separate processes.

K. Ma, W. Zhang (April 2013) has recommend a unique scheme by vacating space prior to encryption with a conventional RDH algorithm, and consequently it is uncomplicated for the data hider to reversingly hide information in the encrypted picture. This system can attain genuine reversibility, which is, information retrieval and picture reconstruction without any fault. W. Zhang, et.al. (June 2014) proposed a method [6] related to an evaluation method, where a great section of pixels is used to evaluate the remaining prior to encryption and the last edition of encrypted picture is produced by joining the encrypted evaluating faults and a huge section of the encrypted pixels. Extra data can be hidden in the encrypted picture by altering the evaluating faults. But both methods requires an extra RDH process by the sender prior to picture encryption. Which means the matter of RDH in encrypted pictures is really changed into a conventional RDH in simple text pictures.

Existing RDH method for pictures can be characterized into two types: “vacating the room after encryption (VRAE)” and “vacating room before encryption (VRBE)” [5]. The techniques in VRAE and VRBE types are efficient for RDH in encrypted pictures. Though, there are a few boundaries in the existing scheme concerning safety.

II. System Description

The proposed scheme is elaborated in Fig 1, which contains of three stages: image encryption, data hiding, and data retrieve. In stage I, the sender sends the actual image to the Data hider. In stage II, the data-hider chooses and contracts few LSB of the image to generate an unused room, and hides encrypted data into the image using an embedding key and encrypts the image using block cipher i.e. Blowfish Algorithm. In stage III, the receiver retrieves the hidden information using the private key and decrypts the image.

If the receiver has secret key, the actual image can be roughly restored using image decryption and evaluation. When both the private and secret keys are on hand, the receiver can retrieve the hidden data and recover the original image.

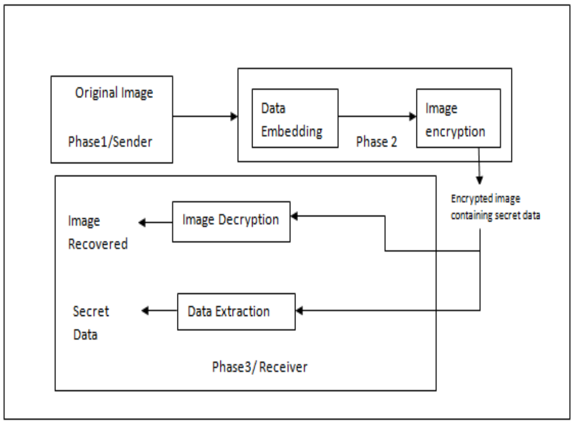

Fig.1. System Architecture of a Proposed System

In the Proposed system, we have implemented the following modules:

Sender: This module includes the sender who selects the original image in which the secret data has been embedded and send it to the data hider for the further information hiding operation.

Data Hider: This Module includes embedding part. The information which is to be hidden in the picture is first encrypted using the ECC i.e. Elliptic Curve Cryptography technique and then get embedded into the image by using LSB technique. After the encrypted data being embedded into picture, the picture with the information embedded in it, is encrypted using block cipher technique i.e. Blowfish algorithm and sent to the receiver.

Receiver: This module involves decryption of the image and extraction of data. With the help of decryption key the receiver can effortlessly decrypt the image and reconstruct it perfectly and by using embedding key it can easily retrieve the hidden information from the image.

III. DATA AND IMAGE ENCRYPTION

In proposed system the data hider encrypt their data using ECC(Elliptical curve cryptograph algorithm) and change to user's original data into binary format, because this algorithm generate equal binary formatted data to the original content, ECC generate two keys for encryption and decryption , here the two key are Public Key and Private Key which are sent to the receiver. With the help of Public key we encrypt the secret message and using the private key we decrypt the hidden message. ECC needed remarkably smaller key size with identical amount of security. The expression for elliptical curve is given below.

The ECC consist of two operations, first is Key Generation which is,

$$Q=d*p \qquad (1)$$

Where, Q is the public key, d is the private key

Second operation is Encryption where two cipher text is generated C1 and C2 which is send to the receiver for the Decryption process,

$$C1=K*p \qquad (2)$$

Here, K is randomly selected

$$C2=M+K*Q \qquad (3)$$

Here, M is the Original Message

The original message M is being decrypted by using,

$$M=C2-d*C1 \qquad (4)$$

The data is concealed in the image with the help of LSB technique. Proposed technique does not alter any colour assessment. The length of the data has to be mentioned into the image prior concealing the secret data. This will prohibit the entrance of garbage values in the decrypted hidden data.

After obtaining bit number 0 from the initial 32 pixels, the bits should be tidily set within an integer variable to know the length of data concealed into the image. Pixels subsequent the 32nd pixel store up the bits required for restoring the byte value required to produce the original thread.

Max to max length of the data that could be concealed in an image at the rate of 1 bit from individual pixel can be evaluated using the expression

$$n = \frac{(P-32)}{8} \qquad (5)$$

Where n is the maximum length of data and P is the number of pixels.

After embedding the secret encrypted data into an image, we give the additional security to the embed image and encrypt the embedded image using Blowfish algorithm, while doing this process, the secret data has still more secure and cannot access the original message by the hackers or attackers. And we share only encrypted image through the communication medium to the shared user. So the sender shares two keys to the legitimate receiver only.

Blowfish is 64-bit block cipher which is substitute of DES algorithm. Ranging from 32 bits to 448 bits, fluctuating key length is used. Variation of 14 round or few are available in Blowfish. Blowfish is unpatented and license-free and is available without any cost for any user. Blowfish is one of the fastest block ciphers flourished till date. There has been not a single attack performed on Blowfish Algorithm.

At the receiver end, the hidden message can be retrieved if the receiver has only the embedding key which is the private key. Suppose the receiver has only the encryption key i.e. the secret key, the receiver can redeem the actual image without any distortion. If the receiver has both the private and secret keys, the receiver can retrieve the hidden data and ideally retrieve the actual image with high security level. The proposed system ensures the enhancement of the security level of image encryption as well as the secret data encryption strongly.

IV. DISCUSSION AND RESULTS

The block cipher technique which is used in the proposed system will improve the security of the scheme as compared to the existing systems which uses the stream cipher. In this proposed method, a symmetric system algorithm is used for enhancing security, which provides secure transmission of information to the receiver. Proposed system uses a block cipher technique for strong encryption. This system centered on the assortment formula to select a block cipher based symmetric key algorithm. The effectiveness of a block cipher algorithm depends on the block mass and key mass. Since, a big chunk size the block cipher method can encrypt a large amount of information in one cycle of the algorithm, thus, it’s speeds up the implementation of algorithm and greater security.

However, a big key concludes in a slower algorithm, because in actuality, all chunks of key are mixed up in an implementation cycle of the algorithm. A big amount of cycles makes the algorithm obtuse but, are hypothetical to offer superior security [8]. Therefore, there is always a deal between security and execution in block cipher algorithms [9]. Eli Biham [10] has proposed that execution of the algorithm should be calculated by the time the small amount number of secure cycle for every algorithm, i.e., the evaluated number of cycles necessary to make a brute force key search which is the most effective form of attack, though, there is no simple way of procuring neutral and extensively acknowledged standards for the smallest amount of secure cycles for every algorithm.

From the study, we have found the following results:

A. Simulation results are specified in Fig. 2 and Fig. 3 for few particular encryption algorithms using various encoding techniques. Fig. 2 depicts the outcomes at base 64 encoding and Fig. 3 depicts the outcome of the hexadecimal base encoding. It has been noticed that there is no noteworthy dissimilarity in these two encoding techniques. With the help of these two techniques, similar documents are encrypted. We can make out that the both graph nearly provide the equivalent outcome.

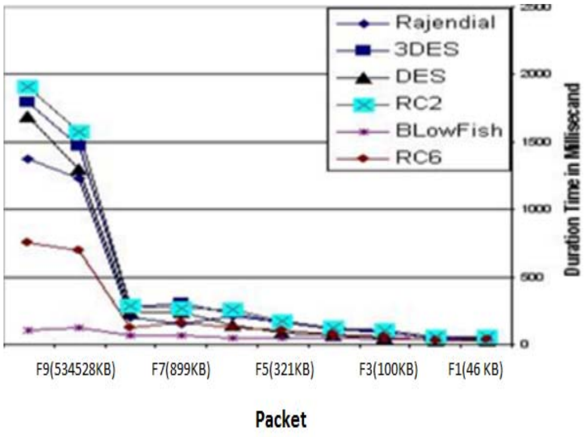

Fig.2. Time consumption of encryption algorithm (base 64 encoding) [11]

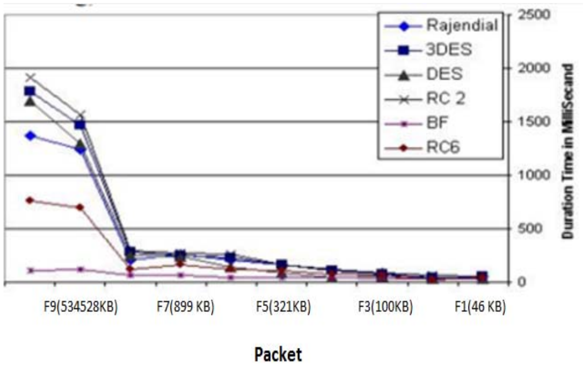

Fig.3. Time consumption of encryption algorithm (hexadecimal encoding) [11]

B. Encryption of various package volumes: To work out the output of an encryption method encryption time is used. It denotes the pace of encryption. The output of the encryption method is considered by dividing the total plain information in MBs encrypted on the overall encryption instance for every algorithm. Since the output rate is improved, the power utilization of the specific encryption system is dropped.

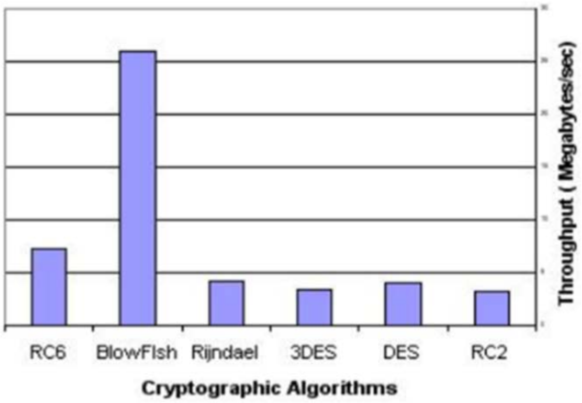

Fig.4. Throughput of each encryption algorithm [11]

The result depicted in Fig.4 shows the dominance of the Blowfish algorithm above former algorithms in terms of the processing time.

Simulation results for this compression part are revealed in Fig. 5 we can discover in decryption that Blowfish is superior to former algorithms in output and power utilization.

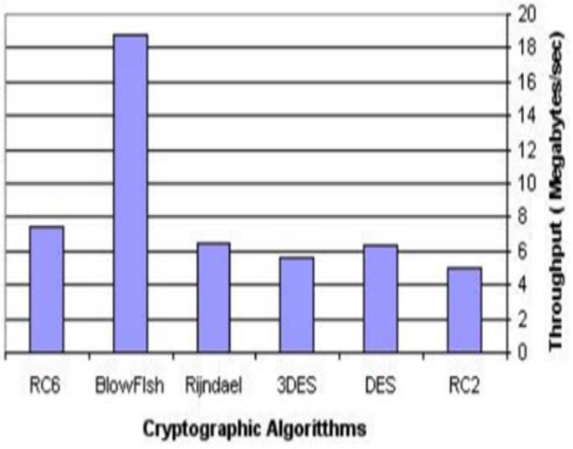

Fig.5. Throughput of each decryption algorithm [11]

C. The group of experiments was performed with ECB mode, the outcome is given away in Fig 6 beneath. The outcome illustrates that the Blowfish algorithm is proficient as comparison with various algorithms in provisions of the dispensation time.

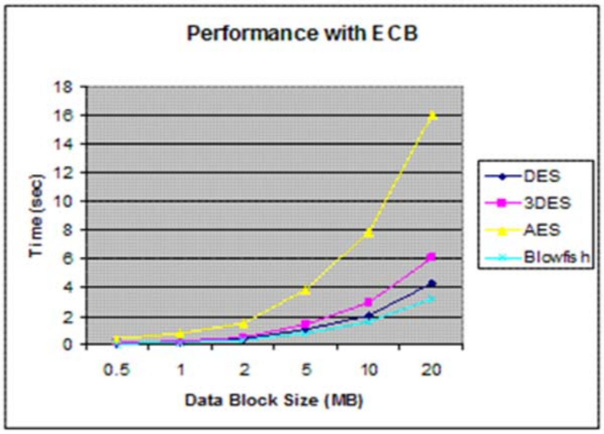

Fig.6. Performance Results with ECB Model [12]

D. As CBC needed more dispensation time than ECB since its key-cycle identity. The outcome illustrates in Fig. 7 designates that the additional instance added is not significant for numerous implementations, knowing that CBC is far improved than ECB in sense of security.

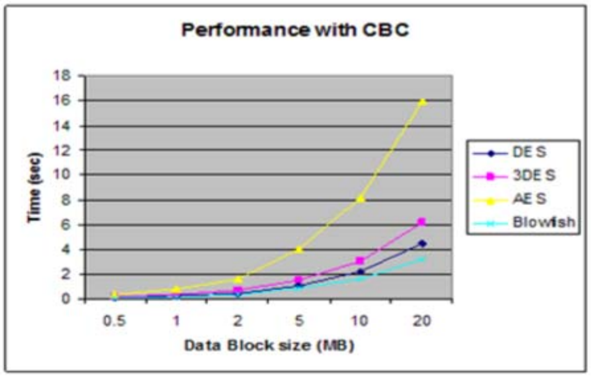

Fig.7. Performance Results with CBC Model [12]

The surveyed simulation results conveyed that Blowfish has a enhanced rendering than various universal encryption algorithms used. As Blowfish has no such known weak security points till now, which makes it an outstanding contender to be measured as a benchmark encryption algorithm.

V. CONCLUSION

The above framework initiates an idea of reversible data hiding in images using the Blowfish algorithm which is a strong block cipher technique. After original image selection it is sent to the data hider for hiding the data, few sections of LSB levels are chosen and compacted to create space for the hidden information. The hidden information is encrypted and then the picture is encrypted. At the receiver end, all secret information is retrieved only with the private key, and the actual picture nearly reconstructs with superior feature only with the help of Secret key. If the secret and private keys are accessible to the receiver, the secret information is retrieved entirely and the actual picture restored completely. With the thought of block cipher, the above system significantly empowers the security in comparison with the current stream cipher schemes.

The studied simulation results depicts that Blowfish has a superior performance compare to other known encryption algorithms used. There are no such known weak security points in Blowfish till now; which makes Blowfish an outstanding candidate to be noted as a benchmarked encryption algorithm.

Since hiding exercises are practiced on the information, the attacker will not be able to retrieve the information of the actual picture, which safeguards the security of the information in information embedding. Since the hiding and reconstruction are secured with the help of secret and private keys, an attacker cannot crack into the system without having both the keys.

.

References

[1] X. Zhang (2015), “Reversible data hiding with distributed source encoding”, IEEE Signal-Trans.circuits and system for video Technology, vol. 16, no. 4, pp. 636-646, Apr. 2015.

[2] W. Puech, M. Chaumont and O. Strauss (2008), “A reversible data hiding method for encrypted images,” Proc. SPIE 6819, Security, Forensics, Steganography, and Water-marking of Multimedia Contents, vol. 6819, pp. 430-438, Feb 2008.

[3] X. Zhang (2011), “Reversible data hiding in encrypted images”, IEEE Signal Process.Lett., vol.18, no. 4, pp. 255-258, Apr. 2011.

[4] W. Hong, T. Chen, and H. Wu (2012),“An improved reversible data hiding in encrypted images using side match”, IEEE Signal Process.Lett., vol. 19, no. 4, pp. 199-202, Apr. 2012.

[5] K. Ma, W. Zhang, K. Ma and N. Yu (2013),“Reversible Data Hiding in Encrypted Images by ReservingRoom Before Encryption”, IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553-562, Apr. 2013.

[6] W. Zhang, K. Ma and N. Yu (2014),“Reversibility improved data hiding in encrypted images, Signal Processing”, vol. 94, pp. 118-127, June 2014.

[7] Z. Ni, Y. Shi, N. Ansari and S. Wei(2006) “Reversible data hiding,” IEEE Trans.Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[8] J. Fridrich and M. Goljan (2002),“Lossless data embedding for all image formats”, in Proc. SPIEProc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, vol. 4675, pp. 572-583, Jan. 2002.

[9] Y. Khiabani, S. Wei, J. Yuan, and J. Wang (2012),“Enhancement of secrecy of block ciphered systems by deliberate noise”, IEEE Trans. Inf. Forensics Security, vol. 7, no.5, pp.1604-1613, Oct. 2012.

[10] S. Wei, J. Wang, R. Yin, and J. Yuan (2013),“Trade-o between security and performance in block ciphered systems with erroneous ciphertexts”, IEEE Trans. Inf. Forensics Security, vol. 8, no. 4, pp. 636-645, Apr. 2013.

[11] MilindMathur, AyushKesarwani (2013) “Comparison Between Des, 3des, Rc2, Rc6, Blowfish And Aes”, Proceedings of National Conference on New Horizons in IT, vol. 2, no. 5, pp. 143-148 Aug. 2013.

[12] Abdel-Karim Al Tamimi (2015), “Performance Analysis of Data Encryption Algorithms”,International Journal of Scientific Research in Netw search in Network Security and Communication, Vol. 3, no. 1, pp. 210-222, Dec 2015.